

DIRECCIÓN DE INTELIGENCIA POLICIAL

Bogotá D.C., 08 de julio de 2020

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

	SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL				
1.1 DESCRIPCIÓN GENERAL DEL OBJETO	CLASIFICACIÓN UNSPSC	Segmento	Familia	Clase	Producto
	43231500	Difusión de tecnologías de información y telecomunicaciones	Software	Software funcional específico de la empresa	
	43211500	Difusión de tecnologías de la información y telecomunicaciones.	Equipo informático y accesorio.	Computadores	
	43232400	Difusión de tecnologías de la información y telecomunicaciones.	Software	Programas de desarrollo	
	81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas	
1.2 VALOR ESTIMADO	El valor estimado del presente proceso es de CUATRO MIL CUATROSCIENTOS NOVENTA Y OCHO MILLONES SEISCIENTOS NOVENTA Y NUEVE MIL OCHOCIENTOS PESOS M/CTE (\$ 4.498.699.800,00)				
	ÍTEM	DESCRIPCIÓN	CANT	VALOR UNITARIO ESTIMADO SIN IVA	VALOR TOTAL ESTIMADO SIN IVA
	1	SERVIDORES	3	\$ 221.500.000,00	\$ 664.500.000,00
	2	SWITCH 48 PUERTOS	1	\$ 71.451.965,00	\$ 71.451.965,00
	3	SWTCH 24 PUERTOS	2	\$ 39.955.761,50	\$ 79.911.523,00
	4	FIREWALL	1	\$ 181.293.302,00	\$ 181.293.302,00
	5	SOFTWARE OSINT	1	\$ 3.397.034.248,00	\$ 3.397.034.248,00
	6	CANAL DEDICADO INTERNET POR UN PERÍODO DE TRES (3) AÑOS	1	\$ 104.508.762,00	\$ 104.508.762,00
	VALOR TOTAL ESTIMADO				\$ 4.498.699.800,00
	VALOR TOTAL POR RECURSO				\$ 4.500.000.000,00
	<i>Nota aclaratoria: para los ítems del 1 al 5, se aplicara lo establecido en la normatividad tributaria, así:</i>				
	<i>* 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%</i>				
1.3 CERTIFICACIÓN PLAN ANUAL DE ADQUISICIONES	<i>El ítem No 6 (Canal de datos dedicado internet), estará grabado con la tarifa del 19% de IVA.</i>				
	Certificado plan de compras No. 075 del 18/02/2020, recurso 11, por valor de \$4.000.000.000,00.				
	Certificado plan de compras No. 105 del 03/04/2020, recurso 11, por valor de \$500.000.000,00.				

1.4 CLASE DE CONTRATO	Compra venta (Art 32 Ley 80 de 1.993, Código Civil y Código de Comercio).
1.5 PERFIL Y CALIDAD DE LOS PROPONENTES	<p>La necesidad debe ser atendida por una compañía experta en el tema de inteligencia artificial, con el fin de realizar las configuraciones necesarias requeridas por la Dirección de Inteligencia Policial que cuente con el nivel de experiencia y confiabilidad, Por tal motivo, deberá garantizar el correcto funcionamiento de hardware y software a instalar.</p> <p>Podrán participar todas las personas naturales o jurídicas, fabricantes o productores o desarrolladores, comercializadores o distribuidores autorizados, nacionales o extranjeras con representación en Colombia, en forma individual o conjunta (consorcio, unión temporal, promesas de sociedad), que estén en capacidad de suministrar el objeto de este proceso y cumplan con todos los requisitos exigidos para el mismo.</p> <p>La convocatoria se limitará a Mipymes siempre y cuando se verifique las reglas establecidas en el artículo 2.2.1.2.4.2.2. del Decreto 1082 del 2015.</p>
1.6 IDENTIFICACIÓN DE LA NECESIDAD Y JUSTIFICACIÓN	
<p>La expansión y uso masivo de las tecnologías de la información y las comunicaciones, así como la progresiva participación de la sociedad en actividades en el entorno digital, advierte nuevos retos para la Inteligencia Policial considerando los actores internos y externos en el ciberespacio que representan amenazas latentes contra la estabilidad estatal, institucional y la seguridad ciudadana; en este sentido, el Estado Colombiano ha fijado la política Marco Convivencia Seguridad Ciudadana y la política pública denominada "Seguridad Digital", cuyo objetivo es contrarrestar adecuadamente las amenazas ciberneticas y los incidentes en el entorno digital apoyados de estrategias, donde el rol de la Inteligencia es indispensable para la caracterización de los fenómenos y actores delictivos que confluyen en la red.</p> <p>Dentro de las líneas de la política Marco Convivencia Seguridad Ciudadana de diciembre de 2019, se estableció la línea "Ciudadanos Ciberseguros" la cual pretende atender los riesgos y las nuevas dinámicas criminales que trajo consigo el avance tecnológico. <i>El ciberespacio es sinónimo de nuevas oportunidades para todas las personas y comunidades, pero también un escenario de actividades delictivas de diversa índole. Desde comportamientos de acoso escolar y extorsión, hasta reclutamiento criminal. Esto representa un reto en materia de seguridad ciudadana, particularmente en cuanto a prevención... y articulación institucional</i>¹. Dentro de esta línea la atención del Gobierno nacional se centra en tres (3) principales objetivos, así: 1. Prevención de los delitos en el ciberespacio, 2. Persecución contra el ciberdelincuente y 3. Articulación Institucional contra el ciberdelito.</p> <p>Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, aunado a la anterior dentro del marco del CONPES 3854 "Seguridad Digital" y el papel de la Inteligencia para recolectar información en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores, la Policía Nacional a través del Servicio de Inteligencia Policial cuenta con capacidades de recolección y análisis de información, que es considerada el apoyo y una fuente de información articulada al Centro de Capacidades para la Ciberseguridad de Colombia C4 (DIJIN), en el despliegue de actividades de cibermonitoreo, ciberpatrullaje y recolección técnica del ciberespacio.</p> <p>Considerando que las actividades de ciberpatrullaje y cibermonitoreo actualmente se realizan de manera manual y empírica, sin el apoyo de herramientas tecnológicas que optimicen los tiempos de respuesta y que permitan tener una visión más global de la información disponible en internet, DARK y DEEP WEB y el presente proyecto atiende de manera directa los objetivos del plan estratégico institucional.</p> <p>Aunado a lo anterior, no se cuenta con la capacidad de procesamiento y análisis de grandes volúmenes de información recolectada sobre los fenómenos criminales y todas las demás conductas que hacen uso de las tecnologías de información y comunicaciones como fin o como medio para cometer ilícitos, por ello es necesario, realizar la transformación de la inteligencia policial hacia las nuevas formas de anticipación donde se evidencian las mutaciones criminales, puntuizando en los siguientes aspectos:</p>	

¹ <https://id.presidencia.gov.co/Documents/191220-Politica-Marco-Convivencia-Seguridad-Ciudadana.pdf>

- Identificación de actores, intencionalidades y objetivos en el ciberespacio en grandes volúmenes de información.
- Levantamiento de información que permita anticipar posibles ataques provenientes del ciberespacio, que afecten los intereses nacionales o pongan en riesgo la vida de los habitantes de Colombia.
- Generar alertas tempranas en la atención e identificación de fenómenos e incidentes de seguridad digital bajo las mejores prácticas internacionales.
- Optimizar tiempos de respuesta en la recolección técnica disponible en el ciberespacio.

Por lo anterior, el servicio de inteligencia en aras de estar a la vanguardia de las amenazas que hoy en día se gestan en el ciberespacio, requiere adquirir herramientas tecnológicas, capacitación y capacidades de desarrollo de software que faciliten la automatización de la recolección de información, para fortalecer las capacidades; a partir de los siguientes aspectos:

- Capacidad propia en desarrollo de software.
- Desarrollo de Crawlers y enlaces de búsqueda.
- Desarrollo de neuronas.
- Tratamiento preliminar.
- Consulta de información consolidada (Big Data estructuras y no estructuradas) y Machine Learning.
- Análisis de información en tiempo real, que permita evidenciar el panorama actual y proyecciones.
- Desarrollar habilidades de programación en Inteligencia Artificial.

En este contexto, actualmente se utilizan herramientas Free para realizar búsquedas en la web, por tal motivo, se han identificado en el mercado herramientas que indexan y exponen la información que se encuentra actualmente oculta. Estas herramientas a su vez, facilitan el anonimato del usuario y permite la obtención de datos que relacionan actuaciones de criminalidad y ciberdelincuencia, entre otros.

En la actualidad se tiene una capacidad reducida de personal para la realización de este tipo de actividades; es por esto que, se requiere la automatización de dicho proceso, que conduzcan a buenas prácticas en la recolección de información en la web, a fin de optimizar los tiempos de respuesta.

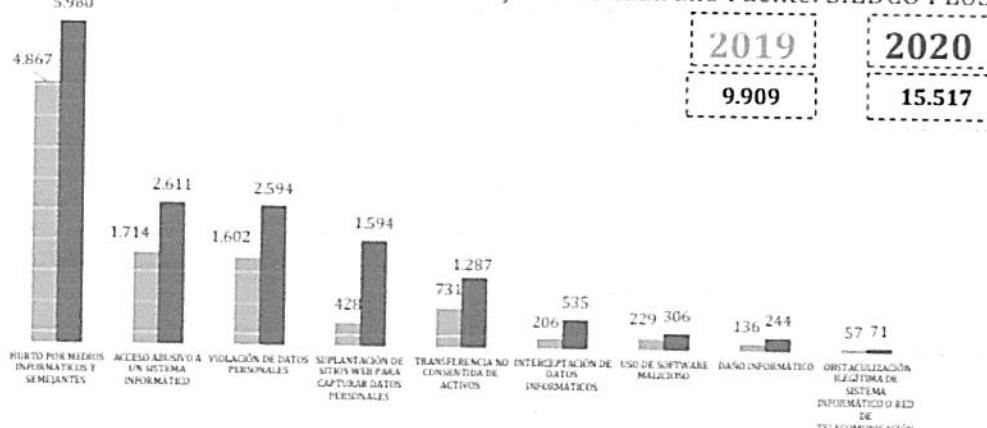
Considerando el contexto actual de la pandemia del COVID-19, durante el año 2020 se han presentado diferentes eventos de carácter nacional e internacional que han puesto a prueba la ciberseguridad de la región, situación que ha demandado un exponencial incremento en el uso de la internet y de las tecnologías de la información y las comunicaciones, abriendo con ello una ventana de oportunidades para que los ciberdelincuentes ataquen.

Lo anterior, se ha visto reflejado en los siguientes eventos, que han afectado la convivencia y seguridad ciudadana a nivel país, así:

- Aumento de delitos contra menores de edad en el ciberespacio (sexting, pornografía infantil).
- Generación de noticias falsas.
- Incremento del **150%** de la actividad maliciosa en internet para robar datos personales.
- Realización de saqueos a establecimientos comerciales.
- Amotinamientos en centros carcelarios.
- Entre otros eventos.

Es por esto que, durante el presente año la fluctuación delictiva ha marcado las siguientes tendencias:

Denuncias ley 1273 - 2009
Corte del 01 de enero al 15 de junio de cada año Fuente: SIEDCO PLUS



- 57% de incremento en denuncias por delitos informáticos del 01 de enero al 15 de junio del presente año, comparado con el año anterior 5.608 casos más.
- 351% de incremento en la suplantación de sitios web, portales falsos que buscan apoderarse de información personal, principalmente bancaria 1.501 casos más.
- 160% de incremento en el delito de Interceptación de datos Informáticos.
- 79% de incremento en el delito de daño informático.
- 76% de incremento en el delito de transferencia no consentida de activos.
- 62% de incremento en el delito de violación de datos personales.
- 52% de incremento en el delito de acceso abusivo a un Sistema Informático.
- 23% de incremento en el delito de hurto por medios informáticos y semejantes.

De igual forma, el COVID-19 ha generado las siguientes tendencias delictivas en el ciberespacio:

- **Sector Financiero:** Casi el 60% de transacciones bancarias se realiza de manera virtual, por lo que los delincuentes buscan captar las contraseñas y datos financieros de sus víctimas para hurtar el capital; otro método es la utilización de falsos productos o servicios para generar estafas.
- **Phishing:** incremento en la suplantación de sitios web para capturar datos personales, esta modalidad ha sido identificada como uno de los principales vectores de ataque por parte de los cibadelincuentes, para obtener información privada de sus víctimas.
- **Malware:** la propagación de los también conocidos como virus en el mundo ciber, cada día se incrementa; cada vez estos software son más sofisticados y en muchos casos indetectables por las víctimas que por lo general, no tienen buena "higiene digital".
- **Noticias Falsas:** con las que se crea incertidumbre y otros vectores de ataque, llamando la atención de la potencial víctima, invitándola a dar clic sobre algún link o imagen para infectar su dispositivo o captar su información personal.
- **Portales oficiales de entidades del Estado:** un sector apetecido por los delincuentes informáticos, en ocasiones con temas reputacionales y otras para extraer recursos, este último principalmente en entes territoriales engañando a los administradores de los portales transaccionales.

Por otra parte, considerando los riesgos a los que se enfrenta la Dirección de Inteligencia Policial, frente a la navegación en el ciberespacio, con el objetivo de proteger la identidad de los funcionarios de inteligencia en este entorno, se hace necesario la adquisición de servidores para el almacenamiento de dicha información y posterior análisis, evaluación y tratamiento de las áreas que requieran estos insumos.

Como entidad gubernamental los equipos de cómputo deben contar con las herramientas ofimáticas básicas licenciadas; en este sentido se visibiliza la necesidad de solicitar equipos de cómputo que requieran estas

certificaciones. Así como, herramientas que faciliten la búsqueda de información ya procesada en tal sentido se requiere indexadores que reduzcan los tiempos de respuesta en la búsqueda de información.

Es imprescindible que cada funcionario que despliega la actividad de recolección, cuente con un equipo de cómputo que soporte las aplicaciones que de manera empírica se están construyendo para tal fin, actualmente la unidad cuenta con un solo equipo y una descripción tardía obtenida.

En este orden de ideas, y considerando las necesidades expuestas anteriormente, se hace necesario el desarrollo de una plataforma tecnológica compuesta de software, hardware y servicio; así como, la potenciación de las habilidades del talento humano a partir de la transferencia de conocimiento, enfocadas en la producción de insumos, capacidad de desarrollo de software y productos de inteligencia basados en datos técnicos recolectados en la web pública, Deep Web y Darknet, e información disponible a través de técnicas de OSINT, minería de datos y análisis de redes que apoyen los procesos estratégicos y operacionales de la Policía Nacional, traducido en las siguientes necesidades:

- Uso de herramientas de OSINT: sistemas de información de fuente abierta pública plataformas de OSINT (OPEN SOURCE INTELLIGENCE).
- Uso de herramientas de procesamiento y análisis.
- Técnicas de minería de datos.
- Seguimiento de tendencias mediáticas en redes sociales.
- Identificación de falsas noticias.
- Análisis de redes.
- Inteligencia artificial para la producción de inteligencia predictiva y prospectiva.
- Capacitación integral y especializada para fortalecer las habilidades de búsqueda en el ciberespacio; así como aspectos normativos en informática.
- Fortalecimiento de la infraestructura tecnológica:
 - Canal de datos de internet.
 - Switch.
 - Servidores con gran capacidad.
 - Herramientas especializadas de hardware y software para aplicar técnicas de OSINT y búsquedas en la Dark y Deep Web.
 - Licencias.

Mediante comunicación oficial No. S-2019-007576/OFPLA-GUDER, del 24 de octubre del 2019, la Oficina de Planeación, se realizó la aprobación para la adquisición del "Sistema de Ciberinteligencia Basado en Inteligencia Artificial".

Mediante comunicación oficial No. S 2020-004921-OFITE, la Oficina de Telemática emite viabilidad técnica para adelantar el proceso cuyo objeto es "**SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL**".

El Sistema de Ciberinteligencia basado en Inteligencia Artificial, contará con una plataforma tecnológica que estará aislada de la red de datos de la Dirección de Inteligencia Policial, considerando que esta infraestructura hará uso de Internet, cumpliendo con los protocolos de seguridad de la información establecidos para su operación, la infraestructura tecnológica para su funcionamiento contará con 3 servidores físicos con procesamiento mínimo de 32 núcleos por máquina con una frecuencia base de 2.1 GHz- RAM 256GB- discos en estado sólido que soporte 15 TB y 24 bahías de expansión , dos (2) de estos servidores se usarán como servidores de aplicación en los cuales se virtualizarán los servidores necesarios de acuerdo a la arquitectura de la solución de software, que soportará los motores de búsqueda configurados, crawlers o algoritmos, flujo de información, la recolección de información, el análisis y las correlaciones de la información pública y un tercer servidor que se empleará para almacenar la información ya validada, aunado a lo anterior, un (1) canal de datos dedicado de internet de 100 MB que soporte la navegación de los usuarios en el sistema, el cual tendrá seguridad perimetral a través de un firewall de rendimiento mínimo de 10 Gbps, 8 Millones de sesiones concurrentes mínimas (TCP y 10.000 políticas), generando de esta manera una capa de seguridad a la plataforma.

La estructura de red y la conectividad interna de los equipos de cómputo del usuario final, estarán conectados a través de un Switch Core capa 3 administrable, que conecta la solución con las dos áreas de trabajo (ARPIN, ATASI) cada una con dos switches de 24 puertos. Toda esta infraestructura física de hardware debe soportar alrededor de 5.000 transacciones por minuto.

El software estará basado en inteligencia artificial con crawlers (bots que se encargarán de analizar sitios web y buscar información específica y relevante que se le hayan establecido²) que han sido diseñados a la medida por los usuarios finales, los cuales realizan proceso de extraer enlaces de las páginas para evaluarlas a partir de filtros y entregarlos a un transformador de datos. De esta manera los analistas pueden crear de manera automática y fácil algoritmos personalizados basado en variables definidas por el usuario (palabras clave, consultas de búsqueda, ubicaciones, tiempos, orientados para leer contenido específico de cualquier fuente como motores de búsqueda, sitios web, fuentes web profundas y oscuras, redes sociales, redes, blogs o incluso los foros).

Otra de las funcionalidades del software se basará en la de verificación de entidades, análisis de relaciones o enlaces de manera visual, agrupación de datos, geoanálisis, análisis de sentimientos, análisis de tendencias, generación de alertas de recolección, módulo de administración y auditoría de usuarios, adicionalmente se requiere que la solución este construida como mínimo con el 80% de los solicitado en las especificaciones técnicas, para lo cual se realizará una prueba para evaluar el cumplimiento de los requerimientos, lo que no esté desarrollado y sea de autoría intelectual del personal de policía debe realizarse cesión de derechos patrimoniales de autor, de la misma manera el licenciamiento debe ser perpetuo. Con el fin de garantizar el correcto funcionamiento, se solicita una garantía y soporte de 3 años, además de la transferencia de conocimiento en la construcción de crawlers, administración y gestión de la infraestructura física y la capacitación de usuario final.

Los elementos requeridos objeto de la presente contratación, son requeridos para el primer semestre de 2020.

Acuerdos internacionales y tratados de libre comercio:

Dando cumplimiento a lo contemplado en la SECCIÓN IV SUBSECCIÓN 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 el SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL, por la suma de CUATRO MIL CUATROSCIENTOS NOVENTA Y OCHO MIL SEISCIENTOS NOVENTA Y NUEVE MIL OCHOCIENTOS MILLONES DE PESOS M/CTE (\$ 4.498.699.800) , SI está cuberto bajo las obligaciones de carácter internacional, de acuerdo los criterios se relacionados 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 cuberto por este y, en consecuencia, no es necesario hacer análisis adicional alguno.

² <https://es.ryte.com/wiki/Crawler>

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.

ACUERDOS COMERCIALES VIGENTES		ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR VALOR AL DEL ACUERDO COMERCIAL	EXCLUSIÓN APPLICABLE AL DE PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
Alianza Pacifico	Chile	SI	SI	NO	SI
	México	SI	SI	NO	SI
	Perú	SI	SI	NO	SI
Canadá		SI	SI	NO	SI
Chile		SI	SI	NO	SI
Corea		SI	SI	NO	SI
Costa Rica		SI	SI	NO	SI
ESTADOS AEJC		SI	SI	NO	SI
Estados Unidos		SI	SI	NO	SI
México		SI	SI	NO	SI
Triángulo Norte	El Salvador	SI	SI	NO	SI
	Guatemala	SI	SI	NO	SI
	Honduras	SI	SI	NO	SI
UNIÓN EUROPEA		SI	SI	NO	SI

VALORES A PARTIR DE LOS CUALES SON APLICABLES LOS ACUERDOS COMERCIALES

Acuerdo comercial		Entidades Estatales del nivel municipal y departamental	Entidades generales del nivel nacional	Entidades especiales del nivel nacional
Alianza Pacifico	Chile	Bienes y servicios \$818.781.000 COP	Bienes y servicios \$204.659.000 COP Servicios de construcción \$20.469.524.000 COP	Bienes y servicios \$900.659.000 COP
	Perú	Servicios de construcción \$20.469.524.000 COP	Bienes y servicios \$388.921.000 COP Servicios de construcción \$20.469.524.000 COP	Servicios de construcción \$20.469.524.000 COP
	México	N/A	Bienes y servicios \$204.695.000 COP Servicios de Construcción* \$10'335.931 USD	Bienes y Servicios* \$397,535 USD Servicios de construcción* \$12'721.740 USD
	Canadá	N/A	Bienes y servicios \$241.786.000 COP Servicios de construcción \$20.469.524.000 COP	Bienes y servicios \$1.208.928.000 COP Servicios de construcción \$38.687.607.000 COP
Chile	Bienes y servicios \$818.650.000 COP	Bienes y servicios \$204.663.000 COP	Bienes y servicios \$900.515.000 COP	

	Servicios de construcción \$20.466.528.000 COP	Servicios de construcción \$20.466.258.000 COP	Servicios de construcción \$20.466.258.000 COP
Corea	Bienes y servicios \$834.620.000 COP Servicios de construcción \$62.596.500.000 COP (Aplica para departamentos)	Bienes y servicios \$292.117.000 COP Servicios de construcción \$20.865.500.000 COP	Bienes y servicios \$1.669.240.000 COP Servicios de construcción \$62.596.500.000 COP
Estados AELC	Bienes y servicios \$818.600.000 COP Servicios de construcción \$20.465.000.000 COP	Bienes y servicios \$532.090.000 COP Servicios de construcción \$20.465.000.000 COP	Bienes y servicios \$900.460.000 COP Servicios de construcción \$20.465.000.000 COP
Estados Unidos y Costa Rica	Bienes y servicios \$1.481.116.000 COP Servicios de construcción \$20.868.078.000 COP	Bienes y servicios \$241.786.000 COP Servicios de construcción \$20.868.078.000 COP	Bienes y servicios \$752.599.000 COP Servicios de construcción \$20.868.078.000 COP
México	N/A	Bienes y servicios* \$84.918 USD Servicios de construcción* \$11'039.387 USD	Bienes y servicios* \$424.592 USD Servicios de construcción* \$13'586.938 USD
Triángulo Norte	El Salvador Guatemala Honduras	Límite inferior del valor de la menor cuantía de la Entidad N/A	Valor de la menor cuantía de la Entidad
Unión Europea	Bienes y servicios \$818.660.000 COP Servicios de construcción \$20.466.500.000 COP	Bienes y servicios \$532.129.000 COP Servicios de construcción \$20.466.500.000 COP	Bienes y servicios \$818.660.000 COP Servicios de construcción \$20.466.500.000 COP

Fuente: Ministerio de Comercio, Industria y Turismo

* Para los valores en dólares, la Entidad Estatal debe definir el valor en pesos colombianos con la tasa representativa del mercado divulgada por la Superintendencia Financiera de Colombia del día de publicación del Aviso de Convocatoria (<https://www.superfinanciera.gov.co>).

Los valores en pesos colombianos de los Acuerdos Comerciales están vigentes hasta el 31 de diciembre de 2021.

2. ANTECEDENTES ADMINISTRATIVOS DEL PROCESO

ENTIDAD Y UNIDAD	NÚMERO DEL CONTRATO	OBJETO	ACIERTOS	PROBLEMAS
AGENCIA NACIONAL DE TIERRAS	CM - 003 DE 2018	INTELIGENCIA ARTIFICIAL	El proceso se encuentra en desarrollo contractual	No Registra
FISCALÍA GENERAL DE LA NACIÓN	FGN-IPSE-040-2019 NC	ADQUISICIÓN DE INFRAESTRUCTURA DE T.I Y SERVICIOS DE RENOVACIÓN DE SOPORTE PARA LAS PLATAFORMAS TECNOLÓGICAS DE LOS CENTROS DE COMPUTO DE LA FISCALÍA GENERAL DE LA NACIÓN	El proceso se encuentra en desarrollo contractual	No Registra
SUPERINTENDENCIA DE SOCIEDADES	DID-2-Inteligencia artificial	INTELIGENCIA ARTIFICIAL	Proceso en evaluación y observaciones	No Registra
DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL	PN DIJIN SA MC 029 DE 2019	ACCESO A PLATAFORMA DE FUENTES ABIERTAS PARA EL CIBERPATRULLAJE	Proceso adjudicado y celebrado	No Registra

INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI	CM No. 03 de 2017	PRESTACIÓN DE SERVICIOS PARA REALIZAR EL ANÁLISIS DE SENTIMIENTO DE FUENTES ABIERTAS	Proceso adjudicado y celebrado	No Registra
COMANDO GENERAL DE LAS FUERZAS MILITARES	191 CGFM 2018	ACCESO SISTEMA OSINT-DARKWEB	Proceso adjudicado y celebrado	No Registra

Se concluye que durante las vigencias anteriores, se realizaron contrataciones con objeto similares al que nos ocupa en el presente estudio.

3. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS PARA LA DEFENSA Y SEGURIDAD NACIONAL

Teniendo en cuenta que los bienes a adquirir poseen características técnicas uniformes, y que además existen varias empresas que están en capacidad de satisfacer la necesidad cumpliendo con las especificaciones técnicas requeridas, el presente proceso de selección se debe adelantar bajo la modalidad de: SELECCIÓN ABREVIADA, PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES, en cumplimiento al artículo No. 2, numeral 2, literal "a" de la ley 1150 de 2007, en concordancia con las disposiciones establecidas en el libro 2, parte 2, título 1, capítulo 2, sección 1, subsección 2, artículos 2.2.1.2.1.2.1 y 2.2.1.2.1.2.2 del Decreto 1082 de 2015 y demás normas que la complementen, modifiquen o reglamenten y por las normas civiles y comerciales que regulen el objeto de la presente contratación.

4. CRITERIOS DE SELECCIÓN

4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS

Los factores de verificación técnicas están descritos en el Anexo No. 2 del presente estudio previo, los cuales se comprobarán como CUMPLE o NO CUMPLE.

4.1.1. EXPERIENCIA PROPONENTE EN PRODUCIR O COMERCIALIZAR EL BIEN Y/O OFRECER EL SERVICIO

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 43231500 y/o 43211500 y/o 43232400 y/o 81111800, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 3.584,42 S.M.M.L.V., de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).

4.1.1.1 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 contratista deberá anexar mínimo tres (3) y máximo cinco (5) certificaciones de contratos (una certificación por contrato) celebrados y ejecutados durante los años 2017 y/o 2018 y/o 2019, con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTÍFICIAL" y/o "BIG DATA"y/o "MACHINE LEARNING" y/o "CIENCIA DE DATOS", que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 70% del presupuesto oficial asignado.

Este aspecto se verificará en el Anexo 2 Especificaciones Técnicas Mínimas.

4.1.2 PERFIL ACADÉMICO

Se requiere el personal en las cantidades mínimas, con el perfil profesional, para desempeñarse en el proyecto como se describe en la siguiente tabla:

CANTIDAD/PERFIL	NIVEL ACADÉMICO
-----------------	-----------------

1 Gerente de proyecto.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magister en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. <p>Los estudios de pregrado y posgrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p>
1 Ingeniero con conocimientos en sistemas operativos.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico, con conocimientos en sistemas operativos especialmente Windows y Linux. o equivalentes o afines en función de país de titulación..</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente, - Copia diploma o acta de pregrado. - Certificación en "Installation, Storage, and Compute with Windows Server". - Certificación en Linux. <p>Los estudios de pregrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> <p>NOTA: en caso de no cumplir una sola persona con todas las certificaciones exigidas, el oferente podrá suplir el requerimiento con otra persona, adjuntando igualmente el perfil profesional y experiencia solicitada para cada caso que aplique.</p>
2 Ingenieros con conocimientos en desarrollo.	<p>Ingeniero de sistemas y/o ingeniero de software y/o ingeniero de desarrollo y/o ingeniero electrónico especialista o magister en desarrollo de software, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría

4.1.3 EXPERIENCIA DEL PERSONAL PROFESIONAL

CANTIDAD/PERFIL	EXPERIENCIA/CERTIFICACIONES
1 Gerente de proyecto.	<p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante.</p>

	<p>B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>	
1 Ingeniero con conocimientos en sistemas operativos.	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . - Certificar experiencia mínima de tres (03) años, laborados en lo referente a instalación y mantenimiento de sistemas operativos Windows o Linux. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>	
2 Ingenieros con conocimientos en desarrollo	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación de proyectos de desarrollo. - Certificar experiencia mínima de tres (03) años, en proyectos de desarrollo Python o java o visual studio, adjuntando las certificaciones respectivas. - Certificar experiencia mínima de dos (02) años participación conocimiento y soporte en el desarrollo de las plataformas ofertadas igual o similar al sistema de Ciberinteligencia Basado e Inteligencia artificial ó plataformas de OSINT, DARKNET Y DEEPWEB durante los años 2017 y/o 2018 y/o 2019, anexando a su propuesta certificación expedida por la firma donde se desarrolló el proyecto. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>	

Este aspecto se verificará en el **Anexo 2 Especificaciones Técnicas Mínimas**.

4.2. EVALUACIÓN ECONÓMICA Y FINANCIERA

4.2.1. Evaluación Económica

Se tendrá en cuenta el menor valor ofertado en la audiencia de subasta inversa a través de la plataforma del SECOP II.

5. CONDICIONES DEL CONTRATO

5.1. LUGAR DE ENTREGA O LUGAR DE PRESTACIÓN DEL SERVICIO

La entrega del Sistema de Ciberinteligencia basado en Inteligencia Artificial, se hará en el almacén de intendencia de la Dirección de Inteligencia Policial, ubicada en la Avenida Boyacá No. 142 A 55, Barrio Colina Campestre, Bogotá D.C., e instalado previo acuerdo con el supervisor del contrato.

5.2. FORMA DE EJECUCIÓN DEL CONTRATO

La forma de ejecución será en forma total, de acuerdo a lo acordado con el supervisor del contrato, el proveedor debe entregar instalados y funcionando a todo costo los productos y servicios adquiridos.

5.3. PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato será hasta el 10 de diciembre 2020.

5.4. FORMA DE PAGO

El pago se realizará en moneda legal colombiana, en dos (2) pagos parciales, los cuales deben ser avalados y coordinados con la supervisión del contrato, en la primera entrega se recibirá el firewall, hardware e internet, mientras que la segunda entrega se obtendrá el software y soporte técnico, estos pagos se realizarán al recibido a satisfacción, dentro de los 60 días calendario siguientes a la radicación de la factura y recibido a satisfacción, certificación de la supervisión, junto con los documentos requeridos por el Área Administrativa de la Dirección de Inteligencia Policial, de acuerdo al derecho a turno y la programación del Plan Anual de Caja (PAC). De la siguiente manera así:

Un primer pago se realizará cuando se reciba a satisfacción el firewall, hardware e internet y un segundo pago cuando se encuentre instalado y funcionando el software.

5.5. SUPERVISOR O INTERVENTOR DEL CONTRATO

La supervisión del contrato estará a cargo del Jefe Área de Producción de Inteligencia, Jefe Grupo de Inteligencia de Señales y Geoespacial y la señora Subteniente **Carol Xiomara Aguirre Marín** o quien con posterioridad designe el Director de Inteligencia Policial, 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 del 2018.

5.6. OBLIGACIONES DEL CONTRATISTA

Las obligaciones del contratista están descritas en los anexos No. 2 y No. 4 del presente estudio de conveniencia y oportunidad.

5.7. OBLIGACIONES DE LA POLICÍA NACIONAL

Las obligaciones de la Policía Nacional están descritas en el anexo No. 5 del presente estudio de conveniencia y oportunidad.

6. FORMA Y PROCEDIMIENTO DE ADJUDICACIÓN

La adjudicación será en forma total.

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

Teniendo en cuenta que no existen antecedentes para el presente proceso, se establece que la estimación del riesgo (probabilidad de ocurrencia del siniestro), corresponderá 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 el Anexo No. 6 del presente estudio de Conveniencia y Oportunidad.

8. ANEXOS DE ESTUDIO

Son anexos del presente estudio previo, los siguientes documentos:

Anexo N° 1. Estudio de mercado.
Anexo N° 2. Especificaciones técnicas mínimas requeridas.
Anexo N° 3. Certificación de la necesidad.
Anexo N° 4. Obligaciones del contratista.
Anexo N° 5. Obligaciones de la Policía Nacional.
Anexo N° 6. Análisis de riesgo y la forma de mitigarlo.
Anexo N° 6.1. Estimación, tipificación, asignación de riesgos y determinación de garantías.
Anexo N° 7. Ficha técnica
Anexo N° 8. Justificación del margen mínimo
Anexo N° 9. Cesión de derechos de autor.
Anexo N° 10. Requisitos propuestas conjuntas.
Formulario N° 1 Acuerdo de confidencialidad.
Solicitud de cotización.
Cotizaciones.
Concepto ambiental.
Formato Catalogación
Certificación acuerdos internacionales y tratado de libre comercio.


Capitán MAGDA ESTEFANY PAPAMIJA BEDOYA
Estructurador Estudio Previo


Subintendente JORGE ARMANDO CHAVARRO LOZANO
Estructurador Estudio Previo

ANEXO No. 1

ESTUDIO DE MERCADO

1. ANÁLISIS DE LA DEMANDA

La expansión y uso masivo de las tecnologías de la información y las comunicaciones, así como la progresiva participación de la sociedad en actividades en el entorno digital, advierte nuevos retos para la Inteligencia Policial considerando los actores internos y externos en el ciberespacio que representan amenazas latentes contra la estabilidad estatal, institucional y la seguridad ciudadana; en este sentido, el Estado Colombiano ha fijado la política Marco Convivencia Seguridad Ciudadana y la política pública denominada "Seguridad Digital", cuyo objetivo es contrarrestar adecuadamente las amenazas ciberneticas y los incidentes en el entorno digital apoyados de estrategias, donde el rol de la Inteligencia es indispensable para la caracterización de los fenómenos y actores delictivos que confluyen en la red.

Dentro de las líneas de la política Marco Convivencia Seguridad Ciudadana de diciembre de 2019, se estableció la línea "Ciudadanos Ciberseguros" la cual pretende atender los riesgos y las nuevas dinámicas criminales que trajo consigo el avance tecnológico. *El ciberespacio es sinónimo de nuevas oportunidades para todas las personas y comunidades, pero también un escenario de actividades delictivas de diversa índole. Desde comportamientos de acoso escolar y extorsión, hasta reclutamiento criminal. Esto representa un reto en materia de seguridad ciudadana, particularmente en cuanto a prevención... y articulación institucional³.* Dentro de esta línea la atención del Gobierno nacional se centra en tres (3) principales objetivos, así: 1. Prevención de los delitos en el ciberespacio, 2. Persecución contra el ciberdelincuente y 3. Articulación Institucional contra el ciberdelito.

Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, aunado a la anterior dentro del marco del CONPES 3854 "Seguridad Digital" y el papel de la Inteligencia para recolectar información en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores, la Policía Nacional a través del Servicio de Inteligencia Policial cuenta con capacidades de recolección y análisis de información, que es considerada el apoyo y una fuente de información articulada al Centro de Capacidades para la Ciberseguridad de Colombia C4 (DIJIN), en el despliegue de actividades de cibermonitoreo, ciberpatrullaje y recolección técnica del ciberespacio.

Considerando que las actividades de ciberpatrullaje y cibermonitoreo actualmente se realizan de manera manual y empírica, sin el apoyo de herramientas tecnológicas que optimicen los tiempos de respuesta y que permitan tener una visión más global de la información disponible en internet, DARK y DEEP WEB y el presente proyecto atiende de manera directa los objetivos del plan estratégico institucional.

Aunado a lo anterior, no se cuenta con la capacidad de procesamiento y análisis de grandes volúmenes de información recolectada sobre los fenómenos criminales y todas las demás conductas que hacen uso de las tecnologías de información y comunicaciones como fin o como medio para cometer ilícitos, por ello es necesario, realizar la transformación de la inteligencia policial hacia las nuevas formas de anticipación donde se evidencian las mutaciones criminales, puntualizando en los siguientes aspectos:

- Identificación de actores, intencionalidades y objetivos en el ciberespacio en grandes volúmenes de información.
- Levantamiento de información que permita anticipar posibles ataques provenientes del ciberespacio, que afecten los intereses nacionales o pongan en riesgo la vida de los habitantes de Colombia.
- Generar alertas tempranas en la atención e identificación de fenómenos e incidentes de seguridad digital bajo las mejores prácticas internacionales.
- Optimizar tiempos de respuesta en la recolección técnica disponible en el ciberespacio.

Por lo anterior, el servicio de inteligencia en aras de estar a la vanguardia de las amenazas que hoy en día se gestan en el ciberespacio, requiere adquirir herramientas tecnológicas, capacitación y capacidades de desarrollo de software que faciliten la automatización de la recolección de información, para fortalecer las capacidades; a partir de los siguientes aspectos:

- Capacidad propia en desarrollo de software.

³ <https://id.presidencia.gov.co/Documents/191220-Politica-Marco-Convivencia-Seguridad-Ciudadana.pdf>

- Desarrollo de Crawlers y enlaces de búsqueda.
- Desarrollo de neuronas.
- Tratamiento preliminar.
- Consulta de información consolidada (Big Data estructuras y no estructuradas) y Machine Learning.
- Análisis de información en tiempo real, que permita evidenciar el panorama actual y proyecciones.
- Desarrollar habilidades de programación en Inteligencia Artificial.

En este contexto, actualmente se utilizan herramientas Free para realizar búsquedas en la web, por tal motivo, se han identificado en el mercado herramientas que indexan y exponen la información que se encuentra actualmente oculta. Estas herramientas a su vez, facilitan el anonimato del usuario y permite la obtención de datos que relacionan actuaciones de criminalidad y ciberdelincuencia, entre otros.

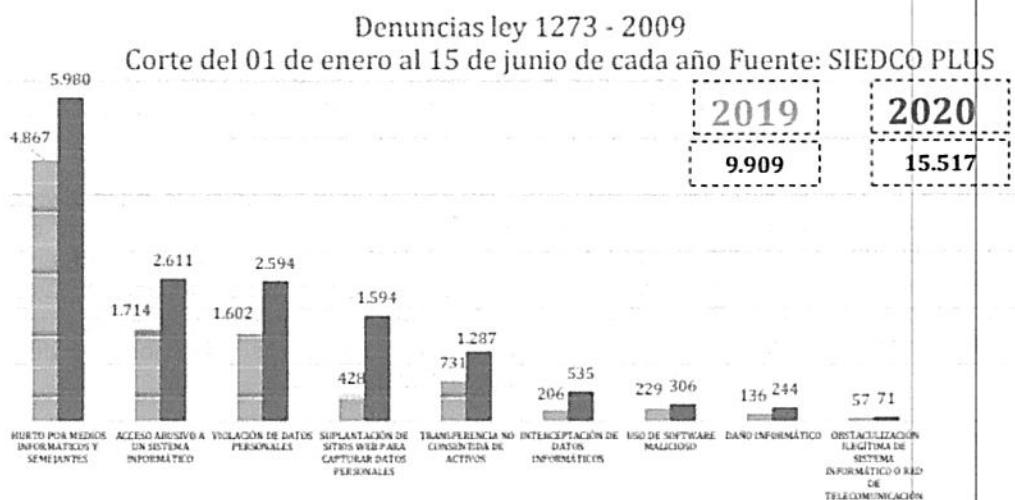
En la actualidad se tiene una capacidad reducida de personal para la realización de este tipo de actividades; es por esto que, se requiere la automatización de dicho proceso, que conduzcan a buenas prácticas en la recolección de información en la web, a fin de optimizar los tiempos de respuesta.

Considerando el contexto actual de la pandemia del COVID-19, durante el año 2020 se han presentado diferentes eventos de carácter nacional e internacional que han puesto a prueba la ciberseguridad de la región, situación que ha demandado un exponencial incremento en el uso de la internet y de las tecnologías de la información y las comunicaciones, abriendo con ello una ventana de oportunidades para que los ciberdelincuentes ataquen.

Lo anterior, se ha visto reflejado en los siguientes eventos, que han afectado la convivencia y seguridad ciudadana a nivel país, así:

- Aumento de delitos contra menores de edad en el ciberespacio (sexting, pornografía infantil).
- Generación de noticias falsas.
- Incremento del **150%** de la actividad maliciosa en internet para robar datos personales.
- Realización de saqueos a establecimientos comerciales.
- Amotinamientos en centros carcelarios.
- Entre otros eventos.

Es por esto que, durante el presente año la fluctuación delictiva ha marcado las siguientes tendencias:



- **57%** de incremento en denuncias por delitos informáticos del 01 de enero al 15 de junio del presente año, comparado con el año anterior **5.608** casos más.
- **351%** de incremento en la suplantación de sitios web, portales falsos que buscan apoderarse de información personal, principalmente bancaria **1.501** casos más.
- **160%** de incremento en el delito de Interceptación de datos Informáticos.

- 79% de incremento en el delito de daño informático.
- 76% de incremento en el delito de transferencia no consentida de activos.
- 62% de incremento en el delito de violación de datos personales.
- 52% de incremento en el delito de acceso abusivo a un Sistema Informático.
- 23% de incremento en el delito de hurto por medios informáticos y semejantes.

De igual forma, el COVID-19 ha generado las siguientes tendencias delictivas en el ciberespacio:

- **Sector Financiero:** Casi el 60% de transacciones bancarias se realiza de manera virtual, por lo que los delincuentes buscan captar las contraseñas y datos financieros de sus víctimas para hurtar el capital; otro método es la utilización de falsos productos o servicios para generar estafas.
- **Phishing:** incremento en la suplantación de sitios web para capturar datos personales, esta modalidad ha sido identificada como uno de los principales vectores de ataque por parte de los ciberdelincuentes, para obtener información privada de sus víctimas.
- **Malware:** la propagación de los también conocidos como virus en el mundo ciber, cada día se incrementa; cada vez estos software son más sofisticados y en muchos casos indetectables por las víctimas que por lo general, no tienen buena "higiene digital".
- **Noticias Falsas:** con las que se crea incertidumbre y otros vectores de ataque, llamando la atención de la potencial víctima, invitándola a dar clic sobre algún link o imagen para infectar su dispositivo o captar su información personal.
- **Portales oficiales de entidades del Estado:** un sector apetecido por los delincuentes informáticos, en ocasiones con temas reputacionales y otras para extraer recursos, este último principalmente en entes territoriales engañando a los administradores de los portales transaccionales.

Por otra parte, considerando los riesgos a los que se enfrenta la Dirección de Inteligencia Policial, frente a la navegación en el ciberespacio, con el objetivo de proteger la identidad de los funcionarios de inteligencia en este entorno, se hace necesario la adquisición de servidores para el almacenamiento de dicha información y posterior análisis, evaluación y tratamiento de las áreas que requieran estos insumos.

Como entidad gubernamental los equipos de cómputo deben contar con las herramientas ofimáticas básicas licenciadas; en este sentido, se visibiliza la necesidad de solicitar equipos de cómputo que requieran estas certificaciones. Así como, herramientas que faciliten la búsqueda de información ya procesada en tal sentido se requiere indexadores que reduzcan los tiempos de respuesta en la búsqueda de información.

Es imprescindible que cada funcionario que despliega la actividad de recolección, cuente con un equipo de cómputo que soporte las aplicaciones que de manera empírica se están construyendo para tal fin, actualmente la unidad cuenta con un solo equipo y una descripción tardía obtenida.

En este orden de ideas, y considerando las necesidades expuestas anteriormente, se hace necesario el desarrollo de una plataforma tecnológica compuesta de software, hardware y servicio; así como, la potenciación de las habilidades del talento humano a partir de la transferencia de conocimiento, enfocadas en la producción de insumos, capacidad de desarrollo de software y productos de inteligencia basados en datos técnicos recolectados en la web pública, Deep Web y Darknet, e información disponible a través de técnicas de OSINT, minería de datos y análisis de redes que apoyen los procesos estratégicos y operacionales de la Policía Nacional, traducido en las siguientes necesidades:

- Uso de herramientas de OSINT: sistemas de información de fuente abierta pública plataformas de OSINT (OPEN SOURCE INTELLIGENCE).
- Uso de herramientas de procesamiento y análisis.
- Técnicas de minería de datos.
- Seguimiento de tendencias mediáticas en redes sociales.
- Identificación de falsas noticias.
- Análisis de redes.
- Inteligencia artificial para la producción de inteligencia predictiva y prospectiva.

- Capacitación integral y especializada para fortalecer las habilidades de búsqueda en el ciberespacio; así como aspectos normativos en informática.
- Fortalecimiento de la infraestructura tecnológica:
 - Canal de datos de internet.
 - Switch.
 - Servidores con gran capacidad.
 - Herramientas especializadas de hardware y software para aplicar técnicas de OSINT y búsquedas en la Dark y Deep Web.
 - Licencias.

Mediante comunicación oficial No. S-2019-007576/OFPLA-GUDER, del 24 de octubre del 2019, la Oficina de Planeación, se realizó la aprobación para la adquisición del “Sistema de Ciberinteligencia Basado en Inteligencia Artificial”.

Mediante comunicación oficial No. S 2020-004921-OFITE, la Oficina de Telemática emite viabilidad técnica para adelantar el proceso cuyo objeto es “SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL”.

El Sistema de Ciberinteligencia basado en Inteligencia Artificial, contará con una plataforma tecnológica que estará aislada de la red de datos de la Dirección de Inteligencia Policial, considerando que esta infraestructura hará uso de Internet, cumpliendo con los protocolos de seguridad de la información establecidos para su operación, la infraestructura tecnológica para su funcionamiento contará con 3 servidores físicos con procesamiento mínimo de 32 núcleos por máquina con una frecuencia base de 2.1 GHz- RAM 256GB- discos en estado sólido que soporte 15 TB y 24 bahías de expansión , dos (2) de estos servidores se usarán como servidores de aplicación en los cuales se virtualizarán los servidores necesarios de acuerdo a la arquitectura de la solución de software, que soportará los motores de búsqueda configurados, crawlers o algoritmos, flujo de información, la recolección de información, el análisis y las correlaciones de la información pública y un tercer servidor que se empleará para almacenar la información ya validada, aunado a lo anterior, un (1) canal de datos dedicado de internet de 100 MB que soporte la navegación de los usuarios en el sistema, el cual tendrá seguridad perimetral a través de un firewall de rendimiento mínimo de 10 Gbps, 8 Millones de sesiones concurrentes mínimas (TCP y 10.000 políticas), generando de esta manera una capa de seguridad a la plataforma.

La estructura de red y la conectividad interna de los equipos de cómputo del usuario final, estarán conectados a través de un Switch Core capa 3 administrable, que conecta la solución con las dos áreas de trabajo (ARPIN, ATASI) cada una con dos switches de 24 puertos. Toda esta infraestructura física de hardware debe soportar alrededor de 5.000 transacciones por minuto.

El software estará basado en inteligencia artificial con crawlers (bots que se encargarán de analizar sitios web y buscar información específica y relevante que se le hayan establecido⁴) que han sido diseñados a la medida por los usuarios finales, los cuales realizan proceso de extraer enlaces de las páginas para evaluarlas a partir de filtros y entregarlos a un transformador de datos. De esta manera los analistas pueden crear de manera automática y fácil algoritmos personalizados basado en variables definidas por el usuario (palabras clave, consultas de búsqueda, ubicaciones, tiempos, orientados para leer contenido específico de cualquier fuente como motores de búsqueda, sitios web, fuentes web profundas y oscuras, redes sociales, redes, blogs o incluso los foros).

Otra de las funcionalidades del software se basará en la de verificación de entidades, análisis de relaciones o enlaces de manera visual, agrupación de datos, geoanálisis, análisis de sentimientos, análisis de tendencias, generación de alertas de recolección, módulo de administración y auditoria de usuarios, adicionalmente se requiere que la solución este construida como mínimo con el 80% de los solicitado en las especificaciones técnicas, para lo cual se realizará una prueba para evaluar el cumplimiento de los requerimientos, lo que no esté desarrollado y sea de autoría intelectual del personal de policía debe realizarse cesión de derechos patrimoniales de autor, de la misma manera el licenciamiento debe ser perpetuo. Con el fin de garantizar el correcto funcionamiento, se solicita una garantía y soporte de 3 años,

⁴ <https://es.ryte.com/wiki/Crawler>

además de la transferencia de conocimiento en la construcción de crawlers, administración y gestión de la infraestructura física y la capacitación de usuario final.

Los elementos requeridos objeto de la presente contratación, son requeridos para el primer semestre de 2020.

Acuerdos internacionales y tratados de libre comercio:

Dando cumplimiento a lo contemplado en la SECCIÓN IV SUBSECCIÓN 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 el SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL, por la suma de CUATRO MIL CUATROSCIENTOS NOVENTA Y OCHO MIL SEISCIENTOS NOVENTA Y NUEVE MIL OCHOCIENTOS MILLONES DE PESOS M/CTE (\$ 4.498.699.800) , SI está cubierto bajo las obligaciones de carácter internacional, de acuerdo los criterios se relacionados 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.

ACUERDOS COMERCIALES VIGENTES		ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR ACUERDO COMERCIAL	EXCLUSIÓN APlicable AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
Alianza Pacifico	Chile	SI	SI	NO	SI
	México	SI	SI	NO	SI
	Perú	SI	SI	NO	SI
Canadá		SI	SI	NO	SI
Chile		SI	SI	NO	SI

Corea	SI	SI	NO	SI
Costa Rica	SI	SI	NO	SI
ESTADOS AEJC	SI	SI	NO	SI
Estados Unidos	SI	SI	NO	SI
México	SI	SI	NO	SI
Triángulo Norte	El Salvador	SI	SI	NO
	Guatemala	SI	SI	NO
	Honduras	SI	SI	NO
UNIÓN EUROPEA	SI	SI	NO	SI

VALORES A PARTIR DE LOS CUALES SON APLICABLES LOS ACUERDOS COMERCIALES

Acuerdo comercial		Entidades Estatales del nivel municipal y departamental	Entidades generales del nivel nacional	Entidades especiales del nivel nacional
Alianza Pacífico	Chile	Bienes y servicios \$818.781.000 COP Servicios de construcción \$20.469.524.000 COP	Bienes y servicios \$204.659.000 COP Servicios de construcción \$20.469.524.000 COP	Bienes y servicios \$900.659.000 COP Servicios de construcción \$20.469.524.000 COP
	Perú		Bienes y servicios \$388.921.000 COP	
	México		Servicios de construcción \$20.469.524.000 COP	Bienes y servicios* \$397.535 USD
	Canadá	N/A	Bienes y servicios \$204.695.000 COP Servicios de Construcción* \$10'335.931 USD	Servicios de construcción* \$12'721.740 USD
Chile		Bienes y servicios \$818.650.000 COP Servicios de construcción \$20.466.528.000 COP	Bienes y servicios \$204.663.000 COP Servicios de construcción \$20.466.258.000 COP	Bienes y servicios \$900.515.000 COP Servicios de construcción \$20.466.258.000 COP
Corea		Bienes y servicios \$834.620.000 COP Servicios de construcción \$62.596.500.000 COP (Aplica para departamentos)	Bienes y servicios \$292.117.000 COP Servicios de construcción \$20.865.500.000 COP	Bienes y servicios \$1.669.240.000 COP Servicios de construcción \$62.596.500.000 COP
Estados AEJC		Bienes y servicios \$818.600.000 COP Servicios de construcción \$20.465.000.000 COP	Bienes y servicios \$532.090.000 COP Servicios de construcción \$20.465.000.000 COP	Bienes y servicios \$900.460.000 COP Servicios de construcción \$20.465.000.000 COP
Estados Unidos y Costa Rica		Bienes y servicios \$1.481.116.000 COP Servicios de construcción \$20.868.078.000 COP	Bienes y servicios \$241.786.000 COP Servicios de construcción \$20.868.078.000 COP	Bienes y servicios \$752.599.000 COP Servicios de construcción \$20.868.078.000 COP
México		N/A	Bienes y servicios* \$84.918 USD Servicios de construcción* \$11'039.387 USD	Bienes y servicios* \$424.592 USD Servicios de construcción* \$13'586.938 USD
El Salvador				Valor de la menor cuantía de la Entidad

Triángulo Norte	Guatemala	Límite inferior del valor de la menor cuantía de la Entidad	
	Honduras	N/A	
Unión Europea	Bienes y servicios \$818.660.000 COP Servicios de construcción \$20.466.500.000 COP	Bienes y servicios \$532.129.000 COP Servicios de construcción \$20.466.500.000 COP	Bienes y servicios \$818.660.000 COP Servicios de construcción \$20.466.500.000 COP

Fuente: Ministerio de Comercio, Industria y Turismo

* Para los valores en dólares, la Entidad Estatal debe definir el valor en pesos colombianos con la tasa representativa del mercado divulgada por la Superintendencia Financiera de Colombia del día de publicación del Aviso de Convocatoria (<https://www.superfinanciera.gov.co>).

Los valores en pesos colombianos de los Acuerdos Comerciales están vigentes hasta el 31 de diciembre de 2021.

2. ANÁLISIS DE LA OFERTA DEL MERCADO

DESCRIPCIÓN MERCADEO

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

Estas técnicas y herramientas para la recopilación y análisis de información son cada vez más populares y son un aspecto clave de la seguridad de la información. En este sentido en la 15va edición de Ekoparty, el equipo de OSINT Latam Group presentó un taller de herramientas de OSINT e Ingeniería Social aplicadas a las investigaciones⁵.

Perspectiva regional y análisis de tendencias:

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

Información competitiva:

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

Perspectiva de la industria y análisis de tendencias:

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

Segmentación de mercado:

⁵ <https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/>

El mercado de inteligencia de código abierto está segmentado en función del tipo, la tecnología y la aplicación. Según el tipo, el mercado se segmenta en dividido en inteligencia humana, análisis web oscuro, análisis de enlaces / redes, inteligencia de contenido, análisis de texto, análisis de datos, inteligencia artificial y big data. De estos, big data, análisis de texto y análisis de enlaces / redes dominan el mercado. Esto se debe a las progresiones tecnológicas y los análisis en el espacio cibernetico que provocan una mayor amenaza de ciberataques, piratería y otros ejercicios ilegales. Basado en la tecnología, el mercado está segmentado en análisis de Big Data, análisis web, análisis de texto, seguridad cibernetica, análisis de video y análisis de redes sociales. El software Big Data permite a OSINT proporcionar soporte productivo e importante para las técnicas e inteligencia empresarial de una organización.⁶

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

Por tipo:

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

Por tecnología:

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

Por aplicación:

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

ANÁLISIS DEL SECTOR

A nivel mundial el despliegue y uso masivo de las tecnologías de la información en las labores cotidianas de los ciudadanos, ha permitido una interacción que no conoce fronteras, la cual genera un flujo continuo de información, la creación de cuentas anónimas, generación de nuevas tendencias, la movilización de masas y la incidencia de factores delictivos que se han convertido en una preocupación y reto de cada uno de los países por la falta de gobernanza sobre el ciberespacio; es así como, en diversos estudios realizados por las organizaciones policiales y organizaciones que emiten parámetros para contrarrestar los fenómenos que generan afectación social han generado pautas y cursos de acción para disminuir o contrarrestar los incidentes de seguridad informática y los ciberdelitos.

De esta manera, el ciberespacio trae consigo amenazas sobre los sectores industriales, políticos, sociales y ecológicos de los países; por lo cual, se deben desarrollar las capacidades y destrezas en el entorno digital para mitigar el impacto de los riesgos sobre los activos de información, lo que permite evidenciar el surgimiento de términos y áreas como la Ciberseguridad, Ciberdefensa y Ciberinteligencia, con el fin de anticipar, prevenir, atender y evaluar los incidentes de seguridad información.

- La oferta: se ofrece la adquisición de un sistema basado en inteligencia artificial, que permitirá realizar recolección de información y análisis situacional, predictivo y prospectivo de información disponible en el ciberespacio.
 - La demanda: para desarrollar las funciones del presente sistema, se requiere de medios tecnológicos y la adquisición de herramientas especializadas para la búsqueda y perfilación en fuentes abiertas; así como, la implementación de infraestructura para el procesamiento y almacenamiento de información producto de la recolección técnica.
- a) **IDENTIFICACIÓN DE VENTAJAS:** la oferta expuesta permitirá desarrollar apropiadamente la misión, las funciones, los procesos institucionales y misionales de la Dirección de Inteligencia Policial; así como, la generación de conocimiento para la obtención de resultados y la prestación de un servicio efectivo.

⁶ <https://steemit.com/utopian-io/@difelice/segmentos-de-mercado-de-open-source-intelligence-osint-estrategias-de-jugadores-clave-y-mas-hasta-2023-esto-aporta-el-informa>

- b) EJECUCIÓN:** recolectar información a través de medios técnicos, con el propósito de aportar a la producción de inteligencia estratégica, operacional y para el Servicio de Policía, que permita prevenir las amenazas y riesgos que puedan atentar contra la Seguridad y Defensa de la Nación, a través del ciberespacio.

PROCEDENCIA Y DISPONIBILIDAD DE LOS BIENES

Los bienes solicitados son de origen de proyecto de inversión de la Policía Nacional y teniendo en cuenta la naturaleza del bien a contratar, se ha establecido que pueden ser de carácter nacional o extranjero siempre y cuando cumpla con los términos exigidos.

MONEDA A CONTRATAR

El pago se realizará en moneda colombiana (Pesos).

FORMA DE PAGO:

El pago se realizará en moneda legal colombiana, en dos (2) pagos parciales, los cuales deben ser avalados y coordinados con la supervisión del contrato, en la primera entrega se recibirá el firewall, hardware e internet, mientras que la segunda entrega se obtendrá el software y soporte técnico, estos pagos se realizarán al recibido a satisfacción, dentro de los 60 días calendario siguientes a la radicación de la factura y recibido a satisfacción, certificación de la supervisión, junto con los documentos requeridos por el Área Administrativa de la Dirección de Inteligencia Policial, de acuerdo al derecho a turno y la programación del Plan Anual de Caja (PAC). De la siguiente manera así:

Un primer pago se realizará cuando se reciba a satisfacción el firewall, hardware e internet y un segundo pago cuando se encuentre instalado y funcionando el software.

DESCRIPCIÓN MERCADO

A partir de pruebas concepto realizadas a 10 herramientas robustas, dedicadas a la recolección y correlación de información disponible en la web que se encuentran en el mercado, se logró determinar las funcionalidades acordes a las necesidades del Servicio de Inteligencia y la Policía Nacional, así como la identificación de empresas a nivel local y en el exterior que existen en el mercado actual y que pueden satisfacer los requerimientos descritos en el anexo técnico del presente proceso contractual, cuyas variaciones u optimización en el manejo y recolección de información está cimentada en la cantidad de fuentes integradas a las plataformas, la organización y presentación de la información, así como tiempos de respuesta, consumo de canal de internet y el posicionamiento de empresas que han ofrecido soluciones de este mismo orden al sector gobierno de otros países, dentro de las cuales tenemos :

MELTEC COMUNICACIONES S.A.

Hector Ortiz Guerrero

hortiz@meltec.com.co

Dirección: Calle 130 A # 58A – 29 Bogotá

Mollitiam

Samuel Álvarez González

salvarez@mollitiamindustries.com

Dirección: Calle Río Jarama, No. 132 Edificio singular 4.03, Bajo C, Toledo

NET COLOMBIA S.A.S.

Luis Genaro Ríos Muñoz

net.colombia@hotmail.com

Dirección: Carrera 23 No 33 – 17 Bucaramanga

INDICADORES FINANCIEROS

Con base a una muestra de endeudamiento de 18 (dieciocho) empresas, dentro de las cuales se encuentran firmas cotizantes la Dirección de Inteligencia Policial, se tomó muestra de los indicadores financieros y de capacidad organizacional, así:

NIT	RAZON SOCIAL	CIU	TOTAL ACTIVO CORRIENTE	TOTAL ACTIVO	TOTAL PASIVO CORRIENTE	TOTAL PASIVO	TOTAL PATRIMONIO	GASTOS DE INTERESES	UTILIDAD OPERACIONAL	LIQUIDEZ	ENDEUDAMIENTO	RAZON DE COBERTURA DE INTERESES	RENTABILIDAD SOBRE ACTIVO	RENTABILIDAD SOBRE PATRIMONIO
800082633	HOSPIIMPORT S.A.	G4651	6402635	8476756	2794945	4121817	4354939	318786	951803	2,29079	0,486249	2,98571142	0,11228387	0,21855714
802015514	EASY SYSTEMS S.A.S	G4651	9573609	15204681	5622114	9545489	5659192	499158	1152259	1,70285	0,6277599	2,30840535	0,07578317	0,20360839
830025967	I3NET S.A.S.	G4651	13035980	14708658	5681496	9191106	5517552	268189	641135	2,29446	0,624877	2,39060886	0,04358895	0,11619918
830027956	XOREX DE COLOMBIA S.A.S	G4651	5482563	9000848	2517187	4309203	4691645	318362	993478	2,17605	0,478755	3,12059228	0,11037604	0,21175473
830050654	COMPUTEL SYSTEM SAS	G4651	37271263	42025944	15178589	25178589	16847355	719527	2283545	2,45552	0,59912	3,17367521	0,05433655	0,13554324
830111723	NEX COMPUTER S.A.	G4651	15336248	15584833	7715059	12462943	3121890	291717	645964	1,98783	0,799684	2,21435158	0,04144825	0,2069144
830142604	JAAMSA COLOMBIA S A	G4651	8712882	17536670	6244111	8069186	9467484	318265	957800	1,39538	0,460132	3,00944182	0,05461698	0,10116732
891703002	GAMMA INGENIEROS S.A.S.	G4651	7169831	7960627	3765763	3765763	4194864	143300	627259	1,90395	0,473049	4,37724355	0,07879518	0,14953024
900042741	COMPUORIENTE IMPORT AND EXPORT LTDA.	G4651	9016976	12507117	4449077	9829997	2677120	543290	2307868	2,02671	0,785952	4,24794861	0,18452438	0,86207118
900163129	IKONO TECH SA	G4651	6086274	8334502	4532938	6278363	2056139	517143	1158383	1,34268	0,753298	2,23996651	0,13898647	0,56337777
900270815	HERITAGE GROUP S.A.S	G4651	23486204	25950034	14322151	18159979	7790055	512358	5046265	1,63985	0,699806	9,84909965	0,19446085	0,64778297
900274644	TECNOPROCES OS SAS	G4651	3852590	3956112	1005286	1668065	2288047	89930	494624	3,83233	0,421643	5,50010008	0,12502781	0,21617738
900616678	SITEC SUMINISTROS S.A.S.	G4651	6184149	7590676	2180532	5091770	2498906	90756	185597	2,83607	0,670793	2,0450108	0,02445065	0,0742713
900009482	DEINTEKO	G4651	625319960	713678188	155806343	1,56E+08	5,58E+08	11782891	63280085	4,01	0,21	7,06	0,11	0,14
830040391	EAGLE COMMERCIAL	G4651	3,385E+09	4,999E+09	495462842	1,83E+09	3,17E+09	7255183	5,97E+08	6,83	0,36	82,30	0,11	0,18
800225235	SF INTERNATIONAL	G4651	3,101E+09	5,541E+09	2,031E+09	3,32E+09	2,22E+09	2,13E+08	3,06E+08	1,52	0,59	1,43	0,05	0,13
830079015	MELTEC COMUNICACIONES S A	G4651	2,894E+10	3,856E+10	1,345E+10	1,89E+10	1,96E+10	1,41E+08	2,64E+09	2,15	0,49	18,66	0,06	0,13
900396176	MNEMO COLOMBIA SAS	G4651	1,809E+10	2,167E+10	3,287E+09	1,42E+10	7,47E+09	1,96E+08	7,57E+08	5,50	0,65	3,85	0,03	0,10

No	INDICADOR	CRITERIO DE SELECCIÓN
1	Liquidez	I L < 3 Excluyente
2	Nivel de Endeudamiento	I E > 0.65 Excluyente
3	Capital de Trabajo	C T < 50% Presupuesto oficial Excluyente
4	Razón cobertura de interés	R C I < 3 Excluyente
5	Rentabilidad sobre Activo	R A < 0.12 Excluyente
6	Rentabilidad sobre Patrimonio	R P < 0.20 Excluyente

Nota: Los resultados de los indicadores se trabajan con dos decimales. Si los oferentes presentan los gastos de intereses en cero (0), no podrán calcular el indicador de razón de cobertura de intereses. Por lo tanto, cumplen con el indicador, salvo que la utilidad operacional sea negativa, caso en el cual no cumple con el indicador de razón de cobertura de intereses.

Para la evaluación de los indicadores de Capital de Trabajo, Razón de cobertura de interés, Rentabilidad del patrimonio y Rentabilidad del activo, si el proponente es una Unión Temporal, los indicadores financieros, serán el resultado de la suma de cada uno de estos afectado según el porcentaje de participación de los miembros; si el proponente es un consorcio los indicadores financieros, serán el resultado de la sumatoria de cada uno de sus integrantes.

Para la evaluación de los indicadores de Liquidez y Nivel de Endeudamiento, el resultado será la suma de cada uno de estos de todos los integrantes

La anterior información se verificará con el registro único de proponentes RUP, el cual debe contener la información financiera a corte 31 de diciembre 2019 (en firme).

3. ANÁLISIS DE PRECIOS

3.1. Precios referencia SECOP

ENTIDAD	OBJETO	NÚMERO DE CONTRATO	FECHA	VALOR
DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL	ACCESO A PLATAFORMA DE FUENTES ABIERTAS PARA EL CIBERPATRULLAJE	PN DIJIN SA MC 029 DE 2019	2019	\$ 3.993.000.000
https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE				
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI	PRESTACIÓN DE SERVICIOS PARA REALIZAR EL ANÁLISIS DE SENTIMENTO DE FUENTES ABIERTAS	CM No. 03 de 2017	2017	\$ 76.055.556
https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE				
COMANDO GENERAL DE LAS FUERZAS MILITARES	ACCESO SISTEMA OSINT-DARKWEB	191 CGFM 2018	2018	\$ 697.850.000
https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE				
https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE				
AGENCIA NACIONAL DE TIERRAS	INTELIGENCIA ARTIFICIAL	CM - 003 DE 2018	2018	\$ 728.878.939
https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE				

3.2. ANÁLISIS DE PRECIOS HISTÓRICOS

ÍTEM	DESCRIPCIÓN	CONTRATO PN DIJIN SA MC 029 DE 2019	Valor unitario Proyectado 6.77 %	CONTRATO CM - 003 DE 2018	Valor unitario Proyectado 5.75 %	CONTRATO 191 CGFM 2018	Valor unitario Proyectado 4.09%	VALOR HISTÓRICO PROYECTADO A TOMAR
1	SISTEMA DE CIBERINTeligencia BASADO EN INTELIGENCIA ARTIFICIAL	\$ 3.993.000.000	\$ 4.020.032.610	\$ 728.878.939	\$ 778.224.043	\$ 697.850.000	\$ 745.094.445	N/A

Nota: los precios históricos no serán tenidos en cuenta, toda vez que las especificaciones técnicas difieren con respecto al presente proceso.

3.3 ANÁLISIS PRECIOS DE MERCADO

Considerando que se han logrado evidenciar las capacidades de herramientas disponibles en el mercado, y que se realizó cotización a más de 8 empresas, cuya solicitud determinó los términos de ejecución del proyecto, forma de pago, garantías, y especificaciones técnicas, se tomaron los precios promedio obtenidos del mercado actual, cotizaciones presentadas por las empresas MOLLITIAN, MELTEC, NET COLOMBIA S.A.S, cuyos valores se ajustan al presupuesto, tiempos de entrega y las condiciones técnicas descritas en el presente pliego, así:

ANÁLISIS DE PRECIOS DE MERCADO						
ÍTEM	DESCRIPCIÓN	CANT	MELTEC	MOLLITIAN	NET COLOMBIA S.A.S	MENOR VALOR COTIZADO
1	SERVIDORES	3	\$ 221.500.000	\$ 221.933.400	\$ 290.730.000	\$ 221.500.000,00
2	SWITCH 48 PUERTOS	1	\$ 71.500.000	\$ 71.451.965	\$ 72.650.300	\$ 71.451.965,00
3	SWTCH 24 PUERTOS	2	\$ 41.000.000	\$ 39.955.761,50	\$ 41.955.800	\$ 39.955.761,50
4	FIREWALL	1	\$ 185.000.000	\$ 181.293.302	\$ 181.320.000	\$ 181.293.302,00
5	SOFTWARE OSINT	1	\$ 4.624.000.000	\$ 3.397.034.248	\$ 3.510.050.000	\$ 3.397.034.248,00
6	CANAL DEDICADO INTERNET POR UN PERÍODO DE TRES (3) AÑOS	1	\$ 329.000.000	\$ 104.508.762	\$ 106.556.832	\$ 104.508.762,00

NOTA: En el presente análisis de precios de mercado se determina que con base a las cotizaciones, se toma como referencia el menor valor cotizado presentado por los oferentes MELTEC, MOLLITIAN y NET COLOMBIA S.A.S, en el entendido que los productos ofertados cumplen con las condiciones técnicas requeridas por esta Dirección.

Nota aclaratoria: para los ítems del 1 al 5, se aplicara lo establecido en la normatividad tributaria, así:

*** 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%**

El ítem No 6 (Canal de datos dedicado internet), estará grabado con la tarifa del 19% de IVA.

3.4. ANÁLISIS VALOR ESTIMADO

ÍTEM	DESCRIPCIÓN	PRECIO SECOP	PRECIOS HISTÓRICOS PROYECTADOS	PRECIO DE MERCADO	VALOR ESTIMADO TOTAL
1	SERVIDORES	NO APLICA	NO APLICA	\$ 221.500.000,00	\$ 221.500.000,00
2	SWITCH 48 PUERTOS	NO APLICA	NO APLICA	\$ 71.451.965,00	\$ 71.451.965,00
3	SWITCH 24 PUERTOS	NO APLICA	NO APLICA	\$ 39.955.761,50	\$ 39.955.761,50
4	FIREWALL	NO APLICA	NO APLICA	\$ 181.293.302,00	\$ 181.293.302,00
5	SOFTWARE OSINT	NO APLICA	NO APLICA	\$ 3.397.034.248,00	\$ 3.397.034.248,00
6	CANAL DEDICADO INTERNET POR UN PERÍODO DE TRES (3) AÑOS	NO APLICA	NO APLICA	\$ 104.508.762,00	\$ 104.508.762,00

3.5. VALOR ESTIMADO DE LA CONTRATACIÓN

El valor estimado del presente proceso es de CUATRO MIL CUATROSCIENTOS NOVENTA Y OCHO MILLONES SEISCIENTOS NOVENTA Y NUEVE MIL OCHOCIENTOS PESOS M/CTE (\$ 4.498.699.800,00)

ÍTEM	UNIDAD DE DESTINO	DESCRIPCIÓN	CANT	VALOR UNITARIO ESTIMADO SIN IVA	VALOR TOTAL ESTIMADO SIN IVA
1	DIPOL	SERVIDORES	3	\$ 221.500.000,00	\$ 664.500.000,00
2	DIPOL	SWITCH 48 PUERTOS	1	\$ 71.451.965,00	\$ 71.451.965,00
3	DIPOL	SWITCH 24 PUERTOS	2	\$ 39.955.761,50	\$ 79.911.523,00
4	DIPOL	FIREWALL	1	\$ 181.293.302,00	\$ 181.293.302,00
5	DIPOL	SOFTWARE OSINT	1	\$ 3.397.034.248,00	\$ 3.397.034.248,00
6	DIPOL	CANAL DEDICADO INTERNET POR UN PERÍODO DE TRES (3) AÑOS	1	\$ 104.508.762,00	\$ 104.508.762,00
VALOR TOTAL ESTIMADO					\$ 4.498.699.800,00
VALOR TOTAL POR RECURSO					\$ 4.500.000.000,00

Nota aclaratoria: para los ítems del 1 al 5, se aplicara lo establecido en la normatividad tributaria, así:

*** 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%**

El ítem No 6 (Canal de datos dedicado internet), estará grabado con la tarifa del 19% de IVA.

ANEXO No. 2
CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
1.	El contratista deberá implementar una solución que incluya el software, el hardware y el desarrollo necesario para proveer un Sistema de Ciberinteligencia basado en Inteligencia Artificial, que integre diversas fuentes de información abierta, información estructurada y no estructurada, así como información y contenido dispuesto en internet, con el fin de enriquecer el análisis y la elaboración de productos prospectivos y anticipativos, a través de la generación automática de organización de información de manera gráfica y alertas.		
1.1	El contratista se encargará de realizar todas las acometidas eléctricas y lógicas necesarias para la instalación de los equipos ofertados e integración del software en los equipos dispuestos; tales como, router, cables de potencia, breaker, switch, interfaces de conexión como patch-cord de fábrica thermoformados, cables FC, transceiver de fibra óptica en origen y destino, software de configuración (drivers) y utilitarios del sistema, para cada uno de los componentes de la solución y los necesarios que garanticen su pleno funcionamiento; fuera de la red que tiene contratada la POLICÍA NACIONAL. Asimismo, la instalación de los servidores en el Datacenter de la Dirección de Inteligencia Policial sin que se comprometa de alguna forma la red de la Policía Nacional.		
1.2	Considerando que se conectarán treinta (30) equipos de computo a la infraestructura a implementar, el contratista debe tender el cableado físico que grantice la conexión desde el datacenter a los switches de piso de las áreas de trabajo (los que ofertan en el presente proceso), considerando que actualmente los equipos de computo en cada piso cuenta con su punto de conexión.		
1.3	<p>Con el fin de verificar las condiciones del datacenter y distancias para la instalación de cableado, se programará visita técnica dos (2) días después de publicado el pliego definitivo del presente proceso, para lo cual deberán enviar datos del personal que realizará visita técnica (máximo dos personas por oferente) a través de la sección de mensajes de la plataforma SECOP II, con los siguientes datos:</p> <p>Nombres y apellidos: Número de identificación: Nombre de la empresa oferente: Nacionalidad:</p> <p>Por políticas de seguridad de la información, no está permitido el ingreso de equipos de cómputo, celulares, dispositivos USB y demás elementos electrónicos que posean capacidad de almacenamiento, de igual forma se deben diligenciar los formatos de compromiso de reserva y estudio de credibilidad y confiabilidad.</p>		
1.4	El contratista instalará, configurará, integrará y entregará en completa operación los elementos que hacen parte del hardware de la solución en el Datacenter de la Dirección de Inteligencia Policial o el espacio asignado para tal fin, dentro de las instalaciones.		
1.5	El Sistema debe ser una plataforma de Inteligencia efectiva, ágil, escalable, intuitiva al usuario, que utilice técnicas de correlación y		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>análisis, empleando tecnologías de procesamiento de lenguaje natural, procesamiento de imágenes y de textos en imágenes a partir de técnicas de machine learning e IA.</p>		
1.6	<p>Considerando que es un sistema con unas necesidades específicas y que existen en el mercado algunas que se ajustan en un 80% a lo requerido, se hace necesario la realización de un co-desarrollo por parte del contratista con acompañamiento del contratante, con el fin de integrar otras fuentes de información pública y disponibles para la Policía Nacional. El contratista se compromete a realizar un Co-Desarrollo equivalente al 20% del sistema, el cual debe ser a la medida y cumpliendo con los requerimientos establecidos por el contratante.</p> <p>Con el fin de verificar el cumplimiento de las funcionalidades del producto ofertado, el comité técnico, evaluará el funcionamiento del sistema a través de una prueba técnica descrita a continuación:</p> <p>Consideraciones:</p> <p>La Dirección de Inteligencia Policial, a través del comité técnico, se evaluará mediante una prueba técnica, si cumple o no cumple cada uno de los subítems que se describe en el Cuadro No. 1 Metodología de Evaluación.</p> <p>Con la entrega de la oferta deben entregar correo con el cual se podrán contactar para efectuar videoconferencia.</p> <p>El día de la entrega de las ofertas, se realizará reunión de coordinación con los representantes legales y un técnico de las firmas oferentes, a través de videoconferencia, con el fin de suministrar información técnica para la realización de la prueba.</p> <p>El mismo día se pueden realizar preguntas a los estructuradores, con el fin de que resuelvan dudas y realicen las conexiones necesarias para la realización de la prueba.</p> <p>El cronograma para la presentación de las pruebas, se hará de acuerdo al orden en que se reciban las ofertas y la cantidad de oferentes, la prueba se realizará dos días después de recibir la oferta, fecha y hora que se indicará una vez se reciban todas las ofertas a través de la sección de mensajes de la plataforma SECOP II a cada firma oferente.</p> <p>Se tiene previsto el espacio de un día desde las 09:00 horas hasta las 17:00 horas para que los oferentes, realicen las pruebas.</p> <p>El oferente deberá incluir en la oferta el nombre de los técnicos (máximo dos), que guiarán al funcionario designado para la interacción en la plataforma ofertada.</p> <p>Para la prueba se asignará un funcionario por plataforma ofertada en un equipo con internet.</p> <p>Los oferentes deben entregar:</p> <ul style="list-style-type: none"> -Usuario y Contraseña para ingresar a la plataforma. <p>Durante la realización de las pruebas un moderador entregará los datos y simultáneamente los funcionarios asignados realizarán las</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>búsquedas, generaran las alertas y verificarán el funcionamiento uno a uno de los requerimientos.</p> <p>En esta prueba se verificarán las funcionalidades del software del oferente, teniendo en cuenta cada uno de los 160 subítems establecidos en la tabla “Evaluación detallada”, poniendo frente a cada actividad si cumple o no cumple.</p> <p>En este sentido, la evaluación se requiere que cumpla con el 80% de los ítem a verificar.</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS			CUMPLE	NO CUMPLE
Cuadro No.1 Metodología de evaluación EVALUACIÓN DETALLADA					
NOMBRE DE LA EMPRESA		Cumple	No cumple		
1	Gestión de usuarios: Mostrar el panel de administrador	Adicionar nuevos usuarios			
		Conectar un email a cada usuario			
		Defina usuarios regulares y administradores y podría cambiar el usuario correctamente fácilmente			
		Cambiar la contraseña			
		Bloquear y desbloquear usuarios			
2	Asignación y Gestión del espacio de trabajo a usuarios	Adicionar nuevos espacios de trabajo, o asignar roles de los módulos			
		Definir usuario activo y no activo			
		Cambiar los usuarios en cada espacio de trabajo			
		Administre la política de retención para cada espacio de trabajo.			
3	Manejo de la Cuenta de navegación	Importar números masivos de cuentas de navegación (al menos 500)			
		Sube cuentas de navegación configurados de todas las redes sociales			
		Definir si la cuenta de navegación se usa a través de API / o login			
		Crea una cuenta de navegación con algunas redes sociales			
4	Auditoria	Mostrar el panel o módulo de administrador			
		Permite personalizar un tablero para administrar todos los datos de auditoría			
		Visualizar todas las acciones principales realizadas en el entorno divididas por tiempo, usuarios, espacios de trabajo o módulos y más			
		Auditar las actividades de todos los usuarios internos del sistema.			
5	Capacidades de Análisis: Se darán temáticas para realizar búsquedas y se debe mostrar los análisis y colección efectuada.	Análisis de temas y discursos			
		Línea de tiempo en un gráfico			
		Análisis de sentimientos			
		Influenciadores			
		Análisis geográfico en un mapa			
		información demográfica			
		Principales interactoros			
		Detección de cuentas falsas			
		hashtags principales			
		URL principales			
		Análisis de entidades			
		Cuentas de redes sociales			
		Contenido que incluye a los principales interactoros y participantes			
		Acerca del Usuario			
		Conexión agrupada por lugar de trabajo, ciudad natal, educación, grupos internos, fuerza de conexión, cuentas falsas.			
		<u>Análisis de grupo</u>			
		o Intersección entre dos entidades.			
		o Principales interactoros de una página web o red social			
		o Acerca de la página			
		o Fans superiores de la página			
		o Publicaciones principales			
		<u>Análisis organizacional</u>			
		• cuentas de redes sociales			
		• Los mejores interactoros			
		• Presencia web			
		• Posibles miembros			

NUMERAL	CARACTERÍSTICAS TÉCNICAS				CUMPLE	NO CUMPLE
		Demostrar la recolección de horarios • Recolectando la información cada X cantidad de tiempo				
		Nuevas fuentes Mostrar toda la información que se recopiló utilizando los nuevos buscadores que se crearon.				
		Recolección Dark Web • Mostrar los diferentes filtros que se pueden usar • Motores de búsqueda Darknet				
6	Biblioteca algoritmos de búsqueda: El sistema debe tener una biblioteca de algoritmos de búsqueda a la que se pueda acceder fácilmente desde varias pantallas. Mostrar las siguientes fuentes:	Algoritmos de búsqueda en redes sociales Facebook Twitter YouTube Instagram Algoritmos Surface web: Motores de búsqueda (por lo menos 5 al mismo tiempo) Web pages RSS DarkNet Motores de búsqueda Web pages Otras fuentes				
7	Consulta: El usuario debe poder controlar la recopilación de datos.	Insertar diferentes tipos de entrada (nombres de usuario, ID de usuario) Cambiar el nombre de la consulta Se puede definir qué cuenta de navegación recogerá los datos. Crear una tarea de recopilación programada Definir la cantidad de tiempo que se realizará la recolección. Escribir una descripción para cada consulta Agregar múltiples consultas Definir a qué caso va esta consulta				
8	Reintentar mecanismo	Demuestre que el sistema sabe cómo superar el bloqueo de las cuentas de navegación y enviar al menos tres cuentas de navegación diferentes de forma automatizada para realizar una sola consulta.				
9	Geo-cercado	Generar una consulta señalando un área geográfica específica, devolviendo resultados de un área específica				
10	Medios de comunicación – Búsqueda de cuenta	Encuentre diferentes nombres de identidad basados en palabras clave en las siguientes redes: • Facebook • Twitter • Instagram Recopilar información sobre las cuentas directamente desde la pantalla de búsqueda				

NUMERAL	CARACTERÍSTICAS TÉCNICAS				CUMPLE	NO CUMPLE
11	Colección de redes sociales Recopile la siguiente información:	Facebook identidad Feed (comentariastas, reacciones) Conexiones Acerca de (ingresos, paginas) Ubicaciones Página de Facebook Feed (comentariastas, reacciones) Interactores de página Acerca de la página Grupo de Facebook Feed (comentariastas, reacciones) Miembros del grupo, Facebook post comentariastas, reacciones seguidores Búsqueda genérica– palabras claves Twitter Identidad Feed (comentariastas, reacciones) Seguidores Hashtags Cuenta mencionada Retweets Búsqueda genérica– palabras claves Instagram: Identidad Feed (comentariastas, reacciones) Hashtags User location Seguidores Page locations YouTube: Identidad YouTube búsqueda – Avanzada YouTube búsqueda				
12	Web Page	Elija cualquier sitio web normal y muestre las capacidades de recopilación				
13	Motores de búsqueda	Mostrar la colección de los motores de búsqueda. Esto debe incluir al menos 5 diferentes				
14	RSS	colección RSS Feeds				
		Dark Web				
15	Motores de búsqueda	Mostrar la colección de los motores de búsqueda de dark net				
16	Web page	Mostrar la colección de un sitio web oscuro específico (TOR)				
		Aplicaciones				
17	Telegram	Mostrar la colección de un canal de Telegram con una cuenta de navegación dedicada				
		Nuevas fuentes				
18	Adicionar nuevas fuentes: El proponente recibirá por adelantado algunas fuentes y mostrará	El sistema debe poder agregar nuevas fuentes a la lista. Crear y agregar Foros – dark web y surface web Crear y agregar noticias website				

NUMERAL	CARACTERÍSTICAS TÉCNICAS				CUMPLE	NO CUMPLE
	el flujo de trabajo de creación y la recopilación y análisis (las fuentes serán entregadas el día de la entrega de las ofertas)	Data base Online Crear y agregar un Excel				
19	Parámetros de búsqueda de entidad	Búsqueda por un parámetro que tenga la herramienta. Búsqueda por Email (<i>realizada sobre información pública</i>). Búsqueda por número de cédula (<i>realizada sobre información pública</i>). Búsqueda por Facebook ID Búsqueda por Twitter ID Búsqueda por Instagram ID				
20	Reporte o informe Generar el reporte con la siguiente información:	Crear un informe dentro del sistema. Imágenes de entidad Nombres Informacion publica disponible Cuentas de redes sociales Conexiones Ubicaciones (desde redes sociales) Guardar y pegar capturas de pantalla del sistema Visualiza el flujo de investigación y muestre la conexión entre las diferentes pruebas encontradas. Medios de comunicación				
21	Exportar	Exportar el informe en formato PDF Exportar informe en formato JSON Exportar informe en otro formato Mostrar los reportes				
22	Extracción de entidad	Organizaciones Nombres de entidad URL Etiquetas Localizaciones Idiomas Fuentes				
23	Búsqueda basada en palabras:	Crear una lista dedicada de palabras para buscar en una de las consultas Muestre que el sistema lo extrajo				
24	Clasificación cuentas falsas	Clasificar las cuentas en Facebook y Twitter como falsas Mostrar los motivos de clasificación				
25	Clasificación	Ordenar la información según tiempo de publicación Ordenar la información según fuente Ordenar la información según Compromiso Ordenar la información leido / No leido				
26	Exporte	Mostrar las capacidades de exportación del feed y de otras características del sistema, incluidos CSV, PNG, i2 y otros formatos.				
27	Medios y Display	Mostrar imágenes y videos.				

NUMERAL	CARACTERÍSTICAS TÉCNICAS					CUMPLE	NO CUMPLE
			Mostrar cómo el usuario puede descargar todas las imágenes y videos.				
			Mostrar los resultados en "Modo de chat" en aplicaciones.				
28	Datos resumidos	Nube de palabras					
		Línea de tiempo en un gráfico					
		Sentimiento					
		Conexiones de hashtags en un gráfico					
		Demografía en un gráfico					
		Mejores influenciadores					
		Distribución de cuenta falsa					
29	Geo-Analysis	Muestra la información en un mapa que se puede cambiar.					
		Mostrar puntos calientes en función de la cantidad de resultados					
30	Análisis de relaciones – Análisis link	Agrupar los resultados por ciudad de nacimiento					
		Agrupar los resultados por ciudad actual					
		Agrupar los resultados por lugar de trabajo					
		Agrupar los resultados por nombre y apellido					
		Grupos internos – mostrar la relación entre las conexiones de grupos para encontrar aquellos que sean de interés					
		Fuerza de conexión – muestra la fuerza de la conexión basada en me gusta, comentarios, pariente.					
	Lista de entidades con actividad Inusual	Intersección – muestra la intersección de las conexiones de algunas cuentas para encontrar conexiones mutuas.					
31		Marcar cuenta					
	Alertas	Gestionar lista.					
32		Generar como mínimo 4 tipos de alertas y vistas guardadas					
		Alerta basada en geografía					
		Alerta basada en feed					
		Alerta indicativa basada en palabras					
	Visualizando el flujo de Investigación	Envío de alerta por correo electrónico					
33		Muestra una visualización gráfica del flujo de investigación completo.					
		Conectar diferentes tipos de entidades (cuentas sociales, datos públicos encontrados).					
	1.7	Enlaces a sitios web, videos y pantallas					
		Desde el inicio del proyecto, la seguridad del sistema se debe prever, teniendo en cuenta controles, auditorías, accesos e infraestructura.					
1.8	El contratista debe garantizar que cuenta con un sistema o herramienta tecnológica base ya desarrollada en 80% con las necesidades descritas en el presente pliego, que permita integrar nuevas funcionalidades y los casos de uso específicos descritos en el presente pliego de condiciones, la cual debe ser entregada a POLICÍA NACIONAL con licenciamiento perpetuo, que no genere costos adicionales al proyecto de tal manera que incluya el licenciamiento de toda la solución de hardware ofertada, es decir, licenciamiento de todos los Cores de la solución y de todos los usuarios solicitados. Para tal efecto, debe anexar la ficha técnica para el ítem 1 descrito adelante,						

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>que enuncie las especificaciones técnicas y funcionalidades actuales del sistema.</p> <p>Adicionalmente y durante el periodo de mantenimiento el contratista debe priorizar dar solución a cualquier inconveniente que pueda generarse en el normal desarrollo de la plataforma debido a actualizaciones de las APIS por parte de terceros (como Twitter, Facebook o Instagram). La clasificación de la incidencia sobre tecnologías ajenas al contratista debe quedar formalizada en un plazo no superior a 48 horas.</p>		
1.9	<p>Vectores de entrada de datos de fuentes de información:</p> <p>Fuentes Abiertas: (OSINT), basadas en:</p> <ul style="list-style-type: none"> - Redes sociales: Facebook, Twitter y Instagram, - Servicios WEB: Pastebin, Foros, Blogs. - Canales, grupos y supergrupos de Telegram públicos. - Información Darkets (Tor, I2p y freenet al menos). - 5 fuentes de información abierta que serán integradas a petición de la Dirección que tengan acceso abierto y sin controles por navegación web. <p>Fuentes Cerradas: las estructuradas y gestionadas con independencia de la plataforma de inteligencia mediante API de conexión facilitada por la Dirección.</p> <ul style="list-style-type: none"> - Evidencias digitales forenses (EVDF) ya procesadas. (Excel, Word, Pdf, txt, imágenes, videos). <p>Para las fuentes abiertas en internet, durante el mantenimiento, se priorizará el soporte en los controles de acceso que puedan surgir, siendo conscientes que la evolución o modificación de tecnologías ajenas al oferente no pueden ser controladas.</p>		
1.10	<p>La herramienta debe ser construida bajo una arquitectura modular, la cual permite la integración de nuevos módulos de Crawling y organización de la información, integración y escalabilidad de fuentes abiertas, información estructurada y no estructurada disponible para la Policía Nacional.</p>		
1.11	<p>El software que compone el sistema, deberá tener licenciamiento perpetuo, que se pueda desinstalar e instalar en un nuevo hardware sin limitaciones, ya sea por máquina o por número de cores o procesadores, 100% administrable por la Policía Nacional y soporte técnico mínimo de tres (3) años.</p> <p>El sistema completo tendrá dos partes diferenciadas:</p> <p>PARTE 1. Tecnología existente y propiedad del contratista. La Policía Nacional para esta parte no requerirá propiedad intelectual pero SÍ podrá disponer del código fuente, para ser custodiada cumpliendo los términos de licencia del contratista. Es decir, el contratista deberá entregar para custodia el código fuente de toda su tecnología.</p> <p>PARTE 2. Tecnología co-desarrollada. Relativa a la parte de integración de fuentes abiertas colombianas solicitadas por la Policía Nacional así como las fuentes cerradas descritas anteriormente.</p>		
1.12	<p>El contratista deberá garantizar la configuración de un respaldo o copia de la información almacenada en la base de datos que evite una</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	pérdida definitiva e irrecuperable de la información en caso de una eventualidad.		
1.13	El Sistema debe incluir base de datos orientada a grafos, lo que permite la interconexión de los datos obtenidos y la correlación entre diferentes fuentes de datos estructurados y no estructurados de forma eficiente.		
1.14	Es obligación del contratista realizar todos los diseños físicos y lógicos, así mismo disponer de los elementos donde operará el Sistema, para ello debe presentar los diseños para ser aprobados por el supervisor del contrato.		
1.15	La interfaz de la plataforma debe estar en español para su operación y el sistema debe ser multilenguaje, incluyendo como mínimo el "inglés" y pudiendo incorporar otros idiomas como el árabe, mandarín, ruso y portugués.		
1.16	La plataforma debe permitir la traducción de los contenidos recolectados y analizados en los idiomas que establece el numeral 1.13. El contratista debe indicar de que otros idiomas dispone la plataforma para la recolección, análisis y traducción de la información.		
1.17	La aplicación debe identificar y señalar visualmente, de forma automática, entidades como: nombre de entidades, lugares, direcciones; a partir de textos recopilados por la herramienta de búsqueda OSINT(información pública disponible)		
1.18	El contratista debe configurar en caso de ser necesario los componentes de procesamiento y almacenamiento requeridos para la correcta operación de la plataforma durante el tiempo de soporte y garantía.		
1.19	Todos los equipos deben ser nuevos y deben quedar instalados, configurados, programados y operando correctamente.		
1.20	<p>En caso de realizar una fase de desarrollo a la medida para cumplir a totalidad las condiciones técnicas del presente pliego, se deberá realizar levantamiento de información, describiendo la arquitectura del sistema de información propuesta como:</p> <ul style="list-style-type: none"> • Casos de uso. • Planeación de la implementación. • Vista lógica. • Vista de datos. • Vista de despliegue. • Vista de integración con sistema de información externos. <p>El desarrollo que se realice debe ser de uso exclusivo de la Policía Nacional de Colombia, y no con fines de comercialización ni de lucro con otros países y/u organizaciones públicas o privadas</p> <p>Además todas las actividades de desarrollo deberán realizarse in-house, dentro de las instalaciones de DIPOL.</p>		
1.21	<p>El oferente deberá documentar y entregar las siguientes fases para la ejecución del objeto del presente proceso:</p> <p>GESTIÓN Y PLANEACIÓN DEL PROYECTO:</p> <ul style="list-style-type: none"> • Inicio, estructuración y gestión del proyecto: describir visión y alcance, identificar y comprender el contexto organizacional y objetivos estratégicos del proyecto, identificar actores del sistema (usuarios con perspectiva), esbozar la operación deseada, analizar factibilidad, definir integrantes, roles y responsabilidades 		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>del equipo de proyecto, estimar recursos, costos y tiempo de desarrollo, identificación preliminar y gestión proactiva de riesgos.</p> <ul style="list-style-type: none"> • Aseguramiento de calidad: proveerá una visión clara de cómo se garantizará y logrará la calidad del sistema de información, los entregables y el proceso. Contendrá el plan de revisión, pruebas y aseguramiento de calidad para cada una de las fases o flujos de trabajo. • Especificación de requerimientos del sistema y análisis: comprende el contexto, reglas de negocio y procesos de la organización donde apoyará el sistema de información y especificar los requerimientos funcionales y técnicos (atributos de calidad técnica) del sistema de información. La principal tarea consiste en la generación de especificaciones correctas que describan con claridad, sin ambigüedades, en forma consistente y concreta, las necesidades de los usuarios internos y externos del sistema de información. Se enfoca en un objetivo fundamental. La definición de lo que se desea producir a través de especificaciones finales completas, formales y acordadas entre las partes, comprende el levantamiento de información. <p>DISEÑO:</p> <ul style="list-style-type: none"> • Diseño y Arquitectura de Software: la definición de la arquitectura del sistema (vista estructural del sistema) y del entorno tecnológico (software, hardware, comunicaciones, seguridad), la especificación detallada de los componentes del sistema de información. A partir de dicha definición, se generan todas las especificaciones de construcción relativas al propio sistema y al software, así como la descripción técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial de datos (éstos últimos cuando proceda). Comprende diseño funcional, diseño técnico, arquitectura del sistema de información. • Modelo de Casos de Uso del Sistema: Permitirá modelar, visualizar y documentar la funcionalidad y el ambiente deseados en el sistema de solución. A través del modelo se especificará la secuencia de acciones que el sistema de información o software debe ejecutar, y que permite entregar un resultado de valor para un actor (usuario del sistema) en particular. La notación para la elaboración del Diagrama de Casos de Uso será la definida por UML – Unified Modeling Language o similares herramientas de modelación de flujos, se deberá elaborar: diagrama de flujo de datos, diagrama entidad relación, diccionario de datos. • El oferente pasará a la fase de Construcción y Pruebas una vez la Policía Nacional valide y apruebe toda la fase de Gestión, Planeación y Diseño del Proyecto a través de los formatos establecidos por la Policía Nacional o del oferente. <p>CONSTRUCCIÓN Y PRUEBAS:</p> <ul style="list-style-type: none"> • Construcción, pruebas y aceptación: Culminar la construcción del producto de software, aplicar pruebas funcionales y técnicas (atributos de calidad) para verificar su correcto comportamiento, aplicar protocolos de aprobación, aceptación y puesta en operación del software construido, El propósito del plan de 		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>pruebas es explicitar el alcance, enfoque, recursos requeridos, cronograma y calendario, responsables y manejo de riesgos de un proceso de pruebas, verificación, validación y certificación y deberá garantizar y asegurar que el sistema cumpla con los requerimientos funcionales y desempeño; así como, con los estándares (diseño, construcción documentación) y facilidad de mantenimiento.</p> <p>IMPLANTACIÓN:</p> <ul style="list-style-type: none"> • Implantación y puesta en operación: instalación, Distribución y Puesta en Producción del sistema software. • Capacitación: llevar a cabo la transferencia de conocimiento del sistema de información a la comunidad de usuarios. • CIERRE DEL PROYECTO. 		
2.	ITEM 1: PLATAFORMA PARA WEBINT-OSINT-DEEPWEB		
2.1	Herramienta de búsquedas en fuente abierta que permita administrar usuarios, realizar búsquedas específicas, búsquedas compuestas, generar alertas, crear casos y búsquedas por temáticas, y que a su vez esta búsqueda permita correlacionar lo eventos anteriormente consultados y emplear diferentes tipos de filtros como por ejemplo tiempo, ubicación, temática, palabras clave, a partir de la información pública disponible.		
2.2	<p>El Sistema debe permitir al analista definir cualquier tema y monitorear dinámicamente la actividad de las redes sociales y de mensajería instantánea que cuentan con links públicos como Facebook, Telegram, Twitter, Instagram. La plataforma podrá incorporar otras fuentes gracias a su modularidad.</p> <p>De igual manera, debe dar solución a los siguientes requerimientos:</p> <ul style="list-style-type: none"> - Información relevante sobre una publicación, hashtag, comentario, imagen o video que haya sido publicada en alguna red social, así: <ul style="list-style-type: none"> ○ Primera cuenta en haber generado la publicación. ○ Impacto y reacciones de la publicación. ○ Listado de las cuentas que mayor interacción y dinamización han generado. ○ Geolocalización de las cuentas en función de la información OSINT de las fuentes. ○ Cuentas más influenciadoras (que generen más impacto debido a su cantidad de seguidores). ○ Debe permitir hacer filtros por palabras clave de los comentarios generados. <p>Dicha información deberá ser mostrada de una forma intuitiva, gráfica y amigable para el operador de tal manera que:</p> <ul style="list-style-type: none"> - El operador pueda personalizar de forma visual y dinámica el dashboard de la operación. - Que pueda compartir ese dashboard con otros analistas o para otras operaciones o fuentes de información. - Que el dashboard sea dinámico e interactivo, logrando filtrar o personalizar la vista haciendo click en cualquiera de sus elementos. <p>Con la posibilidad de generar alertas sobre publicaciones, hashtag, identidades y sobre patrones de comportamiento que el analista pueda crear para caracterizar fenómenos o tipos de entidades dentro de la información pública disponible colectada.</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS		CUMPLE	NO CUMPLE
2.3	Usuarios concurrentes mínimos	300 usuarios para búsquedas de entidades y 30 usuarios de sistema completo		
2.4	Creación de usuarios	Ilimitados		
2.5	Creación de casos	Ilimitados		
2.6	Consultas por usuario	Ilimitados- usuarios concurrentes 300		
2.7	El sistema no debe tener limitaciones en la cantidad de fenómenos monitoreados y poder monitorear simultáneamente los casos.			
2.8	Integración de fuentes no estructuradas (Excel, Word, PDF, PowerPoint, CSV, JPG, VGA, Multimedia y demás formatos que se requieran).			
2.9	Extracción de datos de fuentes HTML públicas.			
2.10	El sistema deberá permitir y suministrar tecnología de simulación de acciones y actividades humanas, actividades aleatorizadas, creación de bots durante la fase de obtención o colección de las fuentes abiertas.			
2.11	El sistema debe de ser escalable e interoperable con otros software en y/o aplicaciones en el entendido que no existan conflicto de licencias o protocolos internos de seguridad y exclusividad.			
2.12	<p>Debe contener como mínimo los siguientes módulos:</p> <p>Módulo Consulta de entidad: búsqueda y recolección de información relacionada con eventos y entidades.</p> <p>Módulo Administración y Gestión: gestión de perfiles de usuario, contenido y seguridad del sistema.</p> <p>Módulo Análisis de relaciones: este módulo debe mapear de las redes sociales los tipos de entidades disponibles en las mismas, como amigos, seguidores, interacciones, ubicaciones, organizaciones, y así mismo generar filtros para los datos extraídos.</p> <p>Creación y gestión de casos: con este se administrará la búsqueda relacionada con casos puntuales.</p> <p>Módulo de alertas: el contratista deberá garantizar que la plataforma permita configurar búsquedas teniendo en cuenta temáticas, períodos de tiempo, palabras clave, datos, entidades, así como la generación de alertas basada en palabras clave, fechas y tareas programadas. Así mismo, deberá generar una alerta en el evento que dos o más usuarios del sistema concurrentes estén consultando o hayan consultado el mismo dato.</p> <p>Módulo de agentes: administración y gestión de cuentas de navegación.</p> <p>Módulo de informes y reportes: el analista podrá configurar de forma dinámica el dashboard de explotación de la información para generar los informes de manera personalizada.</p> <p>Módulo de georreferenciación: integración con capacidades de GIS (información geográfica), sincronización en tiempo real con la visualización de cartografía en vivo, así como visualización de eventos, actividades y datos en el mapa.</p>			
2.13	El sistema debe contar con procesamiento del lenguaje natural (Natural Language Processing), el cual debe aprender de acuerdo al idioma que se habla y la ontología propia administrada.			

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
2.14	La visualización de la plataforma debe ser amigable de forma tal, que su visualización sea en lenguaje natural (no en lenguaje de código); con el fin que el usuario final pueda entenderla fácilmente.		
2.15 g	Debe contener un diseño gráfico amigable, interactivo, liviano y con imagen institucional (Policía Nacional), para lo cual el contratista debe presentar como mínimo 3 propuestas para que el supervisor del contrato realice la elección en cuanto a personalización de colores además de que la plataforma debe poder ser configurada de forma dinámica por el analista para elegir cómo desea ver representada la explotación de la información de cada operación.		
2.16	El contratista entregará un cronograma de pruebas necesarias para lograr la aprobación técnica y funcional del sistema a implementar.		
2.17	<p>Debe tener como mínimo los siguientes motores de recolección de datos para:</p> <ul style="list-style-type: none"> - Páginas web estáticas. - Motores de recolección basados en RSS. - Motores basados en navegadores. - Motores basados en API de sitios web. - Motores basados en API de flujos. <p>Se dará un listado inicial de 5 fuentes de información pública expuesta a internet para integrar mediante el desarrollo de una API o el método más apropiado para cada una de ellas e integración en la plataforma. Estas fuentes se podrán ir ampliando de acuerdo la necesidad dentro de periodo de implementación.</p> <p>En caso de contar con Motores de búsqueda para aplicaciones móviles, debe integrarlo a la solución.</p>		
2.17.1	El sistema deberá permitir la creación independiente de algoritmos / rastreadores (crawlers) que automaticen la navegación web humana.		
2.17.2	Los nuevos crawlers deben cargarse fácilmente en el sistema tras la creación, sin necesidad de reiniciar el sistema.		
2.17.3	El crawler deberá ejecutar un script personalizado durante su ejecución, que incluye: Una entrada y salida predefinidas.		
2.17.4	El operador debe poder usar algoritmos personalizados, independientemente de su método de búsqueda.		
2.17.5	El operador debería ser capaz de crear crawlers personalizados que recopilen información las fuentes definidas para el sistema incluidas TOR y Darknet.		
2.17.6	El sistema debe admitir la recolección del contenido publicado por la entidad de las Redes Sociales, los detalles biográficos y las interacciones sociales (likes, shares, comments, friends) cuando estén disponibles públicamente.		
2.17.7	El sistema debe admitir la recolección de los amigos y/o seguidores de la entidad en redes sociales, mediante la aplicación de flujos de derivación, cuando estén disponibles públicamente. Además, deberá permitir recolectar la información de entidades en segundo nivel si la estructura y relaciones está bajo naturaleza OSINT.		
2.17.8	El sistema debe admitir la recolección de información pública de un		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	grupo, incluidos: miembros, información, publicaciones, interacciones, comentarios y recursos compartidos.		
2.17.9	El sistema debe permitir el acceso a grupos de Facebook utilizando cuentas de navegación del sistema dedicados, que ingresarán al grupo y recopilarán la información pública.		
2.17.10	El sistema debe permitir el acceso a los canales públicos de Telegram y otras aplicaciones de mensajería instantánea, utilizando cuentas de navegación del sistema dedicados, que ingresarán al canal y recopilarán la información.		
2.17.11	El sistema debe admitir como elemento de escalabilidad la futura creación de crawlers, que extraigan datos de cualquier fuente web pública navegable, incluidos foros, blogs, redes sociales, además de los ya incorporados como alcance del proyecto.		
2.17.12	El diseñador del crawler debe permitir al operador solicitar una captura de pantalla de un elemento específico en la página web o de toda la página web.		
2.17.13	El sistema debería permitir al administrador, cargar automáticamente un número ilimitado de cuentas de navegación al sistema desde un archivo CSV.		
2.17.14	El sistema debe proporcionar una extensión de navegador que permita al usuario navegar usando la identidad de la cuenta de navegación de manera consistente a su huella digital. Adicionalmente, el sistema deberá evaluar el nivel de credibilidad y operatividad de la cuenta de navegación y mostrarlo de forma gráfica, con el fin de que se logre la credibilidad máxima del mismo y su salida a operación o proporcionar salida de cuentas de navegación a internet para la verificación de la información a consultar.		
2.17.15	El sistema debe implementar solución tecnológica que permita reducir el riesgo de suspensión de cuenta y bloqueo de la cuenta de navegación.		
2.17.16	El sistema debe implementar un mecanismo de simulación humana.		
2.17.17	El sistema debe tener un mecanismo de retención de cookies para aumentar la credibilidad de identidad de la cuenta de navegación.		
2.17.18	El operador podrá establecer definiciones de recolección programadas para que se ejecuten en intervalos fijos, estableciendo sus parámetros de programación.		
2.17.19	El operador elegirá una cuenta de navegación específica entre una lista de cuentas registradas, cuando el rastreador (crawler) requiera inicio de sesión o autenticación de API.		
2.18	Las búsquedas podrán realizarse de manera textual, simple o avanzada: soportando operadores boléanos (selección múltiple, operadores como AND/OR/EXCLUDE), comodines, búsqueda semántica. Además, esta opción avanzada de filtros podrá ser realizada en un entorno gráfico y visual, en tiempo real, sobre toda la información mostrada al operador.		
2.19	El sistema debe permitir, ingresar y actualizar la ontología propia identificada.		
2.20	<p>PUNTOS DESTACADOS:</p> <p>Admisión de múltiples unidades distribuidas de búsqueda (cuenta de navegación, bot) trabajando simultáneamente.</p> <p>Compatibilidad las Darknets (específicamente Tor, Ip2P y Freenet).</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>Navegador web incorporado, que permita extracción sencilla del contenido.</p> <p>Tener una función para que las cuentas de navegación tengan un ambiente propio que minimice los riesgos en caso de recibir un ataque cibernético.</p> <p>Paquete incorporado de flujos que soporte la mayor cantidad de redes sociales, blogs y plataformas de debates.</p>		
2.21	Módulo Consulta de entidad:		
2.21.1	<p>Debe permitir la búsqueda por entidad con los siguientes parámetros, en fuentes públicas:</p> <ul style="list-style-type: none"> Nombres y apellidos. Número de identificación. Pasaporte. Nick name en redes sociales. Dirección, ubicación y/o lugar. <p>Debe permitir la búsqueda por organización con los siguientes parámetros, en fuentes públicas:</p> <ul style="list-style-type: none"> Nombre organización. Página web. Número de Identificación Tributaria (NIT). Nick name en redes sociales. Dirección, ubicación y/o lugar. <p>La información recolectada deberá estar en un formato editable y permitir su actualización automática a solicitud del operador.</p>		
2.21.2	<p>El resultado de la búsqueda de fuente pública disponible debe arrojar de manera organizada los siguientes datos:</p> <ol style="list-style-type: none"> 1. Nombres de usuario (como está registrado o guardado en las diferentes redes sociales y demás plataformas). 2. Id o identificador de usuario en redes sociales. 3. Imágenes relacionadas con la cuenta, principalmente imágenes de la entidad o etiqueta. 4. Entidades asociadas a la búsqueda. 5. Cuentas en redes sociales sobre las fuentes incorporadas. (por ejemplo, Facebook, Instagram, Twitter) 6. Páginas web relacionadas. 7. Fecha de nacimiento. 8. Ubicación, incluida la actividad de itinerancia. 9. Datos en la Darknet. 10. Organizaciones (lugares de trabajo, educación, relaciones comerciales, entre otros). 11. Ubicaciones y direcciones. 12. Entidades relacionadas, verificación de metadatos: <ul style="list-style-type: none"> 12.1 Fecha cuando se agregó. 12.2 Última actualización. 12.3 Modificado por. 12.4 Creado por. 		
2.21.3	Debe desplegar en una ventana ya sea en la parte inferior o a la izquierda o abrir los sitios web, documentos, o cualquier otra fuente de información asociada.		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
2.21.4	<p>La búsqueda por organización, en caso de encontrar una página web, deberá traer los datos del administrador de la misma, disponibles públicamente:</p> <ol style="list-style-type: none"> 1. IP de página. 2. Dominio. 3. Nombre del administrador. 4. Dirección. 5. Correo. 6. Información general. 7. Ubicación. 		
2.22	Módulo Administración y Gestión:		
2.22.1	<p>Gestión de perfiles de usuario del sistema:</p> <ol style="list-style-type: none"> 1. Creación y eliminación de usuario. 2. Creación de roles. 3. Permisos de usuario. 4. Verificación de actividades realizadas 5. Bloqueo de usuario. 		
2.22.2	<p>Seguridad</p> <ol style="list-style-type: none"> 1. Generación de auditoría sobre actividades del usuario en la plataforma. 2. Asignación de módulos y permisos sobre fuentes de información. 3. Clasificación de usuarios por perfil. 		
2.22.3	<p>Contenido</p> <ol style="list-style-type: none"> 1. Fuentes integradas. 2. Diseño de crawlers. 3. Seguimiento casos. 		
2.23	Módulo Análisis de casos y relaciones:		
2.23.1	<p>ANÁLISIS:</p> <p>La pantalla “anализar” deberá ser modular y controlable fácilmente mediante acciones de arrastrar y soltar en pantalla. Esto permitirá a los usuarios centrarse en los elementos deseados en la pantalla, y contendrá las siguientes capacidades:</p> <ul style="list-style-type: none"> • Permitir a los usuarios inspeccionar cada resultado: verlo de forma completa e individual, incluidos los detalles del contenido y los medios archivos adjuntos. • Permitir a los usuarios buscar, recopilar, visualizar y analizar microblogging pública sobre un mapa interactivo basado en sus metadatos geoetiquetados. • Presentación de mapa de calor. Partes del mapa con un mayor grupo de elementos se destacan con mayor intensidad. • Mostrar en una gráfica los hashtags más mencionados en los resultados, los hashtags más relacionados debido a su nivel de menciones compartidas; de igual forma deberá permitir la visualización y análisis de picos de tendencia en líneas de tiempo. • Análisis de sentimiento: Detectar el sentimiento expresado en publicaciones sociales no estructuradas, en idiomas compatibles, y permite a los usuarios filtrar los resultados para mostrar solo contenido positivo, negativo o neutral. • Ubicación de publicación en un gráfico de mapa, visualizando el número de publicaciones geo etiquetadas por país y estado. 		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<ul style="list-style-type: none"> Identificar Influenciadores: Detectar quiénes son los influyentes en la interacción. Se mostrará una lista de los usuarios más influyentes. Detección de bots: Determina si una cuenta de red social es real o falsa. Si una cuenta es clasificada como falsa, el sistema enumera los motivos de esa clasificación, ejemplo: horarios, tiempos de interacción, fecha de uso, temporalidad, correlación con otras redes. 		
2.23.2	Este módulo debe extraer y mapear las redes sociales (entidades) y generar filtros.		
2.23.3	Determinación de relaciones más fuertes.		
2.23.4	Entorno social.		
2.23.5	Relaciones más cercanas.		
2.23.6	Aplicación de filtros.		
2.23.7	Generación de líneas de tiempo de la información.		
2.23.8	Seleccionar eventos, mensajes o entidades para correlacionar y graficar cronológicamente las relaciones fuertes.		
2.23.9	<p>Debe permitir monitorear actividades, tendencias y patrones de comportamiento de multitudes en el espacio digital.</p> <p>Así mismo, permite la graficación utilizando líneas de tiempo donde se evidencie las interacciones y la utilización de filtros.</p>		
2.24	Módulo de alertas:		
2.24.1	Generación de alertas basados en palabras clave, fechas, y tareas programadas.		
2.24.2	Programar recolección de acuerdo a la programación de búsquedas por palabras.		
2.24.3	Alertas basadas en la búsqueda.		
2.24.4	Alertas por duplicidad de consultas.		
2.25	Módulo de agentes: Administración y gestión de cuentas de navegación.		
2.25.1	La técnica empleada debe ser mediante la creación de entidades o algoritmos de recolección automáticamente.		
2.25.2	Usar las cuentas de navegación ya existentes con las reglas de seguridad y emulación de ubicación.		
2.25.3	Se podrán automatizar, controlar y ejecutar algoritmos. La plataforma analiza los datos colectados utilizando las herramientas y algoritmos analíticos avanzados.		
2.25.4	Poner en cuarentena las cuentas de navegación y bots.		
2.25.5	Realizar hoja de vida de cada entidad, cuenta de navegación y bot, que contenga como mínimo fecha de creación tipo de contenido publicado.		
2.26	Módulo de georreferenciación:		
2.26.1	Capacidades de GIS (Sistema de Información Geográfica), sincronización en tiempo real con la visualización del mapa en vivo, vista de eventos, actividades y otros datos en el mapa.		
2.26.2	Puede usar la capacidad de ARGIS y ESRI de la Policía Nacional o garantizar que se tenga actualizada la cartografía.		
2.26.3	Graficar ubicaciones de publicaciones, contenidas en la descripción de la entidad y las relacionadas en los comentarios.		
2.27	Módulo de informes y reportes: como mínimo debe permitir la generación de 5 tipos de reportes o que el propio operador pueda		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	diseñar el dashboard para decidir qué incluye en cada reporte de la operación.		
2.27.1	Los reportes deben permitir exportar en Excel, Word y Pdf.		
2.27.2	Debe existir la opción de escoger los campos que se van a visualizar en el reporte.		
2.27.3	Los reportes deben tener una vista de previsualización.		
2.28	TRANSFERENCIA DE CONOCIMIENTOS		
2.28.1	Con el fin de garantizar el funcionamiento, mantenimiento y adicionar desarrollo al Sistema de Inteligencia Artificial, es necesaria la instrucción de mínimo 41 funcionarios del servicio, los cuales deberán tener conocimientos sobre el manejo, gestión y administración del sistema IA, como se describe en el ítem 2.28.2. Esta transferencia de conocimiento deberá ser certificada por el fabricante. Deberá contener al menos temáticas de: 1) Bigdata. 2) Machine Learning. 3) IA. 4) Métodos de representación gráfica y relaciones de metainformación.		
2.28.2	<p>La transferencia de conocimiento se debe desarrollar en tres (3) grupos, así:</p> <p>Usuario final - recolector: deberá capacitarse a las personas designadas por la Policía Nacional (mínimo 30 funcionarios) en el uso de plataforma con todas sus bondades, Tiempo mínimo para la transferencia de conocimiento, 80 horas.</p> <p>Administradores del sistema: dirigida como mínimo a 6 personas quienes tendrán la capacidad de gestionar y administrar servidores, conexiones y la infraestructura de TI (Tecnologías de la información) dispuesta para la plataforma (servidores, switch, firewall). Tiempo mínimo para la transferencia de conocimiento, 80 horas.</p> <p>Entrenador de entrenadores: un módulo de entrenador de entrenadores para 5 personas como mínimo, con el material (videos, ayudas interactivas) los cuales deben quedar con la capacidad de administración del sistemas y uso. Tiempo mínimo para la transferencia de conocimiento, 80 horas.</p>		
2.28.3	La accesibilidad de la información del sistema y los servidores deberán ser de acceso exclusivo de los funcionarios de la Dirección de Inteligencia Policial. Cualquier herramienta de telemetría y monitoreo del software deberá ser completamente deshabilitada al exterior de DIPOL.		
3.	ITEM 2: INFRAESTRUCTURA		
3.1	Los equipos de infraestructura deben ser entregados, instalados y configurados por el contratista.		
3.2	GARANTÍA EQUIPOS		
3.2.1	Garantía mínima: tres (03) años para todos los ítems, contada a partir de la fecha del acta de recibo a satisfacción por parte del supervisor del contrato.		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
3.2.2	El oferente debe anexar certificación que indique que los equipos ofrecidos (servidores, switch y firewall con sus componentes) son de un fabricante con representación en Colombia.		
3.2.3	El oferente debe anexar certificación de distribuidor autorizado en Colombia del fabricante.		
3.2.4	El oferente debe anexar manifestación escrita sobre el tipo de garantía, soporte técnico y garantizar el suministro de repuestos del hardware que compone los servidores, switch y demás componentes por un tiempo no menor a cinco (05) años.		
3.2.5	Los servidores deben cumplir como mínimo con certificación EPEAT nivel Bronze, será verificable en la página web EPEAT.		
3.2.6	Los servidores deben cumplir con certificación Energy Star. En los servidores se debe identificar la certificación Energy Star, a través de sticker de identificación pegado en el equipo.		
3.2.7	<p>La garantía ofrecida por el fabricante deberá tener un control y seguimiento de los tickets generados para los mantenimientos correctivos donde se escale a los niveles adecuados para su solución y cierre.</p> <p>El contratista deberá entregar un usuario que permita acceder al sistema de información que soporta la mesa de ayuda o autoservicio (acceso vía web), con el objeto de realizar seguimiento a los casos reportados y tickets generados. El funcionario policial será asignado por el supervisor del contrato.</p> <p>Además, se deberán presentar informes mensuales al supervisor del contrato de los casos reportados a la mesa de servicio del contratista y el estado en que se encuentran.</p>		
3.3	RESTAURACIÓN DE LA MÁQUINA		
3.3.1	<p>El contratista deberá garantizar el soporte para la recuperación de datos, o para la restauración de la máquina a su estado original de fábrica.</p> <p>El contratista deberá entregar un video tutorial que sirva como guía y se evidencie, el paso a paso para realizar la restauración de la máquina a su estado original de fábrica.</p>		
3.4	LICENCIAS Y ACCESORIOS		
3.4.1	<p>SISTEMA OPERATIVO Considerando el sistema operativo a implementar para la solución (Windows o Linux), se deberá entregar el siguiente licenciamiento de acuerdo al sistema operativo a implementar así:</p> <p>Windows: Licenciamiento para los servidores Windows SERVER 2019 64 bits última versión en español para ambiente corporativo; los equipos a entregar deberán tener instalado y funcionando el sistema operativo.</p> <p>Ó</p> <p>Linux: Licenciamiento para los servidores LINUX UBUNTU 18.04 LTS última versión en español para ambiente corporativo; los equipos a entregar deberán tener instalado y funcionando el sistema operativo.</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS		CUMPLE	NO CUMPLE
	Durante el tiempo de la garantía el contratista debe prestar todo el acompañamiento necesario para realizar las actualizaciones de los equipos, cuando se instalen nuevas versiones.			
3.4.2	Considerando que la arquitectura de TI debe ser flexible y deben virtualizarse o crearse servidores virtuales, el contratista debe entregar las licencias necesarias de plataforma usada para la virtualización ya sea VMware vSphere Essentials Plus o Microsoft Hyper-v. o la empleada en el desarrollo de la arquitectura.			
3.4.3	Considerando que la arquitectura de TI debe ser segura y contar con los protocolos de seguridad se debe entregar instalado y funcionando el antivirus para los servidores con Windows Antivirus for servers Microsoft Security Essentials ó el más indicado para la protección de los equipos y el sistema.			
3.5	PATCH CORD			
3.5.1	Suministro Patch Cord categoría 6A de fábrica, UL listado y CSA.			
3.6	SERVIDOR DE APLICACIÓN			
3.6.1	Cantidad.	Tres (03).		
3.6.2	Marca.	Especificar.		
3.6.3	Modelo.	Especificar.		
3.6.4	Tipo.	Rack.		
3.6.5	Año de fabricación.	Mínimo 2019 última versión (todos los componentes del presente ítem).		
3.6.6	Software.	Los nodos deben ser con procesadores certificados para alta disponibilidad misión-critica, Debe incluir herramienta de virtualización, de gestión de almacenamiento y de administración de la solución		
3.6.7	Fuente de poder	Dos fuentes de poder como mínimo.		
3.6.8	PROCESADOR			
3.6.8.1	Cantidad de procesadores mínima por nodo.	2 procesadores como mínimo.		
3.6.8.2	Tipo procesador mínimo.	Especificar.		
3.6.8.3	Cantidad de núcleos por procesador mínimo.	16 núcleos.		
3.6.8.4	Frecuencia base mínima.	2.1 Ghz.		
3.6.8.5	Memoria caché mínimo.	22 MB.		
3.6.9	MEMORIA RAM POR NODO			
3.6.9.1	Capacidad mínima:	8 DIMM cada uno de 32GB, Total Memoria RAM 256GB.		
3.6.9.2	Tipo	DDR4-2666 o equivalente		
3.6.10	ALMACENAMIENTO POR CADA NODO			
3.6.10.1	SSD mínimo por nodo.	4 SSD de 3.8TB.		
3.6.10.2	Bahías de expansión.	Capacidad mínima de 24 bahías hot-swap		

NUMERAL	CARACTERÍSTICAS TÉCNICAS		CUMPLE	NO CUMPLE
3.6.10.3	Capacidad	20 TB o superior configurados después de RAID 5 conformado por unidades de estado sólido intercambiables en caliente; este espacio debe estar disponible y no debe hacer parte del disco que se designe para que corra el sistema operativo.		
3.6.10.4	Redundancia.	El equipo ofertado debe permitir configuración correspondiente a las unidades de estado sólido en mínimo RAID 0,1,5,6,10		
3.6.11 CONECTIVIDAD				
3.6.11.1	Puertos mínimos por nodo.	Dos tarjetas de red 10Gbe para conexión a la red LAN, UN (1) 1Gbe para administración.		
3.7 FIREWALL				
3.7.1	Marca	Especificar		
3.7.2	Referencia	Especificar		
3.7.3	Cantidad	Uno (01)		
3.7.4	Puertos GE RJ45	8 a 16		
3.7.5	Puertos USB	Mínimo 2		
3.7.6	Puerto consola RJ45	1		
3.7.7	Rendimiento mínimo del FIREWALL (IPS THROUGHTPUT)	10 Gbps		
3.7.8	Sesiones concurrentes mínimas (TCP):	8 Millones		
3.7.9	Políticas de FIREWALL Mínimo	10.000		
3.7.10	Túneles VPN IPSec de puerta de enlace a puerta de enlace:	2.000		
3.7.11	Túneles VPN Cliente-a-Puerta enlace Ipsec	50.000		
3.7.12	Usuarios concurrentes SSL-VPN (Máximo recomendado)	10.000		
3.7.13	Rendimiento IPS	8 Gbps		
3.7.14	Rendimiento de la inspección SSL	SI		
3.7.15	Certificaciones	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6		
3.7.16	Factor de forma Rack	Rack Mount, 1 RU		
3.7.17	Corriente máxima	6A @ 100V; fuente de alimentación 100–240V 50–60Hz		
3.7.18	Consumo de energía (promedio / máximo):	129 W / 244 W		
3.7.19	Disipación de calor:	832 BTU/h		
3.7.20	Temperatura de funcionamiento	32–104°F (0–40°C)		
3.7.21	Humedad	10% - 90% sin condensación.		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
3.8	CONECTIVIDAD		
3.8.1	Considerando las actividades de uso del internet, se debe suministrar un canal de internet dedicado, independiente a los canales existentes en la Policía Nacional, con una capacidad de navegación de mínimo 100 MB, por un término de 3 años. En caso de cambio de operador el contratista deberá garantizar el servicio sin ninguna clase de interrupción en la conectividad. Así mismo se debe garantizar en los acuerdos de nivel de servicio que los tiempos de indisponibilidad no superen las 12 horas, y se atiendan los incidentes de conexión con mesa de ayuda 5x8		
3.8.2	Puertos mínimos por nodo.	Dos tarjetas de red de 10Gbe para conexión a la red LAN, UN (1) 1Gbe para administración.	
3.9	SWITCH		
3.9.1	Marca	Especificar	
3.9.2	Modelo	Especificar	
3.9.3	Cantidad	Uno (01)	
3.9.4	CARACTERÍSTICAS		
3.9.4.1	Tipo:	Administrable	
3.9.4.2	Administración:	Capa 3	
3.9.4.3	Calidad de servicio (QoS) soporte:	Si	
3.9.4.4	Energía sobre Ethernet (PoE)	Si	
3.9.4.5	Capacidad de apilamiento:	(04) Cuatro unidades	
3.9.4.6	Compatibilidad:	con otras marcas del mercado	
3.9.4.7	Documentación y Accesorios:	Software de administración. Los necesarios para su instalación y funcionamiento	
3.9.4.8	QoS (Calidad de Servicio):	Mínimo 8 colas por puerto para control de tráfico y optimización de la red	
3.9.4.9	Puerto de consola:	Con cable de conexión, RJ45, Serial	
3.9.4.10	Capacidad de crecimiento mediante software y hardware		
3.9.4.11	Cantidad de puertos básicos de conmutación RJ-45 Ethernet:	Ptos 48, Tecnología de cableado ethernet de cobre: 10BASE-T,100BASE-T,1000BASE-T, 1GB BASE -T	
3.9.4.12	Cantidad de puertos SFP+ (10 Gbps):	mínimo 2	
3.9.4.13	IEEE 802.1Q (VLANs), 802.1X (Security), 802.3ab (Copper Gigabit), 802.3ad (Link Aggregation), 802.3ae (10G Ethernet) ó 802.3bz, 802.3i (10 baseT), 802.3u (fast Ethernet), 802.3x (Flow Control), 802.1p , 802.1w (RSTP) y 802.3z (Fiber Gigabit).		
3.9.4.14	Integración de red:	Se integra a la Red LAN, lo cual incluye medio de transmisión y conversores de medio.	
3.9.4.15	Soporte VLAN:	Si, mínimo 128.	
3.9.4.16	Fuentes de alimentación redundantes		
3.9.4.17	Memoria interna:	128 MB o superior	
3.9.4.18	Memoria Flash:	16 MB o superior	

NUMERAL	CARACTERÍSTICAS TÉCNICAS		CUMPLE	NO CUMPLE
3.9.4.19	Firmware actualizable:	Si		
3.9.5	GESTIÓN Y PROTOCOLOS			
3.9.5.1	SNMP, RMON, IEEE802.1D, SSL y/o SSH, QoS, IPv4, IPv6, Vlans, WEB, ACL			
3.9.5.2	Protocolos de red compatibles:	HTTP/HTTPS		
3.9.5.3	El protocolo de conexión entre el servidor y las estaciones de trabajo será ejecutado a través de conexión web.			
3.9.5.4	El equipo debe soportar Autenticación vía RADIUS, TACACS + que facilite el control del equipo y restrinja el acceso no autorizado de usuarios que puedan modificar la configuración del mismo.			
3.10	SWITCH			
3.10.1	Marca	Especificar		
3.10.2	Modelo	Especificar		
3.10.3	Cantidad	Dos (02)		
3.10.4	CARACTERÍSTICAS			
3.10.5	Tipo de interruptor:	Administrable		
3.10.6	Capa del interruptor:	Capa 3		
3.10.7	Calidad de servicio (QoS) soporte:	Si		
3.10.8	Energía sobre Ethernet (PoE)			
3.10.9	Capacidad de apilamiento:	(04) Cuatro unidades		
3.10.10	Compatibilidad:	con otras marcas del mercado		
3.10.11	Documentación y Accesorios:	Software de administración. Los necesarios para su instalación y funcionamiento		
3.10.12	QoS (Calidad de Servicio):	Mínimo 4 colas por puerto para control de tráfico y optimización de la red		
3.10.13	Puerto de consola:	Con cable de conexión, RJ45, Serial		
3.10.14	Capacidad de crecimiento mediante software y hardware			
3.10.15	Cantidad de puertos básicos de conmutación RJ-45 Ethernet:	Ptos 24, conectores RJ-45 para 10BASE-T/100BASE-T/1000BASE-T, 1GB BASE -T, con 4 ranuras Gigabit SFP compartidas		
3.10.16	Cantidad de puertos SFP+ (10 Gbps):	mínimo 2		
3.10.17	NORMAS	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3bz ó 802.3z , 802.3x control de flujo, 802.3ad LACP, 802.3af PoE, 802.1d protocolo de árbol de expansión (STP), 802.1Q/p VLAN, 802.1w STP rápida, 802.1s STP múltiple, 802.1X autenticación de acceso a puertos		

NUMERAL	CARACTERÍSTICAS TÉCNICAS		CUMPLE	NO CUMPLE
3.10.18	Integración de red:	Se integra a la Red LAN, lo cual incluye medio de transmisión y conversores de medio.		
3.10.19	Soporte VLAN:	Si, mínimo 128.		
3.10.20	Fuentes de alimentación redundantes	Puerto RPS ó similares para conexión a unidad de alimentación redundante		
3.10.21	Firmware actualizable:	Si		
3.10.22	GESTIÓN Y PROTOCOLOS			
3.10.23	Control de acceso	SNMP, RMON, IEEE802.1D, SSL y/o SSH, QoS, IPv4, IPv6, Vlans, WEB, ACL		
3.10.24	Protocolos de red compatibles:	HTTP/HTTPS		
3.10.25	El equipo debe soportar gestión vía.	<ul style="list-style-type: none"> • Traceroute • Gestión IP simple • Seguridad SSL para interfaz de usuario para Internet • SSH • RADIUS • Replicación de puertos • Actualización TFTP • Cliente de protocolo de configuración dinámica del servidor (DHCP) • Cliente Telnet (soporte seguro SSH) 		
3.11	CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR, Y LICENCIAMIENTOS PARA SOFTWARE A LA MEDIDA (esta cesión de derechos es para los desarrollos a la medida que resulten adicionales contemplados en la solución, haciendo claridad que la Policía Nacional no los usará con fines comerciales).			
3.11.1	Respecto al software a medida desarrollado, el contratista se obliga a transferir a título gratuito todos los derechos patrimoniales del objeto del contrato a través del documento anexo "CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR" y debe estar debidamente registrado ante la Dirección Nacional de Derechos de Autor Unidad Administrativa Especial del Ministerio del Interior y protocolizado ante notaria. (otorgar licencia a perpetuidad de todos los componentes físicos y lógicos que integren el sistema).			
3.11.2	El contratista debe registrar el presente contrato en la entidad competente para el Registro de Derecho de Autor y remitir el certificado de inscripción como requisito previo para la suscripción del acta de recibo final a satisfacción y para la realización del último contado de pago correspondiente para cada una de las soluciones desarrolladas y/o mantenimientos implementados.			
3.11.3	La licencia de funcionamiento será de cubrimiento nacional, ya que generalmente se accederá al sistema de información desde todas las regionales y centros zonales del país.			
3.11.4	Dada la diversidad de las soluciones que se implementarán, si en alguna de ellas se requiere la incorporación de software base adicional para la construcción o mantenimiento de las aplicaciones, estas deberán ser entregadas a la Policía Nacional, y serán propiedad del mismo a perpetuidad (en caso que aplique).			

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE																
3.11.5	El licenciamiento será a perpetuidad y el mantenimiento por espacio de tres (3) años, contado a partir de la entrega a satisfacción de la solución.																		
3.11.6	El licenciamiento de uso correspondiente será propiedad de la Policía Nacional.																		
3.11.7	El contratista debe anexar como documentos entregables al contrato, el Contrato de cesión de Derechos Patrimoniales de Autor y copia del contrato de cesión que se realizó entre los empleados contratados y la firma contratante donde se transfieren los derechos a la empresa.																		
3.11.8	Los trámites de firmas de notaria por registro de firma y huella de la cesión de derechos patrimoniales no deberán generar costo para la Policía Nacional, y dichos costos serán asumidos por el contratista.																		
3.12	RECEPCIÓN DE LOS BIENES																		
3.12.1	Los equipos serán entregados y probados uno a uno (Procedimientos básicos de encendido, cargue de sistema operativo, reconocimiento de dispositivos instalados, verificación de configuración, instalación de software).																		
3.12.2	<p>A todos los equipos que entregará el contratista se les realizará la prueba de recepción de los bienes para verificar el funcionamiento de los equipos (partes externas e internas).</p> <table border="1"> <thead> <tr> <th>PARÁMETRO</th><th>ACEPTACIÓN</th></tr> </thead> <tbody> <tr> <td>Revisión Física</td><td></td></tr> <tr> <td>Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios entregados: Equipo, Cable de alimentación, Manuales, sello de Energy star(Para servidores)</td><td></td></tr> <tr> <td>Verificación externa equipo: Sin rayones, roturas o elementos sueltos.</td><td></td></tr> <tr> <td>Encendido</td><td></td></tr> <tr> <td>Conexión alimentación AC – Encendido.</td><td></td></tr> <tr> <td>Componentes internos y externos.</td><td></td></tr> <tr> <td>Validación componentes internos Herramientas de Sistema.</td><td></td></tr> </tbody> </table> <p>NOVEDADES NO CONFORMES</p> <ul style="list-style-type: none"> • Verificar que los equipos de cómputos no presenten rayones, fragmentaciones, golpes o abolladuras. • Comprobar que todos los componentes estén colocados y conectados correctamente. • La carcasa que recubre la parte interna del equipo de cómputo no debe poseer tornillería. 	PARÁMETRO	ACEPTACIÓN	Revisión Física		Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios entregados: Equipo, Cable de alimentación, Manuales, sello de Energy star(Para servidores)		Verificación externa equipo: Sin rayones, roturas o elementos sueltos.		Encendido		Conexión alimentación AC – Encendido.		Componentes internos y externos.		Validación componentes internos Herramientas de Sistema.			
PARÁMETRO	ACEPTACIÓN																		
Revisión Física																			
Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios entregados: Equipo, Cable de alimentación, Manuales, sello de Energy star(Para servidores)																			
Verificación externa equipo: Sin rayones, roturas o elementos sueltos.																			
Encendido																			
Conexión alimentación AC – Encendido.																			
Componentes internos y externos.																			
Validación componentes internos Herramientas de Sistema.																			

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>Los equipos deben ser customizados de fábrica, y no pueden estar ensamblados de manera artesanal en su diseño y carcasa externa, como por ejemplo uniones de la parte externa con tornillería, cables, cintas, conexiones indebidas que afecten la instalación, funcionamiento y operacionalización del componente tecnológico por parte del usuario final.</p> <p>El contratista deberá tener todos los equipos de medición (hardware y software) necesarios que permitan verificar la capacidad de todos los componentes que conforman el equipo como por ejemplo: fuente, disco duro, memoria, entre otros.</p> <p>El contratista será el responsable de disponer del personal idóneo, en profesiones de Ingeniería de Sistemas y/o Eléctrica y/o Electrónica y/o Telecomunicaciones y/o técnico en sistemas y/o electrónicos, instalaciones físicas, logística, conexiones, transporte del personal técnico de la Policía Nacional designado por el supervisor de contrato a las instalaciones donde se realizará la prueba y todo lo necesario para realizar la prueba de recepción de los bienes. Los gastos que llegase a generarse con ocasión a las diferentes revisiones y pruebas correrán a cargo del contratista.</p> <p>Durante el periodo de la prueba de recepción de los bienes, el contratista deberá cumplir con el protocolo de seguridad de instalaciones y seguridad de la información de la Policía Nacional.</p>		
3.13	MANTENIMIENTO		
3.13.1	El contratista es responsable de realizar los mantenimientos correctivos a todos los equipos de cómputo del presente proceso.		
3.13.2	Es responsabilidad del contratista suministrar toda la logística necesaria para realizar los mantenimientos correctivos de los equipos.		
3.13.3	Cualquier actividad de mantenimiento correctivo o preventivo del sistema, deberá realizarse en las instalaciones de la Dirección de Inteligencia Policial, teniendo en cuenta y acogiéndose a las políticas de seguridad de la información establecidas en la Policía Nacional.		
3.13.4	LUGAR DE ENTREGA		
3.13.4.1	La entrega del hardware, software, licenciamiento de acuerdo con las especificaciones técnicas mínimas requeridas establecidas en el presente estudio previo; se realizará en el almacén de la Dirección de Inteligencia Policial y quedará instalado y funcionando en las mismas instalaciones de la Dirección de Inteligencia Policial.		
3.13.5	MANUALES		
3.13.5.1	<p>El contratista deberá entregar toda la documentación técnica de cada uno de los equipos, elementos y periféricos.</p> <p>El contratista deberá entregar los manuales técnicos y de usuario originales de fábrica para operación; con todos sus catálogos de partes, en idioma castellano y/o inglés, debidamente actualizados a la fecha de entrega y correspondiente certificado de suscripción de actualización.</p>		
3.13.6	GARANTÍA		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
3.13.6.1	Todo el hardware, software y los componentes de la solución deben tener un tiempo de garantía mínimo de tres (3) años, ofrecida por el contratista contado a partir del recibido a satisfacción por parte del supervisor del contrato.		
3.13.6.2	El tiempo de garantía iniciará a partir del recibo a satisfacción de los elementos por parte del supervisor del contrato, con los equipos instalados y funcionando.		
3.13.6.3	Durante el periodo de garantía, el proveedor deberá suministrar todos los repuestos de iguales o superiores características a los originales, sin costo alguno para la Policía Nacional – Dirección de Inteligencia Policial.		
3.13.6.4	Durante el periodo de garantía, el proveedor deberá instalar las actualizaciones de software o versiones que sean lanzadas en el mercado durante la vigencia de la garantía sin costo para la Policía Nacional – Dirección de Inteligencia Policial, así mismo las versiones de firmware con el fin de garantizar el correcto funcionamiento del equipo, previa coordinación con el supervisor del contrato.		
3.13.7	SOPORTE		
3.13.7.1	El contratista deberá poner a disposición de la Policía Nacional – Dirección de Inteligencia Policial, de manera permanente, los siguientes medios para el reporte de incidentes: <ul style="list-style-type: none"> • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico. • Número móvil celular de un contacto directo 		
3.13.7.2	El contratista debe garantizar soporte técnico vía telefónica e Internet, como primer nivel de atención.		
3.13.7.3	El grupo de soporte del contratista debe garantizar que el ticket del problema tenga un seguimiento adecuado, se maneje rápida y eficientemente, y se lleve a los niveles adecuados hasta su cierre. Además, se debe tener informado constantemente por escrito al supervisor del contrato o quien éste delegue, los progresos en la búsqueda de la solución.		
3.13.7.4	Al inicio del contrato se establecerá el procedimiento de solicitud de la garantía y soporte técnico, tanto para el hardware como para el software ofertado.		
3.13.7.5	Durante el tiempo de la garantía se debe prestar todo el acompañamiento necesario para realizar las actualizaciones de la solución, cuando se liberen nuevas versiones.		
3.13.7.6	Brindar planes de mantenimiento preventivo y correctivo durante la garantía para toda la solución ofertada.		
3.13.7.7	El contratista debe recomendar procedimientos operacionales que mitiguen los riesgos de fallas del sistema.		
3.13.7.8	Actualizar las versiones de software cuando sean liberadas durante el tiempo de garantía.		
3.13.7.9	Realizar mínimo una (1) visita anual de mantenimiento preventivo durante el período de la garantía que incluya la limpieza externa e interna y diagnóstico de los equipos y software adquiridos.		
3.13.7.10	Se debe entregar la documentación, usuarios, contraseñas de administración usadas durante las fases de implementación.		
3.13.7.11	Especificar los mecanismos de mantenimiento y actualización del software suministrado, los elementos que se cubren, el tiempo en que		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	se actualiza el software y el paquete que incluye la actualización durante el tiempo de garantía.		
3.13.7.12	El contratista debe garantizar que el soporte se preste con personal certificado y con experiencia en este tipo de soluciones.		
3.13.7.13	Debe garantizarse la corrección de defectos de funcionamiento.		
3.13.7.14	Existirá un mecanismo de contacto de urgencia 5x8 además del nivel de servicio ofrecido que deberá ser también 5x8, por parte del proveedor para el mantenimiento correctivo y soporte técnico.		
3.13.7.15	Durante el periodo de garantía, el proveedor se compromete a atender las llamadas de mantenimiento correctivo, en un tiempo máximo de dos (2) horas sobre el nivel de servicio contratado.		
3.13.7.16	Con el fin de contar con una capacidad de respuesta oportuna y eficiente en cuanto a soporte técnico y asesorías, las instalaciones principales de la empresa contratista, deberá estar ubicada dentro una zona horaria con una diferencia no mayor a 6 horas de la de Colombia (UTC); lo que comprendería las zonas horarias UTC +1, 0, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11.		
3.13.7.17	Durante el periodo de garantía, el proveedor se compromete a solucionar las fallas presentadas en el sistema dejándolo en perfecto estado de funcionamiento en un plazo máximo de 24 horas.		
3.13.7.18	En caso de que la reparación del equipo demore más de setenta y dos (72) horas, el proveedor deberá suministrar en forma inmediata un equipo de soporte de iguales o superiores características durante el tiempo que dure la reparación o reemplazo de la misma.		
3.13.7.19	INFORME MENSUAL		
3.13.7.20	<p>Durante los tres (3) años de garantía, el contratista mensualmente deberá entregar informe (físico y medio digital) al supervisor del contrato en el que se describa como mínimo los siguientes campos:</p> <ul style="list-style-type: none"> • El informe debe estar rotulado con el nombre y logo de la compañía. • Fecha. • Ciudad. • Centro de servicio. • Número de contrato. • Serie del equipo. • Modelo. • Número del reporte que genera Help Desk para la atención de los requerimientos. • Número total de equipos a los cuales se le realizó los correctivos. • Número de correcciones o incidentes con el software. • Tipo de falla. • Dispositivo o módulos del software que presentó la falla. • Número de fallas. • Describir el correctivo del componente tecnológico reparado, reemplazado. • Nombre del funcionario que reportó el incidente. <p>Nota: el modelo del informe debe ser presentado al supervisor del contrato para su aprobación, durante la apertura del acta de inicio.</p>		
3.14	ENTREGA SOLUCIÓN Y COMPONENTES		
3.14.1	A partir de la entrega total de la plataforma se empezará a contar la garantía del licenciamiento y garantías del hardware. El Contratista		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE				
	<p>debe entregar para el recibo a satisfacción de la plataforma lo siguiente:</p> <ul style="list-style-type: none"> - Documentación donde se incluyan diagramas de componentes de hardware y software y la planeación de la capacidad (incluye plataforma, almacenamiento, respaldos, red). - Documentación donde se incluya información de niveles de disponibilidad y la guía de operación para la plataforma implementada. - Documentación de buenas prácticas en el mantenimiento y administración de la arquitectura definida. <p>Documentación técnica y de usuario final donde describa en su totalidad y en forma detallada la solución instalada, con el fin de permitir futuras modificaciones o reinstalación de toda la plataforma.</p>						
3.15	CERTIFICADOS						
3.15.1	El oferente anexará a su oferta carta firmada por el representante legal en la cual conste que cuenta con centros de atención o convenios con centros de atención en Colombia autorizados por el fabricante de los equipos.						
3.15.2	El oferente anexará certificación expedida directamente por el fabricante en donde garantice el suministro de repuestos de los equipos ofertados por un término mínimo de cinco (5) años, después del recibido a satisfacción por parte del supervisor del contrato.						
3.15.3	El contratista se compromete con la Policía Nacional – Dirección de Inteligencia Policial, cuando el supervisor lo requiera, a entregar certificado de disposición final de los elementos técnicos cambiados a los equipos en aplicación de la garantía durante el tiempo de la misma, a excepción de los dispositivos de almacenamiento los cuales por política de seguridad de la información, la Policía Nacional hará la disposición final de los mismos, cumpliendo con la normatividad ambiental vigente y entes de control (Ministerio del Medio Ambiente y/o autoridad ambiental competente).						
4.	NIVEL ACADÉMICO DEL PERSONAL						
	<p>Se requiere el personal en las cantidades mínimas, con el perfil profesional, para desempeñarse en el proyecto como se describe en la siguiente tabla:</p> <table border="1"> <thead> <tr> <th>CANTIDAD/PERFIL</th> <th>NIVEL ACADÉMICO</th> </tr> </thead> <tbody> <tr> <td>1 Gerente de proyecto.</td> <td> <p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. </td></tr> </tbody> </table>	CANTIDAD/PERFIL	NIVEL ACADÉMICO	1 Gerente de proyecto.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. 		
CANTIDAD/PERFIL	NIVEL ACADÉMICO						
1 Gerente de proyecto.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. 						
4.1.1							

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>- Copia diploma de especialización o maestría.</p> <p>Los estudios de pregrado y posgrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p>		
1 Ingeniero con conocimientos en sistemas operativos.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico, con conocimientos en sistemas operativos especialmente Windows y Linux, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente, - Copia diploma o acta de pregrado. - Certificación en "Installation, Storage, and Compute with Windows Server". - Certificación en Linux. <p>Los estudios de pregrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> <p>NOTA: en caso de no cumplir una sola persona con todas las certificaciones exigidas, el oferente podrá suplir el requerimiento con otra persona, adjuntando igualmente el perfil profesional y experiencia solicitada para cada caso que aplique.</p>		
2 Ingenieros con conocimientos en desarrollo.	<p>Ingeniero de sistemas y/o ingeniero de software y/o ingeniero de desarrollo y/o ingeniero electrónico especialista o magister en desarrollo de software, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. 		

NOTA 1: en caso de que el personal inicialmente contratado deba ser cambiado por otra persona, ésta deberá contar con las mismas características mínimas académicas, descritas en la tabla anterior.

NOTA 2: el personal profesional que sea designado para las fases del desarrollo del proyecto, deberá ser el que se relacione en el contrato; así mismo, deberá cumplir con el perfil profesional mencionado en el

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE												
	<p>presente ítem, y asegurar que durante su ejecución se procure por mantener la continuidad del mismo, a fin de evitar traumatismos.</p> <p>En caso de realizarse cambios de personal profesional, se debe garantizar que el profesional reemplazante, ostente la formación académica igual o superior, a la establecida en el contrato.</p>														
4.1.2	<p>Con el fin de cumplir con el objeto contractual del proceso, se requiere que el personal solicitado cumpla con el desempeño y dedicación más adelante relacionado, desde el inicio del contrato hasta la finalización del mismo.</p> <table border="1"> <thead> <tr> <th>CANTIDAD/PERFIL</th><th>DESEMPEÑO EN EL PROYECTO</th><th>TIEMPO REQUERIDO</th></tr> </thead> <tbody> <tr> <td>1 Gerente de proyecto.</td><td>Quien estará a disposición de la Dirección de Inteligencia de la Policía Nacional, para efectos de coordinación y toma de decisiones en la ejecución del presente proceso contractual en todos los apartes contratados.</td><td>Tiempo bajo demanda durante la ejecución del contrato.</td></tr> <tr> <td>1 Especialista en sistemas operativos.</td><td>Se desempeñará laboralmente conforme al perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información en la instalación y configuración de sistemas operativos.</td><td>Tiempo bajo demanda durante la ejecución del contrato.</td></tr> <tr> <td>2 Especialista en desarrollo.</td><td>se desempeñará laboralmente conforme a su perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información para los temas referentes al codesarrollo de los componentes de software ofertados.</td><td>Tiempo bajo demanda durante la ejecución del contrato.</td></tr> </tbody> </table>	CANTIDAD/PERFIL	DESEMPEÑO EN EL PROYECTO	TIEMPO REQUERIDO	1 Gerente de proyecto.	Quien estará a disposición de la Dirección de Inteligencia de la Policía Nacional, para efectos de coordinación y toma de decisiones en la ejecución del presente proceso contractual en todos los apartes contratados.	Tiempo bajo demanda durante la ejecución del contrato.	1 Especialista en sistemas operativos.	Se desempeñará laboralmente conforme al perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información en la instalación y configuración de sistemas operativos.	Tiempo bajo demanda durante la ejecución del contrato.	2 Especialista en desarrollo.	se desempeñará laboralmente conforme a su perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información para los temas referentes al codesarrollo de los componentes de software ofertados.	Tiempo bajo demanda durante la ejecución del contrato.		
CANTIDAD/PERFIL	DESEMPEÑO EN EL PROYECTO	TIEMPO REQUERIDO													
1 Gerente de proyecto.	Quien estará a disposición de la Dirección de Inteligencia de la Policía Nacional, para efectos de coordinación y toma de decisiones en la ejecución del presente proceso contractual en todos los apartes contratados.	Tiempo bajo demanda durante la ejecución del contrato.													
1 Especialista en sistemas operativos.	Se desempeñará laboralmente conforme al perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información en la instalación y configuración de sistemas operativos.	Tiempo bajo demanda durante la ejecución del contrato.													
2 Especialista en desarrollo.	se desempeñará laboralmente conforme a su perfil profesional exigido, para cubrir los requerimientos establecidos en el plan de trabajo de acuerdo al levantamiento de información para los temas referentes al codesarrollo de los componentes de software ofertados.	Tiempo bajo demanda durante la ejecución del contrato.													
4.1.3	Conforme al numeral anterior, el contratista deberá estimar la cantidad de personal necesario, que permita dar cumplimiento al objeto contractual del presente proceso en los tiempos establecidos para la ejecución del mismo.														
4.1.4	La Dirección de Inteligencia de la Policía Nacional, se reserva solicitar el cambio de personas vinculadas al proyecto por parte del contratista, en cualquier momento a partir de la suscripción del contrato y el cual deberá ser sustituido por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta del presente proyecto.														

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
4.1.5	El contratista deberá solicitar por escrito a la Dirección de Inteligencia de la Policía Nacional, autorización para reemplazar a cualquier integrante del equipo de trabajo mínimo requerido, igualmente debe presentar al supervisor del contrato un plan de entrenamiento entre la empresa y el funcionario entrante, con el fin de garantizar la continuidad en la ejecución de las actividades a cargo.		
4.1.6	El contratista deberá realizar reuniones semanales con el supervisor del contrato para verificar los avances estipulados en el plan de trabajo inicialmente aprobado y programar nuevas tareas, durante la duración del mismo, con el fin de revisar, evaluar y sugerir mejoras en la ejecución.		
4.1.7	El equipo de trabajo designado por el contratista, debe contar con todo el equipo logístico requerido para la ejecución del presente proyecto, equipos de cómputo con sus respectivas herramientas licenciadas, personales y/o del contratista, la Dirección de Inteligencia de la Policía Nacional, suministrará el espacio físico necesario para desplegar ambientes de trabajo necesarios para el proyecto en las instalaciones de la Dirección de Inteligencia de la Policía Nacional, Avenida Boyacá No. 142A-55.		
4.2	EXPERIENCIA DEL PROPONENTE		
4.2.1	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 43231500 y/o 43211500 y/o 43232400 y/o 81111800, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 3.584,42 S.M.M.L.V., de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
4.2.1.1	<p>Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el contratista deberá anexar máximo cinco (5) certificaciones de contratos (una certificación por contrato) celebrados y ejecutados durante los años 2017 y/o 2018 y/o 2019, con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL" y/o "BIG DATA" y/o "MACHINE LEARNING" y/o "CIENCIA DE DATOS" y/o "VENTA o IMPLEMENTACIÓN INFRAESTRUCTURA DE TI", que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 70% del presupuesto oficial asignado.</p> <p>En caso que la empresa haya implementado este tipo de soluciones bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia específica a través de un documento certificado ante un notario, en el cual se especifique los valores de los contratos celebrados y ejecutados durante los años 2017 y/o 2018 y/o 2019, 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 "SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL" y/o "BIG DATA" y/o "MACHINE LEARNING" y/o "CIENCIA DE DATOS" y/o "VENTA o IMPLEMENTACIÓN INFRAESTRUCTURA DE TI".</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE						
	<p>NOTA: La certificación de experiencia en "VENTA o IMPLEMENTACIÓN DE INFRAESTRUCTURA DE TI" no podrá superar el 20% del total de la experiencia exigida.</p> <p>EXPERIENCIA DEL PERSONAL Y CERTIFICACIONES: con el fin de garantizar el cumplimiento del objeto contractual, se requiere que el personal gerencial y técnico cumpla con la experiencia de acuerdo a lo establecido en el Decreto Ley 0019 del 2012 (Ley Anti trámites) artículo 229 donde establece que "la experiencia profesional se computará a partir de la terminación y aprobación del pensum académico de educación superior", igualmente el oferente debe anexar certificaciones solicitadas en la siguiente tabla:</p> <table border="1"> <thead> <tr> <th>CANTIDAD/PERFIL</th><th>EXPERIENCIA/CERTIFICACIONES</th></tr> </thead> <tbody> <tr> <td>1 Gerente de proyecto.</td><td> <p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p> </td></tr> <tr> <td>1 Ingeniero con conocimientos en sistemas operativos.</td><td> <p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . - Certificar experiencia mínima de tres (03) años, laborados en lo referente a instalación y mantenimiento de sistemas operativos Windows o Linux. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista.</p> </td></tr> </tbody> </table>	CANTIDAD/PERFIL	EXPERIENCIA/CERTIFICACIONES	1 Gerente de proyecto.	<p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>	1 Ingeniero con conocimientos en sistemas operativos.	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . - Certificar experiencia mínima de tres (03) años, laborados en lo referente a instalación y mantenimiento de sistemas operativos Windows o Linux. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista.</p>		
CANTIDAD/PERFIL	EXPERIENCIA/CERTIFICACIONES								
1 Gerente de proyecto.	<p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>								
1 Ingeniero con conocimientos en sistemas operativos.	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . - Certificar experiencia mínima de tres (03) años, laborados en lo referente a instalación y mantenimiento de sistemas operativos Windows o Linux. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista.</p>								
4.2.2									

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>C-Nombre del Ingeniero que participó en el desarrollo tecnológico.</p> <p>D-Descripción del ítem contratado.</p> <p>E- Fecha de Inicio y Fin del Contrato.</p> <p>F-Valor del contrato.</p> <p>G-Concepto cumplimiento del contrato.</p>		
2 Ingenieros con conocimientos en desarrollo	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación de proyectos de desarrollo. - Certificar experiencia mínima de tres (03) años, en proyectos de desarrollo Python o java o visual studio, adjuntando las certificaciones respectivas. - Certificar experiencia mínima de dos (02) años participación conocimiento y soporte en el desarrollo de las plataformas ofertadas igual o similar al sistema de Ciberinteligencia Basado e Inteligencia artificial ó plataformas de OSINT, DARKNET Y DEEPWEB durante los años 2017 y/o 2018 y/o 2019, anexando a su propuesta certificación expedida por la firma donde se desarrolló el proyecto. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>		
4.3	SISTEMA AMBIENTAL		
4.3.1	El fabricante y el representante del fabricante en Colombia para los computadores y todos sus componentes, certificará que cumple con lo estipulado en la Resolución 1512/2010 expedida por el Ministerio de Ambiente, Vivienda y Desarrollo Territorial "Por la cual se establecen los Sistemas de Recolección Selectiva y Gestión Ambiental de Residuos de Computadores y/o Periféricos y se adoptan otras disposiciones. (Anexar certificación en la oferta).		
4.3.2	Informar si la empresa presenta sanciones vigentes en el registro único de infractores ambientales (RUIA) del Ministerio de Ambiente y Desarrollo Sostenible por el concepto que se va a contratar, la cual se encuentra disponible en la página web de la Agencia Nacional de Licencias Ambientales ANLA www.anla.gov.co , (Link: "trámites y servicios", luego click en "RUIA" y escoger la opción "RUIA VITAL").		
4.3.3	Cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a la actividad.		
4.3.4	El contratista deberá garantizar que los equipos eléctricos cumplan con normas técnicas de eficiencia energética, es decir, que tengan un		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	bajo consumo de energía y que cuenten con opciones de encendido, hibernación y apagado en los equipos que aplique y entregarán al supervisor del contrato las fichas técnicas de los equipos a adquirir.		
4.3.5	El contratista deberá garantizar que todo el material que se entregue a la unidad policial sea en forma digital, se realice en un medio reutilizable; los escritos deberán estar ajustados de acuerdo a la Directiva Presidencial 04 de 2012 "política cero papel".		
4.3.6	El contratista deberá aplicar las buenas prácticas ambientales, participar de los programas y campañas ambientales, así como las demás exigencias que se establezcan en el Sistema de Gestión Ambiental, en todas las actividades que realice durante la prestación del servicio dentro de la instalación policial.		
4.3.7	Cualquier infracción ambiental por omisión de permisos, concesiones o licencias ambientales que hubiese sido necesario tramitar antes del inicio del contrato, en el transcurso y después de la actividad del proceso, serán asumidas como responsabilidad del oferente o futuro contratista.		
4.4	SEGURIDAD Y SALUD EN EL TRABAJO En cumplimiento al Decreto 1072 del 26/05/2015 y con el fin de dar continuidad a políticas de SG-SST de la Policía Nacional, el oferente debe certificar que los funcionarios presentados en la oferta económica quienes van cumplir las distintas actividades solicitadas en el anexo No. 2 especificaciones técnicas, cumplen con los siguientes aspectos: <ul style="list-style-type: none">• Entregar los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal contratado que ejecutará la tarea contratada, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación y nivel de la cobertura del riesgo, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.• Deberá evidenciar objetivamente que cumple en su totalidad con los requisitos legales establecidos en el artículo 2.2.4.6.28 del Decreto 1072 de 2015, en relación con sus dependientes y contratistas durante toda la ejecución contractual.• Evidenciar objetivamente la activa participación en las actividades que la Policía Nacional o el contratante desarrolle en materia de promoción y prevención de riesgos laborales.• Evidenciar objetivamente, el uso continuo y permanente de los elementos de protección personal, durante la ejecución contractual, acorde a los peligros y riesgos relacionados con la tarea contratada.• 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.• Para el ingreso de los visitantes, usuarios o el personal que se autorice para el uso de espacios en los centros de trabajo e instalaciones de la Policía Nacional, estos deberán participar previamente en una capacitación en seguridad y salud en el trabajo, diseñada por la Policía Nacional y/o el centro de trabajo respectivo, acorde a la normatividad vigente y donde se evidencien los riesgos identificados previamente en el centro de trabajo y las actividades		
4.4.1			

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
	<p>del plan de emergencias y el plan de evacuación de la unidad policial.</p> <ul style="list-style-type: none"> • 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. • El contratista deberá garantizar que durante la ejecución de las obras se disponga de un kit de emergencias que permita la adecuada y oportuna atención ante posibles accidentes laborales. • Solo podrá acceder a los espacios de los centros del trabajo, previamente autorizados y delimitados, según la priorización del riesgo y deberá permanecer únicamente en el espacio delimitado y autorizado, no podrá acceder a espacios críticos en materia de seguridad, o lugares abiertos o cerrados donde se puedan producir eventos de alto riesgo en la integridad del visitante o usuario. 		
4.5	SEGURIDAD DE INSTALACIONES		
4.5.1	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física de las instalaciones policiales y Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional (resolución 08310 del 28/12/2016).		
4.6	SEGURIDAD DE LA INFORMACIÓN		
4.6.1	<p>El contratista acatará los controles establecidos para la seguridad de la información en la Dirección de Inteligencia Policial, así como la firma del compromiso de reserva y la aplicación de los estudios de credibilidad y confiabilidad.</p> <p>para ello el personal que realice la instalación, configuración de equipos y sistemas, deberá someterse a un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato. En el evento de no cumplir dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán someterse al estudio de confiabilidad requerido.</p>		
4.6.2	<p>Cláusula de Confidencialidad: Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso del proyecto, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata, se considera también información confidencial: a) aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) la que no sea de fácil acceso, y c) aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial, duración. El acuerdo regirá durante el tiempo que dure el proyecto, derechos de propiedad, toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso, modificación o terminación. El acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.</p>		

NUMERAL	CARACTERÍSTICAS TÉCNICAS	CUMPLE	NO CUMPLE
4.6.3	Confidencialidad e integridad de la información institucional: Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la preservación de la integridad y confidencialidad de la información institucional a la cual llegare a tener acceso directamente o por intermedio de terceros; en tal virtud, adoptará todas las medidas que sean necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida y suscribirá con la entidad los formatos de confidencialidad o reserva a que haya lugar.		
4.6.4	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de la labor. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el formulario establecido por la entidad contratante.		
4.6.5	El manejo de toda la información de arquitectura del sistema se considera CONFIDENCIAL, de manera que los planos, diseño, manuales técnicos y cualquier otro tipo de información estarán limitados únicamente a la interveniente o supervisión. El suministro de copias para otras personas o entidades deberá ser solicitada a la DIRECCIÓN DE INTELIGENCIA DE LA POLICÍA NACIONAL.		
4.7	PRESENTACIÓN DE LA OFERTA		
4.7.1	Las propuestas se harán en forma clara y en idioma español. Deberán presentar la carta de representación del fabricante o de distribuidor autorizado donde se indique su nombramiento por lo menos por el tiempo de ejecución del contrato, tiempo de garantías.		
4.7.2	La propuesta presentada, deberá ser firmada y avalada por un ingeniero electrónico y/o de sistemas, y/o electricista y/o telecomunicaciones anexando tarjeta profesional, como lo indica el ARTÍCULO 20 de la LEY 842 DE 2003 "PROPUESTAS Y CONTRATOS. Las propuestas que se formulen en las licitaciones y concursos abiertos por entidades públicas del orden nacional, seccional o local, para la adjudicación de contratos cuyo objeto implique el desarrollo de las actividades catalogadas como ejercicio de la ingeniería, deberán estar avalados, en todo caso, cuando menos, por un ingeniero inscrito y con tarjeta de matrícula profesional en la respectiva rama de la ingeniería." NOTA: Los oferentes deberán allegar el componente técnico firmado y avalado por el profesional en mención.		
4.7.3	Se deben anexar todas las fichas técnicas de los equipos de hardware ofertados.		
4.7.4	Las ofertas deben estar debidamente numeradas y relacionar al frente de cada especificación la página donde se encuentra el documento soporte.		



Capitán **MAGDA ESTEFANY PAPAMIJA BEDOYA**
Estructurador Estudio Previo



Subintendente **JORGE ARMANDO CHAVARRO LOZANO**
Estructurador Estudio Previo

ANEXO No. 3

CERTIFICACIÓN DE NECESIDAD

En mí calidad de Almacenista de Intendencia, manifiesto con la suscripción de esta CERTIFICACIÓN que, verificado los inventarios, no se cuenta con los elementos disponibles, solicitados en la presente contratación; por tal motivo, la única forma de resolver la necesidad es mediante la contratación de estos elementos.

ÍTEM	CÓDIGO SAP SILOG	DESCRIPCIÓN	NECESIDAD REAL	EXISTENCIA ALMACÉN	CANTIDAD ADQUIRIR	DÉFICIT %
1.	1282165	SERVIDORES	3	0	3	100%
3.	1062974	SWITCH 48 PUERTOS	1	0	1	100%
4.	1821176	SWTCH 24 PUERTOS	1	0	1	100%
5.	1669052	FIREWALL	2	0	2	100%
6.	1406118	SOFTWARE OSINT	1	0	1	100%

Firma,

Intendente JORGE ARMANDO JURADO PAREDES
Almacenista de Intendencia DIPOL

ANEXO No. 4
OBLIGACIONES DEL CONTRATISTA

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 ésta 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 Administrativa y Financiera o quien haga sus veces, dentro de los cinco (5) 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. En caso de ser necesario reemplazar al personal asignado a las actividades del presente contrato, se deberá informar oportunamente al supervisor anexando los documentos solicitados para el nuevo profesional.
8. 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 Administrativa y Financiera de la Policía Nacional y a las autoridades competentes para que se adopte las medidas necesarias.
9. 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.
10. 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 que se hayan suministrado.
11. **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 el 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.
12. El CONTRATISTA, deberá acatar y cumplir con los protocolos y lineamientos de seguridad establecidos por la Dirección de Inteligencia Policial y la Policía Nacional, entorno al Sistema de Gestión de Seguridad SGSI.
13. 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.

14. El proponente conoce y acepta que, en desarrollo de los principios de transparencia, igualdad, imparcialidad y publicidad, toda la información incluida en su propuesta para acreditar el cumplimiento de los requisitos de participación y para efectos de la evaluación es pública y cualquier persona podrá obtener copia de la misma.

Si la información o documentos suministrados presentan algún tipo de reserva o confidencialidad, deberá señalarse en forma específica, indicando su fundamento legal; caso en el cual y de acuerdo a la estructura de la plataforma SECOP II, la entidad tiene la potestad de analizar dicha justificación y proceder o no al otorgamiento de la clasificación solicitada.

El proponente será responsable por el manejo de la información recibida por parte de esta Dirección y deberá guardar la confidencialidad que sea requerida.

ANEXO No. 5
OBLIGACIONES DE LA POLICÍA NACIONAL

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 ó 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.

ANEXO No. 6
ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO

En la definición de los parámetros de mecanismos de cobertura de los riesgos deberán efectuarse dentro de los términos definidos en la Parte 2 – Título 1 – Capítulo 1 – Sección 1 – Subsección 6 del Decreto 1082 de 2015.

GARANTÍAS DEL PROCESO

ETAPA PRECONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACION DEL RIESGO	ASIGNACION DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
GARANTIA DE SERIEDAD	RIESGO JURÍDICO	LA NO SUSCRIPCION DEL CONTRATO SIN JUSTA CAUSA	VEINTE POR CIENTO (20%) DEL MONTO DEL PRESUPUESTO OFICIAL.	PROONENTE SELECCIONADO.	DESDE LA PRESENTACIÓN DE LA OFERTA Y HASTA LA APROBACIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO	AMPARA LA NO SUSCRIPCIÓN DEL CONTRATO SIN JUSTA CAUSA POR EL VEINTE POR CIENTO (20%) DEL PRESUPUESTO OFICIAL DESDE LA PRESENTACIÓN DE LA OFERTA Y HASTA LA APROBACIÓN DE LA GARANTÍA DE CUMPLIMIENTO DEL CONTRATO
	RIESGO JURÍDICO	LA NO AMPLIACIÓN DE LA VIGENCIA DE LA GARANTÍA DE SERIEDAD DE OFERTA CUANDO EL TERMINO PREVISTO EN LA INVITACIÓN PARA LA ADJUDICACIÓN DEL CONTRATO SE PRORROGUE O CUANDO EL TERMINO PREVISTO PARA LA SUSCRIPCION DEL CONTRATO SE PRORROGUE SIEMPRE Y CUANDO ESAS PRORROGAS NO EXCEDAN UN TÉRMINO DE TRES MESES.				
	RIESGO JURÍDICO	LA FALTA DE OTORGAMIENTO POR PARTE DEL PROONENTE SELECCIONADO DE GARANTIA DE CUMPLIMIENTO EXIGIDA POR LA ENTIDAD PARA AMPARAR EL INCUMPLIMIENTO DE LAS OBLIGACIONES DEL CONTRATO.				
	RIESGO JURÍDICO	EL RETIRO DE LA OFERTA DESPUES DE VENCIDO EL TERMINO FIJADO PARA LA PRESENTACIÓN DE LAS OFERTAS.				

ETAPA CONTRACTUAL la no ampliación de la vigencia de la garantía de seriedad

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
GARANTÍA ÚNICA	RIESGO JURÍDICO	INCUMPLIMIENTO DEL CONTRATO.	VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TÉRMINO IGUAL A LA VIGENCIA DEL CONTRATO Y CUATRO (04) MESES MAS	AMPARA EL RIESGO DE INCUMPLIMIENTO DURANTE EL PLAZO DE EJECUCIÓN Y LIQUIDACIÓN DEL CONTRATO LA ESTIMACIÓN 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 TÉRMINOS DE LA CLAUSULA PENAL PECUNIARIA.
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD DE LOS BIENES	CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TÉRMINO IGUAL A LA VIGENCIA DEL CONTRATO Y TRES AÑOS MAS.	AMPARA EL RIESGO DE MALA CALIDAD DEL BIENES Y SERVICIO DURANTE LA VIGENCIA DEL CONTRATO, BUSCANDO RESARCIR EL DETERIMENTO CAUSADO A LA ENTIDAD POR MALA CALIDAD DE LOS SERVICIOS O INSUFICIENCIA DE LOS PRODUCTOS ENTREGADOS.
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD SERVICIO.	VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR TRES (03) AÑOS CONTADO A PARTIR DE LA FECHA DE RECIBIDO DEL DESARROLLO.	AMPARA EL RIESGO DE MALA CALIDAD DE LOS SERVICIOS O MAL FUNCIONAMIENTOS DE LOS MISMOS DURANTE LA VIGENCIA DEL CONTRATO Y TRES (03) AÑOS MAS BUSCANDO RESARCIR EL DETERIMENTO CAUSADO A LA ENTIDAD POR MALA CALIDAD O INSUFICIENCIA DEL SERVICIO PRESTADO.
GARANTÍA ÚNICA	RIESGO JURÍDICO	NO PAGO DE SALARIOS PRESTACIONES E INDEMNIZACIONES LABORALES.	CINCO POR CIENTO (5%) DEL VALOR DEL CONTRATO.	CONTRATISTA	VIGENTE POR UN TÉRMINO IGUAL A LA VIGENCIA DEL CONTRATO Y TRES (3) AÑOS MAS	AMPARA A LA ENTIDAD DE LOS PERJUICIOS QUE SE LE OCASIONE COMO CONSECUENCIA DEL INCUMPLIMIENTO DE LAS OBLIGACIONES LABORALES A QUE ESTE OBLIGADO EL CONTRATISTA DERIVADAS DE LA CONTRATACIÓN DEL PERSONAL UTILIZADOS PARA LA EJECUCIÓN DEL CONTRATO.

CLÁUSULAS SANCIONATORIAS Incumplimiento total declaratoria de caducidad

MULTA	RIESGO JURÍDICO	LA NO CONSTITUCIÓN DENTRO DEL TÉRMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS LA PÓLIZA DE GARANTÍA ÚNICA	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 DÍA DE RETARDO Y HASTA POR DIEZ (10) DÍAS	CUANDO EL CONTRATISTA NO CONSTITUYA DENTRO DEL TÉRMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS, A PÓLIZA DE GARANTÍA ÚNICA
MULTA	RIESGO JURÍDICO	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 DÍA DE RETARDO HASTA POR UN PLAZO DE QUINCE (15) DÍAS CALENDARIO QUE SE DESCONTARÁ DEL SALDO QUE LE ADEUDE LA ENTIDAD. ESTA SANCIÓN 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 OBLIGACIÓN DERIVADA DEL CONTRATO POR CAUSAS IMPUTABLES AL CONTRATISTA
CLAUSULA PENAL PECUNIARIA	RIESGO JURÍDICO	INCUMPLIMIENTO TOTAL DECLARATORIA CADUCIDAD	VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO	CONTRATISTA	EL VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO CUANDO SE TRATE DE INCUMPLIMIENTO TOTAL DEL CONTRATO Y PROPORCIONAL AL INCUMPLIMIENTO PARCIAL DEL CONTRATO	AMPARA EL INCUMPLIMIENTO PARCIAL O DEFINITIVO DEL CONTRATO POR PARTE DEL CONTRATISTA, SE BUSCA EL PAGO PARCIAL Y DEFINITIVO DE LOS PERJUICIOS QUE SE CAUSEN A LA ENTIDAD

ANÁLISIS DE RIESGO DEL PROCESO

GARANTÍA TÉCNICA	RIESGO OPERATIVO	DAÑOS DE LOS ELEMENTOS DESPERFECTOS CON LOS MISMOS	VALOR DESPERFECTOS Y/O COMPONENTES DE LOS ELEMENTOS	CONTRATISTA	TODO EL HARDWARE, SOFTWARE Y LOS COMPONENTES DE LA SOLUCIÓN HIPERCONVERGENTE, QUE HACE PARTE DEL PRESENTE PROCESO DEBEN TENER UN TIEMPO DE GARANTÍA MÍNIMO DE TRES (3) AÑOS, OFRECIDA POR EL CONTRATISTA, CONTADOS A PARTIR DEL RECIBIDO A SATISFACCIÓN POR PARTE DEL SUPERVISOR DEL CONTRATO.	AMPARA EL CORRECTO FUNCIONAMIENTO DE LOS EQUIPOS, SOFTWARE Y DESARROLLO SISTEMA DE INTELIGENCIA POLICIAL DESDE EL MOMENTO DEL TÉRMINO DE LA ADQUISICIÓN Y CONFIGURACIÓN Y HASTA POR EL PERÍODO ESTIPULADO EN LAS ESPECIFICACIONES TÉCNICAS.
------------------	------------------	--	---	-------------	--	---

ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

20.	19.	18.	17.	16.	15.	14.	13.	12.	11.	10.
General	General	General	General	General	General	General	General	General	General	General
Externo	Externo	Externo	Externo	Externo	Externo	Externo	Externo	Externo	Externo	Externo
Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución	Ejecución
Tecnológico	Operacional	Operacionales	Operacional	Regulatorios	Operacional	Operacional	Operacional	Tecnológico	Económico	Social o político
Cambios en las especificaciones técnicas por parte del fabricante	Entrega incompleta de los componentes de hardware	Reevaluación de las actividades y plan de ejecución del contrato	Replanteamiento del tiempo de ejecución y aplicaciones de condiciones legales.	Extensión en los plazos de ejecución del contrato	Retardos en la importación de los equipos objeto del contrato	Uso, destrucción y/o divulgación de información privilegiada a la que tenga acceso el personal del contratista	Falsedad en documentos que conforman la oferta	Incumplimiento del contrato	Volatilidad de los precios y oferta de los componentes	Demoras en la entrega de los elementos
No	No	No	Si	Si	Si	Si	Si	Si	Si	Si
Contratista	Entidad Estatal	Entidad Estatal	Contratista	Contratista	Contratista	Contratista	Contratista	Contratista	Contratista	Contratista
Validación vía homologación con los requisitos solicitados	Demoras en las ejecuciones del objeto contractual	Inicio de la ejecución contractual segmentada para los desarrollos	Revisión e inspección a los bienes a recibir	Revisión minuciosa de la documentación y pliego de condiciones	Garantía de seriedad	Garantía de seriedad	Evitar el riesgo/realizar formato de compromiso de reserva y prueba de polígrafo	Evitar el riesgo/realizar formato de compromiso de reserva y prueba de polígrafo a los intermediarios que suministran	Garantía única	Costos incluidos en la oferta presentada
Bajo	bajo	bajo	Medio	Medio	Medio	Alto	Alto	Alto	Medio	Medio
No	No	No	Si	Si	Si	Si	Si	Si	No	Si
Contratista	Entidad Estatal y Contratista	Entidad Estatal y Contratista	Contratista	Contratista	Contratista	Entidad Estatal	Entidad Estatal	Entidad Estatal	Contratista	Contratista
Inicio en la ejecución	Fecha entregas pactadas	Desde la firma del contrato	Desde la firma del contrato	Según entregas pactadas	Desde la firma del contrato	Desde la firma del contrato	Desde la firma del contrato	Desde la firma del contrato	Desde la firma del contrato	Desde la firma del contrato
Fecha entrega elementos de hardware	Recibido a satisfacción	Inicio de ejecución	Inicio de ejecución	En las fechas de cada entregable	Una vez inicie el contrato	Una vez inicie el contrato	Publicaciones de las evaluadoras	3 meses después de la presentación de la oferta	Recibido a satisfacción	3 meses después de la presentación de la oferta
Revisión de las características de los equipos	Contraste de elementos entregados	Seguimiento a cumplimiento de tareas del contratista	Control de liquidez	Chequeo del cronograma de ejecución	Verificar que el ingeniero va a realizar las actividades de soporte sea él autorizado	Verificar que el ingeniero va a realizar las actividades de soporte sea él autorizado	Verificación de los documentos que integra la oferta	Verificación de la calidad de los productos que serán entregados e instalados periódicas	Recibido a satisfacción	Seguimiento del Proceso Contractual
Cada entrega	Cada entrega	Periódico	Una vez	Cada entrega	Toda vez que haya una vista de soporte y mantenimiento	Toda vez que haya una vista de soporte y mantenimiento	De acuerdo a la cronología del proceso	Una vez	Una vez	Una vez

ANEXO No. 7

FICHA TÉCNICA DE PRODUCTOS O SERVICIOS

Para desarrollar este punto de debe tener en cuenta la siguiente Ficha Técnica de Producto o servicios.

FICHA TÉCNICA DE PRODUCTO	
DENOMINACIÓN DE BIEN O SERVICIO	
<i>Sistema de Ciberinteligencia basado en Inteligencia Artificial</i>	
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO	
<i>Sistema de Ciberinteligencia basado en Inteligencia Artificial</i>	
UNIDAD DE MEDIDA	
<i>Unidad</i>	
DESCRIPCIÓN GENERAL	
NUMERAL	CARACTERÍSTICAS TÉCNICAS
1.	El contratista deberá implementar una solución que incluya el software, el hardware y el desarrollo necesario para proveer un Sistema de Ciberinteligencia basado en Inteligencia Artificial, que integre diversas fuentes de información abierta, información estructurada y no estructurada, así como información y contenido dispuesto en internet, con el fin de enriquecer el análisis y la elaboración de productos prospectivos y anticipativos, a través de la generación automática de organización de información de manera gráfica y alertas.
1.1	El contratista se encargará de realizar todas las acometidas eléctricas y lógicas necesarias para la instalación de los equipos ofertados e integración del software en los equipos dispuestos; tales como, router, cables de potencia, breaker, switch, interfaces de conexión como patch-cord de fábrica thermoformados, cables FC, transceiver de fibra óptica en origen y destino, software de configuración (drivers) y utilitarios del sistema, para cada uno de los componentes de la solución y los necesarios que garanticen su pleno funcionamiento; fuera de la red que tiene contratada la POLICÍA NACIONAL. Así mismo, la instalación de los servidores en el Datacenter de la Dirección de Inteligencia Policial sin que se comprometa de alguna forma la red de la Policía Nacional.
1.2	Considerando que se conectarán treinta (30) equipos de computo a la infraestructura a implementar, el contratista debe tender el cableado físico que garantice la conexión desde el datacenter a los switches de piso de las áreas de trabajo (los que ofertan en el presente proceso), considerando que actualmente los equipos de computo en cada piso cuenta con su punto de conexión.
1.3	Con el fin de verificar las condiciones del datacenter y distancias para la instalación de cableado, se programará visita técnica dos (2) días después de publicado el pliego definitivo del presente proceso, para lo cual deberán enviar datos del personal que realizará visita técnica

	<p>(máximo dos personas por oferente) a través de la sección de mensajes de la plataforma SECOP II con los siguientes datos:</p> <p>Nombres y apellidos: Número de identificación: Nombre de la empresa oferente: Nacionalidad:</p> <p>Por políticas de seguridad de la información, no está permitido el ingreso de equipos de cómputo, celulares, dispositivos usb y demás elementos electrónicos que posean capacidad de almacenamiento, de igual forma se deben diligenciar los formatos de compromiso de reserva y estudio de credibilidad y confiabilidad.</p>
1.4	<p>El contratista instalará, configurará, integrará y entregará en completa operación los elementos que hacen parte del hardware de la solución en el Datacenter de la Dirección de inteligencia Policial o el espacio asignado para tal fin, dentro de las instalaciones.</p>
1.5	<p>El Sistema debe ser una plataforma de Inteligencia efectiva, ágil, escalable, intuitiva al usuario, que utilice técnicas de correlación y análisis, empleando tecnologías de procesamiento de lenguaje natural, procesamiento de imágenes y de textos en imágenes a partir de técnicas de machine learning e IA.</p>
1.6	<p>Considerando que es un sistema con unas necesidades específicas y que existen en el mercado algunas que se ajustan en un 80% a lo requerido, se hace necesario la realización de un co-desarrollo por parte del contratista con acompañamiento del contratante, con el fin de integrar otras fuentes de información pública y disponibles para la Policía Nacional. El contratista se compromete a realizar un Co-Desarrollo equivalente al 20% del sistema, el cual debe ser a la medida y cumpliendo con los requerimientos establecidos por el contratante.</p> <p>Con el fin de verificar el cumplimiento de las funcionalidades del producto ofertado, el comité técnico, evaluará el funcionamiento del sistema a través de una prueba técnica descrita a continuación:</p> <p>Consideraciones:</p> <p>La Dirección de Inteligencia Policial, a través del comité técnico, evaluará mediante una prueba técnica, si cumple o no cumple cada uno de los subitems que se describe en el Cuadro No. 1 Metodología de Evaluación.</p> <p>Con la entrega de la oferta deben entregar correo con el cual se podrán contactar para efectuar videoconferencia.</p> <p>El día de la entrega de las ofertas, se realizará reunión de coordinación con los representantes legales y un técnico de las firmas oferentes, a través de videoconferencia, con el fin de suministrar información técnica para la realización de la prueba.</p> <p>El mismo día se pueden realizar preguntas a los estructuradores, con el fin de que resuelvan dudas y realicen las conexiones necesarias para la realización de la prueba.</p>

	<p>El cronograma para la presentación de las pruebas, se hará de acuerdo al orden en que se reciban las ofertas y la cantidad de oferentes, la prueba se realizará dos días después de recibir la oferta, fecha y hora que se indicará una vez se reciban todas las ofertas a través de la sección de mensajes de la plataforma SECOP II a cada firma oferente.</p> <p>Se tiene previsto el espacio de un día desde las 09:00 horas hasta las 17:00 horas para que los oferentes, realicen las pruebas.</p> <p>El oferente deberá incluir en la oferta el nombre de los técnicos (máximo dos), que guiarán al funcionario designado para la interacción en la plataforma ofertada.</p> <p>Para la prueba se asignará un funcionario por plataforma ofertada en un equipo con internet.</p> <p>Los oferentes deben entregar:</p> <ul style="list-style-type: none">-Usuario y Contraseña para ingresar a la plataforma. <p>Durante la realización de las pruebas un moderador entregará los datos y simultáneamente los funcionarios asignados realizarán las búsquedas, generaran las alertas y verificarán el funcionamiento uno a uno de los requerimientos.</p> <p>En esta prueba se verificarán las funcionalidades del software del oferente, teniendo en cuenta cada uno de los 160 subítems establecidos en la tabla "Evaluación detallada", poniendo frente a cada actividad si cumple o no cumple.</p> <p>En este sentido, la evaluación se requiere que cumpla con el 80% de los ítem a verificar.</p>
--	--

Cuadro No.1 Metodología de evaluación EVALUACIÓN DETALLADA				
NOMBRE DE LA EMPRESA			Cumple	No cumple
1	Gestión de usuarios: Mostrar el panel de administrador	Adicionar nuevos usuarios		
		Conectar un email a cada usuario		
		Defina usuarios regulares y administradores y podría cambiar el usuario correctamente fácilmente		
		Cambiar la contraseña		
		Bloquear y desbloquear usuarios		
2	Asignación y Gestión del espacio de trabajo a usuarios	Adicionar nuevos espacios de trabajo, o asignar roles de los módulos		
		Definir usuario activo y no activo		
		Cambiar los usuarios en cada espacio de trabajo		
		Administre la política de retención para cada espacio de trabajo.		
3	Manejo de la Cuenta de navegación	Importar números masivos de cuentas de navegación (al menos 500)		
		Sube cuentas de navegación configurados de todas las redes sociales		
		Definir si la cuenta de navegación se usa a través de API / o login		
		Crea una cuenta de navegación con algunas redes sociales		
4	Auditoria	Mostrar el panel o módulo de administrador		
		Permite personalizar un tablero para administrar todos los datos de auditoría		
		Visualizar todas las acciones principales realizadas en el entorno divididas por tiempo, usuarios, espacios de trabajo o módulos y más		
		Auditar las actividades de todos los usuarios internos del sistema.		
5	Capacidades de Análisis: Se darán temáticas para realizar búsquedas y se debe mostrar los análisis y colección efectuada.	Análisis de temas y discursos		
		Línea de tiempo en un gráfico		
		Análisis de sentimientos		
		Influenciadores		
		Análisis geográfico en un mapa		
		información demográfica		
		Principales interactores		
		Detección de cuentas falsas		
		hashtags principales		
		URL principales		
		Análisis de entidades		
		Cuentas de redes sociales		
		Contenido que incluye a los principales interactores y participantes		
		Acerca del Usuario		
		Conexión agrupada por lugar de trabajo, ciudad natal, educación, grupos internos, fuerza de conexión, cuentas falsas.		
		Análisis de grupo		
		o Intersección entre dos entidades.		
		o Principales interactores de una página web o red social		
		o Acerca de la página		
		o Fans superiores de la página		
		o Publicaciones principales		
		Análisis organizacional		
		• cuentas de redes sociales		
		• Los mejores interactores		
		• Presencia web		
		• Posibles miembros		

			Demostrar la recolección de horarios <ul style="list-style-type: none"> • Recolectando la información cada X cantidad de tiempo 			
			Nuevas fuentes Mostrar toda la información que se recopiló utilizando los nuevos buscadores que se crearon.			
			Recolección Dark Web <ul style="list-style-type: none"> • Mostrar los diferentes filtros que se pueden usar • Motores de búsqueda Darknet 			
6	Biblioteca algoritmos de búsqueda: El sistema debe tener una biblioteca de algoritmos de búsqueda a la que se pueda acceder fácilmente desde varias pantallas. Mostrar las siguientes fuentes:		Algoritmos de búsqueda en redes sociales Facebook Twitter YouTube Instagram Algoritmos Surface web: Motores de búsqueda (por lo menos 5 al mismo tiempo) Web pages RSS DarkNet Motores de búsqueda Web pages Otras fuentes			
7	Consulta: El usuario debe poder controlar la recopilación de datos.		Insertar diferentes tipos de entrada (nombres de usuario, ID de usuario) Cambiar el nombre de la consulta Se puede definir qué cuenta de navegación recogerá los datos. Crear una tarea de recopilación programada Definir la cantidad de tiempo que se realizará la recolección. Escribir una descripción para cada consulta Agregar múltiples consultas Definir a qué caso va esta consulta			
8	Reintentar mecanismo		Demuestre que el sistema sabe cómo superar el bloqueo de las cuentas de navegación y enviar al menos tres cuentas de navegación diferentes de forma automatizada para realizar una sola consulta.			
9	Geo-cercado		Generar una consulta señalando un área geográfica específica, devolviendo resultados de un área específica			
10	Medios de comunicación – Búsqueda de cuenta		Encuentre diferentes nombres de identidad basados en palabras clave en las siguientes redes: <ul style="list-style-type: none"> • Facebook • Twitter • Instagram Recopilar información sobre las cuentas directamente desde la pantalla de búsqueda			

11	<u>Colección de redes sociales</u> Recopile la siguiente información:	Facebook identidad Feed (comentaristas, reacciones) Conexiones Acerca de (ingresos, páginas) Ubicaciones		
		Página de Facebook Feed (comentaristas, reacciones) Interactores de página Acerca de la página		
		Grupo de Facebook Feed (comentaristas, reacciones) Miembros del grupo,		
		Facebook post comentaristas, reacciones seguidores Búsqueda genérica– palabras claves		
		Twitter Identidad Feed (comentaristas, reacciones)		
		Seguidores		
		Hashtags		
		Cuenta mencionada		
		Retweets		
		Búsqueda genérica– palabras claves		
		Instagram: Identidad		
		Feed (comentaristas, reacciones)		
		Hashtags		
		User location		
		Seguidores		
		Page locations		
		YouTube: Identidad		
		YouTube búsqueda – Avanzada		
		YouTube búsqueda		
12	Web Page	Elija cualquier sitio web normal y muestre las capacidades de recopilación		
13	Motores de búsqueda	Mostrar la colección de los motores de búsqueda. Esto debe incluir al menos 5 diferentes		
14	RSS	Colección RSS Feeds		
		Dark Web		
15	Motores de búsqueda	Mostrar la colección de los motores de búsqueda de dark net		
16	Web page	Mostrar la colección de un sitio web oscuro específico (TOR)		
		Aplicaciones		
17	Telegram	Mostrar la colección de un canal de Telegram con una cuenta de navegación dedicada		
		Nuevas fuentes		
18	Adicionar nuevas fuentes: El proponente recibirá por adelantado algunas fuentes y mostrará el flujo de trabajo de creación y la	El sistema debe poder agregar nuevas fuentes a la lista. Crear y agregar Foros – dark web y surface web Crear y agregar noticias website Data base Online		

		recopilación y análisis. (las fuentes serán entregadas el día de la entrega de las ofertas)	Crear y agregar un Excel			
19	Parámetros de búsqueda de entidad	Búsqueda por un parámetro que tenga la herramienta. Búsqueda por Email (realizada sobre información pública). Búsqueda por número de cédula (realizada sobre información pública). Búsqueda por Facebook Búsqueda por Twitter ID Búsqueda por Instagram ID				
20	Reporte o informe Generar el reporte con la siguiente información:	Crear un informe dentro del sistema. Imágenes de entidad Nombres Información pública disponible Cuentas de redes sociales Conexiones Ubicaciones (desde redes sociales) Guardar y pegar capturas de pantalla del sistema Visualiza el flujo de investigación y muestre la conexión entre las diferentes pruebas encontradas. Medios de comunicación				
21	Exportar	Exportar el informe en formato PDF Exportar informe en formato JSON Exportar informe en otro formato Mostrar los reportes				
22	Extracción de entidad	Organizaciones Nombres de entidad URL Etiquetas Localizaciones Idiomas Fuentes				
23	Búsqueda basada en palabras:	Crear una lista dedicada de palabras para buscar en una de las consultas Muestre que el sistema lo extrajo				
24	Clasificación cuentas falsas	Clasificar las cuentas en Facebook y Twitter como falsas Mostrar los motivos de clasificación				
25	Clasificación	Ordenar la información según tiempo de publicación Ordenar la información según fuente Ordenar la información según Compromiso Ordenar la información leído / No leído				
26	Exporte	Mostrar las capacidades de exportación del feed y de otras características del sistema, incluidos CSV, PNG, I2 y otros formatos.				
27	Medios y Display	Mostrar imágenes y videos. Mostrar cómo el usuario puede descargar todas las imágenes y videos.				

			Mostrar los resultados en "Modo de chat" en aplicaciones.		
28	Datos resumidos		Nube de palabras Línea de tiempo en un gráfico Sentimiento Conexiones de hashtags en un gráfico Demografía en un gráfico Mejores influenciadores Distribución de cuenta falsa		
29	Geo-Analysis		Muestra la información en un mapa que se puede cambiar. Mostrar puntos calientes en función de la cantidad de resultados		
30	Análisis de relaciones – Análisis link		Agrupar los resultados por ciudad de nacimiento Agrupar los resultados por ciudad actual Agrupar los resultados por lugar de trabajo Agrupar los resultados por nombre y apellido Grupos internos – mostrar la relación entre las conexiones de grupos para encontrar aquellos que sean de interés Fuerza de conexión – muestra la fuerza de la conexión basada en me gusta, comentarios, conexiones familiares. Intersección – muestra la intersección de las conexiones de algunas cuentas para encontrar conexiones mutuas.		
31	Lista de entidades con actividad inusual		Marcar cuenta Gestionar lista.		
32	Alertas		Generar como mínimo 4 tipos de alertas y vistas guardadas Alerta basada en geografía Alerta basada en feed Alerta indicativa basada en palabras Envío de alerta por correo electrónico		
33	Visualizando el flujo de investigación		Muestra una visualización gráfica del flujo de investigación completo. Conectar diferentes tipos de entidades (cuentas sociales, datos públicos encontrados, todo). Enlaces a sitios web, videos y pantallas		
1.7	Desde el inicio del proyecto, la seguridad del sistema se debe prever, teniendo en cuenta controles, auditorías, accesos e infraestructura.				
1.8	El contratista debe garantizar que cuenta con un sistema o herramienta tecnológica base ya desarrollada en 80% con las necesidades descritas en el presente pliego, que permita integrar nuevas funcionalidades y los casos de uso específicos descritos en el presente pliego de condiciones, la cual debe ser entregada a POLICÍA NACIONAL con licenciamiento perpetuo, que no genere costos adicionales al proyecto de tal manera que incluya el licenciamiento de toda la solución de hardware ofertada, es decir, licenciamiento de todos los Cores de la solución y de todos los usuarios solicitados. Para tal efecto, debe anexar la ficha técnica para el ítem 1 descrito adelante, que enuncie las especificaciones técnicas y funcionalidades actuales del sistema.				

	<p>Adicionalmente y durante el periodo de mantenimiento el contratista debe priorizar dar solución a cualquier inconveniente que pueda generarse en el normal desarrollo de la plataforma debido a actualizaciones de las APIS por parte de terceros (como Twitter, Facebook o Instagram). La clasificación de la incidencia sobre tecnologías ajenas al contratista debe quedar formalizada en un plazo no superior a 48 horas.</p>
1.9	<p>Vectores de entrada de datos de fuentes de información:</p> <p>Fuentes Abiertas: (OSINT), basadas en:</p> <ul style="list-style-type: none"> - Redes sociales: Facebook, Twitter y Instagram, - Servicios WEB: Pastebin, Foros, Blogs. - Canales, grupos y supergrupos de Telegram públicos. - Información Darkets (Tor, I2p y freenet al menos). - 5 fuentes de información abierta que serán integradas a petición de la Dirección que tengan acceso abierto y sin controles por navegación web. <p>Fuentes Cerradas: las estructuradas y gestionadas con independencia de la plataforma de inteligencia mediante API de conexión facilitada por la Dirección.</p> <ul style="list-style-type: none"> - Evidencias digitales forenses (EVDF) ya procesadas. (Excel, Word, Pdf, txt, imágenes, videos). <p>Para las fuentes abiertas en internet, durante el mantenimiento, se priorizará el soporte en los controles de acceso que puedan surgir, siendo conscientes que la evolución o modificación de tecnologías ajenas al oferente no pueden ser controladas.</p>
1.10	<p>La herramienta debe ser construida bajo una arquitectura modular, la cual permite la integración de nuevos módulos de Crawling y organización de la información, integración y escalabilidad de fuentes abiertas, información estructurada y no estructurada disponible para la Policía Nacional.</p>
1.11	<p>El software que compone el sistema, deberá tener licenciamiento perpetuo, que se pueda desinstalar e instalar en un nuevo hardware sin limitaciones, ya sea por máquina o por número de cores o procesadores, 100% administrable por la Policía Nacional y soporte técnico mínimo de tres (3) años.</p> <p>El sistema completo tendrá dos partes diferenciadas:</p> <p>PARTE 1. Tecnología existente y propiedad del contratista. La Policía Nacional para esta parte no requerirá propiedad intelectual pero SÍ podrá disponer del código fuente, para ser custodiada cumpliendo los términos de licencia del contratista. Es decir, el contratista deberá entregar para custodia el código fuente de toda su tecnología.</p> <p>PARTE 2. Tecnología co-desarrollada. Relativa a la parte de integración de fuentes abiertas colombianas solicitadas por la Policía Nacional así como las fuentes cerradas descritas anteriormente.</p>
1.12	<p>El contratista deberá garantizar la configuración de un respaldo o copia de la información almacenada en la base de datos que evite una pérdida definitiva e irrecuperable de la información en caso de una eventualidad.</p>
1.13	<p>El Sistema debe incluir base de datos orientada a grafos, lo que permite la interconexión de los datos obtenidos y la correlación entre</p>

		diferentes fuentes de datos estructurados y no estructurados de forma eficiente.
1.14		Es obligación del contratista realizar todos los diseños físicos y lógicos, así mismo disponer de los elementos donde operará el Sistema, para ello debe presentar los diseños para ser aprobados por el supervisor del contrato.
1.15		La interfaz de la plataforma debe estar en español para su operación y el sistema debe ser multilenguaje, incluyendo como mínimo el "inglés" y pudiendo incorporar otros idiomas como el árabe, mandarín, ruso y portugués.
1.16		La plataforma debe permitir la traducción de los contenidos recolectados y analizados en los idiomas que establece el numeral 1.13. El contratista debe indicar de que otros idiomas dispone la plataforma para la recolección, análisis y traducción de la información.
1.17		La aplicación debe identificar y señalar visualmente, de forma automática, entidades como: nombre de entidades, lugares, direcciones; a partir de textos recopilados por la herramienta de búsqueda OSINT(información pública disponible)
1.18		El contratista debe configurar en caso de ser necesario los componentes de procesamiento y almacenamiento requeridos para la correcta operación de la plataforma durante el tiempo de soporte y garantía.
1.19		Todos los equipos deben ser nuevos y deben quedar instalados, configurados, programados y operando correctamente.
1.20		<p>En caso de realizar una fase de desarrollo a la medida para cumplir a totalidad las condiciones técnicas del presente pliego, se deberá realizar levantamiento de información, describiendo la arquitectura del sistema de información propuesta como:</p> <ul style="list-style-type: none"> • Casos de uso. • Planeación de la implementación. • Vista lógica. • Vista de datos. • Vista de despliegue. • Vista de integración con sistema de información externos. <p>El desarrollo que se realice debe ser de uso exclusivo de la Policía Nacional de Colombia, y no con fines de comercialización ni de lucro con otros países y/u organizaciones públicas o privadas</p> <p>Además todas las actividades de desarrollo deberán realizarse in-house, dentro de las instalaciones de DIPOL.</p>
1.21		<p>El oferente deberá documentar y entregar las siguientes fases para la ejecución del objeto del presente proceso:</p> <p>GESTIÓN Y PLANEACIÓN DEL PROYECTO:</p> <ul style="list-style-type: none"> • Inicio, estructuración y gestión del proyecto: describir visión y alcance, identificar y comprender el contexto organizacional y objetivos estratégicos del proyecto, identificar actores del sistema (usuarios con perspectiva), esbozar la operación deseada, analizar factibilidad, definir integrantes, roles y responsabilidades del equipo de proyecto, estimar recursos, costos y tiempo de desarrollo, identificación preliminar y gestión proactiva de riesgos. • Aseguramiento de calidad: proveerá una visión clara de cómo se garantizará y logrará la calidad del sistema de información, los entregables y el proceso. Contendrá el plan de revisión, pruebas

	<p>y aseguramiento de calidad para cada una de las fases o flujos de trabajo.</p> <ul style="list-style-type: none"> • Especificación de requerimientos del sistema y análisis: comprende el contexto, reglas de negocio y procesos de la organización donde apoyará el sistema de información y especificar los requerimientos funcionales y técnicos (atributos de calidad técnica) del sistema de información. La principal tarea consiste en la generación de especificaciones correctas que describan con claridad, sin ambigüedades, en forma consistente y concreta, las necesidades de los usuarios internos y externos del sistema de información. Se enfoca en un objetivo fundamental. La definición de lo que se desea producir a través de especificaciones finales completas, formales y acordadas entre las partes, comprende el levantamiento de información. <p>DISEÑO:</p> <ul style="list-style-type: none"> • Diseño y Arquitectura de Software: la definición de la arquitectura del sistema (vista estructural del sistema) y del entorno tecnológico (software, hardware, comunicaciones, seguridad), la especificación detallada de los componentes del sistema de información. A partir de dicha definición, se generan todas las especificaciones de construcción relativas al propio sistema y al software, así como la descripción técnica del plan de pruebas, la definición de los requisitos de implantación y el diseño de los procedimientos de migración y carga inicial de datos (éstos últimos cuando proceda). Comprende diseño funcional, diseño técnico, arquitectura del sistema de información. • Modelo de Casos de Uso del Sistema: Permitirá modelar, visualizar y documentar la funcionalidad y el ambiente deseados en el sistema de solución. A través del modelo se especificará la secuencia de acciones que el sistema de información o software debe ejecutar, y que permite entregar un resultado de valor para un actor (usuario del sistema) en particular. La notación para la elaboración del Diagrama de Casos de Uso será la definida por UML – Unified Modeling Language o similares herramientas de modelación de flujos, se deberá elaborar: diagrama de flujo de datos, diagrama entidad relación, diccionario de datos. • El oferente pasará a la fase de Construcción y Pruebas una vez la Policía Nacional valide y apruebe toda la fase de Gestión, Planeación y Diseño del Proyecto a través de los formatos establecidos por la Policía Nacional o del oferente. <p>CONSTRUCCIÓN Y PRUEBAS:</p> <ul style="list-style-type: none"> • Construcción, pruebas y aceptación: Culminar la construcción del producto de software, aplicar pruebas funcionales y técnicas (atributos de calidad) para verificar su correcto comportamiento, aplicar protocolos de aprobación, aceptación y puesta en operación del software construido, El propósito del plan de pruebas es explicitar el alcance, enfoque, recursos requeridos, cronograma y calendario, responsables y manejo de riesgos de un proceso de pruebas, verificación, validación y certificación y deberá garantizar y asegurar que el sistema cumpla con los requerimientos funcionales y desempeño; así como, con los
--	--

		estándares (diseño, construcción documentación) y facilidad de mantenimiento.	
IMPLANTACIÓN:			
2.		ITEM 1: PLATAFORMA PARA WEBINT-OSINT-DEEPWEB	
2.1		Herramienta de búsquedas en fuente abierta que permita administrar usuarios, realizar búsquedas específicas, búsquedas compuestas, generar alertas, crear casos y búsquedas por temáticas, y que a su vez esta búsqueda permita correlacionar los eventos anteriormente consultados y emplear diferentes tipos de filtros como por ejemplo tiempo, ubicación, temática, palabras clave, a partir de la información pública disponible.	
2.2		<p>El Sistema debe permitir al analista definir cualquier tema y monitorear dinámicamente la actividad de las redes sociales y de mensajería instantánea que cuentan con links públicos como Facebook, Telegram, Twitter, Instagram. La plataforma podrá incorporar otras fuentes gracias a su modularidad.</p> <p>De igual manera, debe dar solución a los siguientes requerimientos:</p> <ul style="list-style-type: none"> - Información relevante sobre una publicación, hashtag, comentario, imagen o video que haya sido publicada en alguna red social, así: <ul style="list-style-type: none"> o Primera cuenta en haber generado la publicación. o Impacto y reacciones de la publicación. o Listado de las cuentas que mayor interacción y dinamización han generado. o Geolocalización de las cuentas en función de la información OSINT de las fuentes. o Cuentas más influyentes (que generen más impacto debido a su cantidad de seguidores). o Debe permitir hacer filtros por palabras clave de los comentarios generados. <p>Dicha información deberá ser mostrada de una forma intuitiva, gráfica y amigable para el operador de tal manera que:</p> <ul style="list-style-type: none"> - El operador pueda personalizar de forma visual y dinámica el dashboard de la operación. - Que pueda compartir ese dashboard con otros analistas o para otras operaciones o fuentes de información. - Que el dashboard sea dinámico e interactivo, logrando filtrar o personalizar la vista haciendo click en cualquiera de sus elementos. <p>Con la posibilidad de generar alertas sobre publicaciones, hashtags, identidades y sobre patrones de comportamiento que el analista pueda crear para caracterizar fenómenos o tipos de entidades dentro de la información pública disponible colectada.</p>	
2.3		Usuarios concurrentes mínimos	300 usuarios para búsquedas de entidades y 30 usuarios de sistema completo
2.4		Creación de usuarios	Ilimitados
2.5		Creación de casos	Ilimitados

	2.6	Consultas por usuario	Ilimitados- usuarios concurrentes 300	
	2.7	El sistema no debe tener limitaciones en la cantidad de fenómenos monitoreados y poder monitorear simultáneamente los casos.		
	2.8	Integración de fuentes no estructuradas (Excel, Word, PDF, PowerPoint, CSV, JPG, VGA, Multimedia y demás formatos que se requieran).		
	2.9	Extracción de datos de fuentes HTML públicas.		
	2.10	El sistema deberá permitir y suministrar tecnología de simulación de acciones y actividades humanas, actividades aleatorizadas, creación de bots durante la fase de obtención o colección de las fuentes abiertas.		
	2.11	El sistema debe de ser escalable e interoperable con otros software en y/o aplicaciones en el entendido que no existan conflicto de licencias o protocolos internos de seguridad y exclusividad.		
	2.12	<p>Debe contener como mínimo los siguientes módulos:</p> <p>Módulo Consulta de entidad: búsqueda y recolección de información relacionada con eventos y entidades.</p> <p>Módulo Administración y Gestión: gestión de perfiles de usuario, contenido y seguridad del sistema.</p> <p>Módulo Análisis de relaciones: este módulo debe mapear de las redes sociales los tipos de entidades disponibles en las mismas, como amigos, seguidores, interacciones, ubicaciones, organizaciones, y así mismo generar filtros para los datos extraídos.</p> <p>Creación y gestión de casos: con este se administrará la búsqueda relacionada con casos puntuales.</p> <p>Módulo de alertas: el contratista deberá garantizar que la plataforma permita configurar búsquedas teniendo en cuenta temáticas, períodos de tiempo, palabras clave, datos, entidades, así como la generación de alertas basada en palabras clave, fechas y tareas programadas. Así mismo, deberá generar una alerta en el evento que dos o más usuarios del sistema concurrentes estén consultando o hayan consultado el mismo dato.</p> <p>Módulo de agentes: administración y gestión de cuentas de navegación.</p> <p>Módulo de informes y reportes: el analista podrá configurar de forma dinámica el dashboard de explotación de la información para generar los informes de manera personalizada.</p> <p>Módulo de georreferenciación: integración con capacidades de GIS (información geográfica), sincronización en tiempo real con la visualización de cartografía en vivo, así como visualización de eventos, actividades y datos en el mapa.</p>		
	2.13	El sistema debe contar con procesamiento del lenguaje natural (Natural Language Processing), el cual debe aprender de acuerdo al idioma que se habla y la ontología propia administrada.		
	2.14	La visualización de la plataforma debe ser amigable de forma tal, que su visualización sea en lenguaje natural (no en lenguaje de código); con el fin que el usuario final pueda entenderla fácilmente.		
	2.15	Debe contener un diseño gráfico amigable, interactivo, liviano y con imagen institucional (Policía Nacional), para lo cual el contratista debe presentar como mínimo 3 propuestas para que el supervisor del contrato realice la elección en cuanto a personalización de colores además de que la plataforma debe poder ser configurada de forma		

	dinámica por el analista para elegir cómo desea ver representada la explotación de la información de cada operación.
2.16	El contratista entregará un cronograma de pruebas necesarias para lograr la aprobación técnica y funcional del sistema a implementar.
2.17	<p>Debe tener como mínimo los siguientes motores de recolección de datos para:</p> <ul style="list-style-type: none"> - Páginas web estáticas. - Motores de recolección basados en RSS. - Motores basados en navegadores. - Motores basados en API de sitios web. - Motores basados en API de flujos. <p>Se dará un listado inicial de 5 fuentes de información pública expuesta a internet para integrar mediante el desarrollo de una API o el método más apropiado para cada una de ellas e integración en la plataforma. Estas fuentes se podrán ir ampliando de acuerdo la necesidad dentro de periodo de implementación.</p> <p>En caso de contar con Motores de búsqueda para aplicaciones móviles, debe integrarlo a la solución.</p>
2.17.1	El sistema deberá permitir la creación independiente de algoritmos / rastreadores (crawlers) que automaticen la navegación web humana.
2.17.2	Los nuevos crawlers deben cargarse fácilmente en el sistema tras la creación, sin necesidad de reiniciar el sistema.
2.17.3	El crawler deberá ejecutar un script personalizado durante su ejecución, que incluye: Una entrada y salida predefinidas.
2.17.4	El operador debe poder usar algoritmos personalizados, independientemente de su método de búsqueda.
2.17.5	El operador debería ser capaz de crear crawlers personalizados que recopilen información las fuentes definidas para el sistema incluidas TOR y Darknet.
2.17.6	El sistema debe admitir la recolección del contenido publicado por la entidad de las Redes Sociales, los detalles biográficos y las interacciones sociales (likes, shares, comments, friends) cuando estén disponibles públicamente.
2.17.7	El sistema debe admitir la recolección de los amigos y/o seguidores de la entidad en redes sociales, mediante la aplicación de flujos de derivación, cuando estén disponibles públicamente. Además, deberá permitir recolectar la información de entidades en segundo nivel si la estructura y relaciones está bajo naturaleza OSINT.
2.17.8	El sistema debe admitir la recolección de información pública de un grupo, incluidos: miembros, información, publicaciones, interacciones, comentarios y recursos compartidos.
2.17.9	El sistema debe permitir el acceso a grupos de Facebook utilizando cuentas de navegación del sistema dedicados, que ingresarán al grupo y recopilarán la información pública.
2.17.10	El sistema debe permitir el acceso a los canales públicos de Telegram y otras aplicaciones de mensajería instantánea, utilizando cuentas de navegación del sistema dedicados, que ingresarán al canal y recopilarán la información.

	2.17.11	El sistema debe admitir como elemento de escalabilidad la futura creación de crawlers, que extraigan datos de cualquier fuente web pública navegable, incluidos foros, blogs, redes sociales, además de los ya incorporados como alcance del proyecto.	
	2.17.12	El diseñador del crawler debe permitir al operador solicitar una captura de pantalla de un elemento específico en la página web o de toda la página web.	
	2.17.13	El sistema debería permitir al administrador, cargar automáticamente un número ilimitado de cuentas de navegación al sistema desde un archivo CSV.	
	2.17.14	El sistema debe proporcionar una extensión de navegador que permita al usuario navegar usando la identidad de la cuenta de navegación de manera consistente a su huella digital. Adicionalmente, el sistema deberá evaluar el nivel de credibilidad y operatividad de la cuenta de navegación y mostrarlo de forma gráfica, con el fin de que se logre la credibilidad máxima del mismo y su salida a operación o proporcionar salida de las cuentas de navegación a internet para la verificación de la información a consultar.	
	2.17.15	El sistema debe implementar solución tecnologica que permita reducir el riesgo de suspensión de cuenta y bloqueo de la cuenta de navegación.	
	2.17.16	El sistema debe implementar un mecanismo de simulación acción humana.	
	2.17.17	El sistema debe tener un mecanismo de retención de cookies para aumentar la credibilidad de identidad de la cuenta de navegación.	
	2.17.18	El operador podrá establecer definiciones de recolección programadas para que se ejecuten en intervalos fijos, estableciendo sus parámetros de programación.	
	2.17.19	El operador elegirá una cuenta de navegacion específica entre una lista de cuentas registradas, cuando el rastreador (crawler) requiera inicio de sesión o autenticación de API.	
	2.18	Las búsquedas podrán realizarse de manera textual, simple o avanzada: soportando operadores boléanos (selección múltiple, operadores como AND/OR/EXCLUDE), comodines, búsqueda semántica. Además, esta opción avanzada de filtros podrá ser realizada en un entorno gráfico y visual, en tiempo real, sobre toda la información mostrada al operador.	
	2.19	El sistema debe permitir, ingresar y actualizar la ontología propia identificada.	
	2.20	<p>PUNTOS DESTACADOS:</p> <p>Admisión de múltiples unidades distribuidas de búsqueda (cuenta de navegacion, bot) trabajando simultáneamente.</p> <p>Compatibilidad las Darknets (específicamente Tor, Ip2P y Freenet).</p> <p>Navegador web incorporado, que permita extracción sencilla del contenido.</p> <p>Tener una función para que las cuentas de navegación tengan un ambiente propio que minimice los riesgos en caso de recibir un ataque cibernético.</p> <p>Paquete incorporado de flujos que soporte la mayor cantidad de redes sociales, blogs y plataformas de debates.</p>	
	2.21	Módulo Consulta de entidad:	
	2.21.1	Debe permitir la búsqueda por entidad con los siguientes parámetros, en fuentes públicas:	

	<p>Nombres y apellidos. Número de identificación. Pasaporte. Nick name en redes sociales. Dirección, ubicación y/o lugar.</p> <p>Debe permitir la búsqueda por organización con los siguientes parámetros, en fuentes públicas:</p> <p>Nombre organización. Página web. Número de Identificación Tributaria (NIT). Nick name en redes sociales. Dirección, ubicación y/o lugar.</p> <p>La información recolectada deberá estar en un formato editable y permitir su actualización automática a solicitud del operador.</p>	
2.21.2	<p>El resultado de la búsqueda de fuente pública disponible debe arrojar de manera organizada los siguientes datos:</p> <ul style="list-style-type: none"> 13. Nombres de usuario (como está registrado o guardado en las diferentes redes sociales y demás plataformas). 14. Id o identificador de usuario en redes sociales. 15. Imágenes relacionadas con la cuenta, principalmente imágenes de la entidad o etiqueta. 16. Entidades asociadas a la búsqueda. 17. Cuentas en redes sociales sobre las fuentes incorporadas. (por ejemplo, Facebook, Instagram, Twitter) 18. Páginas web relacionadas. 19. Fecha de nacimiento. 20. Ubicación, incluida la actividad de itinerancia. 21. Datos en la Darknet. 22. Organizaciones (lugares de trabajo, educación, relaciones comerciales, entre otros). 23. Ubicaciones y direcciones. 24. Entidades relacionadas, verificación de metadatos: <ul style="list-style-type: none"> 24.1 Fecha cuando se agregó. 24.2 Última actualización. 24.3 Modificado por. 24.4 Creado por. 	
2.21.3	Debe desplegar en una ventana ya sea en la parte inferior o a la izquierda o abrir los sitios web, documentos, o cualquier otra fuente de información asociada.	
2.21.4	<p>La búsqueda por organización, en caso de encontrar una página web, deberá traer los datos del administrador de la misma, disponibles públicamente:</p> <ul style="list-style-type: none"> 8. IP de página. 9. Dominio. 10. Nombre del administrador. 11. Dirección. 12. Correo. 13. Información general. 14. Ubicación. 	
2.22	Módulo Administración y Gestión:	
2.22.1	Gestión de perfiles de usuario del sistema:	

	<p>6. Creación y eliminación de usuario. 7. Creación de roles. 8. Permisos de usuario. 9. Verificación de actividades realizadas 10. Bloqueo de usuario.</p>	
2.22.2	<p>Seguridad</p> <p>4. Generación de auditoría sobre actividades del usuario en la plataforma. 5. Asignación de módulos y permisos sobre fuentes de información. 6. Clasificación de usuarios por perfil.</p>	
2.22.3	<p>Contenido</p> <p>4. Fuentes integradas. 5. Diseño de crawlers. 6. Seguimiento casos.</p>	
2.23	Módulo Análisis de casos y relaciones:	
2.23.1	<p>ANÁLISIS:</p> <p>La pantalla “analizar” deberá ser modular y controlable fácilmente mediante acciones de arrastrar y soltar en pantalla. Esto permitirá a los usuarios centrarse en los elementos deseados en la pantalla, y contendrá las siguientes capacidades:</p> <ul style="list-style-type: none"> • Permitir a los usuarios inspeccionar cada resultado: verlo de forma completa e individual, incluidos los detalles del contenido y los medios archivos adjuntos. • Permitir a los usuarios buscar, recopilar, visualizar y analizar microblogging pública sobre un mapa interactivo basado en sus metadatos geoetiquetados. • Presentación de mapa de calor. Partes del mapa con un mayor grupo de elementos se destacan con mayor intensidad. • Mostrar en una gráfica los hashtags más mencionados en los resultados, los hashtags más relacionados debido a su nivel de menciones compartidas; de igual forma deberá permitir la visualización y análisis de picos de tendencia en líneas de tiempo. • Análisis de sentimiento: Detectar el sentimiento expresado en publicaciones sociales no estructuradas, en idiomas compatibles, y permite a los usuarios filtrar los resultados para mostrar solo contenido positivo, negativo o neutral. • Ubicación de publicación en un gráfico de mapa, visualizando el número de publicaciones geo etiquetadas por país y estado. • Identificar Influenciadores: Detectar quiénes son los influyentes en la interacción. Se mostrará una lista de los usuarios más influyentes. • Detección de bots: Determina si una cuenta de red social es real o falsa. Si una cuenta es clasificada como falsa, el sistema enumera los motivos de esa clasificación, ejemplo: horarios, tiempos de interacción, fecha de uso, temporalidad, correlación con otras redes. 	
2.23.2	Este módulo debe extraer y mapear las redes sociales (entidades) y generar filtros.	
2.23.3	Determinación de relaciones más fuertes.	
2.23.4	Entorno social.	
2.23.5	Relaciones más cercanas.	
2.23.6	Aplicación de filtros.	
2.23.7	Generación de líneas de tiempo de la información.	

	2.23.8	Seleccionar eventos, mensajes o entidades para correlacionar y graficar cronológicamente las relaciones fuertes.
	2.23.9	Debe permitir monitorear actividades, tendencias y patrones de comportamiento de multitudes en el espacio digital. Así mismo, permite la graficación utilizando líneas de tiempo donde se evidencie las interacciones y la utilización de filtros.
	2.24	Módulo de alertas:
	2.24.1	Generación de alertas basados en palabras clave, fechas, y tareas programadas.
	2.24.2	Programar recolección de acuerdo a la programación de búsquedas por palabras.
	2.24.3	Alertas basadas en la búsqueda.
	2.24.4	Alertas por duplicidad de consultas.
	2.25	Módulo de agentes: Administración y gestión de cuentas de navegación.
	2.25.1	La técnica empleada debe ser mediante la creación de entidades o algoritmos de recolección automáticamente.
	2.25.2	Usar las cuentas de navegación ya existentes con las reglas de seguridad y emulación de ubicación.
	2.25.3	Se podrán automatizar, controlar y ejecutar algoritmos. La plataforma analiza los datos colectados utilizando las herramientas y algoritmos analíticos avanzados.
	2.25.4	Poner en cuarentena las cuentas de navegación y los bots.
	2.25.5	Realizar hoja de vida de cada entidad, cuenta de navegación y bot, que contenga como mínimo fecha de creación tipo de contenido publicado.
	2.26	Módulo de georreferenciación:
	2.26.1	Capacidades de GIS (Sistema de Información Geográfica), sincronización en tiempo real con la visualización del mapa en vivo, vista de eventos, actividades y otros datos en el mapa.
	2.26.2	Puede usar la capacidad de ARGIS y ESRI de la Policía Nacional o garantizar que se tenga actualizada la cartografía.
	2.26.3	Graficar ubicaciones de publicaciones, contenidas en la descripción de la entidad y las relacionadas en los comentarios.
	2.27	Módulo de informes y reportes: como mínimo debe permitir la generación de 5 tipos de reportes o que el propio operador pueda diseñar el dashboard para decidir qué incluye en cada reporte de la operación.
	2.27.1	Los reportes deben permitir exportar en Excel, Word y Pdf.
	2.27.2	Debe existir la opción de escoger los campos que se van a visualizar en el reporte.
	2.27.3	Los reportes deben tener una vista de previsualización.
	2.28	TRANSFERENCIA DE CONOCIMIENTOS
	2.28.1	Con el fin de garantizar el funcionamiento, mantenimiento y adicionar desarrollo al Sistema de Inteligencia Artificial, es necesaria la instrucción de mínimo 41 funcionarios del servicio, los cuales deberán tener conocimientos sobre el manejo, gestión y administración del sistema IA, como se describe en el ítem 2.28.2. Esta transferencia de conocimiento deberá ser certificada por el fabricante. Deberá contener al menos temáticas de: 5) Bigdata. 6) Machine Learning. 7) IA.

	8) Métodos de representación gráfica y relaciones de metainformación.
2.28.2	<p>La trasferencia de conocimiento se debe desarrollar en tres (3) grupos, así:</p> <p>Usuario final - recolector: deberá capacitarse a las personas designadas por la Policía Nacional (mínimo 30 funcionarios) en el uso de plataforma con todas sus bondades. Tiempo mínimo para la transferencia de conocimiento (80 horas).</p> <p>Administradores del sistema: dirigida como mínimo a 6 personas quienes tendrán la capacidad de gestionar y administrar servidores, conexiones y la infraestructura de TI (Tecnologías de la información) dispuesta para la plataforma (servidores, switch, firewall). Tiempo mínimo para la transferencia de conocimiento, 80 horas.</p> <p>Entrenador de entrenadores: un módulo de entrenador de entrenadores para 5 personas como mínimo, con el material (videos, ayudas interactivas) los cuales deben quedar con la capacidad de administración del sistemas y uso. Tiempo mínimo para la transferencia de conocimiento, 80 horas.</p>
2.28.3	La accesibilidad de la información del sistema y los servidores deberán ser de acceso exclusivo de los funcionarios de la Dirección de Inteligencia Policial. Cualquier herramienta de telemetría y monitoreo del software deberá ser completamente deshabilitada al exterior de DIPOL.
3.	ITEM 2: INFRAESTRUCTURA
3.1	Los equipos de infraestructura deben ser entregados, instalados y configurados por el contratista.
3.2	GARANTÍA EQUIPOS
3.2.1	Garantía mínima: tres (03) años para todos los ítems, contada a partir de la fecha del acta de recibo a satisfacción por parte del supervisor del contrato.
3.2.2	El contratista debe anexar certificación que indique que los equipos ofrecidos (servidores, switch y firewall con sus componentes) son de un fabricante con representación en Colombia.
3.2.3	El contratista debe anexar certificación de distribuidor autorizado en Colombia del fabricante.
3.2.4	El contratista debe anexar manifestación escrita sobre el tipo de garantía, soporte técnico y garantizar el suministro de repuestos del hardware que compone los servidores, switch y demás componentes por un tiempo no menor a cinco (05) años.
3.2.5	Los servidores deben cumplir como mínimo con certificación EPEAT nivel Bronce, será verificable en la página web EPEAT.
3.2.6	Los servidores deben cumplir con certificación Energy Star. En los servidores se debe identificar la certificación Energy Star, a través de sticker de identificación pegado en el equipo.
3.2.7	La garantía ofrecida por el fabricante deberá tener un control y seguimiento de los tickets generados para los mantenimientos

	<p>correctivos donde se escale a los niveles adecuados para su solución y cierre.</p> <p>El contratista deberá entregar un usuario que permita acceder al sistema de información que soporta la mesa de ayuda o autoservicio (acceso vía web), con el objeto de realizar seguimiento a los casos reportados y tickets generados. El funcionario policial será asignado por el supervisor del contrato.</p> <p>Además, se deberán presentar informes mensuales al supervisor del contrato de los casos reportados a la mesa de servicio del contratista y el estado en que se encuentran.</p>	
3.3	RESTAURACIÓN DE LA MÁQUINA	
3.3.1	<p>El contratista deberá garantizar el soporte para la recuperación de datos, o para la restauración de la máquina a su estado original de fábrica.</p> <p>El contratista deberá entregar un video tutorial que sirva como guía y se evidencie, el paso a paso para realizar la restauración de la máquina a su estado original de fábrica.</p>	
3.4	LICENCIAS Y ACCESORIOS	
	SISTEMA OPERATIVO	
	Considerando el sistema operativo a implementar para la solución (windows ó linux), se deberá entregar el siguiente licenciamiento de acuerdo aL sistema operativo a implementar así:	
3.4.1	<p>Windows : Licenciamiento para los servidores Windows SERVER 2019 64 bits última versión en español para ambiente corporativo; los equipos a entregar deberán tener instalado y funcionando el sistema operativo.</p> <p>Ó</p> <p>Linux: Licenciamiento para los servidores LINUX UBUNTU 18.04 LTS última versión en español para ambiente corporativo; los equipos a entregar deberán tener instalado y funcionando el sistema operativo.</p> <p>Durante el tiempo de la garantía el contratista debe prestar todo el acompañamiento necesario para realizar las actualizaciones de los equipos, cuando se instalen nuevas versiones.</p>	
3.4.2	Considerando que la arquitectura de TI debe ser flexible y deben virtualizarse o crearse servidores virtuales, el contratista debe entregar las licencias necesarias de plataforma usada para la virtualización ya sea VMware vSphere Essentials Plus o Microsoft Hyper-v. o la empleada en el desarrollo de la arquitectura.	
3.4.3	Considerando que la arquitectura de TI debe ser segura y contar con los protocolos de seguridad se debe entregar instalado y fusionando el antivirus para los servidores con Windows Antivirus for servers Microsoft Security Essentials ó el más indicado para la protección de los equipos y el sistema.	
3.5	PATCH CORD	
3.5.1	Suministro Patch Cord categoría 6A de fábrica, UL listado y CSA.	
3.6	SERVIDOR DE APlicACIÓN	
3.6.1	Cantidad.	Tres (03).
3.6.2	Marca.	Especificar.
3.6.3	Modelo.	Especificar.

	3.6.4	Tipo.	Rack.
	3.6.5	Año de fabricación.	Mínimo 2019 última versión (todos los componentes del presente ítem).
	3.6.6	Software.	Los nodos deben ser con procesadores certificados para alta disponibilidad misión-critica, Debe incluir herramienta de virtualización, de gestión de almacenamiento y de administración de la solución
	3.6.7	Fuente de poder	Dos fuentes de poder como mínimo.
	3.6.8	PROCESADOR	
	3.6.8.1	Cantidad de procesadores mínima por nodo.	2 procesadores como mínimo.
	3.6.8.2	Tipo procesador mínimo.	Especificar.
	3.6.8.3	Cantidad de núcleos por procesador mínimo.	16 núcleos.
	3.6.8.4	Frecuencia base mínima.	2.1 Ghz.
	3.6.8.5	Memoria caché mínimo.	22 MB.
	3.6.9	MEMORIA RAM POR NODO	
	3.6.9.1	Capacidad mínima:	8 DIMM cada uno de 32GB, Total Memoria RAM 256GB.
	3.6.9.2	Tipo	DDR4-2666 o equivalente
	3.6.10	ALMACENAMIENTO POR CADA NODO	
	3.6.10.1	SSD mínimo por nodo.	4 SSD de 3.8TB.
	3.6.10.2	Bahías de expansión.	Capacidad mínima de 24 bahías hot-swap
	3.6.10.3	Capacidad	20 TB o superior configurados después de RAID 5 conformado por unidades de estado sólido intercambiables en caliente; este espacio debe estar disponible y no debe hacer parte del disco que se designe para que corra el sistema operativo.
	3.6.10.4	Redundancia.	El equipo ofertado debe permitir configuración correspondiente a las unidades de estado sólido en mínimo RAID 0,1,5,6,10
	3.6.11	CONECTIVIDAD	
	3.6.11.1	Puertos mínimos por nodo.	Dos tarjetas de red 10Gbe para conexión a la red LAN, UN (1) 1Gbe para administración.
	3.7	FIREWALL	
	3.7.1	Marca	Especificar
	3.7.2	Referencia	Especificar

3.7.3	Cantidad	Uno (01)	
3.7.4	Puertos GE RJ45	8 a 16	
3.7.5	Puertos USB	Mínimo 2	
3.7.6	Puerto consola RJ45	1	
3.7.7	Rendimiento mínimo del FIREWALL (IPS THROUGHPUT)	10 Gbps	
3.7.8	Sesiones concurrentes mínimas (TCP):	8 Millones	
3.7.9	Políticas de FIREWALL Mínimo	10.000	
3.7.10	Túneles VPN IPsec de puerta de enlace a puerta de enlace:	2.000	
3.7.11	Túneles VPN Cliente-a-Puerta enlace Ipsec	50.000	
3.7.12	Usuarios concurrentes SSL-VPN (Máximo recomendado)	10.000	
3.7.13	Rendimiento IPS	8 Gbps	
3.7.14	Rendimiento de la inspección SSL	SI	
3.7.15	Certificaciones	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	
3.7.16	Factor de forma Rack	Rack Mount, 1 RU	
3.7.17	Corriente máxima	6A @ 100V; fuente de alimentación 100–240V 50–60Hz	
3.7.18	Consumo de energía (promedio / máximo):	129 W / 244 W	
3.7.19	Disipación de calor:	832 BTU/h	
3.7.20	Temperatura de funcionamiento	32–104°F (0–40°C)	
3.7.21	Humedad	10% - 90% sin condensación.	
3.8	CONECTIVIDAD		
3.8.1	Considerando las actividades de uso del internet, se debe suministrar un canal de internet dedicado, independiente a los canales existentes en la Policía Nacional, con una capacidad de navegación de mínimo 100 MB, por un término de 3 años. En caso de cambio de operador el contratista deberá garantizar el servicio sin ninguna clase de interrupción en la conectividad. Así mismo se debe garantizar en los acuerdos de nivel de servicio que los tiempos de indisponibilidad no superen las 12 horas, y se atiendan los incidentes de conexión con mesa de ayuda 5x8		
3.8.2	Puertos mínimos por nodo.	Dos tarjetas de red de 10Gbe para conexión a la red LAN, UN (1) 1Gbe para administración.	
3.9	SWITCH		
3.9.1	Marca	Especificar	
3.9.2	Modelo	Especificar	
3.9.3	Cantidad	Uno (01)	
3.9.4	CARACTERÍSTICAS		
3.9.4.1	Tipo:	Administrable	
3.9.4.2	Administración:	Capa 3	
3.9.4.3	Calidad de servicio (QoS) soporte:	Si	
3.9.4.4	Energía sobre Ethernet (PoE)	Si	

	3.9.4.5	Capacidad de apilamiento:	(04) Cuatro unidades	
	3.9.4.6	Compatibilidad:	con otras marcas del mercado	
	3.9.4.7	Documentación y Accesorios:	Software de administración. Los necesarios para su instalación y funcionamiento	
	3.9.4.8	QoS (Calidad de Servicio):	Mínimo 8 colas por puerto para control de tráfico y optimización de la red	
	3.9.4.9	Puerto de consola:	Con cable de conexión, RJ45, Serial	
	3.9.4.10	Capacidad de crecimiento mediante software y hardware		
	3.9.4.11	Cantidad de puertos básicos de conmutación RJ-45 Ethernet:	Ptos 48, Tecnología de cableado ethernet de cobre: 10BASE-T,100BASE-T,1000BASE-T, 1GB BASE -T	
	3.9.4.12	Cantidad de puertos SFP+ (10 Gbps):	mínimo 2	
	3.9.4.13	IEEE 802.1Q (VLANs), 802.1X (Security), 802.3ab (Copper Gigabit), 802.3ad (Link Aggregation), 802.3ae (10G Ethernet) ó 802.3bz, 802.3i (10 baseT), 802.3u (fast Ethernet), 802.3x (Flow Control), 802.1p , 802.1w (RSTP) y 802.3z (Fiber Gigabit).		
	3.9.4.14	Integración de red:	Se integra a la Red LAN, lo cual incluye medio de transmisión y conversores de medio.	
	3.9.4.15	Soporte VLAN:	Si, mínimo 128.	
	3.9.4.16	Fuentes de alimentación redundantes		
	3.9.4.17	Memoria interna:	128 MB o superior	
	3.9.4.18	Memoria Flash:	16 MB o superior	
	3.9.4.19	Firmware actualizable:	Si	
	3.9.5	GESTIÓN Y PROTOCOLOS		
	3.9.5.1	SNMP, RMON, IEEE802.1D, SSL y/o SSH, QoS, IPv4, IPv6, Vlans, WEB, ACL		
	3.9.5.2	Protocolos de red compatibles:	HTTP/HTTPS	
	3.9.5.3	El protocolo de conexión entre el servidor y las estaciones de trabajo	será ejecutado a través de conexión web.	
	3.9.5.4	El equipo debe soportar Autenticación vía RADIUS, TACACS + que facilite el control del equipo y restrinja el acceso no autorizado de usuarios que puedan modificar la configuración del mismo.		
	3.10	SWITCH		
	3.10.1	Marca	Especificar	
	3.10.2	Modelo	Especificar	
	3.10.3	Cantidad	Dos (02)	
	3.10.4	CARACTERÍSTICAS		
	3.10.5	Tipo de interruptor:	Administrable	
	3.10.6	Capa del interruptor:	Capa 3	
	3.10.7	Calidad de servicio (QoS) soporte:	Si	
	3.10.8	Energía sobre Ethernet (PoE)		
	3.10.9	Capacidad de apilamiento:	(04) Cuatro unidades	
	3.10.10	Compatibilidad:	con otras marcas del mercado	

	3.10.11	Documentación y Accesorios:	Software de administración. Los necesarios para su instalación y funcionamiento	
	3.10.12	QoS (Calidad de Servicio):	Mínimo 4 colas por puerto para control de tráfico y optimización de la red	
	3.10.13	Puerto de consola:	Con cable de conexión, RJ45, Serial	
	3.10.14	Capacidad de crecimiento mediante software y hardware		
	3.10.15	Cantidad de puertos básicos de conmutación RJ-45 Ethernet:	Ptos 24, conectores RJ-45 para 10BASE-T/100BASE-T/1000BASE-T, 1GB BASE -T, con 4 ranuras Gigabit SFP compartidas	
	3.10.16	Cantidad de puertos SFP+ (10 Gbps):	mínimo 2	
	3.10.17	NORMAS	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3bz ó 802.3z , 802.3x control de flujo, 802.3ad LACP, 802.3af PoE, 802.1d protocolo de árbol de expansión (STP), 802.1Q/p VLAN, 802.1w STP rápida, 802.1s STP múltiple, 802.1X autenticación de acceso a puertos	
	3.10.18	Integración de red:	Se integra a la Red LAN, lo cual incluye medio de transmisión y conversores de medio.	
	3.10.19	Soporte VLAN:	Sí, mínimo 128.	
	3.10.20	Fuentes de alimentación redundantes	Puerto RPS ó similares para conexión a unidad de alimentación redundante	
	3.10.21	Firmware actualizable:	Sí	
	3.10.22	GESTIÓN Y PROTOCOLOS		
	3.10.23	Control de acceso	SNMP, RMON, IEEE802.1D, SSL y/o SSH, QoS, IPv4, IPv6, Vlans, WEB, ACL	
	3.10.24	Protocolos de red compatibles:	HTTP/HTTPS	
	3.10.25	El equipo debe soportar gestión vía:	<ul style="list-style-type: none"> ● Traceroute ● Gestión IP simple ● Seguridad SSL para interfaz de usuario para Internet ● SSH ● RADIUS ● Replicación de puertos ● Actualización TFTP ● Cliente de protocolo de configuración dinámica del servidor (DHCP) ● Cliente Telnet (soporte seguro SSH) 	

	3.11	CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR, Y LICENCIAMIENTOS PARA SOFTWARE A LA MEDIDA (esta cesión de derechos es para los desarrollos a la medida que resulten adicionales contemplados en la solución, haciendo claridad que la Policía Nacional no los usará con fines comerciales).						
	3.11.1	Respecto al software a medida desarrollado, el contratista se obliga a transferir a título gratuito todos los derechos patrimoniales del objeto del contrato a través del documento anexo "CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR" y debe estar debidamente registrado ante la Dirección Nacional de Derechos de Autor Unidad Administrativa Especial del Ministerio del Interior y protocolizado ante notaria. (otorgar licencia a perpetuidad de todos los componentes físicos y lógicos que integren el sistema).						
	3.11.2	El contratista debe registrar el presente contrato en la entidad competente para el Registro de Derecho de Autor y remitir el certificado de inscripción como requisito previo para la suscripción del acta de recibo final a satisfacción y para la realización del último contado de pago correspondiente para cada una de las soluciones desarrolladas y/o mantenimientos implementados.						
	3.11.3	La licencia de funcionamiento será de cubrimiento nacional, ya que generalmente se accederá al sistema de información desde todas las regionales y centros zonales del país.						
	3.11.4	Dada la diversidad de las soluciones que se implementarán, si en alguna de ellas se requiere la incorporación de software base adicional para la construcción o mantenimiento de las aplicaciones, estas deberán ser entregadas a la Policía Nacional, y serán propiedad del mismo a perpetuidad (en caso que aplique).						
	3.11.5	El licenciamiento será a perpetuidad y el mantenimiento por espacio de tres (3) años, contado a partir de la entrega a satisfacción de la solución.						
	3.11.6	El licenciamiento de uso correspondiente será propiedad de la Policía Nacional.						
	3.11.7	El contratista debe anexar como documentos entregables al contrato, el Contrato de cesión de Derechos Patrimoniales de Autor y copia del contrato de cesión que se realizó entre los empleados contratados y la firma contratante donde se transfieren los derechos a la empresa.						
	3.11.8	Los trámites de firmas de notaria por registro de firma y huella de la cesión de derechos patrimoniales no deberán generar costo para la Policía Nacional, y dichos costos serán asumidos por el contratista.						
	3.12	RECEPCIÓN DE LOS BIENES						
	3.12.1	Los equipos serán entregados y probados uno a uno (Procedimientos básicos de encendido, cargue de sistema operativo, reconocimiento de dispositivos instalados, verificación de configuración, instalación de software).						
	3.12.2	A todos los equipos que entregará el contratista se les realizará la prueba de recepción de los bienes para verificar el funcionamiento de los equipos (partes externas e internas).						
<table border="1"> <thead> <tr> <th>PARÁMETRO</th> <th>ACEPTACIÓN</th> </tr> </thead> <tbody> <tr> <td>Revisión Física</td> <td></td> </tr> <tr> <td>Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios</td> <td></td> </tr> </tbody> </table>			PARÁMETRO	ACEPTACIÓN	Revisión Física		Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios	
PARÁMETRO	ACEPTACIÓN							
Revisión Física								
Apertura de cajas respectivamente identificadas, marcadas y verificación del equipo y accesorios								

		entregados: Equipo, Cable de alimentación, Manuales, sello de Energy star(Para servidores)		
		Verificación externa equipo: Sin rayones, roturas o elementos sueltos.		
		Encendido		
		Conexión alimentación AC – Encendido.		
		Componentes internos y externos.		
		Validación componentes internos Herramientas de Sistema.		

NOVEDADES NO CONFORMES

- Verificar que los equipos de cómputos no presenten rayones, fragmentaciones, golpes o abolladuras.
- Comprobar que todos los componentes estén colocados y conectados correctamente.
- La carcasa que recubre la parte interna del equipo de cómputo no debe poseer tornillería.

Los equipos deben ser customizados de fábrica, y no pueden estar ensamblados de manera artesanal en su diseño y carcasa externa, como por ejemplo uniones de la parte externa con tornillería, cables, cintas, conexiones indebidas que afecten la instalación, funcionamiento y operacionalización del componente tecnológico por parte del usuario final.

El contratista deberá tener todos los equipos de medición (hardware y software) necesarios que permitan verificar la capacidad de todos los componentes que conforman el equipo como por ejemplo: fuente, disco duro, memoria, entre otros.

El contratista será el responsable de disponer del personal idóneo, en profesiones de Ingeniería de Sistemas y/o Eléctrica y/o Electrónica y/o Telecomunicaciones y/o técnico en sistemas y/o electrónicos, instalaciones físicas, logística, conexiones, transporte del personal técnico de la Policía Nacional designado por el supervisor de contrato a las instalaciones donde se realizará la prueba y todo lo necesario para realizar la prueba de recepción de los bienes. Los gastos que llegase a generarse con ocasión a las diferentes revisiones y pruebas correrán a cargo del contratista.

Durante el periodo de la prueba de recepción de los bienes, el contratista deberá cumplir con el protocolo de seguridad de instalaciones y seguridad de la información de la Policía Nacional.

3.13

MANTENIMIENTO

3.13.1

El contratista es responsable de realizar los mantenimientos correctivos a todos los equipos de cómputo del presente proceso.

	3.13.2	Es responsabilidad del contratista suministrar toda la logística necesaria para realizar los mantenimientos correctivos de los equipos.	
	3.13.3	Cualquier actividad de mantenimiento correctivo o preventivo del sistema, deberá realizarse en las instalaciones de la Dirección de Inteligencia Policial, teniendo en cuenta y acogiéndose a las políticas de seguridad de la información establecidas en la Policía Nacional.	
	3.13.4	LUGAR DE ENTREGA	
	3.13.4.1	La entrega del hardware, software, licenciamiento de acuerdo con las especificaciones técnicas mínimas requeridas establecidas en el presente estudio previo; se realizará en el almacén de la Dirección de Inteligencia Policial y quedará instalado y funcionando en las mismas instalaciones de la Dirección de Inteligencia Policial.	
	3.13.5	MANUALES	
	3.13.5.1	El contratista deberá entregar toda la documentación técnica de cada uno de los equipos, elementos y periféricos. El contratista deberá entregar los manuales técnicos y de usuario originales de fábrica para operación; con todos sus catálogos de partes, en idioma castellano y/o inglés, debidamente actualizados a la fecha de entrega y correspondiente certificado de suscripción de actualización.	
	3.13.6	GARANTÍA	
	3.13.6.1	Todo el hardware, software y los componentes de la solución deben tener un tiempo de garantía mínimo de tres (3) años, ofrecida por el contratista contado a partir del recibido a satisfacción por parte del supervisor del contrato.	
	3.13.6.2	El tiempo de garantía iniciará a partir del recibo a satisfacción de los elementos por parte del supervisor del contrato, con los equipos instalados y funcionando.	
	3.13.6.3	Durante el periodo de garantía, el proveedor deberá suministrar todos los repuestos de iguales o superiores características a los originales, sin costo alguno para la Policía Nacional – Dirección de Inteligencia Policial.	
	3.13.6.4	Durante el periodo de garantía, el proveedor deberá instalar las actualizaciones de software o versiones que sean lanzadas en el mercado durante la vigencia de la garantía sin costo para la Policía Nacional – Dirección de Inteligencia Policial, así mismo las versiones de firmware con el fin de garantizar el correcto funcionamiento del equipo, previa coordinación con el supervisor del contrato.	
	3.13.7	SOPORTE	
	3.13.7.1	El contratista deberá poner a disposición de la Policía Nacional – Dirección de Inteligencia Policial, de manera permanente, los siguientes medios para el reporte de incidentes: <ul style="list-style-type: none"> • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico. • Número móvil celular de un contacto directo 	
	3.13.7.2	El contratista debe garantizar soporte técnico vía telefónica e Internet, como primer nivel de atención.	
	3.13.7.3	El grupo de soporte del contratista debe garantizar que el ticket del problema tenga un seguimiento adecuado, se maneje rápida y eficientemente, y se lleve a los niveles adecuados hasta su cierre. Además, se debe tener informado constantemente por escrito al	

		supervisor del contrato o quien éste delegue, los progresos en la búsqueda de la solución.
3.13.7.4		Al inicio del contrato se establecerá el procedimiento de solicitud de la garantía y soporte técnico, tanto para el hardware como para el software ofertado.
3.13.7.5		Durante el tiempo de la garantía se debe prestar todo el acompañamiento necesario para realizar las actualizaciones de la solución, cuando se liberen nuevas versiones.
3.13.7.6		Brindar planes de mantenimiento preventivo y correctivo durante la garantía para toda la solución ofertada.
3.13.7.7		El contratista debe recomendar procedimientos operacionales que mitiguen los riesgos de fallas del sistema.
3.13.7.8		Actualizar las versiones de software cuando sean liberadas durante el tiempo de garantía.
3.13.7.9		Realizar mínimo una (1) visita anual de mantenimiento preventivo durante el período de la garantía que incluya la limpieza externa e interna y diagnóstico de los equipos y software adquiridos.
3.13.7.10		Se debe entregar la documentación, usuarios, contraseñas de administración usadas durante las fases de implementación.
3.13.7.11		Especificar los mecanismos de mantenimiento y actualización del software suministrado, los elementos que se cubren, el tiempo en que se actualiza el software y el paquete que incluye la actualización durante el tiempo de garantía.
3.13.7.12		El contratista debe garantizar que el soporte se preste con personal certificado y con experiencia en este tipo de soluciones.
3.13.7.13		Debe garantizarse la corrección de defectos de funcionamiento.
3.13.7.14		Existirá un mecanismo de contacto de urgencia 5x8 además del nivel de servicio ofrecido que deberá ser también 5x8, por parte del proveedor para el mantenimiento correctivo y soporte técnico.
3.13.7.15		Durante el periodo de garantía, el proveedor se compromete a atender las llamadas de mantenimiento correctivo, en un tiempo máximo de dos (2) horas sobre el nivel de servicio contratado.
3.13.7.16		Con el fin de contar con una capacidad de respuesta oportuna y eficiente en cuanto a soporte técnico y asesorías, las instalaciones principales de la empresa contratista, deberá estar ubicada dentro una zona horaria con una diferencia no mayor a 6 horas de la de Colombia (UTC); lo que comprendería las zonas horarias UTC +1, 0, -1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11.
3.13.7.17		Durante el periodo de garantía, el proveedor se compromete a solucionar las fallas presentadas en el sistema dejándolo en perfecto estado de funcionamiento en un plazo máximo de 24 horas.
3.13.7.18		En caso de que la reparación del equipo demore más de setenta y dos (72) horas, el proveedor deberá suministrar en forma inmediata un equipo de soporte de iguales o superiores características durante el tiempo que dure la reparación o reemplazo de la misma.
3.13.7.19	INFORME MENSUAL	Durante los tres (3) años de garantía, el contratista mensualmente deberá entregar informe (físico y medio digital) al supervisor del contrato en el que se describa como mínimo los siguientes campos:
3.13.7.20		<ul style="list-style-type: none"> • El informe debe estar rotulado con el nombre y logo de la compañía. • Fecha. • Ciudad.

	<ul style="list-style-type: none"> • Centro de servicio. • Número de contrato. • Serie del equipo. • Modelo. • Número del reporte que genera Help Desk para la atención de los requerimientos. • Número total de equipos a los cuales se le realizó los correctivos. • Número de correcciones o incidentes con el software. • Tipo de falla. • Dispositivo o módulos del software que presentó la falla. • Número de fallas. • Describir el correctivo del componente tecnológico reparado, reemplazado. • Nombre del funcionario que reportó el incidente. <p>Nota: el modelo del informe debe ser presentado al supervisor del contrato para su aprobación, durante la apertura del acta de inicio.</p>
3.14	ENTREGA SOLUCIÓN Y COMPONENTES
3.14.1	<p>A partir de la entrega total de la plataforma se empezará a contar la garantía del licenciamiento y garantías del hardware. El Contratista debe entregar para el recibo a satisfacción de la plataforma lo siguiente:</p> <ul style="list-style-type: none"> - Documentación donde se incluyan diagramas de componentes de hardware y software y la planeación de la capacidad (incluye plataforma, almacenamiento, respaldos, red). - Documentación donde se incluya información de niveles de disponibilidad y la guía de operación para la plataforma implementada. - Documentación de buenas prácticas en el mantenimiento y administración de la arquitectura definida. <p>Documentación técnica y de usuario final donde describa en su totalidad y en forma detallada la solución instalada, con el fin de permitir futuras modificaciones o reinstalación de toda la plataforma.</p>
3.15	CERTIFICADOS
3.15.1	El oferente anexará a su oferta carta firmada por el representante legal en la cual conste que cuenta con centros de atención o convenios con centros de atención en Colombia autorizados por el fabricante de los equipos.
3.15.2	El oferente anexará certificación expedida directamente por el fabricante en donde garantice el suministro de repuestos de los equipos ofertados por un término mínimo de cinco (5) años, después del recibido a satisfacción por parte del supervisor del contrato.
3.15.3	El contratista se compromete con la Policía Nacional – Dirección de Inteligencia Policial, cuando el supervisor lo requiera, a entregar certificado de disposición final de los elementos técnicos cambiados a los equipos en aplicación de la garantía durante el tiempo de la misma, a excepción de los dispositivos de almacenamiento los cuales por política de seguridad de la información, la Policía Nacional hará la disposición final de los mismos, cumpliendo con la normatividad ambiental vigente y entes de control (Ministerio del Medio Ambiente y/o autoridad ambiental competente).
4.	NIVEL ACADÉMICO DEL PERSONAL

		<p>Se requiere el personal en las cantidades mínimas, con el perfil profesional, para desempeñarse en el proyecto como se describe en la siguiente tabla:</p> <table border="1"> <thead> <tr> <th>CANTIDAD/PERFIL</th><th>NIVEL ACADÉMICO</th></tr> </thead> <tbody> <tr> <td>1 Gerente de proyecto.</td><td> <p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. <p>Los estudios de pregrado y posgrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> </td></tr> <tr> <td>4.1.1</td><td> <p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico, con conocimientos en sistemas operativos especialmente Windows y Linux. o equivalentes o afines en función de país de titulación..</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente, - Copia diploma o acta de pregrado. - Certificación en "Installation, Storage, and Compute with Windows Server". - Certificación en Linux. <p>Los estudios de pregrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> <p>NOTA: en caso de no cumplir una sola persona con todas las certificaciones exigidas, el oferente podrá suplir el requerimiento con otra persona, adjuntando igualmente el perfil profesional y experiencia solicitada para cada caso que aplique.</p> </td></tr> <tr> <td></td><td>2 Ingenieros con conocimientos en desarrollo.</td><td>Ingeniero de sistemas y/o ingeniero de software y/o ingeniero de desarrollo y/o ingeniero electrónico especialista o magíster en desarrollo</td></tr> </tbody> </table>	CANTIDAD/PERFIL	NIVEL ACADÉMICO	1 Gerente de proyecto.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. <p>Los estudios de pregrado y posgrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p>	4.1.1	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico, con conocimientos en sistemas operativos especialmente Windows y Linux. o equivalentes o afines en función de país de titulación..</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente, - Copia diploma o acta de pregrado. - Certificación en "Installation, Storage, and Compute with Windows Server". - Certificación en Linux. <p>Los estudios de pregrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> <p>NOTA: en caso de no cumplir una sola persona con todas las certificaciones exigidas, el oferente podrá suplir el requerimiento con otra persona, adjuntando igualmente el perfil profesional y experiencia solicitada para cada caso que aplique.</p>		2 Ingenieros con conocimientos en desarrollo.	Ingeniero de sistemas y/o ingeniero de software y/o ingeniero de desarrollo y/o ingeniero electrónico especialista o magíster en desarrollo
CANTIDAD/PERFIL	NIVEL ACADÉMICO										
1 Gerente de proyecto.	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico y especialista o magíster en gerencia de proyectos o similares, y/o MBA y/o Dirección de empresas y con formación continuada en gerencia de Proyectos, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. <p>Los estudios de pregrado y posgrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p>										
4.1.1	<p>Ingeniero de sistemas y/o informático y/o telecomunicaciones y/o electrónico, con conocimientos en sistemas operativos especialmente Windows y Linux. o equivalentes o afines en función de país de titulación..</p> <p>Deberá anexar el oferente los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente, - Copia diploma o acta de pregrado. - Certificación en "Installation, Storage, and Compute with Windows Server". - Certificación en Linux. <p>Los estudios de pregrado deben haber sido cursados en institución educativa debidamente acreditada por el ministerio de educación (tener registro SNIES o su equivalente en caso de ser realizado en una institución fuera del país).</p> <p>NOTA: en caso de no cumplir una sola persona con todas las certificaciones exigidas, el oferente podrá suplir el requerimiento con otra persona, adjuntando igualmente el perfil profesional y experiencia solicitada para cada caso que aplique.</p>										
	2 Ingenieros con conocimientos en desarrollo.	Ingeniero de sistemas y/o ingeniero de software y/o ingeniero de desarrollo y/o ingeniero electrónico especialista o magíster en desarrollo									

		<p>de software, o equivalentes o afines en función de país de titulación.</p> <p>Deberá anexar los siguientes documentos para verificar el nivel académico y perfil profesional del personal que ejecutará el proyecto.</p> <ul style="list-style-type: none"> - Copia de la tarjeta profesional vigente. - Copia diploma o acta de grado pregrado. - Copia diploma de especialización o maestría. 	
		<p>NOTA 1: en caso de que el personal inicialmente contratado deba ser cambiado por otra persona, ésta deberá contar con las mismas características mínimas académicas, descritas en la tabla anterior.</p> <p>NOTA 2: el personal profesional que sea designado para las fases del desarrollo del proyecto, deberá ser el que se relacione en el contrato; así mismo, deberá cumplir con el perfil profesional mencionado en el presente ítem, y asegurar que durante su ejecución se procure por mantener la continuidad del mismo, a fin de evitar traumatismos.</p> <p>En caso de realizarse cambios de personal profesional, se debe garantizar que el profesional reemplazante, ostente la formación académica igual o superior, a la establecida en el contrato.</p>	
4.1.2		<p>Con el fin de cumplir con el objeto contractual del proceso, se requiere que el personal solicitado cumpla con el desempeño y dedicación más adelante relacionado, desde el inicio del contrato hasta la finalización del mismo.</p>	

		levantamiento de información para los temas referentes al codesarrollo de los componentes de software ofertados.	
4.1.3	Conforme al numeral anterior, el contratista deberá estimar la cantidad de personal necesario, que permita dar cumplimiento al objeto contractual del presente proceso en los tiempos establecidos para la ejecución del mismo.		
4.1.4	La Dirección de Inteligencia de la Policía Nacional, se reserva solicitar el cambio de personas vinculadas al proyecto por parte del contratista, en cualquier momento a partir de la suscripción del contrato y el cual deberá ser sustituido por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta del presente proyecto.		
4.1.5	El contratista deberá solicitar por escrito a la Dirección de Inteligencia de la Policía Nacional, autorización para reemplazar a cualquier integrante del equipo de trabajo mínimo requerido, igualmente debe presentar al supervisor del contrato un plan de entrenamiento entre la empresa y el funcionario entrante, con el fin de garantizar la continuidad en la ejecución de las actividades a cargo.		
4.1.6	El contratista deberá realizar reuniones semanales con el supervisor del contrato para verificar los avances estipulados en el plan de trabajo inicialmente aprobado y programar nuevas tareas, durante la duración del mismo, con el fin de revisar, evaluar y sugerir mejoras en la ejecución.		
4.1.7	El equipo de trabajo designado por el contratista, debe contar con todo el equipo logístico requerido para la ejecución del presente proyecto, equipos de cómputo con sus respectivas herramientas licenciadas, personales y/o del contratista, la Dirección de Inteligencia de la Policía Nacional, suministrará el espacio físico necesario para desplegar ambientes de trabajo necesarios para el proyecto en las instalaciones de la Dirección de Inteligencia de la Policía Nacional, Avenida Boyacá No. 142A-55.		
4.2	EXPERIENCIA DEL PROPONENTE		
4.2.1	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 43231500 y/o 43211500 y/o 43232400 y/o 81111800, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 3.584,42 S.M.M.L.V., de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
4.2.1.1	Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el contratista deberá anexar máximo cinco (5) certificaciones de contratos (una certificación por contrato) celebrados y ejecutados durante los años 2017 y/o 2018 y/o 2019, con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL" y/o "BIG DATA"y/o "MACHINE LEARNING" y/o "CIENCIA DE DATOS" y/o "VENTA o IMPLEMENTACIÓN INFRAESTRUCTURA DE TI", que hayan sido ejecutados y terminados, y cuya suma o valor		

		<p>individual sea igual o superior al 70% del presupuesto oficial asignado.</p> <p>En caso que la empresa haya implementado este tipo de soluciones bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia específica a través de un documento certificado ante un notario, en el cual se especifique los valores de los contratos celebrados y ejecutados durante los años 2017 y/o 2018 y/o 2019, 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 "SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL" y/o "BIG DATA" y/o "MACHINE LEARNING" y/o "CIENCIA DE DATOS" y/o "VENTA o IMPLEMENTACIÓN INFRAESTRUCTURA DE TI".</p> <p>NOTA: La certificación de experiencia en "VENTA o IMPLEMENTACIÓN DE INFRAESTRUCTURA DE TI" no podrá superar el 20% del total de la experiencia exigida.</p>							
4.2.2		<p>EXPERIENCIA DEL PERSONAL Y CERTIFICACIONES: con el fin de garantizar el cumplimiento del objeto contractual, se requiere que el personal gerencial y técnico cumpla con la experiencia de acuerdo a lo establecido en el Decreto Ley 0019 del 2012 (Ley Anti trámites) artículo 229 donde establece que "la experiencia profesional se computará a partir de la terminación y aprobación del pensum académico de educación superior", igualmente el oferente debe anexar certificaciones solicitadas en la siguiente tabla:</p> <table border="1"> <thead> <tr> <th>CANTIDAD/PERFIL</th><th>EXPERIENCIA/CERTIFICACIONES</th></tr> </thead> <tbody> <tr> <td>1 Gerente de proyecto.</td><td> <p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p> </td></tr> <tr> <td>1 Ingeniero con conocimientos en sistemas operativos.</td><td> <p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . </td></tr> </tbody> </table>	CANTIDAD/PERFIL	EXPERIENCIA/CERTIFICACIONES	1 Gerente de proyecto.	<p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>	1 Ingeniero con conocimientos en sistemas operativos.	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . 	
CANTIDAD/PERFIL	EXPERIENCIA/CERTIFICACIONES								
1 Gerente de proyecto.	<p>Deberá presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones expedidas donde demuestre la participación de proyectos informáticos. - Certificar experiencia mínima de tres (03) años, en gerencia de proyectos informáticos, adjuntando las certificaciones respectivas. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>								
1 Ingeniero con conocimientos en sistemas operativos.	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación en proyectos con referencia a la instalación, configuración de sistemas operativos Windows o Linux . 								

		<ul style="list-style-type: none"> - Certificar experiencia mínima de tres (03) años, laborados en lo referente a instalación y mantenimiento de sistemas operativos Windows o Linux. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>
	2 Ingenieros con conocimientos en desarrollo	<p>Deberán presentar hoja de vida y los siguientes documentos:</p> <ul style="list-style-type: none"> - Tres (03) certificaciones, donde demuestre la participación de proyectos de desarrollo. - Certificar experiencia mínima de tres (03) años, en proyectos de desarrollo Python o java o visual studio, adjuntando las certificaciones respectivas. - Certificar experiencia mínima de dos (02) años participación conocimiento y soporte en el desarrollo de las plataformas ofertadas igual o similar al sistema de Ciberinteligencia Basado e Inteligencia artificial ó plataformas de OSINT, DARKNET Y DEEPWEB durante los años 2017 y/o 2018 y/o 2019, anexando a su propuesta certificación expedida por la firma donde se desarrolló el proyecto. <p>Para efectos de verificar la experiencia de los empleados, deberá presentar certificaciones de las entidades, las cuales debe contener como mínimo los siguientes aspectos:</p> <p>A-Nombre o razón social del contratante. B-Nombre o razón social del contratista. C-Nombre del Ingeniero que participó en el desarrollo tecnológico. D-Descripción del ítem contratado. E- Fecha de Inicio y Fin del Contrato. F-Valor del contrato. G-Concepto cumplimiento del contrato.</p>
4.3	SISTEMA AMBIENTAL	
4.3.1	El fabricante y el representante del fabricante en Colombia para los computadores y todos sus componentes, certificará que cumple con lo estipulado en la Resolución 1512/2010 expedida por el Ministerio de Ambiente, Vivienda y Desarrollo Territorial "Por la cual se establecen los Sistemas de Recolección Selectiva y Gestión Ambiental de Residuos de Computadores y/o Periféricos y se adoptan otras disposiciones. (Anexar certificación en la oferta).	

	4.3.2	Informar si la empresa presenta sanciones vigentes en el registro único de infractores ambientales (RUIA) del Ministerio de Ambiente y Desarrollo Sostenible por el concepto que se va a contratar, la cual se encuentra disponible en la página web de la Agencia Nacional de Licencias Ambientales ANLA www.anla.gov.co , (Link: "trámites y servicios", luego click en "RUIA" y escoger la opción "RUIA VITAL").	
	4.3.3	Cumplir con la normatividad ambiental vigente nacional para reducir los aspectos e impactos ambientales asociados a la actividad.	
	4.3.4	El contratista deberá garantizar que los equipos eléctricos cumplan con normas técnicas de eficiencia energética, es decir, que tengan un bajo consumo de energía y que cuenten con opciones de encendido, hibernación y apagado en los equipos que aplique y entregarán al supervisor del contrato las fichas técnicas de los equipos a adquirir.	
	4.3.5	El contratista deberá garantizar que todo el material que se entregue a la unidad policial sea en forma digital, se realice en un medio reutilizable; los escritos deberán estar ajustados de acuerdo a la Directiva Presidencial 04 de 2012 "política cero papel".	
	4.3.6	El contratista deberá aplicar las buenas prácticas ambientales, participar de los programas y campañas ambientales, así como las demás exigencias que se establezcan en el Sistema de Gestión Ambiental, en todas las actividades que realice durante la prestación del servicio dentro de la instalación policial.	
	4.3.7	Cualquier infracción ambiental por omisión de permisos, concesiones o licencias ambientales que hubiese sido necesario tramitar antes del inicio del contrato, en el transcurso y después de la actividad del proceso, serán asumidas como responsabilidad del oferente o futuro contratista.	
	4.4	SEGURIDAD Y SALUD EN EL TRABAJO	
	4.4.1	<p>En cumplimiento al Decreto 1072 del 26/05/2015 y con el fin de dar continuidad a políticas de SG-SST de la Policía Nacional, el oferente debe certificar que los funcionarios presentados en la oferta económica quienes van cumplir las distintas actividades solicitadas en el anexo No. 2 especificaciones técnicas, cumplen con los siguientes aspectos:</p> <ul style="list-style-type: none"> • Entregar los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal contratado que ejecutará la tarea contratada, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación y nivel de la cobertura del riesgo, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada. • Deberá evidenciar objetivamente que cumple en su totalidad con los requisitos legales establecidos en el artículo 2.2.4.6.28 del Decreto 1072 de 2015, en relación con sus dependientes y contratistas durante toda la ejecución contractual. • Evidenciar objetivamente la activa participación en las actividades que la Policía Nacional o el contratante desarrolle en materia de promoción y prevención de riesgos laborales. • Evidenciar objetivamente, el uso continuo y permanente de los elementos de protección personal, durante la ejecución contractual, acorde a los peligros y riesgos relacionados con la tarea contratada. • Notificar a la mayor brevedad, al supervisor del contrato, la ocurrencia de incidentes, accidentes de trabajo o el diagnóstico de 	

	<p>enfermedades laborales, así como las condiciones de peligro que detecte durante la ejecución de la actividad contratada.</p> <ul style="list-style-type: none"> Para el ingreso de los visitantes, usuarios o el personal que se autorice para el uso de espacios en los centros de trabajo e instalaciones de la Policía Nacional, estos deberán participar previamente en una capacitación en seguridad y salud en el trabajo, diseñada por la Policía Nacional y/o el centro de trabajo respectivo, acorde a la normatividad vigente y donde se evidencien los riesgos identificados previamente en el centro de trabajo y las actividades del plan de emergencias y el plan de evacuación de la unidad policial. 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. El contratista deberá garantizar que durante la ejecución de las obras se disponga de un kit de emergencias que permita la adecuada y oportuna atención ante posibles accidentes laborales. Solo podrá acceder a los espacios de los centros del trabajo, previamente autorizados y delimitados, según la priorización del riesgo y deberá permanecer únicamente en el espacio delimitado y autorizado, no podrá acceder a espacios críticos en materia de seguridad, o lugares abiertos o cerrados donde se puedan producir eventos de alto riesgo en la integridad del visitante o usuario.
4.5	SEGURIDAD DE INSTALACIONES
4.5.1	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física de las instalaciones policiales y Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional (resolución 08310 del 28/12/2016).
4.6	SEGURIDAD DE LA INFORMACIÓN
4.6.1	<p>El contratista acatará los controles establecidos para la seguridad de la información en la Dirección de Inteligencia Policial, así como la firma del compromiso de reserva y la aplicación de los estudios de credibilidad y confiabilidad.</p> <p>para ello el personal que realice la instalación, configuración de equipos y sistemas, deberá someterse a un estudio de confiabilidad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato. En el evento de no cumplir dicho estudio algunas de las personas vinculadas a este proyecto, el contratista deberá realizar el cambio de estas personas por otras que también deberán someterse al estudio de confiabilidad requerido.</p>
4.6.2	<p>Cláusula de Confidencialidad: Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el transcurso del proyecto, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata, se considera también información confidencial: a) aquella que como conjunto o por la configuración o estructuración exacta de sus componentes, no sea generalmente conocida entre los expertos en los campos correspondientes. b) la que no sea de fácil acceso, y c) aquella información que no esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su</p>

		carácter confidencial, duración. El acuerdo regirá durante el tiempo que dure el proyecto, derechos de propiedad, toda información intercambiada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso, modificación o terminación. El acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.
	4.6.3	Confidencialidad e integridad de la información institucional: Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la preservación de la integridad y confidencialidad de la información institucional a la cual llegare a tener acceso directamente o por intermedio de terceros; en tal virtud, adoptará todas las medidas que sean necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida y suscribirá con la entidad los formatos de confidencialidad o reserva a que haya lugar.
	4.6.4	En virtud del presente contrato, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del futuro contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de la labor. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información para lo cual deberá diligenciar el formulario establecido por la entidad contratante.
	4.6.5	El manejo de toda la información de arquitectura del sistema se considera CONFIDENCIAL, de manera que los planos, diseño, manuales técnicos y cualquier otro tipo de información estarán limitados únicamente a la interventora o supervisión. El suministro de copias para otras personas o entidades deberá ser solicitada a la DIRECCIÓN DE INTELIGENCIA DE LA POLICÍA NACIONAL.
	4.7	PRESENTACIÓN DE LA OFERTA
	4.7.1	Las propuestas se harán en forma clara y en idioma español. Deberán presentar la carta de representación del fabricante o de distribuidor autorizado donde se indique su nombramiento por lo menos por el tiempo de ejecución del contrato, tiempo de garantías.
	4.7.2	La propuesta presentada, deberá ser firmada y avalada por un ingeniero electrónico y/o de sistemas, y/o electricista y/o telecomunicaciones anexando tarjeta profesional, como lo indica el ARTÍCULO 20 de la LEY 842 DE 2003 "PROPUESTAS Y CONTRATOS. Las propuestas que se formulen en las licitaciones y concursos abiertos por entidades públicas del orden nacional, seccional o local, para la adjudicación de contratos cuyo objeto implique el desarrollo de las actividades catalogadas como ejercicio de la ingeniería, deberán estar avalados, en todo caso, cuando menos, por un ingeniero inscrito y con tarjeta de matrícula profesional en la respectiva rama de la ingeniería."
	4.7.3	Se deben anexar todas las fichas técnicas de los equipos de hardware ofertados.
	4.7.4	Las ofertas deben estar debidamente numeradas y relacionar al frente de cada especificación la página donde se encuentra el documento soporte.

ANEXO No. 8
JUSTIFICACIÓN DEL MARGEN MÍNIMO (LANCE)

1 FORMA DE ADJUDICAR.

La adjudicación del presente proceso de selección se ejecutará de manera total.

2 PROCEDIMIENTO DE ADJUDICACIÓN – SUBASTA

Teniendo en cuenta que el proceso de selección es "selección abreviada - bienes y servicios de características técnicas uniformes y de común utilización", la adjudicación se realizará por subasta inversa electrónica.

El porcentaje base para la puja será el siguiente:

DESCRIPCIÓN	PRESUPUESTO OFICIAL	PORCENTAJE LANCE MÍNIMO
ADQUISICIÓN SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	\$ 4.498.699.800	2%

JUSTIFICACIÓN MARGEN MÍNIMO

1- El valor del precio de cada lance deberá hacerse en forma TOTAL. 2- Al precio base unitario, el oferente deberá hacer lances, en menor precio, con el fin de mejorar el valor unitario de su oferta. 3- El valor mínimo de cada lance hecho por los oferentes, no podrá ser inferior al 2% del valor total.

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.

CRITERIOS DE DESEMPEATE

En cumplimiento a lo dispuesto en el Artículo 2.2.1.1.2.2.9., del Decreto 1082 de 2015, en caso de presentarse empate de dos o más ofertas, se tendrán en cuenta, en cuanto sean aplicables, los siguientes criterios de desempate para adjudicar el proceso, así: 1 Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros. 2 Preferir las ofertas presentada por una Mipyme nacional. 3 Preferir la oferta presentada por un consorcio, unión temporal o promesa de sociedad futura siempre que: (a) esté conformado por al menos una Mipyme nacional que tenga una participación de por lo menos el veinticinco por ciento (25%); (b) la Mipyme aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y (c) ni la Mipyme, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del consorcio, unión temporal o promesa de sociedad futura. 4 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 consorcio, unión temporal o promesa de sociedad futura, 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.

5 Si persiste el empate, la Entidad convocará a una audiencia de sorteo mediante mensaje público, y se seleccionará en orden de elegibilidad mediante el procedimiento de sorteo por balotas al oferente que obtenga el mayor número.

En cualquier caso, los factores de desempate contenidos en los numerales 1 al 3 se aplicarán de conformidad con el párrafo 1 del artículo 1 de la Ley 816 de 2003.

ANEXO No. 9
CONTRATO CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR

Entre los suscritos a saber _____, mayor de edad, domiciliado en _____, identificado como aparece al pie de su firma, obrando como representante legal de (Datos del funcionario que delegue el señor Director de la Policía Nacional), quien en adelante se denominará el CESIONARIO, y _____, mayor de edad domiciliado en _____, identificado como aparece al pie de su firma, quien en adelante se denominará el AUTOR-CEDENTE, han convenido en celebrar el siguiente contrato de cesión de derecho de autor, sujeto al siguiente clausulado:

PRIMERA. OBJETO: el AUTOR-CEDENTE transfiere de manera total y sin limitación alguna al CESIONARIO los derechos patrimoniales que le corresponden sobre el(los) sistema(s) de información o software _____, por el tiempo que establezca la ley nacional e internacional y sin perjuicio del respeto al derecho moral consagrado en el artículo 11 de la Decisión Andina 351 de 1993 concordante con el artículo 30 de la Ley 23 de 1982.

SEGUNDA. REMUNERACIÓN: el valor del presente contrato es gratuito, teniendo en cuenta que sobre el Software_____ la Policía Nacional realizó un contrato de compra venta para adquirir el bien.

TERCERA. CONDICIONES Y LEGITIMIDAD DE LOS DERECHOS: por virtud de este contrato, el AUTOR-CEDENTE garantiza que es propietario integral de los derechos de explotación del(los) software y en consecuencia garantiza que puede contratar y transferir los derechos aquí cedidos sin ningún tipo de limitación por no tener ningún tipo de gravamen, limitación o disposición. En todo caso, responderá por cualquier reclamo que en materia de derecho de autor se pueda presentar, exonerando de cualquier responsabilidad al CESIONARIO; por lo tanto, se debe anexar copia del contrato de cesión de transferencia que fue pactada entre los funcionarios contratados y la empresa _____ denominada en el presente contrato como AUTOR-CEDENTE.

CUARTA. FORMALIDADES: como quiera que por virtud del presente contrato se transfiere el derecho de autor, este documento deberá ser reconocido ante notario público, y para tener validez ante terceros, deberá inscribirse en la Oficina de Registro de Derecho de Autor, como lo ordena el artículo 183 de la Ley 23 de 1982.

Dado en Bogotá, D.C., a los _____ () días del mes de _____ de dos mil _____

EL CESIONARIO

EL AUTOR-CEDENTE

ANEXO No. 10
REQUISITOS PROPUESTAS CONJUNTAS
INDICADORES FINANCIEROS A EVALUAR

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

Nota 1: Ponderación de los componentes de los indicadores

En esta opción cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador de acuerdo con su participación en la figura del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

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: los resultados de los indicadores se trabajan con dos decimales. Si los oferentes presentan los gastos de intereses en cero (0), no podrán calcular el indicador de razón de cobertura de intereses. Por lo tanto cumplen con el indicador, salvo que la utilidad operacional sea negativa, caso en el cual no cumple con el indicador de razón de cobertura de intereses.

NOTA: Para efecto de verificar la capacidad patrimonial y 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, el cual debe contener la información financiera a corte 31/12/2019 (en firme).

FORMULARIO No. 1
ACUERDO DE CONFIDENCIALIDAD

El(los) suscrito(s) a saber: (nombre del representante legal de la sociedad, asociación o persona jurídica contratista, o nombre del representante legal del consorcio o unión temporal contratista) 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 de la sociedad, del consorcio, de la unión temporal, o de la asociación contratista, 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 OFERENTE**, manifiesta(n) su voluntad de asumir, de manera unilateral, el presente compromiso, dentro dela invitación teniendo en cuenta las siguientes consideraciones:

PRIMERO: Que **LA POLICÍA NACIONAL** adelanta un proceso de contratación para la celebración de un contrato estatal para “SISTEMA INTEGRADO PARA EL ANÁLISIS DE CONTRABANDO”.

SEGUNDO: Que **EL OFERENTE** 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, y como tal estará marcado como confidencial.

CLAUSULA PRIMERA. COMPROMISOS ASUMIDOS.

EL CONTRATISTA, mediante suscripción del presente documento, asume los siguientes compromisos con relación a la información confidencial:

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. **EL OFERENTE** se obliga a extender la obligación de confidencialidad a sus empleados, agentes, asesores o consultores que haya involucrado, involucre o llegare a involucrar en la ejecución de las actividades que le correspondan para el cumplimiento del objeto del **CONTRATO**, antes de compartir con ellos cualquier información confidencial de **LA POLICÍA NACIONAL**.
7. **EL OFERENTE** mantendrá una lista de usuarios de **LA INFORMACIÓN CONFIDENCIAL** que será entregada a **EL OFERENTE** cuando ella 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. No usar **LA INFORMACIÓN CONFIDENCIAL** de modo que pueda ser de alguna manera, directa o indirectamente, perjudicial para los intereses de **LA POLICÍA NACIONAL**.

11. 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**.
12. Cumplir con la confidencialidad en las mismas condiciones y formas, y con el mismo cuidado con que realiza la protección de su **propia** información confidencial.

Representante Legal contratista

Nombre:

Documento Identidad

**FORMATO No 1
CATALOGACIÓN**

Para la **ADQUISICIÓN DE UN (01) SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL**, objeto del presente contrato.

El contratista proporcionará a **LA DIRECCIÓN DE INTELIGENCIA POLICIAL**, una lista de artículos necesaria para la identificación de los artículos de abastecimiento incluidos en el objeto del contrato, y en el plazo de dos meses (2), a partir de la fecha de formalización del contrato. Esta lista incluirá: la identidad del fabricante verdadero y el número de pieza/referencia y nombre o designación con que dicho fabricante identifica cada artículo objeto del contrato; cuando se trate de equipos, conjuntos o sistemas que hayan de ser mantenidos por la organización logística usuaria, se incluirán los repuestos acordados como necesarios para asegurar el servicio operativo de los mismos y, además, cuantos documentos de carácter técnico suficiente se requieran por ser necesarios para establecer y controlar los datos de identificación de los artículos.

El contratista proporcionará, a **LA DIRECCIÓN DE INTELIGENCIA POLICIAL** en el plazo de un mes (1), la documentación técnica que defina las características físicas y funcionales de aquellos artículos de abastecimiento objeto del contrato, de conformidad con los lineamientos citados por el Grupo de Catalogación de Defensa y, adicionalmente, las que puedan estar especificadas en el Pliego de Condiciones Técnicas del contrato.

A los efectos anteriores, el contratista será responsable de obtener de sus subcontratistas o proveedores, los datos técnicos necesarios para la identificación de los artículos a catalogar procedentes de estas fuentes, así como de la presentación en plazo de estos datos y/o de las propuestas de identificación correspondientes en el objeto para la **ADQUISICIÓN DE UN (01) SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL**. Si los artículos provienen de un país OTAN o apadrinado nivel Tier 2, el contratista deberá suministrar los números OTAN de Catalogo (NOC), relacionados con los artículos objeto del contrato.

El contratista proporcionará a **LA DIRECCIÓN DE INTELIGENCIA POLICIAL**, la información técnica correspondiente a las modificaciones, cambios en el concepto o diseño, que se le realicen al artículo de abastecimiento durante la vida del contrato.

El contratista acreditará el cumplimiento de la cláusula de catalogación, mediante un certificado expedido por él agente contratante **LA DIRECCIÓN DE INTELIGENCIA POLICIAL**, el cual certificará la entrega total de la información de acuerdo a los lineamientos establecidos por el Grupo de Catalogación de Defensa y el Pliego de Condiciones Técnicas del contrato. 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.

*Este formato está sujeto a cambios por parte de la Oficina de Catalogación del Ministerio de Defensa Nacional.

Nombre y Firma del Representante Legal



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCIÓN DE INTELIGENCIA POLICIAL

MINISTERIO DE DEFENSA POLICÍA NACIONAL	
Unidad:	_____
Radicado No:	_____
Recibido por:	_____
Fecha:	_____ Hora: _____

No / DIPOL-ARPIN – 29

En cumplimiento al numeral 8 del artículo 2.2.1.1.2.1.1 del Decreto 1082 del 26 de mayo de 2015, se certifica que una vez verificados por el responsable de Comercio Exterior de la Dirección de Inteligencia Policial, certifica que una vez verificados en la página web de Colombia Compra Eficiente y en la del Ministerio de Comercio, Industria y Turismo, los Acuerdos Comerciales y Tratados de libre Comercio (TLC), negociados por Colombia en los capítulos de contratación pública, se estableció que la ADQUISICIÓN SISTEMA DE CIBERINTELIGENCIA BASADO EN INTELIGENCIA ARTIFICIAL PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL, por valor de CUATRO MIL CUATROCIENTOS NOVENTA Y OCHO MILLONES SEISCIENTOS NOVENTA Y NUEVE MIL OCHOCIENTOS PESOS M/CTE (\$ 4.498.699.800,00); SI está cuberto bajo las obligaciones de carácter internacional derivadas de los Acuerdos: ALIANZA DEL PACÍFICO, CANADÁ, CHILE, COREA, ESTADOS AELC, ESTADOS UNIDOS Y COSTA RICA, MÉXICO, TRIÁNGULO NORTE Y UNIÓN EUROPEA; toda vez que:

- a) La cuantía del proceso excede los umbrales establecidos en los acuerdos publicados
- b) La Policía Nacional se encuentra incluida en los listados de entidades cubiertas de los acuerdos.
- c) Los bienes y/o servicios a contratar no se encuentran cubiertos bajo alguna exclusión de aplicabilidad o excepción.

De acuerdo a lo anterior, se debe tener en cuenta los principios y obligaciones en cuanto a la protección de los principios de derecho internacional, la publicidad de las contrataciones, el uso de medios electrónicos, las modalidades de contratación y la revisión de impugnación en la configuración de los documentos del proceso contractual.

Capitán MAGDA ESTEFANY PAPAMIJA BEDOYA
Estructurador Estudio Previo

