No. GS-2023 021843 -ARPIN-GUCIB

Bogotá D.C, 04 AGO 2023

Coronel
Jorge Hernán Orozco Castaño
Director de Inteligencia Policial (E)

ASUNTO: informe de supervisión del contrato compra No. 04-2-10006-2023

TIPO DE INFORME

PERIÓDICO_X_ O FINAL ___

Periodo del informe de supervisión

Desde	01/06/2023	**Hasta**	30/06/2023

En cumplimiento a los artículos 83 y 84 de la Ley 1474 de 2011 "*Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública*", así como de la Resolución No.03049 del 30 de julio del 2014 "*Por la cual se adopta el Manual de Contratación de la Policía Nacional*", Resolución No. 00090 del 15/01/2018, "*Por la cual se actualiza, modifica y complementa el Manual de Contratación de la Policía Nacional adoptado mediante Resolución No. 03049 de 2014*", y la *"Guía para el ejercicio de las funciones de Supervisión e Interventoría de los contratos del Estado*" expedida por Colombia Compra Eficiente, o las normas que las modifiquen, adicionen o sustituyan, sin perjuicio de las funciones establecidas contractualmente y aquellas inherentes a la naturaleza del ejercicio de la supervisión, me permito presentar el correspondiente informe del contrato u orden de compra del asunto a través del cual se detalla, el seguimiento y el grado de cumplimiento de las obligaciones establecidas en el respectivo contrato u orden, así:

INFORMACIÓN GENERAL:

- Comunicación oficial No. GS-2023-009695 - DIPOL del 05/04/2023, el señor (a) Subintendente, Hamilton de Jesús Velázquez Collazos, jefe Grupo Contratos (E), notificó como supervisor del contrato 04-2-10006-2023 al señor teniente coronel, Wilson Alejandro Muñoz Gómez.

- El 5 de mayo de 2023, mediante 005 SUBIN-ARPIN 2.18, el señor teniente coronel Oscar Leonel Ochoa Sanchez, asume el cargo de Jefe Área Producción de Inteligencia, y por ende asumió como supervisor del contrato 04-2-10006-2023

- **Periodicidad establecida para la entrega del informe de supervisión:** Mensual

- **No. de informes de supervisión presentados y publicados en SECOP II:** Tres (3).

Información del contrato u orden de compra

Contrato No. / Orden de compra No.	04-2-10006-2023
Objeto del Contrato / instrumento de agregación de la orden de compra	ADQUISICIÓN SISTEMA INTELIGENCIA DE AMENAZAS EN LA RED

Contratista	CONSORCIO INTELIGENCIA DE AMENAZAS
Representante legal	HUMBERTO DE JESÚS VÉLEZ CASTRO
Valor inicial del contrato u orden de compra	$ 3.990.200.000,00
Valor adiciones del contrato u orden de compra	No aplica
Valor total del contrato u orden de compra	$ 3.990.200.000,00
Plazo de ejecución inicial	15 julio de 2023
Fecha de inicio del plazo de ejecución del contrato u orden de compra	05/04/2023
Fecha de terminación del plazo de ejecución del contrato u orden de compra (pactada inicialmente)	15 julio de 2023
Fecha de inicio del plazo de ejecución de la(s) adición(es)	No aplica
Fecha de terminación del plazo de ejecución de la(s) adición(es)	No aplica
Adiciones	No aplica
Modificatorios	No aplica
Prorrogas	No aplica
Otros	No aplica

1. DESARROLLO DE LA SUPERVISIÓN AL CONTRATO U ORDEN DE COMPRA

1.1 Acciones adelantadas:

Acta de inicio 115 SUBIN-ARPIN 2.21 Que Trata sobre inicio de contrato N° 04-2-10006-2023 "Adquisición sistema inteligencia de amenazas en la red" para la dirección de inteligencia policial de fecha 11/04/2023.

Transferencia de conocimiento sobre el sistema adquirido, la cual se certifica mediante comunicación oficial del 24/04/2023 firmado por el señor representante legal Humberto de Jesús Vélez Castro CONSORCIO INTELIGENCIA DE AMENAZAS.

Se realiza el despliegue del sistema de inteligencia de amenazas en el grupo de Ciberinteligencia compuesto por "Software inteligencia de amenazas en la res y Servidor inteligencia de amenazas en la red", en los días comprendidos 14/04/2023 al 24/04/2023.

EL 24 de abril de 2023, mediante acta No 135-subin-arpin-2.21 QUE TRATA SOBRE LA VERIFICACIÓN CUMPLIMIENTO REQUERIMIENTOS TÉCNICOS DEL CONTRATO NO 04-2-100006-2023 "ADQUISICIÓN

SISTEMA INTELIGENCIA DE AMENAZAS EN LA RED", PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL, se validó y verificó el cumplimiento del contrato en mención.

El 04/05/2023 se realizó el recibo a satisfacción de bienes o servicios objeto del contrato, perfeccionado mediante la firma del supervisor del contrato y el representante legal de la empresa.

El 16/05/2023 se generó ordene de pago presupuestal No 146467123.

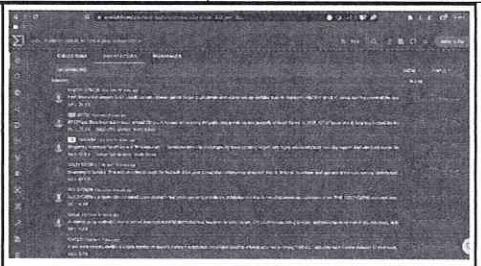
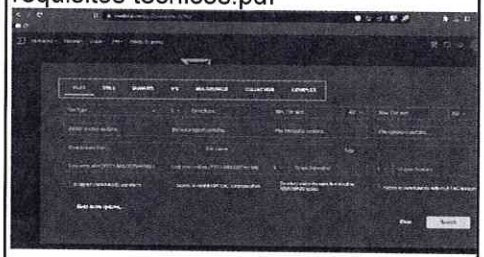
2. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES

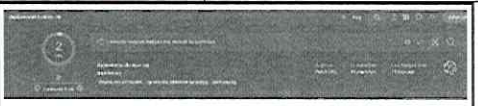
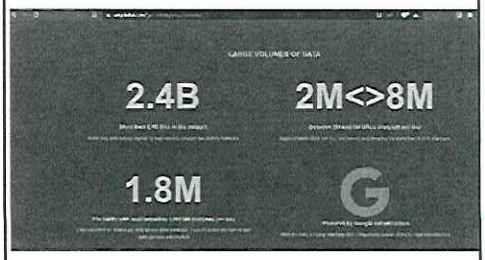
CUMPLIMIENTO OBLIGACIONES LEGALES DEL CONTRATISTA

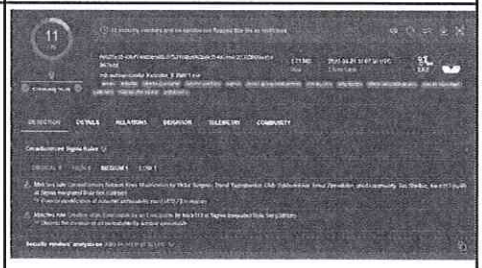
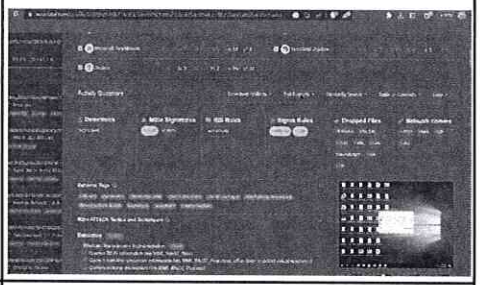
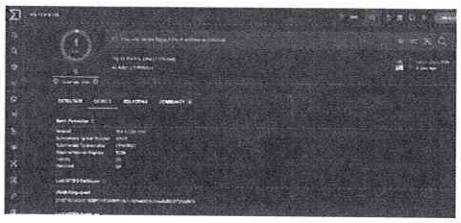
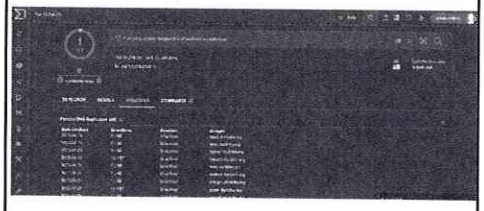
OBLIGACIONES DEL CONTRATISTA LEGALES	CUMPLIÓ	OBSERVACIONES
Ejemplo: cumplir cabalmente con sus obligaciones, frente al sistema de seguridad social, parafiscales, (cajas de compensación familiar, SENA e ICBF) …	SI	Se hace entrega de la planilla integrada de autoliquidación de aportes con No. 9449563045 (Cyber Sec Mnemo) – (9449614559 Mnemo Colombia).

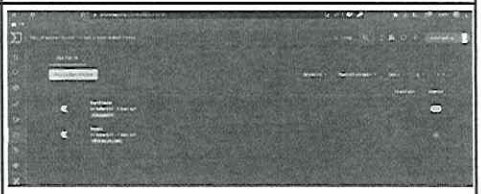
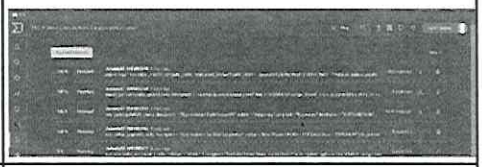
CUMPLIMIENTO ESPECIFICACIONES TÉCNICAS

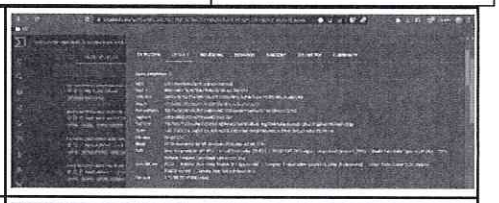
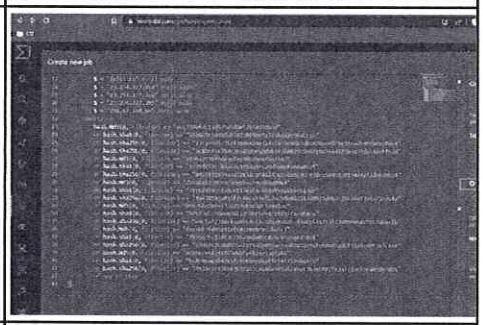
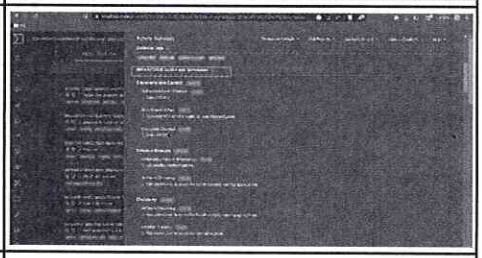
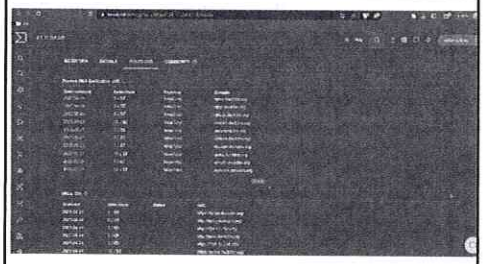
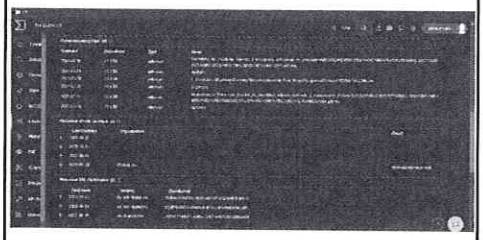
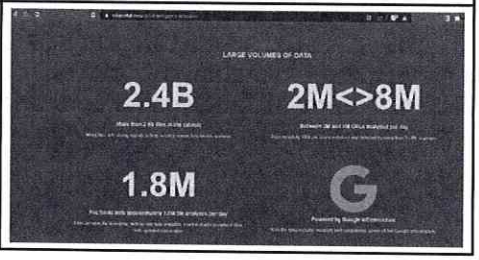
ÍTEM	ESPECIFICACIONES TÉCNICAS MÍNIMAS	CUMPLIÓ	OBSERVACIONES
1.	**SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED**		
1.1	Contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: la actividad de actores, malwares activos, alertas de actividades de amenazas e informes analizados por inteligencia. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con (a) direccionamiento IP Colombiano. Los datos, aunque en primera medida deben estar enfocados al direccionamiento IP Colombiano también deberá traer en su dashboard, información relacionada con ciberamenazas que se presente de otros direccionamientos IP pero que puedan afectar el direccionamiento IP colombiano. La información debe ser recopilada de los centros de ciberinteligencia del oferente y esta debe tener como mínimo, lo siguiente: • URL o direcciones IP maliciosas Origen • Perfil de actor • Motivaciones, malware asociado	Si	Referente servicio de inteligencia de amenazas, Ver documento "1. VT - Referente en servicios de inteligencia de ciberamenazas.PDF" IOC direccionamiento colombiano, ver documento "2. VT - IoCs desde IP colombiana y descarga de ficheros.pdf"  

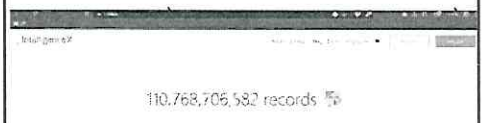
	• Descarga de malware (junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, impacto.) • Phishing • Comando y control • Spammer El oferente debe estar referenciado como referente en servicios de inteligencia de ciberamenazas, para lo cual debe presentar los soportes e informes que lo acrediten. En caso de ser líder del sector, se aceptan estudios de Forrester o Gartner, en los cuales debe estar claramente definido "inteligencia de ciberamenazas en la red" o similares. Junto con la propuesta se deberá anexar un documento emitido por casa matriz, en el cual se observe la correlación entre indicadores de compromiso del direccionamiento IP colombiano y que permita la descarga de archivos sospechosos, así como el cumplimiento de las demás especificaciones técnicas solicitadas en el presente proceso. Lo anterior deberá ser soportado con un acceso web que evidencie lo descrito en el documento.		
1.1.1	El oferente debe hacer entrega de un certificado de casa matriz en el que se **certifique** que la herramienta ofertada para la inteligencia de amenazas cumple con todos los requerimientos técnicos solicitados. Por lo anterior, el oferente debe especificar la marca de la herramienta a ofrecer, así: Marca: **VIRUS TOTAL**	Si	El contratista realizó la entrega de los soportes al comité técnico los cuales reposan en los documentos entregados en la oferta (SECOP II).
1.2	El sistema deberá permitir realizar búsquedas de las ciberamenazas mínimo con los siguientes parámetros, así: • Máscaras y URL Maliciosas • Hashes MD5 • Direcciones IP El sistema debe en detalle entregar información referente a Reputación de IP: conjunto de direcciones IP con un contexto que cubre hosts sospechosos y malintencionados	Si	Certificado cumplimiento requerimientos técnicos, Ver documento "3. VT - Cumplimiento requisitos técnicos.pdf" 

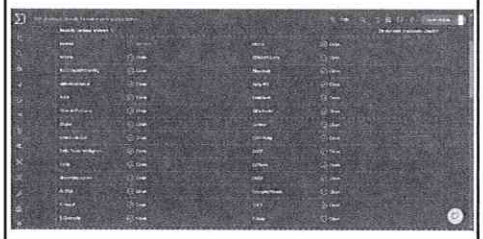
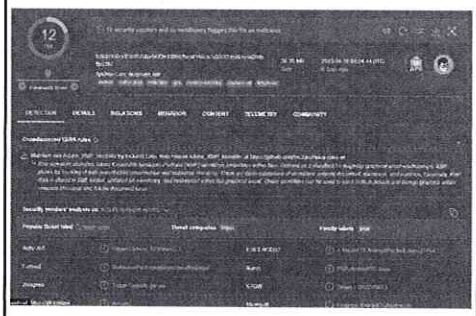
	Direcciones URL maliciosas: conjunto de direcciones URL formado por enlaces y sitios web malintencionados. En los cuales se pueda buscar en registros enmascarados y no enmascarados. Direcciones URL de phishing: conjunto de direcciones URL identificadas por la ciberinteligencia de la casa matriz como sitios de phishing. En los cuales se pueda buscar en registros enmascarados y no enmascarados. Direcciones URL de C&C de malware: conjunto de direcciones URL de servidores de comando y control (C&C) y objetos malintencionados relacionados. Hashes de malware móvil: conjunto de hashes de archivos para detectar objetos malintencionados que infectan plataformas móviles. Fuente de datos sobre malware: conjunto de hashes de troyanos con su contexto correspondiente para detectar troyanos para dispositivos móviles que cargan cobros a los usuarios móviles y que además permiten a un atacante robar, eliminar y responder mensajes. Direcciones URL de C&C móviles de botnets: conjunto de direcciones URL con contexto que contempla servidores C&C móviles de botnets. Investigaciones Manuales: La interfaz web debe permitir búsquedas y descargas manuales, para realizar análisis profundo de muestras y obtener indicadores adicionales, por medio de otras herramientas. Adicionalmente el oferente debe tener foros, redes sociales y contenido web, en los que se traten temáticas en tendencia de CTI.		  
1.3	El sistema ofertado debe tener como mínimo lo siguiente, esto con el fin de contar con la mayor cantidad de información relacionada con ciber inteligencia que permita anticiparse a la posible materialización de amenazas en el direccionamiento IP Colombiano o con relación a este, así: • Una red de seguridad propia de identificación de amenazas, de la cual el oferente debe anexar un soporte con la cantidad de fuentes de las cuales	Si	Fuentes de datos, Ver documento "4. VT - Fuentes de datos.pdf" 

	recopilan información. Esto se debe anexar junto con la oferta • Partners de seguridad, enumerar en la propuesta cuales son. • Identificación de C&C o Botnets		
1.4	El sistema debe garantizar la confiabilidad de la inteligencia de amenazas, entregando siempre un contexto (detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados, impacto.) y permitir la definición de un puntaje (score) producido por algoritmos machine learning para transmitir la confianza de un indicador es benigno o malicioso. En donde 0 se considera benigno de alta confianza y 100 es maliciosos de alta confianza, según la escala de medición.	Si	 
1.5	La inteligencia de amenazas se debe generar automáticamente y en tiempo real. Este debe tener como insumo de hallazgos a nivel mundial (mínimo en 100 países, esto debe ser soportado con una certificación de la casa matriz), información recopilada de la red de identificación de amenazas de la casa matriz que se presente en la oferta.	Si	Ver documento "6. VT - Información generada en tiempo real desde todo el mundo.pdf"
1.6	El sistema debe entregar unos datos enriquecidos con el fin de dar más contexto a la inteligencia de amenazas relacionadas con: • Whois • DNS • GeoIP • Hosting • Atributos de archivos • Datos estadísticos y de comportamiento • Cadenas de descarga El sistema de inteligencia de amenazas debe contar con una infraestructura altamente tolerable a fallas, garantizar	Si	 

	disponibilidades del sitio web de 99,99% al año.		
1.7	El sistema de inteligencia de amenazas debe utilizar técnicas de Threat Hunting, que hace referencia al proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.		 
1.8	El sistema de inteligencia de amenazas debe permitir crear reglas YARA de forma automática y configurar alertas que permitan la detección en tiempo real, de comportamientos que coincidan con dichas reglas. De igual forma debe permitir exportar las reglas YARA, para ser integradas en herramientas en herramientas SANDBOX propias. Adicionalmente debe permitir personalizar los reportes emitidos por la herramienta. De igual forma además que se cuenta con un acceso a nivel web, este debe permitir tener acceso a través de API, para integrar de forma programática todo el conjunto de datos y automatizar flujos de trabajo, como también el enriquecimiento de alertas basados en los indicadores de compromiso identificados, desplegables a herramientas perimetrales (SIEM, Firewall, SOAR, entre otros).	Si	
1.9	El sistema de inteligencia de amenazas debe contar con un proceso de inspección y afinamiento el cual debe utilizar técnicas de preprocesamiento, como criterios estadísticos, sistemas de sandboxes, motores de heurística, herramientas de similitud y perfiles de comportamiento.	Si	

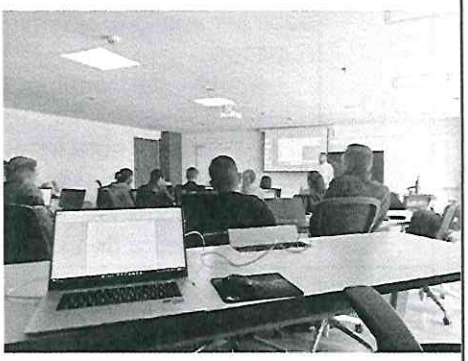
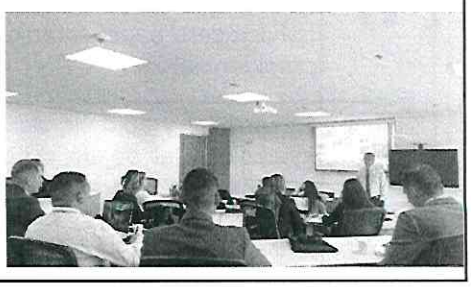
			
1.10	El sistema de inteligencia de amenazas deberá permitir realizar búsquedas históricas hasta de un año atrás, de igual forma deberá poder definir etiquetas o registros sobre cada una de las alertas enviadas, donde se evidencia, hora, fecha, comentario y usuario que realizó la gestión de la alerta de ciberinteligencia.	Si	
1.11	El Sistema debe estar actualizado y configurado para detectar tácticas y técnicas enumeradas en el marco MITRE ATTACK, de igual forma los insumos de información deberán poderse categorizar en amenazas estratégicas, operacionales o tácticas.	Si	
1.12	El sistema debe contar con correlación avanzada que involucre técnicas de analítica y/o *data science* para determinar tendencias o patrones anormales en el direccionamiento IP Colombiano. Adicionalmente, el sistema debe permitir configurar alertas de acuerdo con la necesidad del administrador, por ejemplo (alertas sobre direcciones IP específicas, dominios específicos, cyber crime, hacktivismo, entre otros). La herramienta debe mapear visualmente la correlación entre los indicadores de amenaza (archivos, URLs, dominios, IPs, entre otros. No se aceptan soluciones que requieran previamente un listado de archivos, URLs, dominios o IPs para su funcionamiento.	Si	 
1.13	El Sistema deberá permitir consumo de inteligencia de amenazas de fuentes públicas y por suscripción	Si	

1.14	La interfaz web del Sistema debe contar con una interfaz Web GUI compatible con navegadores estándares tales como Chrome, EDGE, Firefox/Mozilla, Safari entre otros.	Si	Si, cumple 
1.15	El sistema deberá permitir el acceso a diferentes tipos de reportes a través de la consola basada en GUI, sin uso de SQL por parte del usuario.	Si	
1.16	El sistema debe contar con lo siguiente: • Acceso a la fuente de datos INTELX-IntelligenceX, la cual permita realizar búsquedas con un motor de búsqueda sobre archivos de datos global, alimentado desde múltiples fuentes, inclusive la dark web, durante todo el periodo de mantenimiento y soporte • Acceso a la fuente de datos Shodan, incluyendo la capacidad de búsqueda por vulnerabilidad, monitoreo y escaneo de hasta 65.000 direcciones IP, durante todo el periodo de mantenimiento y soporte • Debe tener selectores de búsqueda específicos como email, dominios, URL, dirección IP, entre otros. • Debe permitir realizar consulta de datos expuestos por cibercriminales, producto de ciberataques a los sistemas informáticos de las entidades. • Debe permitir identificar cuentas gubernamentales comprometidas en las filtraciones de datos llevadas a cabo por ciberdelincuentes, entre otras capacidades. • En caso de que la funcionalidad integrada sea descontinuada, se debe establecer junto con el supervisor del contrato las opciones para ser reemplazada.	Si	 

1.17	El sistema de inteligencia de amenazas debe contar adicionalmente con las siguientes características. • Realizar solicitudes de análisis de ficheros con un conjunto de, al menos, 70 motores antivirus distintos, y recuperación de los resultados de dichos análisis. Estos resultados deben incluir información sobre el análisis propiamente dicho, como el fichero analizado o la fecha, y sobre cada motor antivirus utilizado (nombre del motor, versión, fecha de actualización de firmas, alias o nombre de la amenaza identificada). • Permitir la descarga de los ficheros almacenados en el repositorio en base a su hash (MD5, SHA1 o SHA256) para que se puedan realizar procesamientos o análisis personalizados de los mismos. • Permitir consultas de información del comportamiento de ficheros en entornos aislados con base a su hash (MD5, SHA1 o SHA256). • Permitir la realización de búsquedas de ficheros con base a diferentes propiedades de los mismos (nombre, contenido, tamaño, cabeceras, tipo de fichero, firma digital, etc.), las detecciones de los antivirus, características estáticas, patrones de comportamiento y otros metadatos. • Contar con filtros de selección como país desde donde se adjuntó el archivo sospechoso, rango de fechas, cantidad de interacción con dominios o direcciones IP, palabras, entre otros, con el fin de identificar amenazas de forma específica.	Si	  
2	**SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED**		
2.1	El oferente debe entregar un servidor de aplicación con las siguientes características:		Servidor DELL con número de serie JH2LCW3
2.2	Cantidad: uno (01)	Si	Se recibe equipo hardware tipo servidor con las especificaciones pactadas en el contrato el cual son:

			Marca: DELL, Modelo PowerEdge R650
2.3	**Marca: DELL**	Si	Se recibe con satisfacción equipo hardware tipo servidor con la marca descrita en el contrato: **Marca DELL**
2.4	**Modelo: PowerEdge R650**	Si	Se recibe con satisfacción equipo hardware tipo servidor con modelo descrito en el contrato: **PowerEdge R650.**
2.5	Tipo: Rack	Si	Cumple con las especificaciones y fue instalado en el Data Center DIPOL.
2.6	Año de fabricación: Mínimo 2021 última versión (todos los componentes del presente ítem).	Si	Se recibe hardware tipo servidor modelo PowerEdge R650, con año de fabricación 12/05/2021
2.7	Software: Como sistema operativo debe incluir herramienta de virtualización, que permita la creación y gestión de máquinas virtuales, debidamente licenciado.	Si	Se incluye herramienta de virtualización VMWARE vSphere 8 Essentials y vCenter server 8, con suscripción por 3 años.
2.8	Fuente de poder: 2 (dos) como mínimo, debe incluir cables de energía.	Si	Se verificó en la entrega realizada mediante documento de fecha 24/04/2023 – "Referencia entrega servidor".
2.9	Cantidad de procesadores mínima: 2 (dos) como mínimo	Si	Se verificó en las capacidades del servidor una vez encendido
2.10	Tipo de procesador: Intel Xeon Gold	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.11	Cantidad de núcleos por procesador: 12 (doce) como mínimo	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.12	Frecuencia base procesador: 3Ghz como mínimo	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.13	Memoria mínima procesador: 18 MB	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.14	Memoria RAM: mínimo 128 GB tipo DDR4	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.15	Almacenamiento: Mínimo 2 TB en SSD en RAID1 y mínimo 8 en HD en RAID 5	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.
2.16	Conectividad: 01 tarjeta de red de 10Gbps para conexión a la red LAN por fibra; 01 tarjeta de red de 1Gbps para	Si	Se verificó en las capacidades del servidor una vez encendido, cumpliendo con lo establecido.

	administración. Debe incluir un cable de fibra y cable UTP.		
2.17	El oferente debe entregar la ficha técnica del servidor de aplicación ofertado.	Si	Se recibe la ficha tecnica del servidor donde se detalla los elementos adquiridos y especificaciones.
3	**SOPORTE Y MANTENIMIENTO**		
3.1	El contratista se compromete con la suscripción del presente documento a otorgar y mantener una garantía de fábrica de los bienes y servicios durante mínimo tres (03) años, a partir del recibo a satisfacción. Igualmente, para el cambio o restitución en caso de cualquier novedad, una vez instalados los bienes y servicios el tiempo de respuesta para algún inconveniente técnico será de 24 horas y para el cambio de un equipo por garantía debe ser máximo de tres (3) días hábiles, sin costo alguno para la Policía Nacional.	Si	Se recibe certificado de licenciamiento por 3 años al igual que el soporte de garantía del servidor con número de serie JH2LCW3.
3.2	El contratista deberá garantizar la correcta entrega y puesta en funcionamiento de cada uno de los elementos y servicios.	Si	Mediante acta 135 SUBIN – ARPIN, se realizó la verificación técnica, del cumplimiento de los requisitos técnicos del contrato.
3.3	El servicio de soporte telefónico debe darse directamente por el oferente para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.	Si	Se recibe matriz de escalamiento de soporte con los abonados teléfonos: • Mesa de servicio: +573183354447 • Gerente de proyecto: +57 573157004794 • Coordinador de operaciones: +573057030674 • Director de operaciones: +573175759403
3.4	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el proveedor deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial o virtual) hasta solucionar el incidente.	Si	Se recibe casa matriz de escalamiento de soporte con los abonados donde se relacionan todos los medios de contacto para el soporte en caso de emergencia.
3.5	Horario de atención de 7X24, para la atención de casos durante el periodo de garantía.	Si	Se recibe matriz de escalamiento de soporte con los abonados teléfonos:

			• Mesa de servicio: +573183354447 • Gerente de proyecto: +57 573157004794 • Coordinador de operaciones: + +573057030674 • Director de operaciones: +573175759403
3.6	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos con fabricante: • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico.	Si	Se recibe por parte del oferente los siguientes medios para el soporte de casos fabricantes: • Mesa de servicio • Numero Telefonico: +573183354447 • Correo: Soc.col@mnemo.com
3.7	El sistema debe funcionar y contar con un soporte como también actualizaciones por un periodo mínimo de 3 años para todos sus componentes, contados a partir de la recepción del contrato por parte del supervisor.	Si	Se recibe certificado de licenciamiento del contrato PN DIPOL SA No.04-2-10006-2023, por (03) años estipulados con las fechas 24/04/2023 – 24/04-2026
4	**TRANSFERENCIA DE CONOCIMIENTO**		
4.1	El contratista deberá realizar un entrenamiento para 10 funcionarios, los cuales deberán tener una duración de 48 horas. Entrenamiento con certificado de asistencia, brindado por el contratista con instructor en sitio con perfil idóneo para permitir la adquisición de conocimientos y habilidades referentes al manejo de las herramientas explicando su funcionalidad. Adicionalmente se deberán tratar las siguientes temáticas en la transferencia de conocimiento: • Entender claramente la inteligencia cibernética y la importancia de la capacidad de inteligencia de amenazas cibernéticas (CTI) • Explicar los conceptos del modelo de amenazas y por qué los usamos. • Indicar los conceptos básicos de la composición del malware. • Aplicar conocimientos en el manejo de las herramientas adquiridas.	Si	 

	• Ejemplos de investigaciones CTI con las herramientas adquiridas y toma de notas detalladas del caso con sus aspectos relevantes.		
4.2	Todos los costos para el desarrollo de la transferencia de conocimiento estarán a cargo del contratista. Los entrenamientos deberán dictarse por entidades acreditadas y/o personal calificado con experiencia en los bienes o servicios ofrecidos.	Si	La transferencia de conocimiento fue dictada por parte de la empresa MNEMO, contando con el personal idóneo para la actividad asi: • Carlos Andres Guzman: Manager Cyber Threat intelligence Mnemo. • Ramiro Merchán: Docente implementador.
4.3	Se debe entregar certificación a cada asistente que participe en el curso.	Si	
5	**AUDITORIAS**		
5.1	Con el fin de cumplir con protocolos de seguridad de la información, todo el sistema debe ser auditado con mínimo los siguientes registros: • IP del equipo que realiza las transacciones • fecha y hora legal • tipo de transacción • descripción de la transacción • nombre de usuario	Si	El sistema cuenta con el módulo de auditoria que realiza las acciones requeridas.
6	**ASPECTOS AMBIENTALES**		
6.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política cero papel establecido en directiva presidencial 04/2012.	Si	Se reciben los manuales digitales, cargados en cada una de las plataformas digitales, Virustotal, Shodan y IntelligenceX, Se adjunta certificado de manuales digitales.
6.2	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del	Si	No se realizó manejo de residuos peligrosos ni afectaciones al sistema de afectación ambiental

	mantenimiento del Sistema de Gestión Ambiental en las instalaciones del contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.		
7	**EXPERIENCIA DE PERSONAL IMPLEMENTADOR**		
7.1	Con el fin de garantizar la idoneidad del personal que se vincula al presente proceso, el proponente deberá acreditar que el mismo cuente con la idoneidad, experiencia general y especifica suficiente, que garantice la calidad de las actividades a desarrollar definidas en las condiciones técnicas del presente proceso. Por consiguiente, el proponente deberá garantizar que, para la instalación, implementación y configuración, cuenta con al menos un (1) ingeniero de sistemas y/o telecomunicaciones y/o áreas afines, con postgrado en seguridad de la información y/o seguridad informática y/o ciberinteligencia y/o afines, quien deberá tener el soporte de haber obtenido una o varias de las certificaciones que se relacionan a continuación. • CISM (Certified Information Security Manager) • CTIA (Certified Threat Intelligence Analyst) • GCTI – GIAC Cyber Threat Intelligence • RCIA – Rocheston Cyberthreat Intelligence Analyst • CCTIA by the NICCS – Certified Cyber Threat Intelligence Analyst • CTIP – Certified Threat Intelligence Professional • Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft • CPTIA – CREST Practitioner Threat Intelligence Analyst • CRTIA – CREST Registered Threat Intelligence Analyst • CCTIM – CREST Certified Threat Intelligence Manager • MTIA - Certified Threat Intelligence Analyst • OSCP - Offensive Security Certified Professional	Si	Este ítem fue evaluado por el comité de evaluación técnica

	Nota 1. El oferente deberá adjuntar en su propuesta, la copia verificable de la certificación realizada. No serán tenidas en cuenta certificaciones de asistencia **Nota 2.** El oferente deberá adjuntar en su propuesta la copia legible del acta de grado o diploma expedido por entidad educativa reconocida por el Ministerio de Educación. **Nota 3.** En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.		
7.2	Es importante para la Dirección de Inteligencia Policial que el personal profesional que integrará el equipo de trabajo cuente con la idoneidad, experiencia general y específica suficiente que garantice la calidad de las actividades que se desarrollen sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. Por consiguiente, el oferente deberá acreditar que durante los años: 2020 y/o 2021 y/o 2022, el profesional que presente en su oferta participó en proyectos relacionados al objeto del presente proceso, en los cuales éste haya tenido que instalar y/o implementar y/o configurar alguno de los sistemas relacionadas a continuación: • SIEM (Security Information and Event Management) • OpenCTI • YETI • MISP (Malware Information Sharing Platform) • Sandbox – (Automated Malware Analysis) • The Hive Project • Cortex • Herramientas CTI (Cyber Threat Intelligence) • El producto ofertado por el oferente en el presente proceso. Nota 1. El oferente debe anexar a la propuesta, máximo tres (3) certificaciones de proyectos en los cuales, el profesional que presente en su oferta haya participado durante los últimos tres (3) años en la instalación y/o implementación y/o	Si	Este ítem fue evaluado por el comité de evaluación técnica

	configuración de alguno de los sistemas arriba listados, con fechas anteriores a la apertura del presente proceso. Estas deben ser verificables, para lo cual deberá anexar en cada certificación emitida, los datos de contacto de las empresas donde se desarrollaron los proyectos. Nota 2. El oferente deberá adjuntar en su propuesta copia de la tarjeta profesional que acredita la formación académica e idoneidad en el área específica del conocimiento. Esta no debe tener fecha menor a dos (2) años de expedición.		
7.3	En caso de realizar cambio del personal implementador, el contratista deberá informar y solicitar al supervisor la aprobación del cambio, anexando la documentación que garantice la igualdad o mejora del perfil presentado en la propuesta.	Si	Este ítem fue evaluado por el comité de evaluación técnica
7.4	La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo podrá ser sustituido por el proponente por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.	Si	Este ítem fue evaluado por el comité de evaluación técnica
8	**DOCUMENTACIÓN TÉCNICA ENTREGABLE**		
8.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de los bienes y servicios ofertados siguiendo las recomendaciones de mejores prácticas de la casa matriz.	Si	Se recibe toda la documentación de la metodología e implementación y configuración de los bienes y servicios ofertados.
8.2	Toda la documentación debe entregarse en idioma español y/o inglés.	Si	Se recibe documentación en idioma español.
8.3	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato.	Si	Mediante reunión de inicio contractual se realizó el acta 115 en la cual se estableció el cronograma del contrato.
8.4	Manual de procedimientos de administración y operación de los bienes y servicio implementados	Si	Se recibe manual de procedimientos del administración y uso del sistema.
9	**EXPERIENCIA DEL OFERENTE**		
9.1	El oferente, trátese de personas naturales o jurídicas, nacionales o extranjeras, domiciliadas o con sucursal en Colombia, fabricantes y/o comercializadores y/o distribuidores autorizados en Colombia, en	Si	El contratista realizó la entrega de los soportes al comité técnico los cuales reposan en los documentos entregados en la oferta (SECOP II).

	forma individual o conjunta (consorcio, unión temporal o promesas de sociedad), deberán registrar experiencia en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio con jurisdicción en su domicilio principal, de conformidad con el Artículo 2.2.1.1.1.5.3., del Decreto 1082 de 2015. Con el fin de garantizar la calidad de los bienes a adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222500 y/o 43233200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 1724,13 SMMLV, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
9.2	Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el oferente deberá presentar máximo tres (3) certificaciones de contratos (certificación por contrato) celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS", que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 50% del presupuesto oficial asignado. En caso que la empresa haya implementado este tipo de bienes bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia específica a través de un documento certificado ante un notario, en el cual se especifiquen los valores de los contratos celebrados y ejecutados durante los últimos cinco (5) años (2018 y/o 2019 y/o 2020 y/o 2021 y/o 2022), el país o países donde ha realizado contratación, así como una comunicación	Si	El contratista realizó la entrega de los soportes al comité técnico los cuales reposan en los documentos entregados en la oferta (SECOP II).

	emitida por una entidad del gobierno donde se indique que efectivamente la empresa cuenta con la experiencia, en desarrollo de procesos similares al objeto INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS". Las certificaciones contendrán como mínimo la siguiente información: • Entidad contratante • Contratista • Objeto del contrato • Número de contrato (Si registra) • Valor del contrato • Fecha de inicio (día, mes y año). • Fecha de terminación del contrato (día, mes y año) • Nombre, firma y cargo de la persona que expide la certificación (representante legal o persona autorizada de la empresa que expide la certificación). • Dirección y teléfono de la empresa que expide la certificación. En caso de ser oferente extranjero, deberá diligenciar los formularios "CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL O DOMICILIO EN COLOMBIA" y "FORMULARIO EXPERIENCIA DEL PROPONENTE".		
9.3	La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin de garantizar la transparencia del proceso de contratación.	Si	El contratista realizó la entrega de los soportes al comité técnico los cuales reposan en los documentos entregados en la oferta (SECOP II).
9.4	Los contratos certificados deben estar registrados en el RUP.	Si	El contratista realizó la entrega de los soportes al comité técnico los cuales reposan en los documentos entregados en la oferta (SECOP II).
10	**CONFIDENCIALIDAD DE LA INFORMACIÓN**		
10.1	El contratista deberá entregar al supervisor del contrato una vez adjudicado el contrato la documentación requerida del personal que hará parte del proyecto e implementación de la nueva solución.	Si	Se recibe la documentación requerida del personal que hará parte del proyecto e implementación de la nueva solución.

10.2	Si la Policía Nacional, considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para este fin.	Si	No fueron requeridos estudios de confidencialidad
10.3	El Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales tenga acceso con ocasión de su servicio y sea revelada información marcada como confidencial. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información.	Si	El oferente realizó la entrega del acuerdo de confidencialidad al comité técnico el cual reposa en los documentos entregados en la oferta (SECOP II).
11	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO**		
11.1	El contratista deberá entregar al supervisor del contrato el documento firmado por el representante legal el cual indique el número de trabajadores permanentes y el nivel de riesgo de su principal actividad económica, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST", en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.	Si	Se anexan parafiscales emitidos por la empresa NMEMO. No fueron requeridos trabajadores permanentes.

11.2	El contratista deberá entregar al supervisor del contrato los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.	Si	Se anexan parafiscales emitidos por la empresa NMEMO. No fueron requeridos trabajadores permanentes.
11.3	El contratista deberá cumplir con los protocolos establecidos por el Ministerio de Salud y Protección Social en atención a la Resolución 1238 del 21/07/2022 "Por medio de la cual se dictan medidas para prevención, promoción y conservación de la salud con ocasión de infecciones respiratorias, incluidas las originadas por la COVID-19".	Si	Se cumplieron con todos los protocolos de bioseguridad establecidos por el ministerio de salud.
11.4	El contratista deberá garantizar que el personal que desarrolla las tareas durante la ejecución del contrato cuente con los debidos Elementos de Protección Personal EPP, acorde a los peligros y riesgos relacionados la actividad contratada.	Si	Se cumplieron con todos los elementos de protección reglamentarios a la hora de ejecución del contrato.
11.5	El contratista garantizará que el personal que desarrolle la tarea durante la ejecución del contrato, se encuentre con la debida identificación de la empresa.	Si	El personal que desarrollo la tarea durante la ejecución dl contrato contaron con su debida identificación de la empresa MNEMO.
11.6	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14/05/2007 del Ministerio de Trabajo y Protección Social "Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo" o cualquiera que la modifique, reemplace o sustituya.	Si	No se presentaron accidentes laborales durante la ejecución del contrato.

11.7	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.	Si	No se presentaron accidentes laborales durante la ejecución del contrato.
11.8	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.	Si	No se presentaron auditorias durante la ejecución del contrato.

1.1 NOVEDADES, SITUACIONES ANORMALES O DE RELEVANCIA

Durante la presente vigencia, no se han presentado situaciones anormales o de relevancia, teniendo en cuenta que ya fue recibido a satisfacción el objeto del contrato.

3. AVANCE DE LA EJECUCIÓN DEL CONTRATO U ORDEN DE COMPRA:

A la fecha de corte del presente informe de supervisión han transcurrido (85) días calendario desde que inició el plazo de ejecución del contrato u orden de compra, restando (16) días calendario para que finalice el plazo de ejecución.

4. TRÁMITES Y VERIFICACIÓN DE PAGOS:

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

Si los documentos en referencia no se reciben dentro del plazo o, si recibidos son devueltos por inconsistencias tales como la falta de información o mal diligenciamiento de los mismos, la Policía Nacional — Dirección de Inteligencia Policial, programará el valor a cancelar una vez se hubieren subsanado las observaciones, se haya cumplido con el trámite documental dentro del plazo indicado y de acuerdo al derecho a turno y la disponibilidad del Plan Anual de Caja (PAC).

Si los documentos en referencia son devueltos por la DIRECCIÓN DE INTELIGENCIA POLICIAL, por inconsistencias como la falta de información o mal diligenciamiento de los mismos, la DIRECCIÓN DE INTELIGENCIA POLICIAL, se obliga a la asignación nuevamente del turno, siempre y cuando se hubieren subsanado las observaciones y se haya cumplido con el trámite documental dentro del plazo indicado, El contratista deberá presentar con la oferta la Certificación de existencia de cuenta corriente 0 de ahorros expedida por la entidad bancaria.

El recibido a satisfacción, aunque se encuentre suscrito por el supervisor del contrato, no implica el recibo o aprobación definitiva por parte de la DIRECCIÓN DE INTELIGENCIA POLICIAL del bien o servicio suministrado (según corresponda) y por consiguiente, no exime al CONTRATISTA de su responsabilidad en cuanto a la calidad, cantidad y buena calidad del bien o servicio contratado o de cualquier otra obligación contractual o de responsabilidad civil.

Si el recibido a satisfacción no ha sido bien elaborado o no se acompaña a esta de los documentos que para cada caso se soliciten en esta contratación, los términos anteriores sólo empezarán a contarse desde la fecha en que quede corregida el acta o desde aquella en que se haya aportado el último de los documentos.

Todas las demoras que se presenten por estos conceptos serán de responsabilidad del CONTRATISTA, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza Lo mismo se predicará en el caso de que el CONTRATISTA no elabore y presente las respectivas actas a la DIRECCIÓN DE INTELIGENCIA POLICIAL.

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

La ruta donde puede realizar la consulta de pago la ubica en:

http://www.minhacienda.gov.co/MinHacienda/haciendapubliva/siifnacion/SIIFNacion/consulta%20de%20pagos

NOMBRE BENEFICIARIO: CONSORCIO INTELIGENCIA DE AMENAZAS 2023
BANCO BBVA
TIPO DE CUENTA: AHORROS
NUMERO DE CUENTA: 00130136000200000271
OFICINA: BOGOTÁ D.C

4.1. Ejecución Financiera y Pagos:

a. Balance general de pagos y entregas		
	Valor en pesos	**% del valor del contrato u orden de compra**
Valor total del contrato u orden de compra	$3.990.200.000,00	100%
Valor total de las entregas	$3.990.200.000,00	100%
Valor total facturado	$3.990.200.000,00	100%
Valor facturado pendiente de pago	$3.990.200.000,00	100%
Valor pagado	$3.990.200.000,00	100%
Valor pendiente de entrega	0	0%

b. Detalle de las entregas, valores facturados y pagos efectuados en el periodo informado (la supervisión deberá relacionar de manera discriminada lo correspondiente a la ejecución del contrato u orden de compra **únicamente del periodo que está informando**)

No. de acta o constancia de recibido	Valor recibido	Fecha de recibido	Valor facturado	No. factura	Valor pagado	Valor deducciones	No. orden de pago
001	$3.990.200.000,00	del 14/03/2023 al 24/03/2023	$3.990.200.000,00	FP-1	$3.990.200.000,00	$ 194.221.760,00	146467123

4.2 Entrada de Bienes ***(verificar que los bienes hayan ingresado a los estados contables, si aplica)***

Se realizó entrada al almacén por medio del Acta de recepción de bienes No. 003 del 24/04/2023.

5. RECOMENDACIONES

Dado que todas las actividades desarrolladas se cumplieron a cabalidad, se recomienda seguir con los trámites administrativos necesarios para el pago y la posterior liquidación del contrato.

6. CONCLUSIONES

El supervisor, deberá marcar con una (x) las casillas según corresponda al periodo entregado, con el fin de que la administración tenga claridad frente al cumplimiento o no del contratista. El no diligenciamiento será causal de la devolución del respectivo informe de supervisión.

El contratista cumplió con lo establecido en las cláusulas contractuales	**SI X**	Certifico con la firma del presente informe, que el contratista cumplió con las cláusulas y especificaciones técnicas del contrato, en la fecha o fechas establecidas, para lo cual relaciono y anexo los documentos soportes (técnicos obligatorios establecidos en las especificaciones técnicas, incluyendo las ambientales, de seguridad y salud en el trabajo y otros).
	NO___	En caso de incumplimiento parcial o total del contrato, se informó mediante comunicación oficial No. _____ del _____, dirigida al ordenador del gasto, las obligaciones incumplidas.

Atentamente,

Firma_____

Teniente coronel **OSCAR LEONEL OCHOA SANCHEZ**
Jefe Área Producción de Inteligencia
Supervisor Contrato u orden de Compra No. 04-2-10006-2023
Correo electrónico: oscar.ochoa@correo.policia.gov.co
No. Celular: 3202978361