ANEXO No 2
CONDICIONES TECNICAS

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

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

	• Atributos de archivos • Datos estadísticos y de comportamiento • Cadenas de descarga El sistema de inteligencia de amenazas debe contar con una infraestructura altamente tolerable a fallas, garantizar disponibilidades del sitio web de 99,99% al año.		
1.7	El sistema de inteligencia de amenazas debe utilizar técnicas de Threat Hunting, que hace referencia al proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.		
1.8	El sistema de inteligencia de amenazas debe permitir crear reglas YARA de forma automática y configurar alertas que permitan la detección en tiempo real, de comportamientos que coincidan con dichas reglas. De igual forma debe permitir exportar las reglas YARA, para ser integradas en herramientas en herramientas SANDBOX propias. Adicionalmente debe permitir personalizar los reportes emitidos por la herramienta. De igual forma además que se cuenta con un acceso a nivel web, este debe permitir tener acceso a través de API, para integrar de forma programática todo el conjunto de datos y automatizar flujos de trabajo, como también el enriquecimiento de alertas basados en los indicadores de compromiso identificados, desplegables a herramientas perimetrales (SIEM, Firewall, SOAR, entre otros).		
1.9	El sistema de inteligencia de amenazas debe contar con un proceso de inspección y afinamiento el cual debe utilizar técnicas de preprocesamiento, como criterios estadísticos, sistemas de sandboxes, motores de heurística, herramientas de similitud y perfiles de comportamiento con entornos colaborativos.		
1.10	El sistema de inteligencia de amenazas deberá permitir realizar búsquedas históricas hasta de un año atrás, de igual forma deberá poder definir etiquetas o registros sobre cada una de las alertas enviadas, donde se evidencia, hora, fecha, comentario y usuario que realizó la gestión de la alerta de ciberinteligencia.		
1.11	El Sistema debe estar actualizado y configurado para detectar tácticas y técnicas enumeradas en el marco MITRE ATTACK, de igual forma los insumos de información deberán poderse categorizar en amenazas estratégicas, operacionales o tácticas.		
1.12	El sistema debe contar con correlación avanzada que involucre técnicas de analítica y/o *data science* para determinar tendencias o patrones anormales en el direccionamiento IP Colombiano. Adicionalmente, el sistema debe permitir configurar alertas de acuerdo con la necesidad del administrador, por ejemplo (alertas sobre direcciones IP específicas, dominios específicos, cyber crime, hacktivismo, entre otros). La herramienta debe mapear visualmente la correlación entre los indicadores de amenaza (archivos, URLs, dominios, IPs, entre otros. No se aceptan soluciones que requieran previamente un listado de archivos, URLs, dominios o IPs para su funcionamiento.		
1.13	El Sistema deberá permitir consumo de inteligencia de amenazas de fuentes públicas y por suscripción		
1.14	La interfaz web del Sistema debe contar con una interfaz Web GUI compatible con navegadores estándares tales como Chrome, EDGE, Firefox/Mozilla, entre otros.		
1.15	El sistema deberá permitir el acceso a diferentes tipos de reportes a través de la consola basada en GUI, sin uso de SQL por parte del usuario.		
1.16	El sistema debe contar con lo siguiente: • Acceso a la fuente de datos INTELX- IntelligenceX, la cual permita realizar búsquedas con un motor de búsqueda sobre archivos de datos global, alimentado desde múltiples fuentes, inclusive la dark web, durante todo el periodo de mantenimiento y soporte • Acceso a la fuente de datos Shodan, incluyendo la capacidad de búsqueda por vulnerabilidad, monitoreo y escaneo de hasta 65.000 direcciones IP, durante todo el periodo de mantenimiento y soporte • Debe tener selectores de búsqueda específicos como email, dominios, URL, dirección IP, entre otros. • Debe permitir realizar consulta de datos expuestos por cibercriminales, producto de		

	ciberataques a los sistemas informáticos de las entidades. • Debe permitir identificar cuentas gubernamentales comprometidas en las filtraciones de datos llevadas a cabo por ciberdelincuentes, entre otras capacidades. • En caso de que la funcionalidad integrada sea descontinuada, se debe establecer junto con el supervisor del contrato las opciones para ser reemplazada.		
1.17	El sistema de inteligencia de amenazas debe contar adicionalmente con las siguientes características. • Realizar solicitudes de análisis de archivos con un conjunto de, al menos, 70 motores antivirus distintos, y recuperación de los resultados de dichos análisis. Estos resultados deben incluir información sobre el análisis propiamente dicho, como el archivo analizado o la fecha, y sobre cada motor antivirus utilizado (nombre del motor, versión, fecha de actualización de firmas, alias o nombre de la amenaza identificada). • Permitir la descarga de los archivos almacenados en el repositorio en base a su hash (MD5, SHA1 o SHA256) para que se puedan realizar procesamientos o análisis personalizados de los mismos. • Permitir consultas de información del comportamiento de archivos en entornos aislados con base a su hash (MD5, SHA1 o SHA256). • Permitir la realización de búsquedas de archivos con base a diferentes propiedades de los mismos (nombre, contenido, tamaño, cabeceras, tipo de fichero, firma digital, etc.), las detecciones de los antivirus, características estáticas, patrones de comportamiento y otros metadatos. • Contar con filtros de selección como país desde donde se adjuntó el archivo sospechoso, rango de fechas, cantidad de interacción con dominios o direcciones IP, palabras, entre otros, con el fin de identificar amenazas de forma específica.		
2	**SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED**		
2.1	El contratista debe entregar un servidor de aplicación con las siguientes características:		
2.2	Cantidad: uno (01)		
2.3	**Marca: Especificar por el oferente**		
2.4	**Modelo: Especificar**		
2.5	Tipo: Rack		
2.6	Año de fabricación: Mínimo 2021 última versión (todos los componentes del presente ítem).		
2.7	Software: Como sistema operativo debe incluir herramienta de virtualización, que permita la creación y gestión de máquinas virtuales, debidamente licenciado.		
2.8	Fuente de poder: 2 (dos) como mínimo, debe incluir cables de energía.		
2.9	Cantidad de procesadores mínima: 2(dos) como mínimo		
2.10	Tipo de procesador: Especificar		
2.11	Cantidad de núcleos por procesador: 12 (doce) como mínimo		
2.12	Frecuencia base procesador: 3Ghz como mínimo		
2.13	Memoria mínima procesador: 18 MB		
2.14	Memoria RAM: mínimo 128 GB tipo DDR4		
2.15	Almacenamiento: Mínimo 2 TB en SSD en RAID1 y mínimo 8 en HD en RAID 5		
2.16	Conectividad: 01 tarjeta de red de 10Gbps para conexión a la red LAN por fibra; 01 tarjeta de red de 1Gbps para administración. Debe incluir un cable de fibra y cable UTP.		
2.17	El oferente debe entregar la ficha técnica del servidor de aplicación ofertado.		
3	**SOPORTE Y MANTENIMIENTO**		
3.1	El contratista se compromete con la suscripción del presente documento a otorgar y mantener una garantía de fábrica de los bienes y servicios durante mínimo tres (03) años, a partir del recibo a satisfacción. Igualmente, para el cambio o restitución en caso de cualquier novedad, una vez instalados los bienes y servicios el tiempo de respuesta para algún inconveniente técnico será de 24 horas y para el cambio de un equipo por garantía debe ser máximo de tres (3) días hábiles, sin		

	costo alguno para la Policía Nacional.		
3.2	El contratista deberá garantizar la correcta entrega y puesta en funcionamiento de cada uno de los elementos y servicios.		
3.3	El servicio de soporte telefónico debe darse directamente por el contratista para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.		
3.4	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el proveedor deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial o virtual) hasta solucionar el incidente.		
3.5	Horario de atención de 7X24, para la atención de casos durante el periodo de garantía.		
3.6	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos con fabricante: • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico.		
3.7	El sistema debe funcionar y contar con un soporte como también actualizaciones por un periodo mínimo de 3 años para todos sus componentes, contados a partir de la recepción del contrato por parte del supervisor.		
4	**TRANSFERENCIA DE CONOCIMIENTO**		
4.1	El contratista deberá realizar un entrenamiento para 10 funcionarios, los cuales deberán tener una duración de 48 horas. Entrenamiento con certificado de asistencia, brindado por el contratista con instructor en sitio con perfil idóneo para permitir la adquisición de conocimientos y habilidades referentes al manejo de las herramientas explicando su funcionalidad. Adicionalmente se deberán tratar las siguientes temáticas en la transferencia de conocimiento: • Entender claramente la inteligencia cibernética y la importancia de la capacidad de inteligencia de amenazas cibernéticas (CTI) • Explicar los conceptos del modelo de amenazas y por qué los usamos. • Indicar los conceptos básicos de la composición del malware. • Aplicar conocimientos en el manejo de las herramientas adquiridas. • Ejemplos de investigaciones CTI con las herramientas adquiridas y toma de notas detalladas del caso con sus aspectos relevantes.		
4.2	Todos los costos para el desarrollo de la transferencia de conocimiento estarán a cargo del contratista. Los entrenamientos deberán dictarse por entidades acreditadas y/o personal calificado con experiencia en los bienes o servicios ofrecidos.		
4.3	Se debe entregar certificación a cada asistente que participe en el curso.		
5	**AUDITORIAS**		
5.1	Con el fin de cumplir con protocolos de seguridad de la información, todo el sistema debe ser auditado con mínimo los siguientes registros: • IP del equipo que realiza las transacciones • fecha y hora legal • tipo de transacción • descripción de la transacción • nombre de usuario		
6	**ASPECTOS AMBIENTALES**		
6.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política cero papel establecida en directiva presidencial 04/2012.		
6.2	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las instalaciones del contratante; que		

	contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.		
7	**EXPERIENCIA DE PERSONAL IMPLEMENTADOR**		
7.1	Con el fin de garantizar la idoneidad del personal que se vincula al presente proceso, el proponente deberá acreditar que el mismo cuente con la idoneidad, experiencia general y especifica suficiente, que garantice la calidad de las actividades a desarrollar definidas en las condiciones técnicas del presente proceso. Por consiguiente, el proponente deberá garantizar que, para la instalación, implementación y configuración, cuenta con al menos un (1) ingeniero de sistemas y/o telecomunicaciones y/o áreas afines, con postgrado en seguridad de la información y/o seguridad informática y/o ciberinteligencia y/o afines, quien deberá tener el soporte de haber obtenido una o varias de las certificaciones que se relacionan a continuación. -CISM (Certified Information Security Manager) -CTIA (Certified Threat Intelligence Analyst) -GCTI – GIAC Cyber Threat Intelligence -RCIA – Rocheston Cyberthreat Intelligence Analyst -CCTIA by the NICCS – Certified Cyber Threat Intelligence Analyst -CTIP – Certified Threat Intelligence Professional -Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft -CPTIA – CREST Practitioner Threat Intelligence Analyst -CRTIA – CREST Registered Threat Intelligence Analyst -CCTIM – CREST Certified Threat Intelligence Manager -MTIA - Certified Threat Intelligence Analyst -OSCP - Offensive Security Certified Professional Nota 1. El oferente deberá adjuntar en su propuesta, la copia verificable de la certificación realizada. No serán tenidas en cuenta certificaciones de asistencia Nota 2. El oferente deberá adjuntar en su propuesta la copia legible del acta de grado o diploma expedido por entidad educativa reconocida por el Ministerio de Educación. Nota 3. En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.		
7.2	Es importante para la Dirección de Inteligencia Policial que el personal profesional que integrará el equipo de trabajo cuente con la idoneidad, experiencia general y específica suficiente que garantice la calidad de las actividades que se desarrollen sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. Por consiguiente, el oferente deberá acreditar que durante los años: 2020 y/o 2021 y/o 2022, el profesional que presente en su oferta participó en proyectos relacionados al objeto del presente proceso, en los cuales éste haya tenido que instalar y/o implementar y/o configurar alguno de los sistemas relacionadas a continuación: -SIEM (Security Information and Event Management) -OpenCTI -YETI -MISP (Malware Information Sharing Platform) -Sandbox – (Automated Malware Analysis) -The Hive Project -Cortex -Herramientas CTI (Cyber Threat Intelligence) -El producto ofertado por el oferente en el presente proceso. Nota1. El oferente debe anexar a la propuesta, máximo tres (3) certificaciones de proyectos en los cuales, el profesional que presente en su oferta haya participado durante los últimos tres (3) años en la instalación y/o implementación y/o configuración de alguno de los sistemas arriba listados, con fechas anteriores a la apertura del presente proceso. Estas deben ser verificables, para lo cual deberá anexar en cada certificación emitida, los datos de contacto de las empresas donde se desarrollaron los proyectos. Nota 2. El oferente deberá adjuntar en su propuesta copia de la tarjeta profesional que acredita la formación académica e idoneidad en el área específica del conocimiento. Esta no debe tener fecha menor a dos (2) años de expedición.		

7.3	En caso de realizar cambio del personal implementador, el contratista deberá informar y solicitar al supervisor la aprobación del cambio, anexando la documentación que garantice la igualdad o mejora del perfil presentado en la propuesta.		
7.4	La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo deberá ser sustituido por el contratista por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.		
8	**DOCUMENTACIÓN TÉCNICA – ENTREGABLES**		
8.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de los bienes y servicios ofertados siguiendo las recomendaciones de mejores prácticas de la casa matriz.		
8.2	Toda la documentación debe entregarse en idioma español y/o inglés.		
8.3	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato.		
8.4	Manual de procedimientos de administración y operación de los bienes y servicio implementados		
9	**EXPERIENCIA DEL OFERENTE**		
9.1	El oferente, trátese de personas naturales o jurídicas, nacionales o extranjeras, domiciliadas o con sucursal en Colombia, fabricantes y/o comercializadores y/o distribuidores autorizados en Colombia, en forma individual o conjunta (consorcio, unión temporal o promesas de sociedad), deberán registrar experiencia en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio con jurisdicción en su domicilio principal, de conformidad con el Artículo 2.2.1.1.1.5.3., del Decreto 1082 de 2015. Con el fin de garantizar la calidad de los bienes a adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222500 y/o 43233200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 1724,13 SMMLV, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
9.2	Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el oferente deberá presentar máximo tres (3) certificaciones de contratos (certificación por contrato) celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto “INTELIGENCIA DE AMENAZAS EN LA RED” y/o “CIBERINTELIGENCIA DE AMENAZAS ” y/o “INTELIGENCIA DE AMENAZAS AVANZADAS”, que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 50% del presupuesto oficial asignado. En caso que la empresa haya implementado este tipo de bienes bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia 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 tres (3) años (2020 y/o 2021 y/o 2022), el país o países donde ha realizado contratación, así como una comunicación emitida por una entidad del gobierno donde se indique que efectivamente la empresa cuenta con la experiencia, en desarrollo de procesos similares al objeto INTELIGENCIA DE AMENAZAS EN LA RED” y/o “CIBERINTELIGENCIA DE AMENAZAS ” y/o “INTELIGENCIA DE AMENAZAS AVANZADAS”. Las certificaciones contendrán como mínimo la siguiente información: -Entidad contratante -Contratista -Objeto del contrato -Número de contrato (Si registra) -Valor del contrato -Fecha de inicio (día, mes y año). -Fecha de terminación del contrato (día, mes y año) -Nombre, firma y cargo de la persona que expide la certificación (representante legal o persona		

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

11.6	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14/05/2007 del Ministerio de Trabajo y Protección Social "Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo" o cualquiera que la modifique, reemplace o sustituya.		
11.7	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.		
11.8	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.		

PROPONENTE_____

Declaramos bajo nuestra responsabilidad personal, y comprometiendo la responsabilidad institucional de las personas jurídicas que representamos, que cumplimos en su totalidad con las especificaciones técnicas de verificación y de obligatorio cumplimiento que diligenciamos en la casilla de cumple.

FIRMA,

Representante Legal

ANEXO No 8
FICHA TÉCNICA DE PRODUCTOS O SERVICIOS

De acuerdo al artículo 2.2.1.2.1.2.1., del Decreto 1082 de 2015 “como parte del contenido de los pliegos de condiciones, cada **bien o servicio de características técnicas uniformes** a ser adquirido mediante subasta inversa, tendrá una ficha técnica que incluirá sus características y especificaciones, en términos de desempeño y calidad. La ficha técnica deberá contener, como mínimo”:

a) Denominación del bien o servicio
b) Denominación técnica del bien o servicio
c) Unidad de medida
d) Descripción General

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

De acuerdo con el artículo 2.2.1.2.1.2.1., del Decreto 1082 de 2015 “como parte del contenido de los pliegos de condiciones, cada **bien o servicio de características técnicas uniformes** a ser adquirido mediante subasta inversa, tendrá una ficha técnica que incluirá sus características y especificaciones, en términos de desempeño y calidad. La ficha técnica deberá contener, como mínimo”:

a) Denominación del bien o servicio
b) Denominación técnica del bien o servicio
c) Unidad de medida
d) Descripción General

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
INTELIGENCIA DE AMENAZAS EN LA RED
DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO
INTELIGENCIA DE AMENAZAS EN LA RED
UNIDAD DE MEDIDA
UNIDAD
DESCRIPCIÓN GENERAL

ÍTEM	**REQUERIMIENTO MÍNIMO**
1.	**SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED**
1.1	Contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: la actividad de actores, malwares activos, alertas de actividades de amenazas e informes analizados por inteligencia. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con (a) direccionamiento IP Colombiano. Los datos, aunque en primera medida deben estar enfocados al direccionamiento IP Colombiano también deberá traer en su dashboard, información relacionada con ciberamenazas que se presente de otros direccionamientos IP pero que puedan afectar el direccionamiento IP colombiano. La

		información debe ser recopilada de los centros de ciberinteligencia del oferente y esta debe tener como mínimo, lo siguiente: • URL o direcciones IP maliciosas Origen • Perfil de actor • Motivaciones, malware asociado • Descarga de malware (junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, impacto.) • Phishing • Comando y control • Spammer El oferente debe estar referenciado como referente en servicios de inteligencia de ciberamenazas, para lo cual debe presentar los soportes e informes que lo acrediten. En caso de ser líder del sector, se aceptan estudios de Forrester o Gartner, en los cuales debe estar claramente definido “inteligencia de ciberamenazas en la red” o similares. Junto con la propuesta se deberá anexar un documento emitido por casa matriz, en el cual se observe la correlación entre indicadores de compromiso del direccionamiento IP colombiano y que permita la descarga de archivos sospechosos, así como el cumplimiento de las demás especificaciones técnicas solicitadas en el presente proceso. Lo anterior deberá ser soportado con un acceso web que evidencie lo descrito en el documento.
	1.1.1	El oferente debe hacer entrega de un certificado de casa matriz en el que se certifique que la herramienta ofertada para la inteligencia de amenazas cumple con todos los requerimientos técnicos solicitados. Por lo anterior, el oferente debe especificar la marca de la herramienta a ofrecer, así: Marca: Especificar por el oferente
	1.2	El sistema deberá permitir realizar búsquedas de las ciberamenazas mínimo con los siguientes parámetros, así: • Máscaras y URL Maliciosas • Hashes MD5 • Direcciones IP El sistema debe en detalle entregar información referente a **Reputación de IP**: conjunto de direcciones IP con un contexto que cubre hosts sospechosos y malintencionados **Direcciones URL maliciosas**: conjunto de direcciones URL formado por enlaces y sitios web malintencionados. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de phishing:** conjunto de direcciones URL identificadas por la ciberinteligencia de la casa matriz como sitios de phishing. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de C&C de malware**: conjunto de direcciones URL de servidores de comando y control (C&C) y objetos malintencionados relacionados. **Hashes de malware móvil:** conjunto de hashes de archivos para detectar objetos malintencionados

	que infectan plataformas móviles. **Fuente de datos sobre malware:** conjunto de hashes de troyanos con su contexto correspondiente para detectar troyanos para dispositivos móviles que cargan cobros a los usuarios móviles y que además permiten a un atacante robar, eliminar y responder mensajes. **Direcciones URL de C&C móviles de botnets:** conjunto de direcciones URL con contexto que contempla servidores C&C móviles de botnets. **Investigaciones Manuales:** La interfaz web debe permitir búsquedas y descargas manuales, para realizar análisis profundo de muestras y obtener indicadores adicionales, por medio de otras herramientas. Adicionalmente el oferente debe tener foros, redes sociales y contenido web, en los que se traten temáticas en tendencia de CTI.
1.3	El sistema ofertado debe tener como mínimo lo siguiente, esto con el fin de contar con la mayor cantidad de información relacionada con ciber inteligencia que permita anticiparse a la posible materialización de amenazas en el direccionamiento IP Colombiano o con relación a este, así: • Una red de seguridad propia de identificación de amenazas, de la cual el oferente debe anexar un soporte con la cantidad de fuentes de las cuales recopilan información. Esto se debe anexar junto con la oferta • Partners de seguridad, enumerar en la propuesta cuales son. • Identificación de C&C o Botnets
1.4	El sistema debe garantizar la confiabilidad de la inteligencia de amenazas, entregando siempre un contexto (detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados, impacto.) y permitir la definición de un puntaje (score) producido por algoritmos machine learning para transmitir la confianza de un indicador es benigno o malicioso. En donde 0 se considera benigno de alta confianza y 100 es maliciosos de alta confianza, según la escala de medición.
1.5	La inteligencia de amenazas en la red se debe generar automáticamente y en tiempo real. Este debe tener como insumo de hallazgos a nivel mundial (mínimo en 100 países, esto debe ser soportado con una certificación de la casa matriz), información recopilada de la red de identificación de amenazas de la casa matriz que se presente en la oferta.
1.6	El sistema debe entregar unos datos enriquecidos con el fin de dar más contexto a la inteligencia de amenazas relacionadas con: • Whois • DNS • GeoIP • Hosting • Atributos de archivos • Datos estadísticos y de comportamiento • Cadenas de descarga El sistema de inteligencia de amenazas debe contar con una infraestructura altamente tolerable a fallas, garantizar disponibilidades del sitio web de 99,99% al año.
1.7	El sistema de inteligencia de amenazas debe utilizar técnicas de Threat Hunting, que hace referencia al proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.
1.8	El sistema de inteligencia de amenazas debe permitir crear reglas YARA de forma automática y configurar alertas que permitan la detección en tiempo real, de comportamientos que coincidan con

	dichas reglas. De igual forma debe permitir exportar las reglas YARA, para ser integradas en herramientas en herramientas SANDBOX propias. Adicionalmente debe permitir personalizar los reportes emitidos por la herramienta. De igual forma además que se cuenta con un acceso a nivel web, este debe permitir tener acceso a través de API, para integrar de forma programática todo el conjunto de datos y automatizar flujos de trabajo, como también el enriquecimiento de alertas basados en los indicadores de compromiso identificados, desplegables a herramientas perimetrales (SIEM, Firewall, SOAR, entre otros).
1.9	El sistema de inteligencia de amenazas debe contar con un proceso de inspección y afinamiento el cual debe utilizar técnicas de preprocesamiento, como criterios estadísticos, sistemas de sandboxes, motores de heurística, herramientas de similitud y perfiles de comportamiento con entornos colaborativos.
1.10	El sistema de inteligencia de amenazas deberá permitir realizar búsquedas históricas hasta de un año atrás, de igual forma deberá poder definir etiquetas o registros sobre cada una de las alertas enviadas, donde se evidencia, hora, fecha, comentario y usuario que realizó la gestión de la alerta de ciberinteligencia.
1.11	El Sistema debe estar actualizado y configurado para detectar tácticas y técnicas enumeradas en el marco MITRE ATTACK, de igual forma los insumos de información deberán poderse categorizar en amenazas estratégicas, operacionales o tácticas.
1.12	El sistema debe contar con correlación avanzada que involucre técnicas de analítica y/o *data science* para determinar tendencias o patrones anormales en el direccionamiento IP Colombiano. Adicionalmente, el sistema debe permitir configurar alertas de acuerdo con la necesidad del administrador, por ejemplo (alertas sobre direcciones IP específicas, dominios específicos, cyber crime, hacktivismo, entre otros). La herramienta debe mapear visualmente la correlación entre los indicadores de amenaza (archivos, URLs, dominios, IPs, entre otros. No se aceptan soluciones que requieran previamente un listado de archivos, URLs, dominios o IPs para su funcionamiento.
1.13	El Sistema deberá permitir consumo de inteligencia de amenazas de fuentes públicas y por suscripción
1.14	La interfaz web del Sistema debe contar con una interfaz Web GUI compatible con navegadores estándares tales como Chrome, EDGE, Firefox/Mozilla, entre otros.
1.15	El sistema deberá permitir el acceso a diferentes tipos de reportes a través de la consola basada en GUI, sin uso de SQL por parte del usuario.
1.16	El sistema debe contar con lo siguiente: • Acceso a la fuente de datos INTELX- IntelligenceX, la cual permita realizar búsquedas con un motor de búsqueda sobre archivos de datos global, alimentado desde múltiples fuentes, inclusive la dark web, durante todo el periodo de mantenimiento y soporte • Acceso a la fuente de datos Shodan, incluyendo la capacidad de búsqueda por vulnerabilidad, monitoreo y escaneo de hasta 65.000 direcciones IP, durante todo el periodo de mantenimiento y soporte • Debe tener selectores de búsqueda específicos como email, dominios, URL, dirección IP, entre otros. • Debe permitir realizar consulta de datos expuestos por cibercriminales, producto de ciberataques a los sistemas informáticos de las entidades. • Debe permitir identificar cuentas gubernamentales comprometidas en las filtraciones de datos llevadas a cabo por ciberdelincuentes, entre otras capacidades. • En caso de que la funcionalidad integrada sea descontinuada, se debe establecer junto con el

	supervisor del contrato las opciones para ser reemplazada.
1.17	El sistema de inteligencia de amenazas debe contar adicionalmente con las siguientes características. • Realizar solicitudes de análisis de archivos con un conjunto de, al menos, 70 motores antivirus distintos, y recuperación de los resultados de dichos análisis. Estos resultados deben incluir información sobre el análisis propiamente dicho, como el archivo analizado o la fecha, y sobre cada motor antivirus utilizado (nombre del motor, versión, fecha de actualización de firmas, alias o nombre de la amenaza identificada). • Permitir la descarga de los archivos almacenados en el repositorio en base a su hash (MD5, SHA1 o SHA256) para que se puedan realizar procesamientos o análisis personalizados de los mismos. • Permitir consultas de información del comportamiento de archivos en entornos aislados con base a su hash (MD5, SHA1 o SHA256). • Permitir la realización de búsquedas de archivos con base a diferentes propiedades de los mismos (nombre, contenido, tamaño, cabeceras, tipo de fichero, firma digital, etc.), las detecciones de los antivirus, características estáticas, patrones de comportamiento y otros metadatos. • Contar con filtros de selección como país desde donde se adjuntó el archivo sospechoso, rango de fechas, cantidad de interacción con dominios o direcciones IP, palabras, entre otros, con el fin de identificar amenazas de forma específica.
2	**SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED**
2.1	El contratista debe entregar un servidor de aplicación con las siguientes características:
2.2	Cantidad: uno (01)
2.3	Marca: Especificar por el oferente
2.4	Modelo: Especificar
2.5	Tipo: Rack
2.6	Año de fabricación: Mínimo 2021 última versión (todos los componentes del presente ítem).
2.7	Software: Como sistema operativo debe incluir herramienta de virtualización, que permita la creación y gestión de máquinas virtuales, debidamente licenciado.
2.8	Fuente de poder: 2 (dos) como mínimo, debe incluir cables de energía.
2.9	Cantidad de procesadores mínima: 2(dos) como mínimo
2.10	Tipo de procesador: Especificar
2.11	Cantidad de núcleos por procesador: 12 (doce) como mínimo
2.12	Frecuencia base procesador: 3Ghz como mínimo
2.13	Memoria mínima procesador: 18 MB
2.14	Memoria RAM: mínimo 128 GB tipo DDR4
2.15	Almacenamiento: Mínimo 2 TB en SSD en RAID1 y mínimo 8 en HD en RAID 5
2.16	Conectividad: 01 tarjeta de red de 10Gbps para conexión a la red LAN por fibra; 01 tarjeta de red de 1Gbps para administración. Debe incluir un cable de fibra y cable UTP.
2.17	El oferente debe entregar la ficha técnica del servidor de aplicación ofertado.
3	**SOPORTE Y MANTENIMIENTO**
3.1	El contratista se compromete con la suscripción del presente documento a otorgar y mantener una

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

	• descripción de la transacción • nombre de usuario