MINISTERIO DE DEFENSA NACIONAL UNIDAD GESTIÓN GENERAL DIRECCIÓN ADMINISTRATIVA	CONTRATO DE LICENCIAMIENTO No.	273 /2024 MDN-UGG-DA
	CONTRATANTE:	MINISTERIO DE DEFENSA NACIONAL – UNIDAD GESTIÓN GENERAL - DIRECCIÓN ADMINISTRATIVA
	NIT	899999003-1
	CONTRATISTA:	INFORMACIÓN LOCALIZADA SAS
	NIT No:	830-062-674
	OBJETO:	SUSCRIPCIÓN A PLATAFORMA DE CIBERINTELIGENCIA SAAS PARA DETECCIÓN TEMPRANA DE AMENAZAS CIBERNÉTICAS DEL MINISTERIO DE DEFENSA NACIONAL
	PLAZO:	Será de 20 días calendario, contados a partir de la suscripción del Acta de Inicio, previa aprobación de la garantía de cumplimiento y expedición del registro presupuestal La suscripción de la plataforma corresponde a un (1) año, a partir del recibo a satisfacción de la misma.
	VALOR:	**OCHO MIL QUINIENTOS MILLONES DE PESOS M/CTE ($8.500.000.000,00)** excluido el valor del IVA e incluido demás impuestos, tasas, contribuciones, costos directos e indirectos, a que hubiere lugar

Bogotá D.C., 06 DIC 2024

Entre los suscritos **ADRIANA FERNÁNDEZ GUTIERREZ,** mayor de edad, identificada con cédula de ciudadanía No. 63.525.706 expedida en Bucaramanga, quien actúa en nombre y representación del **MINISTERIO DE DEFENSA NACIONAL,** en su calidad de Directora Administrativa (E), designada para ejercer el cargo mediante Resolución de nombramiento No. 4949 del 13 de noviembre de 2024, y posesionada mediante Acta No. 0216-24 del 18 de

noviembre de 2024, de conformidad con las facultades delegadas por el Ministro de Defensa Nacional en materia contractual, quien en adelante se denominará **EL MINISTERIO**, y por la otra la **CARLOS GIOVANNI PARADA AVILA**, mayor de edad, identificado con cédula de ciudadanía No.79.533.543 de Bogotá D.C., quien actúa en calidad de representante legal del Contratista INFORMACIÓN LOCALIZADA SAS, hemos convenido celebrar el presente contrato, previos los siguientes considerandos: **A)** Que se elaboraron los estudios previos de conformidad con lo señalado en el Decreto 1082 de 2015. **B)** Que al momento de la apertura del proceso de selección, se contó con la respectiva apropiación presupuestal que respalda el presente compromiso. **C)** Que el presente contrato se originó del proceso de **Selección Abreviada de Subasta inversa No. 024 /2024 MDN-UGG-DA**. cuyo objeto fue contratar la "SUSCRIPCIÓN A PLATAFORMA DE CIBERINTELIGENCIA SAAS PARA DETECCIÓN TEMPRANA DE AMENAZAS CIBERNÉTICAS DEL MINISTERIO DE DEFENSA NACIONAL" **D)** Que en virtud de lo anterior, mediante Acto Administrativo No 066 MDN-UGG-DA del 06 DIC 2024, se adjudicó el presente contrato al proponente INFORMACIÓN LOCALIZADA SAS, de conformidad con la oferta presentada el 14 de noviembre de 2024, la cual hace parte integral del presente contrato. **E)** Que en consideración a todo lo anterior, las partes acuerdan celebrar el presente contrato de prestación de servicios el cual se regirá por las siguientes cláusulas;

CLÁUSULA PRIMERA.- OBJETO: SUSCRIPCIÓN A PLATAFORMA DE CIBERINTELIGENCIA SAAS PARA DETECCIÓN TEMPRANA DE AMENAZAS CIBERNÉTICAS DEL MINISTERIO DE DEFENSA NACIONAL.

CLÁUSULA SEGUNDA. - ALCANCE DEL OBJETO: En desarrollo del objeto, **EL CONTRATISTA** deberá entregar los bienes y/o prestar los servicios, de conformidad con las especificaciones técnicas previstas en el **Anexo No. 1 "FICHA TÉCNICA"** del presente contrato, el cual se suscribe por las partes y se avala por el Director de la Dirección de Tecnologías de la Información y las Comunicaciones y el Jefe Oficina de Respuestas **a Incidentes Cibernéticos CSIRT,** quien solicitó la contratación o quien haga sus veces.

CLÁUSULA TERCERA. - VALOR: OCHO MIL QUINIENTOS MILLONES DE PESOS M/CTE ($8.500.000.000,00) excluido el valor del IVA e incluido demás impuestos, tasas, contribuciones, costos directos e indirectos, a que hubiere lugar.

PARÁGRAFO PRIMERO.- El (los) valor(es) ofertado(s) por EL CONTRATISTA, se entiende(n) firme(s) y fijo(s) por lo tanto no está sujeto a ninguna clase de reajuste. Igualmente, dentro de este precio están incluidos los costos proyectados al plazo de ejecución del presente contrato y la utilidad razonable que el contratista pretende obtener, en consecuencia, no se aceptarán solicitudes de reajustes, fundamentados en estas circunstancias.

PARÁGRAFO SEGUNDO. - El **MINISTERIO** efectuará en el Certificado de Registro Presupuestal la liberación del valor que no llegare a ser ejecutado en la respectiva vigencia,

previa solicitud del supervisor del contrato. Lo anterior se verá reflejado en el acta de liquidación correspondiente.

CLÁUSULA CUARTA.- FORMA DE PAGO: El valor del contrato se pagará por intermedio de la Dirección de Finanzas de este Ministerio al CONTRATISTA, de este Ministerio al CONTRATISTA, una vez se encuentre aprobado el P.A.C. (Programa Anual Mensualizado de Caja) por parte del Ministerio de Hacienda y Crédito Público, EN UN ÚNICO PAGO AL RECIBO A SATISFACCIÓN DE BIENES Y/O SERVICIOS, excluido de IVA ofertado por el contratista dentro de los treinta (30) días siguientes al recibido a satisfacción incluyendo la verificación de las condiciones solicitadas en la ficha técnica por parte del supervisor del contrato, previa radicación en el Grupo Financiero de los documentos para pago: factura correspondiente, certificado de cumplimiento a satisfacción por parte del Supervisor del contrato designado por EL MINISTERIO y demás los trámites administrativos a que haya lugar.

La(s) factura(s) deberá(n) ser presentada(s) al vencimiento del período facturado.

La factura de los bienes y/o servicios prestados en diciembre de 2024 deberá ser presentada a más tardar dentro de la presente vigencia.

PARÁGRAFO PRIMERO. - Si la(s) factura(s) no ha(n) sido correctamente elaborada(s) o no se aportan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza.

PARÁGRAFO SEGUNDO. - Si la (s) factura (s) no ha (n) sido correctamente elaborada(s) o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. y aplicará la misma regla de trámite en el mes siguiente a la presentación, **si la corrección no se hace dentro de los cinco (5) días hábiles siguientes a la devolución de la factura.** Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza

PARÁGRAFO TERCERO.- De conformidad con lo establecido en la Directiva Presidencial No. 09 del 17 de Septiembre de 2020 *"Lineamientos para el pago a los proveedores del Estado"*, **en caso que el contratista esté obligado a facturar electrónicamente**, deberá presentar la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia, con lo dispuesto en la Resolución

No. 000042 del 5 de mayo de 2020, y las normas que las modifiquen o sustituyan. Así mismo, deberá haber efectuado el proceso de **Validación de la factura electrónica** en el Sistema SECOP II, de conformidad con lo señalado sobre el particular por Colombia Compra Eficiente.

PARÁGRAFO CUARTO. - Para la realización del(os) pago(s) derivado(s) del presente contrato, **EL CONTRATISTA** deberá deberá entregar al supervisor la **CONSTANCIA DEL PAGO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL INTEGRAL y PARAFISCALES,** de sus trabajadores y de sus contratistas de conformidad con la normatividad vigente, mediante certificación expedida por el revisor fiscal o por el representante legal, según corresponda.

PARÁGRAFO QUINTO- **ABONOS EN CUENTA:** Los pagos se efectuarán mediante consignación en la cuenta corriente No.04013112476 del BANCO Bancolombia que el **CONTRATISTA** acreditó como propia.

Los pagos previstos en esta cláusula se acreditarán en la cuenta antes mencionada, o en otro banco o cuenta que **EL CONTRATISTA** designe, con sujeción a lo previsto en las disposiciones cambiarias y siempre y cuando el supervisor solicite a **EL MINISTERIO** el cambio de cuenta para pagos, con presentación de la nueva certificación bancaria en donde se acredite su apertura. En todo caso el cambio de banco o cuenta para pagos se hará efectivo a más tardar vencidos los treinta (30) días siguientes a la solicitud del supervisor del contrato.

PARÁGRAFO SEXTO.- **REAJUSTE AL PESO: EL CONTRATISTA** con la suscripción del contrato, acepta que en el evento que el valor total a pagar tenga centavos, estos se ajusten o aproximen al peso, ya sea por exceso o por defecto, si la suma es mayor o menor a 50 centavos. Lo anterior, sin que sobrepase el valor total establecido en el presente contrato.

CLÁUSULA QUINTA.- APROPIACIÓN PRESUPUESTAL: Los pagos que el **MINISTERIO** se compromete a cancelar al **CONTRATISTA** como contraprestación por el cumplimiento del objeto contratado será con al Certificado de Disponibilidad Presupuestal No. 69124 del 07 de octubre de 2024, A-02-02-02-008-004 "Servicios de telecomunicaciones, transmisión y suministro de información", expedido por el Coordinador Grupo Gestión Presupuestal de la Dirección de Finanzas de la Unidad de Gestión General del Ministerio de Defensa Nacional.

CLÁUSULA SEXTA. - PLAZO Y LUGAR DE EJECUCIÓN: Será de 20 días calendario, contados a partir de la suscripción del Acta de Inicio, previa aprobación de la garantía de cumplimiento y expedición del registro presupuestal

El lugar de ejecución corresponde a las instalaciones de la Oficina de Respuesta a Incidentes Cibernéticos – CSIRT Defensa del Ministerio de Defensa Nacional.

La suscripción de la plataforma corresponde a un (1) año, a partir del recibo a satisfacción de la misma.

CLÁUSULA SÉPTIMA. - VIGENCIA: La vigencia del presente contrato comprende el plazo de ejecución y cuatro (4) meses más.

CLÁUSULA OCTAVA. - DERECHOS DEL CONTRATISTA: En general, son derechos del Contratista:

1. Recibir el pago que en su favor establece el presente contrato.

2. Tener acceso a los elementos físicos necesarios para desarrollar el objeto del contrato y cumplir con sus obligaciones.

3. Celebrar todos los contratos y operaciones que considere útiles a sus intereses, siempre que se encuentren dentro del ámbito de los derechos y obligaciones que surgen con ocasión del presente contrato y que sean consistentes con su finalidad.

4. Obtener la colaboración necesaria del Ministerio para el adecuado desarrollo del contrato.

CLÁUSULA NOVENA.- OBLIGACIONES DEL CONTRATISTA: En general, son obligaciones del Contratista:

A) OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

1. Prestar los servicios y/o entregar los bienes contratados en las condiciones establecidas en el Anexo No. 1 **"FICHA TÉCNICA"** del presente contrato, dentro de los plazos señalados, de acuerdo con la propuesta presentada y a las indicaciones impartidas por el supervisor del mismo.

2. Suscribir el acta de inicio junto con el supervisor del contrato. (si aplica)

3. Realizar los ajustes a los servicios objeto del contrato, dentro de la oportunidad que establezca el Ministerio, cuando se evidencie el no cumplimiento de las Especificaciones Técnicas establecidas en el Anexo No. 1 "FICHA TÉCNICA" del presente contrato.

4. Presentar al supervisor del contrato, dentro del término estipulado Anexo No. 1 "FICHA TÉCNICA" el equipo de trabajo requerido para desarrollar las actividades objeto del mismo y acreditar que cumple con los requisitos exigidos en el mencionado anexo para cada uno de ellos, aportando las respectivas certificaciones de experiencia y de idoneidad según corresponda.

5. Presentar al supervisor del contrato, dentro del término estipulado Anexo No. 1 "FICHA TÉCNICA", toda la documentación que le sea requerida con el fin de efectuar los estudios de seguridad del personal que sea asignado al proyecto.

6. Es legítimo titular de la PLATAFORMA Y/O LICENCIAS Y/O SOLUCIONES y su contenido y tiene derecho a transferir su uso.

7. Con la transferencia del el uso de PLATAFORMA Y/O LICENCIAS Y/ SOLUCIONES Y/O no se están violando de cualquier otra manera derechos de propiedad intelectual protegidos de terceros, sean de fuente legal o contractual.

8. Que los derechos sobre la PLATAFORMA Y/O LAS LICENCIAS Y SOLUCIONES son válidos, y hasta donde tienen conocimiento, no son, en el momento de la celebración del contrato, violados por terceros.

B) OBLIGACIONES GENERALES DEL CONTRATISTA:

1. Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad. Por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno del CONTRATISTA con el MINISTERIO.

2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones que puedan presentarse, responder por sus actuaciones y omisiones derivadas de la celebración del presente contrato y en general se obliga a cumplir con lo establecido en las Leyes 80 de 1993, 1150 de 2007, 1474 de 2011, sus Decretos Reglamentarios y demás normatividad aplicable.

3. De conformidad con lo estipulado en la Ley 789 de 2002, Ley 828 de 2003, 1562 de 2012, el Decreto 1072 de 2015 "Decreto Único Reglamentario del Sector Trabajo" y el Decreto 1833 de 2016 "Por medio del cual se compilan las normas del Sistema General de Pensiones", y las normas que los modifiquen o sustituyan, dar cumplimiento a sus obligaciones con el Sistema de Seguridad Social Integral y Aportes Parafiscales, para lo cual deberá aportar certificación expedida por el revisor fiscal o Representante Legal, según corresponda.

4. Mantener actualizado su domicilio durante la vigencia del contrato y cuatro meses más y presentarse al MINISTERIO en el momento en que sea requerido por el mismo para la suscripción de la correspondiente acta de liquidación.

5. Estar inscrito en el sistema electrónico de contratación pública SECOP II y mantener habilitado su usuario y contraseña.
6. Proveer a su costo, todos los bienes y servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el presente contrato.

7. Obtener con la oportunidad debida, las licencias, autorizaciones y permisos, cuando fuere el caso, para el cumplimiento de todas las obligaciones que le corresponden en los términos del presente contrato.

8. Informar oportunamente al supervisor del contrato sobre las imposibilidades o dificultades que se presenten en la ejecución del mismo y ofrecer alternativas para garantizar la buena ejecución.

9. Coordinar con el Supervisor del contrato designado por **EL MINISTERIO**, las acciones tendientes al cumplimiento del objeto contratado.

10. Rendir los informes relacionados con las actividades desarrolladas en relación con el objeto contratado y asistir a las reuniones programadas por EL MINISTERIO a través del Supervisor del Contrato.

11. Mantener la debida reserva frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del contrato, de conformidad con el compromiso de confidencialidad que se suscribe con el contrato y que hace parte integral del mismo.

12. Asistir a las reuniones programadas por EL MINISTERIO.

13. Responder en los plazos que el Ministerio de Defensa Nacional establezca en cada caso, los requerimientos de aclaración o de información que le formule.

14. Mantener los precios ofrecidos durante el término de la ejecución del Contrato.

15. Entregar el certificado de vida útil de cada bien y/o elemento objeto del presente contrato, junto con la remisión o factura al momento de la entrega de los bienes y/o elementos en el almacén general del MDN - UGG, conforme a los rangos del Marco Normativo para entidades de Gobierno-Normas para el Reconocimiento, Medición, Revelación y Presentación de los Hechos Económicos de las Entidades de Gobierno, expedido por la Contaduría General de la Nación mediante Resolución 533 de 2015. **(Cuando aplique).**

16. Contar durante la ejecución del contrato con el Sistema de Gestión en Seguridad y Salud en el Trabajo, establecido en el Decreto 1072 de 2015 y cumplir con los lineamientos establecidos en la Resolución 312 de 2019, o las normas que las modifiquen o sustituyan, por el cual se definen los Estándares Mínimos del Sistema de Gestión en Seguridad y Salud en el Trabajo para empleadores y contratantes.

17. Allegar dentro de los tres (3) días siguientes al perfeccionamiento del contrato el certificado de curso virtual de cincuenta (50) horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto 1072 de 2015) y mantenerlo vigente durante la ejecución del contrato.

18. Cumplir con todas las obligaciones relacionadas con el sistema de gestión de seguridad y salud en el trabajo y medio ambiente establecidas en el Manual de Seguridad y Salud en el Trabajo del Ministerio, para lo cual deberá asistir dentro de los tres (3) días hábiles siguientes a la suscripción del contrato a la inducción sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo y Medio Ambiente, realizada por el Área de Talento Humano de la Entidad. Esta obligación será exigible por el supervisor del contrato, para el contratista que asigne personal para que desarrolle actividades relacionadas con la ejecución contractual dentro de las instalaciones del Ministerio de Defensa Nacional.

19. Adjuntar el RUT actualizado en caso que la actividad económica que tenía registrada para la fecha de celebración del presente contrato, haya desaparecido y deba registrar una nueva, de conformidad con la Resolución 000114 del 21 de diciembre de 2020, modificada por la Resolución 0005 del 22 de enero de 2021, expedidas por la DIAN, mediante la cual actualiza el listado de códigos de las actividades económicas que los contribuyentes deberán mantener reportadas en su respectivo RUT.

20. Adjuntar en el expediente contractual electrónico que reposa en el SECOP II, el informe de ejecución, junto con el cumplido a satisfacción, y la factura, esta última si aplica, y todos los demás documentos exigidos para cada pago, con el fin de que el supervisor los apruebe a través del SECOP II y radique posteriormente en la oficina de cuentas por pagar, el trámite respectivo.

21. En general, la obligación de cumplir cabalmente con las condiciones y modalidades previstas contractualmente para la ejecución y desarrollo del Contrato, para lo cual el Contratista deberá actuar razonablemente en el marco de sus obligaciones contractuales.

22. **COMPROMISO ANTISOBORNO Y ANTICORRUPCIÓN DEL CONTRATISTA. EL CONTRATISTA** deberá dar cabal cumplimiento a los compromisos de anticorrupción y antisoborno, apoyando la acción del Estado Colombiano y del Ministerio de Defensa Nacional para fortalecer la transparencia y la responsabilidad de rendir cuentas. Dentro de este marco, EL CONTRATISTA se compromete a impartir instrucciones a todos sus empleados y agentes, así como cualquier representante suyo, exigiéndole el cumplimiento en todo momento de las leyes de Republica de Colombia y especialmente de aquellas que rigen la presente contratación, y les impondrá la obligación de no ofrecer o pagar sobornos o cualquier halago corrupto, a los funcionarios del Ministerio de Defensa Nacional.

CLÁUSULA DÉCIMA. - DERECHOS DEL MINISTERIO:

1. Acceder a los documentos e información que soportan la labor del Contratista, en el marco de la supervisión, el desarrollo y ejecución del presente contrato.

2. Solicitar y recibir información técnica respecto de los servicios y/o bienes y demás elementos que provea el Contratista en desarrollo del objeto del presente contrato.

3. Rechazar los servicios y/o bienes objeto del contrato cuando no cumplan con las Especificaciones Técnicas exigidas, en el **Anexo No. 1: FICHA TÉCNICA "ESPECIFICACIONES TÉCNICAS EXIGIDAS"** o con alguna de las obligaciones establecidas en el presente contrato.

4. Asignar en el presente contrato un Supervisor, a través de quien el Ministerio mantendrá la interlocución permanente y directa con el Contratista.

CLÁUSULA DÉCIMA PRIMERA. - OBLIGACIONES DEL MINISTERIO:

1. Recibir a satisfacción los servicios y/o bienes que sean entregados por el Contratista, cuando éstos cumplan con las condiciones establecidas en el presente contrato.

2. Tramitar diligentemente la apropiación presupuestal que se requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo, como consecuencia del perfeccionamiento del presente contrato.

3. Pagar al Contratista en la forma pactada, con sujeción a las apropiaciones presupuestales y disponibilidades de PAC previstas para el efecto.

4. Asignar al presente contrato un supervisor, a través del cual el Ministerio mantendrá la interlocución permanente y directa con el contratista.

CLÁUSULA DÉCIMA SEGUNDA. - GARANTÍA TÉCNICA: El Contratista garantiza al Ministerio los bienes entregados contra cualquier defecto de fabricación incluida la estructura, sus componentes y funcionamiento y serán nuevos y de primera calidad, de acuerdo con las especificaciones técnicas pactadas. En consecuencia, el Contratista se obliga a reemplazar a sus costos aquellos bienes que resultaren de mala calidad o con defectos de fabricación, durante un plazo máximo señalado en el Anexo Técnico del presente contrato, sin costo adicional para el Ministerio. **(Cuando aplique)**

PARÁGRAFO ÚNICO: Los bienes que presenten fallas durante el tiempo de garantía que no sean reemplazados por el Contratista, o la no realización de los ajustes requeridos sobre los servicios prestados, dará derecho al Ministerio a imponer las sanciones previstas en el presente contrato y/o hacer efectiva las garantías de calidad o cumplimiento.

Dicha garantía se extiende por un término establecido en el estudio previo técnico contados a partir de la fecha en que se reciben a satisfacción los bienes objeto del contrato por parte del Supervisor del contrato de conformidad con la propuesta presentada. **(Cuando aplique)**

CLÁUSULA DÉCIMA TERCERA. - VERIFICACIÓN DE ENTREGA DE LOS BIENES Y/O SERVICIOS PRESTADOS: El supervisor del contrato, verificará que los servicios y/o bienes correspondan a los ofertados por el Contratista y que cumpla con las normas o especificaciones técnicas exigidas en el **Anexo No.1 ANEXO TÉCNICO "FICHA TÉCNICA"** del presente contrato.

CLÁUSULA DÉCIMA CUARTA. - ACTAS DE RECIBO: Cumplidas y superadas las verificaciones previstas para el recibo de los servicios y/o bienes ofrecidos, se suscribirá entre las partes un Acta de Recibo, en la cual se manifestará la conformidad con las condiciones en las que se hace la entrega, la fecha en la que se recibe y el valor de los servicios y/o bienes recibidos. Dichas actas serán suscritas por el representante del contratante y el supervisor designado por el Ministerio, y comprometerá en su contenido tanto al Contratista como al Ministerio. Podrán efectuarse entregas parciales, diferentes a las contractuales, en cuyo caso se suscribirán actas de recibo parcial, pero en todo caso el pago solo se hará contra la suscripción del acta de recibo correspondiente a la fecha de entrega contractual, previo el trámite administrativo a que haya lugar y una vez se cuente con la disponibilidad de PAC. **(EN CASO DE QUE APLLIQUE)**

CLÁUSULA DÉCIMA QUINTA. - GARANTÍAS A CARGO DEL CONTRATISTA: Dentro de los dos (2) días hábiles siguientes a la suscripción del contrato, el Contratista deberá constituir y allegar al Grupo Adquisiciones de la Dirección de Contratación Estatal, oficina 421A, la Garantía de Cumplimiento a favor del Ministerio de Defensa Nacional – Unidad de Gestión General – Dirección Administrativa NIT. 899.999.003-1, a través de un contrato de seguro contenido en una póliza, o a través del patrimonio autónomo, o a través de garantía bancaria, que cubra los siguientes amparos:

(I) GARANTÍA DE CUMPLIMIENTO:

A. CUMPLIMIENTO DEL CONTRATO: Por el diez por ciento (10%) del valor total del contrato, con una vigencia igual al plazo de ejecución de este y cuatro (4) meses más, y de las prórrogas si las hubiere. Que también cubra la cláusula penal y multas si se encuentran establecidas.

B. CALIDAD DEL SERVICIO: Por el cincuenta por ciento (50%) del valor del contrato, con una vigencia igual al plazo de ejecución del mismo y catorce (14) meses más.

PARÁGRAFO PRIMERO: En la garantía de cumplimiento deberá constar expresamente que se ampara el cumplimiento del contrato, las modificaciones unilaterales y de común acuerdo que a ello se le introduzcan, el pago de las multas y de la cláusula penal pecuniaria convenidas y si se trata de garantía **diferente** a una póliza de seguro se entiende que la entidad aseguradora renuncia al beneficio de excusión.

PARÁGRAFO SEGUNDO. - RESTABLECIMIENTO O AMPLIACIÓN DE LAS GARANTÍAS. - El **CONTRATISTA** deberá restablecer el valor de las garantías antes mencionadas, cuando éste se haya visto reducido por razón de las reclamaciones efectuadas por **EL MINISTERIO.** De igual manera, en cualquier evento en que se aumente o adicione el valor del contrato y/o se prorrogue su término, el Contratista deberá ampliar el valor de la garantía única otorgada y la ampliación de su vigencia según el caso. En todo caso el Contratista deberá reponer la garantía, cuando el valor de la misma se vea afectado por razón de siniestros presentados, dentro de los cinco (5) días calendarios siguientes a la notificación del acto que deje en firme la sanción correspondiente.

PARÁGRAFO TERCERO. - Si el Contratista se negare a constituir las garantías, así como a no otorgarlas en los términos, cuantía y duración establecidos en esta cláusula, el Ministerio podrá declarar la caducidad del presente contrato.

PARÁGRAFO CUARTO. - En tratándose de garantías consistentes en pólizas de seguro, éstas no expirarán por falta de pago de la prima o revocatoria unilateral.

PARÁGRAFO QUINTO. - El Contratista se obliga para con el Ministerio a mantener vigente la garantía de cumplimiento hasta la liquidación o término exigido en el respectivo amparo en los términos señalados en el artículo 2.2.1.2.3.1.7 y subsiguientes del Decreto 1082 de 2015.

PARÁGRAFO SEXTO.- En el evento en que la entidad que expide la Póliza de seguro que sirva de garantía del presente contrato, sea intervenida, tomado su control o liquidada por el Gobierno Nacional a través de entidad competente y con ello se genere incertidumbre sobre el pago o efectividad de la garantía aportada por el **CONTRATISTA,** deberá de manera inmediata presentar nuevas pólizas o remplazar la expedida por la compañía de seguros intervenida, sujeta a toma de control o en proceso de liquidación.

CLÁUSULA DÉCIMA SEXTA. - SUPERVISIÓN: La supervisión y control en la ejecución del presente contrato se ejercerá a través del (la) Jefe Oficina de Respuestas a incidentes Cibernéticos CSIRT, o quien haga sus veces, quien a su vez se denominará el Supervisor del mismo. En el evento de cambio de supervisor no será necesario modificar el Contrato y la designación se efectuará mediante comunicación escrita por el competente contractual, copia de la cual deberá enviarse a EL CONTRATISTA. Para estos efectos, el supervisor estará sujeto a lo dispuesto en el numeral 1 del artículo 4 y numeral 1 del artículo 26 de la Ley 80 de 1993, artículo 83 de la Ley 1474 de 2011 y demás normas establecidas sobre la materia. La designación de la presente supervisión se entiende comunicada al funcionario anteriormente mencionado, a través del sistema electrónico de contratación pública SECOP II, en el cual tiene acceso a toda la información y documentación precontractual, contractual y post contractual, para ejercer sus funciones.

EL SUPERVISOR tendrá las siguientes obligaciones:

1. Suministrar toda la información normativa y técnica disponible para la ejecución del contrato, así como también, brindar el apoyo administrativo y logístico que se requiera.

2. Estar inscrito en el sistema electrónico de contratación pública SECOP II y mantener habilitado su usuario, con el fin realizar toda la gestión contractual correspondiente a su supervisión, de conformidad con la Guía vigente que para el efecto expide Colombia compra eficiente.

3. Suscribir el Acta de Inicio de ejecución del contrato junto con el CONTRATISTA (si aplica).

4. Realizar seguimiento técnico, administrativo, financiero, contable, y jurídico a la ejecución del contrato, lo que le permite acceder en cualquier momento a las instalaciones físicas en donde se desarrollen las actividades del **CONTRATISTA** y a los documentos e información relacionada con la ejecución del contrato.

5. Exigir al CONTRATISTA la información que considere necesaria para verificar la correcta ejecución del contrato y para ejercer de manera general el control del mismo.

6. Exigir el cumplimiento del contrato en todas y cada una de sus partes.

7. Verificar directamente que el CONTRATISTA cumpla con las condiciones de ejecución del contrato según los términos pactados, para lo cual tendrá la facultad de requerirlo por escrito, con el fin de que corrija el incumplimiento en el que esté incurriendo o pueda incurrir.

8. Emitir por escrito las instrucciones que sean requeridas para la adecuada ejecución del contrato. En caso de presentarse circunstancias que puedan afectar la correcta ejecución del contrato, el supervisor deberá informarlas mediante oficio, a más tardar dentro de los tres (3) días hábiles siguientes a la ocurrencia de las mismas al competente contractual para su conocimiento y actuación correspondiente

9. Verificar mediante visitas o mediante el examen de los documentos que el supervisor considere pertinente, las condiciones de ejecución del objeto contratado.

10. Realizar si es del caso, las pruebas que considere necesarias para verificar que los servicios y/o bienes cumplan con las características técnicas y funcionales exigidas en el presente contrato.

11. Verificar y dejar constancia del cumplimiento de las obligaciones con el Sistema de Seguridad Social Integral y Parafiscales, de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, en el artículo 23 de la Ley 1150 de 2007, la Ley 1562 de 2012 y el 1072 de 2015 "Decreto Único Reglamentario del Sector Trabajo", el Decreto 1833 de 2016 "Por medio del cual se compilan las normas del Sistema General de Pensiones. En caso contrario deberá dar aviso de esta circunstancia al Grupo Adquisiciones.

12. Verificar que el contratista entregue el certificado de vida útil de cada bien y/o elemento objeto del presente contrato, junto con la remisión o factura al momento de la entrega de los bienes y/o elementos en el almacén general del MDN - UGG, conforme a los rangos del Marco Normativo para entidades de Gobierno-Normas para el Reconocimiento, Medición, Revelación y Presentación de los Hechos Económicos de las Entidades de Gobierno, expedido por la Contaduría General de la Nación mediante Resolución 533 de 2015.

13. Verificar que el contratista adjunte el RUT actualizado en caso que la actividad económica que tenía registrada para la fecha de celebración del presente contrato, haya desaparecido y deba registrar una nueva, de conformidad con la Resolución 000114 del 21 de diciembre de 2020, modificada por la Resolución 0005 del 22 de enero de 2021, expedidas por la DIAN, mediante la cual actualiza el listado de códigos de las actividades económicas que los contribuyentes deberán mantener reportadas en su respectivo RUT, documento que deberá exigir al contratista para el trámite del único o primer pago según corresponda.

14. Solicitar oportunamente al competente contractual las modificaciones, prórrogas y adiciones al contrato.

15. Resolver todas las consultas presentadas por el CONTRATISTA y hacer las observaciones que estime conveniente. Si durante la ejecución del contrato se presentan dudas o diferencias que no puedan ser resueltas por el Supervisor, éste deberá remitirlas mediante oficio, dentro de los tres (3) días hábiles siguientes a la ocurrencia de las mismas, al competente contractual para su consulta y decisión, con copia al Grupo Adquisiciones.

16. Expedir el certificado de cumplimiento al CONTRATISTA respecto de las obligaciones objeto del presente contrato, previa entrega de la factura por parte del mismo (si a ello hubiere lugar) y la copia del documento que acredite el pago por parte del CONTRATISTA al Sistema de Seguridad Social Integral y/o Aportes Parafiscales, según corresponda. La documentación anterior deberá remitirla al Grupo Financiero de la Dirección Administrativa para el trámite de pago correspondiente.

17. Informar a la Dirección Administrativa cualquier demora e incumplimiento en las obligaciones del CONTRATISTA, dentro de los cinco (5) días siguientes a la ocurrencia de la demora o incumplimiento.

18. Rendir informes periódicos o cuando lo considere necesario, sobre la ejecución del contrato de conformidad con lo establecido en la Resolución No. 4130 del 16 de junio de 2022 "Manual de Contratación y de Convenios".

19. Constatar a la fecha de vencimiento del contrato su total cumplimiento. Si llegare a tener observaciones o inquietudes sobre la ejecución del mismo, no podrá expedir el certificado de cumplimiento final hasta tanto no sean clarificadas.

20. Elaborar a la terminación del contrato, el acta de liquidación final del mismo, siguiendo para tal efecto el modelo suministrado por el Grupo Adquisiciones, el cual deberá remitirse a la terminación del contrato al mencionado Grupo para ser revisada y aceptada por éste y proceder al trámite de firmas. La obligación aquí establecida, sólo se entenderá cumplida por el Supervisor, una vez se encuentre suscrita el acta final de liquidación por el Contratista y el Competente contractual.

21. Garantizar que se identifiquen y evalúen en las especificaciones relativas a las compras o adquisiciones de productos y/o servicios, las disposiciones relacionadas con el cumplimiento frente al Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST que exige el Artículo 2.2.4.6.27 del Decreto 1072 de 2015 o las normas que lo modifiquen o sustituyan. Para lo anterior deberá verificar que el contratista asista dentro de los tres (3) días hábiles siguientes a la suscripción del contrato a la inducción sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo y medio ambiente, realizada por el Área de Seguridad y Salud en el Trabajo del Grupo Talento Humano de la entidad.

    Dichas obligaciones estarán sujetas a ser verificadas, constatadas y deberán estar documentadas para su revisión por parte del Área de Seguridad y Salud en el Trabajo de la Dirección de Gestión del Talento Humano del MDN-UGG, en el momento en que se considere necesario de acuerdo con los estándares mínimos establecidos en el Decreto 1072 de 2015, la Resolución 312 de 2019 o la normas que lo complementen, adicionen, modifique o sustituya, y deberá estar vigente durante toda la ejecución del contrato.

22. Solicitar, si llega a ser necesario, la suspensión temporal de la ejecución del contrato por circunstancias de fuerza mayor o caso fortuito, justificando plenamente las circunstancias de tiempo, modo y lugar que originan los hechos de la suspensión, ante el competente contractual mediante documento escrito, para que éste emita su autorización.

23. El supervisor deberá aprobar en el expediente contractual electrónico que reposa en el SECOP II, el informe de ejecución, junto con el cumplido a satisfacción, y la factura, esta última si aplica, y los demás documentos exigidos para cada pago. Para efectos del trámite respectivo en la oficina de cuentas por pagar deberá adjuntar la constancia de aprobación respectiva.

24. El supervisor del contrato deberá de conformidad con el artículo 2.2.1.1.2.4.3 del Decreto 1082 de 2015, hacer seguimiento al cumplimiento y efectividad de las garantías durante su vigencia. Una vez hayan vencido las vigencias de las garantías según corresponda y dentro de los términos contractuales y legales, el supervisor realizará el cierre del expediente contractual, dejando constancia del cumplimiento del contrato y del uso o no de la garantía. Es importante tener en cuenta que en caso de que el Supervisor del Contrato se desvincule de la Entidad sin que se haya cerrado el expediente contractual, deberá entregar una

relación de los contratos a su cargo y que se encuentren en esta situación, a su superior jerárquico para su reasignación, seguimiento y control.

25. Las demás inherentes a la función asignada, contempladas en las Leyes 80 de 1993, 1474 de 2011 y las demás que le sean aplicables, así mismo las señaladas en la Resolución No. 4130 del 16 de junio de 2022 "Manual de Contratación y de Convenios", la cual puede ser consultada en la página WEB del Ministerio.

PARÁGRAFO PRIMERO. - POLÍTICA ANTISOBORNO Dar a conocer al CONTRATISTA la Política de Antisoborno implementada por el Ministerio de Defensa Nacional y los distintos canales dispuestos por el Ministerio – Unidad Ejecutora o Dependencia Delegataria para denunciar cualquier acto de soborno o de corrupción.

PARÁGRAFO SEGUNDO. - CAMBIO DE SUPERVISOR: Si se requiere el cambio de supervisor por razones de fuerza mayor o caso fortuito, ausencia temporal o definitiva, o por circunstancias debidamente justificadas, el competente contractual procederá a designar un nuevo supervisor. Si el supervisor en ejercicio se encuentra en condiciones de suscribir un acta lo hará conjuntamente con el designado en su reemplazo, en ésta constará: estado de ejecución del contrato, relación de documentos que entrega y observaciones que considere pertinentes. Si no es posible la suscripción conjunta dejará constancia del estado en que se encuentra el contrato al asumir el ejercicio de estas funciones.

PARÁGRAFO TERCERO.- PROCEDIMIENTO EN CASO DE INCONFORMIDAD DEL SUPERVISOR CON RELACIÓN A LA EJECUCIÓN DEL CONTRATO: De conformidad con lo dispuesto en el Manual de Contratación y Convenios del Ministerio de Defensa Nacional, cuando el Supervisor del contrato se encuentre en desacuerdo con la ejecución y desarrollo de las obligaciones pactadas en el contrato, o con la forma de los actos, documentos o circunstancias examinadas, deberá sin excepción formular todos sus reparos por escrito ante la Dirección Administrativa del Ministerio de Defensa Nacional, con el cumplimiento de los siguientes requisitos:

1. Los reparos a la ejecución contractual deben ser motivados con razonamientos fundados en hechos, circunstancias y normas en las que se apoye el criterio sustentado y deben comprender todas las observaciones y objeciones correspondientes.

2. El Supervisor deberá reportar los resultados más relevantes de su actuación y recomendará al competente contractual las actuaciones que considere más convenientes u oportunas para la normal ejecución del contrato.

3. En caso de apreciar el supervisor graves irregularidades en la ejecución del contrato que amenace su paralización, es obligación del Supervisor informar por escrito dentro de los cinco (5) días hábiles siguientes a la ocurrencia de los hechos al competente contractual, y

al Director de la Dependencia para la cual se ha contratado el servicio, con los mismos requisitos dispuestos en los numerales anteriores.

PARÁGRAFO CUARTO- LIMITACIÓN DEL SUPERVISOR: El Supervisor no estará facultado, en ningún momento, para adoptar decisiones que impliquen la modificación de los términos y condiciones previstos en el presente contrato, las cuales únicamente podrán ser adoptadas por los representantes legales de las partes, mediante la suscripción de modificaciones al contrato principal.

CLÁUSULA DÉCIMA SÉPTIMA.- SANCIONES EN MATERIA DE ACTUACIONES CONTRACTUALES: Una vez surtido el procedimiento a que alude el artículo 86 de la Ley 1474 de 2011, o la norma que lo sustituya o modifique, el **MINISTERIO** podrá declarar el incumplimiento, y, en consecuencia, imponer las siguientes sanciones: **a. MULTAS.-** En caso de incumplimiento, el **MINISTERIO** con el objeto de conminar al **CONTRATISTA** a cumplir con sus obligaciones, mediante acto administrativo motivado, le impondrá multas cuyo valor corresponderá al 0.5% del valor del contrato por cada día de retardo, sin que el total de estas multas sobrepase el 20% del valor total del contrato. **b. MULTA POR EL INCUMPLIMIENTO EN LA CONSTITUCIÓN DE LAS GARANTÍAS O REQUISITOS DE EJECUCIÓN A CARGO DEL CONTRATISTA:** En caso de incumplimiento por parte del **CONTRATISTA** en (i) la constitución de las garantías o las modificaciones que se deban efectuar a las mismas, o, (ii) los requisitos de ejecución a su cargo, el **MINISTERIO** con el objeto de conminar al **CONTRATISTA** a cumplir con estas obligaciones, mediante acto administrativo motivado, le impondrá multas, cuyo valor corresponderá al 1% del valor del contrato por cada día de retardo, sin que el total de estas multas sobre pase el 10% del valor total del contrato. **c. CLÁUSULA PENAL PECUNIARIA.-** En el evento de declararse la caducidad del contrato o su incumplimiento definitivo, el MINISTERIO, mediante acto administrativo motivado, le impondrá al **CONTRATISTA,** a título de pena pecuniaria y como estimación anticipada de perjuicios, la obligación de pagarle una suma equivalente al veinte por ciento (20%) del valor del contrato, en tratándose de un incumplimiento total, o proporcionalmente de acuerdo a la magnitud del incumplimiento. El **MINISTERIO** se reserva el derecho a reclamar, por cualquiera de los medios previstos por la Ley, los perjuicios adicionales que haya sufrido y que no se encuentren cubiertos por el monto de la cláusula penal pecuniaria cuyo pago se le imponga al **CONTRATISTA.** El pago de la pena no extingue la obligación principal a cargo del **CONTRATISTA.**

PARÁGRAFO PRIMERO.- LEGALIDAD DE LA SANCIÓN: Las sanciones pactadas en el presente contrato, se pactan e imponen con fundamento en el principio de autonomía de la voluntad previsto en el artículo 40 de la Ley 80 de 1993, en respeto al debido proceso que trata el artículo 17 de la Ley 1150 de 2007, y de conformidad con el procedimiento establecido en el artículo 86 de la Ley 1474 de 2011 y en los aspectos allí no contemplados se acudirá a lo señalado en el artículo 47 y subsiguientes de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

PARÁGRAFO SEGUNDO.- PUBLICIDAD DE LA SANCIÓN: Una vez en firme la sanción, **EL MINISTERIO** procederá a publicar la parte resolutiva del acto que la declara en el SECOP II y a comunicarla a la Cámara de Comercio en que se encuentre inscrito el Contratista. También se comunicarán a la Procuraduría General de la Nación. Las anteriores publicaciones se harán de conformidad con lo previsto en el artículo 31 de la Ley 80 de 1993, modificado por el artículo 218 del Decreto Ley 0019 de 2012.

PARÁGRAFO TERCERO.- APLICACIÓN DEL VALOR DE LAS SANCIONES PECUNIARIAS: Una vez se termine la audiencia en la que se impone la sanción, a través de resolución motivada que se entenderá notificada y ejecutoriada en dicho acto público, el **CONTRATISTA** dispondrá de quince (15) días calendario para proceder de manera voluntaria a su pago. Las multas no serán reintegrables aún en el supuesto que el **CONTRATISTA** dé posterior ejecución a la obligación incumplida. En caso de no pago voluntario y una vez en firme el respectivo acto administrativo, podrá ejecutarse la garantía contractual o tomarse del saldo a favor del **CONTRATISTA** si lo hubiere. Si esto último no fuere posible, se cobrará por vía ejecutiva.

CLÁUSULA DÉCIMA OCTAVA. - DEBIDO PROCESO PARA SANCIONES EN MATERIA DE ACTUACIONES CONTRACTUALES: Durante la ejecución del contrato, **EL MINISTERIO** podrá hacer uso de las acciones sancionatorias previstas en el contrato, las cuales se adelantarán respetando el derecho al Debido Proceso consagrado en el artículo 29 de la Constitución Política. En desarrollo del procedimiento para la aplicación de multas, sanciones por retardo en la entrega, efectividad de la cláusula penal pecuniaria, declaración de caducidad, declaraciones de siniestro contractual, y en general para todas aquellas actuaciones que generen sanción con ocasión de la actividad contractual, será precepto rector para la Entidad el respeto y la garantía del Debido Proceso consagrado en la Carta Constitucional. Por tanto, **El MINISTERIO,** en el proceso sancionatorio aplicará el procedimiento señalado en el artículo 86 de la Ley 1474 de 2011 y en los aspectos allí no contemplados se acudirá a lo señalado en el artículo 47 y subsiguientes de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

CLÁUSULA DÉCIMA NOVENA .- SANCIONES A EMPRESAS NACIONALES Y EXTRANJERAS: Se incluye en este contrato el texto del artículo 25 de la Ley 40 de 1993 que prevé: "Sin perjuicio de las demás sanciones a que hubiere lugar, cuando algún directivo de una empresa nacional o extranjera, o su delegado oculten o colaboren en el pago de la liberación de un secuestro de un funcionario o empleado de la misma o de una de sus filiales, el gobierno quedará facultado para decretar la caducidad de los contratos que esta empresa tenga suscritos con entidades estatales. En caso de que el hecho sea cometido por un funcionario o delegado de un subcontratista de la anterior, si ésta es extranjera, el Gobierno ordenará su inmediata expulsión del país. Los subcontratistas nacionales serán objeto de las sanciones previstas en esta Ley.

PARÁGRAFO PRIMERO. - El contratista nacional o extranjero que pague sumas de dinero a extorsionistas se hará acreedor a las sanciones previstas en este artículo.

PARÁGRAFO SEGUNDO. - Los contratos que celebren las entidades estatales colombianas con compañías extranjeras y nacionales llevarán una cláusula en la cual se incluya lo preceptuado en este artículo.

CLÁUSULA VIGÉSIMA. - CADUCIDAD ADMINISTRATIVA: Si se presenta algún hecho constitutivo de incumplimiento de las obligaciones a cargo del Contratista, que afecte de manera grave y directa la ejecución del contrato y evidencie que puede conducir a su paralización, el Ministerio por medio de acto administrativo debidamente motivado podrá decretar la caducidad y ordenar la liquidación en el estado en que se encuentre, todo de conformidad con lo previsto en el artículo 18 de la Ley 80 de 1.993. Ejecutoriada la resolución de caducidad, el contrato quedará definitivamente terminado y el Contratista no tendrá derecho a reclamar indemnización alguna. El Ministerio, hará efectiva la garantía pactada en el mismo, así como el valor de la pena pecuniaria, y procederá a su liquidación. Para efectos de esta liquidación, el Contratista devolverá al Ministerio los dineros que hubiere recibido por concepto del presente contrato, previa deducción del valor de los bienes y/o servicios entregados por aquel y recibidos a satisfacción por el Ministerio de conformidad con lo establecido en la cláusula primera del presente contrato. En el acta de liquidación se determinarán las obligaciones a cargo de las partes, teniendo en cuenta el valor de las sanciones por aplicar o las indemnizaciones a cargo del Contratista, si a esto hubiere lugar, y la fecha de pago.

CLÁUSULA VIGÉSIMA PRIMERA. - OTRAS FACULTADES EXCEPCIONALES: En caso de presentarse cualquiera de las circunstancias establecidas en los artículos 15, 16 y 17 de la Ley 80 de 1993 y demás normas concordantes, debidamente establecidas y documentadas, el Ministerio podrá hacer uso de las facultades excepcionales allí previstas.

CLÁUSULA VIGÉSIMA SEGUNDA. - CESIONES Y SUBCONTRATOS: El Contratista no podrá ceder el presente contrato a persona alguna natural o jurídica, nacional o extranjera, sin previa autorización escrita del Ministerio de Defensa Nacional, pudiendo éste reservarse las razones para negar dicha autorización.

El contratista solo podrá subcontratar parcialmente la ejecución del contrato, en tal caso la celebración de subcontratos no lo relevará de las responsabilidades que asume en virtud del presente contrato. **El Ministerio no adquirirá relación alguna con los Subcontratistas.**

CLÁUSULA VIGÉSIMA TERCERA.- CESIÓN DE DERECHOS ECONÓMICOS: En caso de que el contratista decida efectuar una cesión y/o pignoración de derechos económicos deberá solicitar su aceptación y notificación por parte del MINISTERIO DE DEFENSA NACIONAL, para lo cual deberá anexar como mínimo los siguientes documentos: 1) Contrato de cesión y/o pignoración de derechos económicos del contrato objeto de la cesión, firmado por el cesionario y el cedente donde se relacione en forma explícita lo siguiente: a) Valor de la cesión, b) Especificar si la cesión obedece al contrato principal y/o contratos adicionales. c) Aceptación por parte del cesionario de los descuentos de ley cuando aplique. 2) Acta de junta de socios o documento consorcial, en donde se autorice al representante legal de la figura correspondiente

para efectuar la cesión. 3) Certificado de existencia y representación legal del cesionario y el cedente cuando se trate de persona jurídica y/o certificado de inscripción cuando se trate de persona natural expedido por la Cámara de Comercio del domicilio correspondiente. 4) Certificación bancaria con número de cuenta y beneficiario donde se deben consignar los valores cedidos. 5) Declaración bajo juramento del cesionario en la cual se exprese el cumplimiento de lo previsto en el Decreto 4334 de 2008 en concordancia con el Decreto 1981 de 1988.

CLAUSULA VIGÉSIMA CUARTA. - CASO FORTUITO Y FUERZA MAYOR: Las partes quedan exoneradas de responsabilidad por el incumplimiento de cualquiera de sus obligaciones o por la demora en la satisfacción de cualquiera de las prestaciones a su cargo derivadas del presente contrato, cuando el incumplimiento sea resultado o consecuencia de la ocurrencia de un evento de fuerza mayor o caso fortuito debidamente invocadas y constatadas de acuerdo a la Ley y la jurisprudencia.

CLAUSULA VIGÉSIMA QUINTA. - SOLUCIÓN DE CONTROVERSIAS: Las partes acuerdan que para la solución de las controversias o diferencias que surjan entre el **CONTRATISTA** y **EL MINISTERIO** con ocasión de la firma, ejecución, interpretación, prorroga, terminación o liquidación de este contrato, así como de cualquier otro asunto relacionado con el presente contrato, podrán acudir en primer término a los mecanismos directos de solución de controversias contractuales establecidos en la Ley. Agotando este requisito sin que logre dirimirse la controversia las partes podrán acudir a la jurisdicción de lo contencioso administrativo.

CLÁUSULA VIGÉSIMA SEXTA. - CAUSALES DE TERMINACIÓN: El presente contrato se podrá terminar en los siguientes eventos: **1.** Por vencimiento del plazo de ejecución **2.** Por mutuo acuerdo entre las partes, solicitud que debe ser presentada mínimo con ocho (8) días de antelación a la fecha de solicitud de terminación anticipada del contrato **3.** Por cumplimiento del objeto contractual dentro del plazo de ejecución establecido o con anterioridad al vencimiento del mismo. **4.** En forma unilateral por parte del MINISTERIO conforme a lo establecido en la Ley. **5.** Por causas legales.

CLAUSULA VIGÉSIMA SEPTIMA. - SUSPENSIÓN TEMPORAL DEL CONTRATO: De común acuerdo las partes contratantes podrán suspender la ejecución de este contrato, mediante la suscripción de un acta en la cual conste el evento de suspensión y la fecha de su reinicio sin que para efectos del término de duración del contrato se compute el tiempo de la suspensión.

CLÁUSULA VIGÉSIMA OCTAVA- INDEMNIDAD: El **CONTRATISTA** se obliga para con **EL MINISTERIO,** a mantenerlo libre de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de sus subcontratistas o dependientes y realizadas durante la ejecución del contrato.

CLÁUSULA VIGÉSIMA NOVENA. - INHABILIDADES E INCOMPATIBILIDADES: EL CONTRATISTA declara bajo juramento, que se entenderá prestado con la firma del contrato, que ni el, ni su representante legal, ni sus socios se hallan incursos por sí o por interpuesta persona en las causales de inhabilidad e incompatibilidad señaladas por la Constitución Política, la Ley 80 de 1993, el artículo 18 de la Ley 1150, la Ley 1474 de 2011 y demás disposiciones que rijan la materia.

PARÁGRAFO ÚNICO.- INHABILIDADES E INCOMPATIBILIDADES SOBREVINIENTES: Si llegare a sobrevenir inhabilidad e incompatibilidad en EL CONTRATISTA, éste cederá el contrato previa autorización escrita del MINISTERIO o, si ello no fuere posible, renunciará a su ejecución.

CLÁUSULA TRIGÉSIMA. - DOCUMENTOS: Entre otros, los documentos que a continuación se relacionan se consideran para todos los efectos parte integrante del presente contrato y en consecuencia producen sus mismos efectos u obligaciones jurídicas y contractuales: 1.) Los Estudios y Documentos previos. 2) El Pliego de Condiciones Definitivo, Adendas y Formularios de Preguntas y Respuestas. 3.) Propuesta del Contratista en aquellas partes aceptadas por el Ministerio. 4.) Propuesta Económica 5.) Anexos del contrato 6.) Acto Administrativo de Adjudicación. 7.) Documentos que suscriban las partes.

CLÁUSULA TRIGÉSIMA PRIMERA. - TRIBUTOS: El Contratista pagará todos los impuestos, tasas, contribuciones y similares que se deriven de la ejecución del contrato, de conformidad con la ley colombiana.

CLÁUSULA TRIGÉSIMA SEGUNDA. - RÉGIMEN LEGAL: Este contrato se regirá por el Estatuto General de Contratación Administrativa vigente y sus Decretos Reglamentarios, las leyes de presupuesto, en general las normas Civiles y Comerciales vigentes, las demás normas concordantes que rijan o lleguen a regir los aspectos del presente contrato y las disposiciones Ministeriales que apliquen.

CLÁUSULA TRIGÉSIMA TERCERA. - INFORMACIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN: En virtud del presente contrato, el Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso durante su desarrollo. Igualmente el Contratista, debe suscribir el compromiso de confidencialidad señalado en el **Anexo No. 2** el cual hace parte integral del presente contrato.

CLÁUSULA TRIGÉSIMA CUARTA. - LIQUIDACIÓN: La liquidación del contrato que se suscriba se realizará dentro de **los 4 meses siguientes al termino de la suscripción a la plataforma**, en los términos y oportunidades establecidas en el artículo 60 de la Ley 80 de 1993, modificado por el artículo 32 de la Ley 1150 de 2007, en el artículo 217 del Decreto 0019 de 2012 y el artículo 11 de la Ley 1150 de 2007.

CLÁUSULA TRIGÉSIMA QUINTA. - MONEDA DEL CONTRATO: La moneda del presente contrato es la legal colombiana.

CLÁUSULA TRIGÉSIMA SEXTA. - SUJECIÓN A LA LEY COLOMBIANA: El presente contrato queda sujeto a la ley Colombiana.

CLÁUSULA TRIGÉSIMA SÉPTIMA. - PERFECCIONAMIENTO Y EJECUCIÓN.- El presente contrato se entiende perfeccionado con la suscripción del mismo. Para su ejecución se requiere la suscripción del acta de inicio previa aprobación de las Garantías que debe constituir el **CONTRATISTA**, expedición del registro presupuestal. El presente contrato se entiende comunicado al contratista con la aprobación y firma que este realiza del mismo a través del Sistema electrónico de contratación pública -SECOP II.

CLÁUSULA TRIGÉSIMA OCTAVA. - DOMICILIO CONTRACTUAL: Para efectos del presente contrato, el domicilio contractual será la ciudad de Bogotá D.C.

NOTA: El presente contrato es aprobado y firmado por las partes a través de la Plataforma SECOP II; no obstante, se suscribe por parte de la Directora Administrativa (E) del Ministerio de Defensa Nacional.

POR EL MINISTERIO,

ADRIANA FERNÁNDEZ G.
Directora Administrativa (E)

Revisó. Abogado Dirección Administrativa.
Revisó. Sandra Liliana Rojas Páez– Coordinadora Grupo Adquisiciones
Elaboró: Deisy Eliana Peña Valderrama - Abogada Grupo Adquisiciones

ANEXO No. 1
FICHA TÉCNICA

1.	Servicios para la detección temprana de amenazas cibernéticas		
	1.1	Descripción General	
		Se requiere proporcionar al Ministerio de Defensa Nacional (MDN) suscripción a plataforma de ciberinteligencia sobre amenazas cibernéticas con las capacidades necesarias para la detección temprana de amenazas cibernéticas que permita mitigar riesgos cibernéticos del sector defensa Mencionada plataforma desempeñará un papel fundamental en la ciberseguridad y defensa cibernética del MDN, contribuyendo en la protección proactiva de la disponibilidad, confidencialidad e integridad de la información y tendrá como mínimo las siguientes características: - Credenciales y licencia de acceso a servicios para un número ilimitado de usuarios corporativos. - Acceso a base de datos global de muestras de malware con un repositorio de como mínimo 50 mil millones de archivos desde más de 200 países y 6 mil millones de URL, correspondiente a más de 20 años de detección y análisis. - Capacidad de analítica de datos de mínimo de 1 millón de archivos nuevos, 2 millones de URLs, 1 millón de dominios y direcciones IP analizados por día con mínimo 70 proveedores de seguridad que producen determinaciones de maliciosidad. - Acceso a base de datos de inteligencia curada de amenazas cibernéticas, permitiendo realizar atribuciones y rastreo a mínimo 400 grupos de amenazas. - Capacidades de Inteligencia Artificial Generativa para digerir información de inteligencia sobre amenazas cibernéticas. - Capacidades de Attack Surface Management para monitorear activos externos en busca de vulnerabilidades o configuraciones incorrectas. - Servicio de Monitoreo de Amenazas Digitales para monitorear menciones en la web superficial, profunda y oscura. - Prevención de ataques a la cadena de suministro mediante el monitoreo de la seguridad de los activos de terceros y las menciones en la web superficial, profunda y oscura. - Servicio de análisis de archivos y artefactos en entornos controlados. - Gráficos de amenazas creados por la comunidad de investigación de seguridad y capacidad de crear gráficos privados accesibles solo para los usuarios de la entidad. - Interfaz de programación (API) para acceso automatizado a cualquier número de integraciones, con un límite diario de como mínimo 30.000 peticiones para dicho acceso API y no el número de integraciones.	
	1.2	Descripción de la Suscripción Plataforma por contratar:	
		1.2.1	Nombre de la plataforma: Google Threat Intelligence Marca: Google. Versión. Enterprice.
		1.2.2	El modelo de licenciamiento de la plataforma debe estar basado en un enfoque de suscripción tipo SaaS (Software as a Service). Este modelo incluye la capacidad necesaria de infraestructura tecnológica para operar en la nube, arquitectura multitenant, siendo el Ministerio de Defensa Nacional la matriz y permitiendo como mínimo 5 grupos de usuarios secundarios, garantizando que la información sensible de cada uno se encuentre separada y solo sea visible por ellos, según corresponda
		1.2.3	El contratista deberá garantizar que la plataforma contratada se encuentre alojada en una nube propia del fabricante, la cual podrá estar dentro de una nube pública.

		1.2.4	La plataforma utilizará técnicas de inteligencia artificial y aprendizaje automático para analizar los datos recopilados. Estas técnicas permitirán identificar patrones, anomalías y comportamientos sospechosos que puedan indicar actividades maliciosas o amenazas a la seguridad.
		1.2.5	La plataforma tendrá la capacidad de generar informes sobre la identificación de debilidades y vulnerabilidades potencialmente explotables por actores maliciosos, así como amenazas activas y latentes presentes en los sistemas y la infraestructura actual. Estas debilidades pueden deberse a configuraciones incorrectas, falta de actualizaciones o inherentes a la propia tecnología, entre otros.
	1.3	Plataforma Tecnológica – Arquitectura	
		1.3.1	La plataforma tecnológica debe ser capaz de soportar todos los servicios incluidos, con componentes tecnológicos proporcionados en un modelo cloud SaaS, durante el período de suscripción. Esto debe tener en cuenta las necesidades actuales y futuras del servicio en términos de escalabilidad, resiliencia y capacidades de integración, sin generar costos financieros adicionales para el MDN.
		1.3.2	Cada elemento de la plataforma debe ser capaz de soportar uno o varios procesos de los servicios realizados, y estar integrado en su mayoría mediante conectores nativos out-of-the-box o a través de API. Esto garantizará un funcionamiento óptimo sin fricciones, cumpliendo los más altos estándares de calidad y disponibilidad.
		1.3.3	La plataforma deberá permitir la configuración de visualizaciones exclusivas para los grupos de usuarios, basadas en las alertas identificadas por cada entidad. Se deberán mantener los principios de reserva y compartimentación de la información, asegurando que cada grupo de usuarios solo pueda visualizar lo relacionado a su propia infraestructura.
		1.3.4	La plataforma deberá permitir llevar a cabo una monitorización continua de las alertas generadas, incluyendo una evaluación para determinar su validez y relevancia. En caso de identificar alertas que sean consideradas falsos positivos, el contratista deberá descartar esta información, la cual no representan una amenaza real para el MDN.
		1.3.5	La plataforma debe contar con la capacidad de llevar a cabo el Triage de los eventos identificados, que implica analizar el impacto del evento detectado y determinar la categoría de la alerta, su criticidad y la prioridad correspondiente. Esta etapa es crucial para evaluar rápidamente la gravedad y el nivel de urgencia de cada alerta, lo que permite una gestión eficiente de los recursos y una respuesta adecuada a los incidentes de seguridad.
		1.3.6	La plataforma será responsable de alertar de manera oportuna sobre posibles amenazas de seguridad cibernética al CSIRT-Defensa y al grupo de usuarios donde ocurre el incidente, con el fin de ofrecer una respuesta rápida y eficaz.
		1.3.7	La plataforma deberá permitir generar informes ejecutivos y análisis técnicos detallados que ofrecerán una visión completa de las actividades de seguridad preventiva. Estos informes proporcionarán información precisa sobre las amenazas identificadas, las vulnerabilidades encontradas y posibles cursos de acción / recomendaciones.
		1.3.8	La plataforma tendrá la capacidad de hacer seguimiento a las alertas identificadas, y entregar información consolidada bajo temporalidades específicas, Ej: semanal, mensual, entre otras.
		1.3.9	Los requisitos mínimos de acceso y consumo de la plataforma son: • Acceso a una interfaz web que debe realizarse a través de un protocolo seguro y cifrado.

			• Soporte para un número ilimitado de usuarios. • Soporte para autenticación SSO/SAML. • Se podrá acceder a todas las operaciones y datos ofrecidos por el servicio a través de una interfaz de programación de aplicaciones (API) RESTful, con soporte para cualquier cantidad de integraciones, incluidas ServiceNow, IBM QRadar, AlienVault, Cortex XSOAR y CrowdStrike, entre otras. • Los datos devueltos por la API estarán en un formato estructurado que pueda procesarse automáticamente, por ejemplo, JSON o XML. • La API debe estar respaldada por documentación extensa y ejemplos de los diferentes tipos de solicitudes que se pueden realizar. Las respuestas deben estar en formato JSON y deben seguir estándares ampliamente aceptados y adoptados, como {json:api}. • La documentación de la API debería permitir a sus usuarios integrar su mecanismo de autenticación y probar las distintas llamadas. En este sentido, se valorará positivamente que la documentación proporcionada para la API se realice mediante herramientas de documentación específicas de la API como blueprints, Swagger, readme.io o equivalentes. • La API debe estar respaldada por un conjunto de bibliotecas oficiales para su uso, incluido el soporte para Python y Go. • La plataforma no tendrá limitaciones en el número de integraciones en productos y plataformas de seguridad de terceros donde se puedan activar los correspondientes conectores API de enriquecimiento y detección en dichas plataformas. • La plataforma ofrecerá extensiones de navegador oficiales para contextualizar los indicadores contenidos en interfaces de terceros y análisis automático o semiautomático de archivos e indicadores de red encontrados por sus usuarios.
		1.3.10	La plataforma deberá permitir y facilitar el trabajo en equipo, en concreto, serán requisitos los siguientes: • Mostrar un patrón de navegación a través de enlaces directos a informes de entidades, búsquedas específicas, etc. De forma que una determinada vista filtrada de la plataforma pueda ser compartida con otros usuarios compartiendo la URL asociada. • Poder compartir reglas de YARA con otros miembros del equipo o usuarios de la plataforma. • ACL de visibilidad asociadas a gráficos de investigación. • Ampliación e investigación colaborativa sobre gráficos. • Generación e intercambio de colecciones de IoCs. • Capacidad para estudiar los informes de archivos privados analizados por otros miembros del equipo. Las colecciones de activos de la superficie de ataque deben poder compartirse entre usuarios corporativos.
		1.3.11	La plataforma permitirá la definición de diferentes roles de usuario. Como mínimo, se permitirá la creación de los siguientes roles: • Administrador. Será el encargado de configurar el servicio en función de las necesidades del MDN, incluyendo la adición y eliminación de otros usuarios. • Usuario/analista. Podrá utilizar todas las funcionalidades del servicio, excepto la reservada al administrador.

	1.4	Servicio de Inteligencia curada y comunitaria	
		1.4.1	La plataforma debe tener capacidades para combinar inteligencia colaborativa de bases de datos de malware, inteligencia experta y curada de bases de datos de amenazas cibernéticas y capacidad de inteligencia artificial, proporcionando contexto y visibilidad completos, con las siguientes características mínimas: - Enriquecimiento de telemetría de seguridad. - Inteligencia de amenazas a nivel estratégico, táctico y operativo. - Mejora de procesos forenses y de respuesta a incidentes. - Gestión de la superficie de ataque. - Monitoreo de fuga de datos y marca. - Caza de amenazas. - Escaneo de archivos privados mediante análisis estático, dinámico e inteligencia artificial generativa.
		1.4.2	La plataforma debe reunir observaciones y patrones de amenazas globales, agregados colectivamente por una comunidad global de usuarios, investigadores y proveedores de seguridad, con las siguientes características mínimas: • Análisis de un mínimo de 1 millón de archivos cada día. • Un mínimo de 2 millones de URL analizadas cada día. • Un mínimo de 1 millón de {dominios, IPs} analizados cada día. • Mínimo 400 perfiles de grupos de actores de amenazas. • Mínimo 1.000 campañas/herramientas de actores documentadas cada mes.
		1.4.3	En su totalidad, la base de datos de amenazas deberá contener como mínimo 50 mil millones de archivos y 10 mil millones de indicadores de red. A su vez, debe estar construida a partir de contribuciones y telemetría de mínimo 3 millones de usuarios repartidos en más de 180 países
		1.4.4	La base de datos asociada al servicio debe cubrir una historia de al menos 15 años. A su vez, la información debe actualizarse en el servicio con una frecuencia de actualización cercana al tiempo real, es decir, al detectar una nueva IoC/amenaza, su análisis y caracterización deberían estar disponibles en minutos. Además de los aportes colectivos, el servicio debe contar con otras fuentes de datos como: • Telemetría y observaciones de una red global de SOAR y otras tecnologías de seguridad conectadas colectivamente a este repositorio de amenazas centralizado. • Intercambio de IoC e inteligencia sobre amenazas de una red de más de 50 proveedores de seguridad, incluidas empresas de antivirus/EDR/nextgen, IDS, soluciones de perímetro de red, listas de bloqueo de URL/dominios/IP maliciosos, etc. • Acuerdos de intercambio e intercambio de datos con grandes empresas tecnológicas. • Comentarios de extensiones de navegador instaladas en un parque de al menos más de 80.000 usuarios. • Rastreo de recursos web en línea. • Bucles de retroalimentación en el propio conjunto de datos, por ejemplo. extracción de dominios de archivos, detonación de archivos en entornos

			dinámicos e indexación de puntos de comunicación, descompresión de archivos, etc.
		1.4.5	La plataforma debe aplicar la inteligencia artificial de formas novedosas y debe demostrar una hoja de ruta ambiciosa para la IA aplicada al campo de la inteligencia sobre amenazas, incluyendo nuevos modelos de IA Generativa (LLM) para: • Análisis de fragmentos de código para generar informes en lenguaje natural fáciles de entender que explican el propósito del código y los riesgos potenciales para que los analistas de seguridad puedan identificar fácilmente comportamientos maliciosos dentro del código. • Incorpora artículos en línea que hacen referencia a las IOC y genera resúmenes en lenguaje natural y fáciles de entender para que los analistas puedan detectar lo que es relevante de un vistazo, acelerando la detección/respuesta a las amenazas. • Simplificar la investigación de inteligencia sobre amenazas al sintetizar una vasta base de conocimientos curada y revisada por expertos en resúmenes claros y concisos mediante búsqueda en lenguaje natural. Mencionados resultados de la inteligencia artificial deberán ser curados y filtrados por parte de expertos en ciberseguridad.
		1.4.6	La plataforma brindará a los usuarios la posibilidad de realizar busquedas utilizando el método más conveniente permitiendo: • Consultas en Lenguaje Natural procesadas por Inteligencia Artificial dirigiendo al usuario a: o Un resumen elaborado por IA basado en la base de datos de inteligencia curada que se vincula a las fuentes escritas por humanos para garantizar la fidelidad. o Indicadores de Compromiso asociados a su búsqueda. o Informes seleccionados y de inteligencia sobre amenazas comunitarias. o Perfiles de amenazas persistentes avanzadas comunitarios y seleccionados. o Campañas y colecciones curadas y adversarias comunitarias. • Amenazas dirigidas al Ministerio de Defensa Nacional atribuidas por Inteligencia Artificial que podrían manifestarse como: o Actores de amenaza. o Tácticas, Técnicas y Procedimientos. o Informes de inteligencia de amenazas. o Campañas. o Kits de herramientas de malware. o Vulnerabilidades. o Colecciones comunitarias de Indicadores de Compromiso. • Cargar un archivo para analizarlo o consultar un hash de archivo, URL, dominio o dirección IP específicos. • Búsquedas avanzadas sobre el conjunto de datos en formato de texto libre, utilizando parámetros/modificadores de búsqueda y operadores lógicos. Estas búsquedas avanzadas también deben poder ejecutarse como opciones desde un listado o mediante un asistente que simplifique la experiencia del usuario. Los inmuebles que podrán formar parte de búsquedas avanzadas deberán incluir, al menos:

			○ Detecciones y nombres de malware/amenazas por parte de al menos 60 proveedores de ciberseguridad. ○ Propiedades extraídas del análisis estático de dichas amenazas (por ejemplo, firma de código de autenticación de ejecutables). ○ Propiedades extraídas del análisis dinámico (por ejemplo, escritura en claves de registro). ○ Contenido binario. ○ Telemetría relativa al lugar donde se ha observado una determinada amenaza. ○ Contexto adicional proporcionado por otros usuarios de la plataforma en forma de comentarios. ○ Atribución. ○ Relación con otras entidades en el conjunto de datos. ○ Descripciones y perfiles de actores y campañas. • Capacidad para buscar vulnerabilidades con base en: ○ Fecha de publicación. ○ Puntuación de gravedad. ○ Estado de explotación ○ Consecuencias de la explotación. ○ Disponibilidad de mitigaciones. • Capacidad de buscar actores de amenazas en función de: ○ Región de origen. ○ Industrias y regiones objetivo. ○ Malware y herramientas asociados. • Capacidad para buscar familias de malware según: ○ Sistema operativo. ○ Función del malware, como puerta trasera, descargador, cuentagotas, etc. ○ Capacidades como detener o eliminar un servicio, ocultar ventanas, etc. • Capacidad de buscar campañas adversas basadas en: ○ Fecha de actividad Ej: más temprana o reciente. ○ Campaña global o enfocada individualmente. ○ Industrias y regiones objetivo. ○ Región de origen.
		1.4.7	La plataforma debe proporcionar múltiples indicadores que representen la confiabilidad de los IoC (Indicadores de compromiso) incluyendo: • Puntuación basada en la gravedad del indicador según la atribución a APT, campañas, tipo de malware y tiempo. • Detecciones y nombres de malware/amenazas por parte de al menos 60 proveedores de ciberseguridad. • {YARA, Sigma, IDS} reglas de la comunidad que detectan una determinada entidad. • Veredictos del comportamiento de archivos en un entorno de análisis dinámico (sandbox). • Firmas autenticadas, resaltando también aquellas firmas revocadas. • Votos de otros usuarios de la plataforma. • Inclusión en bases de datos de software legítimo, p.e. NIST NSRL. • Malicia/confiabilidad de entidades relacionadas.

		1.4.8.	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en: Actores de amenaza • Asociación con alias conocidos por la industria. • Fechas de última y primera vista. • País de origen. • Motivaciones. • Asociaciones de grupos con una línea de tiempo de ascendencia, tanto de grupos ya fusionados en un solo actor de amenazas como de aquellos que todavía son sospechosos, pero no confirmados. • Asociaciones con familias de malware, herramientas, vulnerabilidades, campañas e informes de inteligencia de amenazas. • Industrias y regiones objetivo, confirmadas y sospechadas. • TTP apalancados. • Indicadores de compromiso atribuidos. Familias de malware curadas • Papel en un ataque y capacidades. • Sistemas operativos afectados. • Asociaciones con actores de amenazas, indicadores de compromiso TTP e informes. • Nombres de detección. Campañas adversarias • Últimas y primeras fechas de actividad vistas. • País de origen. • Asociaciones con familias de malware, herramientas, vulnerabilidades, campañas e informes de inteligencia de amenazas. • Industrias y regiones objetivo. • TTP apalancados. • Indicadores de compromiso atribuidos. • Cronograma, incluido cuándo se aprovecharon los TTP y eventos para detectar la campaña.

		1.4.9	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en:
			
			Vulnerabilidades
			• Se proporcionará un resumen ejecutivo concreto para comprender rápidamente la vulnerabilidad.
			• Puntuación de gravedad basada en:
			  ○ Calificación de riesgo.
			  ○ Estado de explotación.
			  ○ Si se explota como día cero.
			  ○ Si se explota en la naturaleza.
			• Cronograma de vulnerabilidad.
			• Puntuaciones CVSS y EPSS.
			• Si está asociado a un CWE.

			• Mitigación. • Matriz de estado de explotación y calificación de riesgo, utilizada para priorizar la criticidad de una vulnerabilidad. • Productos vulnerables. • Detalles de reparación del proveedor. • Exploits conocidos. • Fuentes e informes de inteligencia de amenazas relacionados con la vulnerabilidad. • Historial de la vulnerabilidad, que muestra las actualizaciones sobre la vulnerabilidad y la fecha en la que ocurrió.
		1.4.10	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en: Colecciones de IOC creadas por la comunidad • Título y descripción de la colección. • Actores de amenazas asociados, si los hubiera. • Industrias afectadas, si se conocen. • Países afectados, si se conocen. • Listas de IOCs. • Patrones comunes y similitudes: agregación y clasificación de propiedades estáticas y dinámicas exhibidas por los IoC de la colección. • Telemetría: avistamientos en entornos reales, clasificados por país y fecha. • Reglas {YARA, Sigma, IDS} que identifican dicho conjunto de amenazas. • Listado de TTPs asociados, siguiendo el estándar MITRE ATT&CK. • Gráfico de relaciones para el conjunto de IoC. • Artículos y referencias online que hablen de la campaña/herramienta objeto de estudio o de cualquiera de los IoC contenidos en dicha colección. • Otras colecciones que comparten un subconjunto común de IoC. • Comentarios de una comunidad global de más de 1 millón de usuarios.
		1.4.11	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en: Archivos/hashes • Puntuación basada en la gravedad del indicador según la atribución a APT, campañas, tipo de malware y tiempo. • Análisis estático: o Cálculo de {md5, sha1, sha256}, así como otros hashes que pueden usarse para detecciones genéricas o análisis de similitud, incluidos authentihash, ssdeep e imphash. o Identificación del tipo de archivo. o Tamaño del archivo. o Extracción de metadatos Exif. o Disección de tipos de archivos específicos desde el punto de vista de indicadores maliciosos, por ejemplo. extracción y caracterización de macros y código VBA contenidos en documentos Office. o Extracción y visualización de iconos contenidos • Análisis dinámico: o Detonación en múltiples sandboxes, con cobertura para sistemas operativos Windows, OS X, Linux y Android.

- Correlación de la ejecución de las muestras con tácticas y técnicas documentadas en el estándar MITRE ATT&CK.
- Registro de comunicaciones de red, incluidas resoluciones DNS, conexiones a IP y URL. Así como cálculo de algoritmos para estudiar la similitud de comunicaciones, principalmente JA3.
- Actividad relacionada con el sistema de archivos: archivos abiertos, escritos, eliminados, extraídos/descargados y aquellos cuyos atributos se modifican.
- Actividad de registro: claves de registro abiertas, escritas, eliminadas.
- Actividad relacionada con procesos y servicios: procesos iniciados/inyectados/terminados, árbol de procesos, líneas de comando ejecutadas, servicios iniciados/detenidos/eliminados.
- Señales y mecanismos de sincronización: mutex creados, abiertos, eliminados.
- Módulos y bibliotecas cargados dinámicamente

- Relación con otros indicadores de la base de datos:
  - Dominios/URL/IP contactados.
  - Dominios/URL/IP contenidos en el archivo.
  - Archivos que crean el archivo en estudio cuando se ejecutan.
  - Archivos creados durante la ejecución del archivo en estudio.
  - Archivos comprimidos que contienen el archivo estudiado.
  - Correos electrónicos que contengan como archivo adjunto el fichero en estudio.
- Indicadores de entornos/incidentes reales:
  - Nombres de archivos utilizados por los atacantes.
  - Fechas de avistamiento.
  - países de avistamiento.
- Análisis y visualización del contenido del archivo:
  - Cadenas ASCII y Unicode, incluida la clasificación por prioridad/sospecha.
  - Visualización de contenidos en formato Hexadecimal.
  - Representación de documentos y otros formatos textuales para lectura, sin riesgo/filtrado de contenido malicioso, en el navegador.
- Análisis de agrupamiento y similitud:
  - Estándares de la industria: ssdeep, imphash, PE Rich hash, TLSH, TELFHash, etc.
  - Similitud basada en iconos de archivos y miniaturización del contenido visible.
  - Algoritmos propietarios que incluyen hash de propiedades/características estáticas y dinámicas.
- Contexto colectivo:
  - Comentarios de una comunidad de más de 1 millón de usuarios registrados.
- Atribución y contexto sobre los adversarios:
  - Cuando sea posible/tenga sentido, identificación de grupos de atacantes que utilizan el archivo como parte de su actividad maliciosa.
  - Cuando sea posible/tenga sentido, identificación de la campaña/ola de ataque en la que se ha utilizado el expediente en estudio.

			○ Artículos y referencias online que hablan del expediente en estudio.
		1.4.12	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en: Dominios • • Puntuación basada en la gravedad del indicador según la atribución a APT, campañas, tipo de malware y tiempo. • • Identificación, categorización y triangulación: ○ Contenido/categoría de amenaza, por ej. periódico online, phishing, CnC, etc. ○ Favicon extraído de la URL asociada al dominio, si existe. ○ Clasificación de popularidad/prevalencia basada en patrones de navegación de usuarios globales. ○ Resolución y registros DNS (A, AAAA, MX, TXT, etc). ○ Certificados HTTPs asociados, si los hubiera. ○ Información Whois. ○ Referencias al dominio indexado en buscadores. • Relación con otros indicadores de la base de datos: ○ DNS pasivo, ver, lista de IP históricas a las que resolvió dicho dominio. ○ Subdominios del dominio en estudio. ○ Dominios en el mismo nivel de profundidad bajo el dominio principal. ○ URL vistas en ese dominio. ○ Archivos descargados de URL vistas en ese dominio. ○ Archivos que se comunican con ese dominio cuando se ejecutan en un entorno de análisis dinámico. ○ Archivos que contienen dicho dominio en su cuerpo binario. ○ Registros históricos de Whois. ○ Certificados SSL históricos. ○ Registros DNS históricos (CNAME, MX, etc.). • Análisis de agrupamiento y similitud: ○ Estándares de la industria: JARM y JARM se aplican exclusivamente a la configuración del servidor. ○ Nombre de dominio similar (Distancia Levenshtein). • Contexto colectivo: ○ Comentarios de una comunidad de más de 1 millón de usuarios registrados. • Atribución y contexto sobre los adversarios: ○ Cuando sea posible/tenga sentido, identificación de grupos de atacantes que utilizan ese dominio como parte de su actividad maliciosa. ○ Cuando sea posible/tenga sentido, identificación de la campaña/ola de ataque en la que se ha utilizado el dominio en estudio. ○ Artículos y referencias online que hablan del dominio en estudio
		1.4.13	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en:

			Direcciones IP • Puntuación basada en la gravedad del indicador según la atribución a APT, campañas, tipo de malware y tiempo. • Identificación, categorización y triangulación: o Subred a la que pertenece. o Sistema autónomo. o Geolocalización. o Información Whois. o Referencias a la dirección IP indexada en los motores de búsqueda. • Relación con otros indicadores de la base de datos: o DNS pasivo, consulte, lista de dominios históricos que resolvieron dicha dirección IP. o URL avistadas en dicha IP. o Archivos descargados de URL vistas en dicha IP. o Archivos que se comunican con dicha IP cuando se ejecutan en un entorno de análisis dinámico. o Archivos que contienen dicha IP en su cuerpo binario. o Registros históricos de Whois. o Certificados SSL históricos. • Análisis de agrupamiento y similitud: o Estándares de la industria: JARM y JARM se aplican exclusivamente a la configuración del servidor. o IP caracterizadas bajo la misma subred. • Contexto colectivo: o Comentarios de una comunidad de más de 1 millón de usuarios registrados. • Atribución y contexto sobre los adversarios: o Cuando sea posible/tenga sentido, identificación de grupos de atacantes que utilizan dicha IP como parte de su actividad maliciosa. o Cuando sea posible/tenga sentido, identificación de la campaña/ola de ataque en la que se ha utilizado la propiedad intelectual en estudio. o Artículos y referencias online que hablan de la IP objeto de estudio.
		1.4.14	La plataforma contará con capacidades de análisis y contextualización de los informes de inteligencia de amenazas, como mínimo con base en: URL • Puntuación basada en la gravedad del indicador según la atribución a APT, campañas, tipo de malware y tiempo. • Identificación, categorización y triangulación: o Contenido/categoría de amenaza, por ej. periódico online, phishing, CnC, etc. o Favicón. o Extracción del dominio asociado. o Etiquetado desde el punto de vista de propiedades sospechosas/interesantes desde el punto de vista de la seguridad, p. contiene cadenas base64 excesivamente largas que no están asociadas con imágenes incrustadas. • Visita web e inspección:

			○ URL de redireccionamiento final, si la hubiera. ○ Resolución DNS (dirección IP) para el dominio asociado. ○ Código de estado de respuesta HTTP. ○ La longitud del contenido devuelto. ○ hash sha256 del contenido devuelto. ○ Claves y valores de las cabeceras HTTP de la respuesta. ○ Título del HTML devuelto, si corresponde. ○ Metaetiquetas HTML devueltas, si las hubiera. ○ Identificadores de seguimiento contenidos en el HTML devuelto, cuando estén presentes. ○ Redirigir cadena. ○ Enlaces salientes a otros dominios. • Relación con otros indicadores de la base de datos: ○ Archivos descargados desde la URL. ○ Archivos que se comunican con dicha URL cuando se ejecutan en un entorno de análisis dinámico. ○ Archivos que contienen dicha URL en su cuerpo binario. ○ Archivos Javascript utilizados como recursos en dicha URL. ○ URL que comparten los mismos identificadores de rastreador, por ejemplo. marcos publicitarios. • Señales de entornos/incidentes reales: ○ Fechas de avistamiento. ○ Países de avistamiento. • Contexto colectivo: ○ Comentarios de una comunidad de más de 1 millón de usuarios registrados. • Atribución y contexto sobre los adversarios: ○ Cuando sea posible/tenga sentido, identificación de grupos atacantes que utilizan dicha URL como parte de su actividad maliciosa. ○ Cuando sea posible/tenga sentido, identificación de la campaña/ola de ataque en la que se ha utilizado la URL en estudio. ○ Artículos y referencias online que hablan de la URL en estudio.
		1.4.15	Toda esta información analizada y contextualizada debe ser accesible a través de informes web, así como de forma automatizada a través de API. A su vez, estas propiedades deben ser pivotables, es decir, al visualizar y hacer clic en dicha propiedad, la plataforma debe presentar una lista de otros indicadores que comparten el mismo valor para dicha propiedad.
	1.5	Análisis activo de archivos, URL, dominios e IP	
		1.5.1	Los informes y análisis detallados anteriormente no se limitarán exclusivamente a indicadores ya procesados y conocidos por la plataforma. La plataforma debe permitir enviar nuevos artefactos, por ejemplo, archivos, e iniciar un análisis bajo demanda. Dicho análisis incluirá los detalles anteriormente descritos y el tiempo máximo de respuesta será de minutos.
		1.5.2	

			En cuanto al análisis de nuevos archivos, la plataforma debe permitir tanto el análisis colectivo, donde los archivos serán compartidos con otros usuarios y proveedores de seguridad para su estudio y determinación de malicia, como el análisis privado, donde dichos archivos y sus informes asociados no serían accesibles a personal externo al Ministerio de Defensa Nacional.
		1.5.3	Escaneo privado de archivos que incorpore análisis reputacional, estático, dinámico, de código y de similitud, y detonación de archivos en al menos dos (02) sistemas sandbox diferentes por sistema operativo, con mínimo soporte para Windows, Linux, Android y Mac OS X.
	1.6	Alertas y notificaciones	
		1.6.1	La plataforma permitirá seguir actores de amenazas, campañas y vulnerabilidades específicas que se consideren de interés para la entidad y recibir notificaciones por correo electrónico cuando los investigadores actualicen cualquiera de esos objetos. Del mismo modo, la plataforma debe permitir la configuración de alertas y notificaciones, p.e. detección de IoC/observables basada en una determinada regla YARA configurable por el usuario. Las reglas YARA deben aplicarse a todos los IoC/archivos nuevos que se indexen en la plataforma, generando las notificaciones correspondientes en tiempo real. La funcionalidad nativa de YARA debe ampliarse mediante módulos YARA para poder aplicar condiciones no solo al contenido binario de los archivos sino también a las propiedades y características del análisis de archivos y a los indicadores de red (dominios, direcciones IP, URL). Estas notificaciones pueden ser estudiadas en la interfaz web, enviadas vía correo electrónico o ingeridas vía API por aquellos usuarios del servicio que lo tengan configurado. La gestión de reglas de YARA también se puede realizar manualmente a través de la interfaz web o mediante programación a través de API. A su vez, la plataforma debe incluir un explorador de las reglas de la comunidad YARA publicadas en línea, con el fin de identificar nuevas amenazas y sus mecanismos de detección en base a la actividad e investigaciones de otros usuarios de la industria. Dichas reglas deben ser fácilmente exportables y configurables por el Ministerio de Defensa Nacional. Debe permitir obtener trazabilidad sobre los movimientos futuros de los actores, las campañas y las herramientas utilizadas por ellos, para permanecer sincronizados con su actividad global. De la misma manera, la funcionalidad descrita debe responder a otro caso de uso relacionado con el monitoreo de marca e infraestructura corporativa para identificar incidentes como: phishing, aplicaciones falsas, servidores corporativos comprometidos utilizados en campañas de malware, etc.
	1.7	Caza Retroactiva	
		1.7.1	Además de aplicar las reglas YARA al flujo de nuevos observables indexados por la plataforma y ampliar la funcionalidad de búsqueda descrita anteriormente, el servicio

			debe permitir la ejecución de reglas YARA retroactivamente contra la base de datos de archivos. Estas tareas de búsqueda se pueden iniciar manualmente a través de la interfaz web o mediante programación a través de API, permitiendo identificar la actividad histórica relacionada con actores y campañas.
	1.8	Exportación de información	
		1.8.1	La plataforma ofrecerá la posibilidad de exportar la información resultante de las consultas realizadas por los usuarios y los informes sobre IOC y TTP. Debe permitir exportar la información en un formato estructurado que pueda procesarse automáticamente, por ejemplo, JSON, CSV o XML. El soporte de STIX se valorará positivamente para entidades que representen conjuntos de IoC. Debe permitir la descarga de archivos analizados y documentados en la misma, para su potencial estudio y procesamiento en sistemas externos a la plataforma. A su vez, en los casos en que un determinado archivo haya sido detonado exitosamente en un entorno de análisis dinámico (sandbox), la plataforma deberá permitir la descarga de los siguientes artefactos, en caso de existir: • Seguimiento de comunicaciones de red (PCAP). • Registro de eventos de Windows (EVTX). • Volcado de memoria. • Informes de comportamiento detallados, incluidas las llamadas API de Windows asociadas
	1.9	Attack Surface Management	
		1.9.1	La plataforma deberá contar con la capacidad para descubrir activos y tecnología expuesta relacionada con el Ministerio de Defensa Nacional, con al menos los siguientes enfoques: Descubrimiento recursivo Va más allá del inventario desde un escaneo inicial, para descubrir y mapear activos desconocidos que de otro modo permanecerían ocultos y no administrados. Ejecuta tareas diarias de descubrimiento y comprobaciones de vulnerabilidad en cada activo identificado en su superficie de ataque externa. Ofrece un descubrimiento profundo de activos más allá de los rastreos y escaneos iniciales de Internet para descubrir y mapear activos desconocidos que de otro modo permanecerían sin administrar. A medida que analiza la semilla o activo inicial, se descubren nuevos activos relacionados. La capacidad de descubrimiento recursivo le permite volver a ejecutar tareas de descubrimiento y analizar cada nuevo activo descubierto, ampliando aún más el inventario de activos y descubriendo nuevas vulnerabilidades y configuraciones erróneas. Inteligencia de vulnerabilidad y exposición Realiza un amplio descubrimiento de vulnerabilidades, configuraciones erróneas y exposiciones a través de una combinación de comprobaciones activas y pasivas, haciendo coincidir los problemas con la tecnología que se ejecuta en su entorno y validando las exposiciones. Comprobaciones activas: realiza comprobaciones activas, que son cargas útiles benignas o scripts diseñados a partir de IOC para confirmar cuándo el activo de una organización es susceptible a las vulnerabilidades observadas en la naturaleza. Las comprobaciones activas están diseñadas a partir de IOC y otros

exploits conocidos. Depender únicamente de comprobaciones pasivas para identificar vulnerabilidades requiere que el equipo de seguridad confirme las vulnerabilidades antes de priorizar su corrección.

Descubrimiento de activos e integraciones de fuentes de datos
Descubrimiento de activos Las tareas de descubrimiento se ejecutan en cada semilla, especificada por el usuario o entidad identificada, generando una lista completa de inventario de activos externos. Los activos externos incluyen más que dominios, direcciones IP y certificados, y el equipo de seguridad requiere visibilidad del inventario ampliado.

Entidades de descubrimiento (semillas)

- **Puntos finales API**
- **Registro DNS**
- **Dominio**
- **Cuenta GitHub**
- **Repositorio GitHub**
- **Dirección IP**
- **Bloque de red**
- **Palabras clave única**
- **URL**

- Fuentes de datos
  - Repositorios DNS y Whois
  - Raspado web en Internet
  - Búsquedas de cuentas de redes sociales
  - Repositorios de amenazas del COI
  - Tablas de enrutamiento BGP
  - Escaneo de internet
  - Repositorios de activos en la nube
  - Fuerza bruta DNS
  - DNS pasivo
  - Archivos de zona DNS
  - Repositorios de desarrolladores
  - Proveedores de nube

Controles activos y controles pasivos

Cuando se verifica activamente, se toman acciones benignas en la entidad para probar la existencia de una vulnerabilidad conocida o una configuración incorrecta. Las cargas útiles deben diseñarse estratégicamente para evitar interrupciones en los sistemas del Ministerio de Defensa Nacional. Las comprobaciones activas deben utilizar inteligencia de amenazas para validar la exposición a vulnerabilidades y configuraciones incorrectas a través de comprobaciones activas. Las comprobaciones activas deben ser cargas útiles benignas o scripts diseñados a partir de IOC y NIST NVD para confirmar cuándo el activo de una organización es susceptible a las vulnerabilidades observadas en la naturaleza.

Las comprobaciones pasivas se utilizarán en escenarios en los que un exploit público no se puede verificar sin métodos más agresivos. La información de identificación pasiva se utilizará para comprender si es vulnerable según la versión de la tecnología.

			El servicio como mínimo tendrá la capacidad de descubrir los siguientes problemas: • Vulnerabilidades • Configuraciones erróneas • Indicadores de compromiso • Fugas • Certificados caducados o próximos a caducar • Sistemas de desarrollo expuestos. • Cookies inseguras • Cubos de nubes expuestos Además, esos problemas deben clasificarse por gravedad y si se confirman o sospechan. Los analistas del Ministerio de Defensa Nacional deberán poder contar con la capacidad de clasificar si el tema está resuelto o abierto, de igual forma debe ser posible clasificarlo de acuerdo con la prioridad. Toda la información sobre los problemas encontrados, los activos monitoreados y las tecnologías inferidas se agregarán en un panel que permitirá un fácil acceso a las alertas de mayor prioridad.
	1.10	Monitoreo de amenazas digitales	
		1.10.1	La plataforma deberá contar con la capacidad para buscar menciones de palabras clave en diferentes fuentes. Permitiendo tener visibilidad externa para mejorar la seguridad proactiva del Ministerio de Defensa Nacional al anticipar y planificar amenazas y saber si ha ocurrido un posible compromiso. La plataforma deberá cubrir las siguientes fuentes de información: • Red Abierta: También conocida como web de superficie o web clara, se trata de datos de fácil acceso indexados por los motores de búsqueda, pero que sólo comprenden el 10% de la información disponible. • Red Profunda: La mayor parte de la información en línea entra en esta categoría, en la que los datos no están indexados por los motores de búsqueda; esto incluye las redes académicas y la información que requiere pago o registro. • Red Oscura: Esta sección de Internet requiere software (como TOR) y configuraciones especiales para acceder a ella, y en ella suelen alojarse foros y mercados delictivos (la "clandestinidad"). Aprovechando la inteligencia sobre amenazas líder en la industria, el servicio no solo escuchará las discusiones de los ciberdelincuentes, sino que también tendrá acceso a canales privados cifrados y comprenderá los idiomas, la jerga y los códigos utilizados por los ciberdelincuentes. La plataforma utilizará filtros y procesamiento de lenguaje impulsado por aprendizaje automático (ML). La plataforma sabrá si hay un compromiso de datos o si actores maliciosos están apuntando a una organización, VIP y proveedores aprovechando las siguientes fuentes de datos:

			• Descubrimiento de dominio • Publicaciones en foros • Mensajes • Sitios de Copypaste • Listados de tiendas relacionadas con cibercrimen • Contenido web
		1.10.2	La plataforma como mínimo deberá monitorear los siguientes tipos de amenazas: • Amenaza Persistente Avanzada • Anonimización • Red de bots • Infraestructura comprometida • Fuga de documentos confidenciales • Fuga de credenciales • Fuga de tarjeta de crédito • Explotar • Riesgo de salud • Fuga de información • Actividad maliciosa • Infraestructura maliciosa • Malware • Divulgación de información personal • Suplantación de identidad • Secuestro de datos • Listado de víctimas de ransomware • Investigación de seguridad • Correo basura

2	Consideraciones Generales			
	2.1	Despliegue		
		2.1.1	El contratista se compromete a realizar la suscripción y despliegue de la plataforma en el modelo SaaS para la Oficina de Respuesta a Incidentes de Seguridad Cibernética (CSIRT-Defensa) a nivel sectorial.	
		2.1.2	El contratista, durante la ejecución del contrato, se compromete configurar los recursos necesarios para la visualización de la plataforma en las instalaciones correspondientes al CSIRT Defensa, incluyendo:	
			2.1.2.1	El contratista establecerá un panel de visualización personalizado que permita acceder de manera intuitiva a la plataforma. Este panel deberá proporcionar una vista completa y actualizada de la situación de seguridad cibernética en tiempo real de la superficie de ataque de la infraestructura tecnológica.
			2.1.2.2	La plataforma deberá permitir crear tableros interactivos que permitan explorar y analizar los datos de seguridad cibernética de manera dinámica. Estos tableros deberán ser intuitivos y personalizables, permitiendo la visualización de información específica según las necesidades y roles de los grupos de usuarios.
			2.1.2.3	La plataforma permitirá la visualización según las necesidades cambiantes del Ministerio de Defensa Nacional. Esto incluirá la posibilidad de agregar nuevas fuentes de datos, crear nuevos paneles o tableros, y adaptar la visualización a medida que evolucione el entorno de seguridad cibernética.

	2.2	Aspectos Generales	
		2.2.1	La plataforma debe admitir millones de consultas API diarias con una respuesta promedio de menos de un segundo. La plataforma debe poder escalarse de forma transparente y automática para absorber los picos de tráfico.
		2.2.2	La plataforma, deberá incluir la capacidad para describir patrones de amenazas globales basados en la telemetría global observada, a un nivel más digerido y estratégico.
		2.2.3	Durante el plazo de ejecución del contrato, el contratista deberá realizar una transferencia de conocimientos sobre el uso y personalización de la plataforma, así como análisis de la información para al menos 25 miembros del Ministerio de Defensa Nacional de como mínimo 48 horas.
		2.2.4	Toda la información y datos a los que tenga acceso en el marco de este contrato, y durante el tiempo de suscripción, incluyendo datos sensibles y hallazgos de vulnerabilidades, amenazas y riesgos cibernéticos es propiedad exclusiva del MDN de Colombia y no podrá ser divulgada, compartida o suministrada a terceros sin el consentimiento previo y por escrito del Ministerio con visto bueno del CSIRT-Defensa.
		2.2.5	Durante el tiempo de suscripción a la plataforma, toda la información y datos a los que tenga acceso serán almacenados y procesados en instancias de análisis aisladas en la nube, con contextos exclusivos y dedicados para el MDN de Colombia. Se implementarán medidas de seguridad apropiadas para proteger la confidencialidad, integridad y disponibilidad de la información, evitando cualquier acceso no autorizado o divulgación no deseada.
		2.2.6	La plataforma deberá contar con visualización intuitiva y accesible, mediante paneles, gráficos y mapas que presenten la distribución geográfica de las amenazas, las relaciones entre los actores maliciosos y otros datos relevantes.
		2.2.7	La plataforma tendrá la capacidad de compartir grafos privados y reglas YARA y colaborar de manera segura con los grupos de usuarios, facilitando la cooperación y el intercambio de información para una mejor gestión de las amenazas.
		2.2.8	La plataforma deberá incluir una base de conocimiento de adversarios curada que incluya actores, malware y campañas y permita ser analizada con telemetría y análisis de búsqueda de bases de datos de malware colaborativa permitiendo brindar información en términos de prevalencia histórica y en vivo en la naturaleza y distribución geográfica de amenazas, que pueda utilizarse para la ingeniería de detección, la cual deberá ser entregada dentro del plazo de ejecución del contrato.
		2.2.9	La plataforma debe reunir observaciones de amenazas globales y patrones de adversarios con un mínimo de: • 1 millón de archivos analizados por día. • 2 millones de URL analizadas por día. • 1 millón de {dominios, direcciones IP} analizados por día. • Más de 400 perfiles de actores de amenazas contextualizados. • Más de 1000 eventos/campañas/conjuntos de herramientas de malware significativos relacionados con actividad de amenazas notorias documentados mensualmente. En total, la base de datos de amenazas debe contener mínimo de 3 mil millones de archivos y 10 mil millones de indicadores de red. Para garantizar la diversidad de este conjunto de datos y su utilidad para comprender patrones y amenazas emergentes.

		2.2.10	La plataforma deberá tener actualizaciones periódicas para garantizar la incorporación de nuevas técnicas de ataque, variantes de malware y tendencias en el panorama de ciberseguridad.
		2.2.11	Como consecuencia de la suscripción a la plataforma, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato. Serán considerados por el contratista como información confidencial propiedad del Ministerio de Defensa Nacional, la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida, tampoco la duplicará, sustraerá, divulgará o alterará.
		2.2.12	En caso de no renovación de la suscripción, esta debe permitir portar la información de la entidad a una infraestructura propia del Ministerio de Defensa Nacional sea esta on-premise, en nube o ambas. La entrega de la información deberá realizarse en un formato que garantice su integridad y usabilidad. A la finalización de la suscripción, se deberá proporcionar a la entidad documento que certifique, la entrega o eliminación segura de los datos recolectados, almacenados o procesados durante el periodo de suscripción a la plataforma.
2.3		GARANTÍA TÉCNICA MÍNIMA, ASÍ:	
		2.3.1	El contratista deberá garantizar como mínimo la funcionalidad y correcta operación de la plataforma en conformidad con las condiciones del presente anexo, por 12 meses a partir de la suscripción a la misma por parte del Ministerio de Defensa Nacional, previo recibo satisfacción de la suscripción a la plataforma, así:
		2.3.2	El contratista deberá garantizar que, durante la suscripción a la plataforma, se garantizará su mantenimiento y operación, incluyendo la gestión y actualización del software e infraestructura tecnológica requerida para su provisión.
		2.3.2	El contratista se compromete a proporcionar soporte técnico, el cual estará disponible durante la vigencia de la suscripción y se brindará a través de canales de comunicación adecuados 5*8 en idioma español o 7*24 en otros idiomas.
		2.3.3	En caso de afectación a la información de la entidad, se deberá entregar un informe donde se detalle el incidente y la afectación causada a la información de la entidad y las medidas adoptadas para mitigar los daños.
		2.3.4	Durante el periodo de suscripción, la plataforma deberá contar con medios para la notificación de incidentes relacionados a su uso, así como para realizar consultas o aclaraciones sobre la información proporcionada por esta, tales como portal web, wiki, teléfono, correo, entre otros.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, el mismo **es aprobado y firmado por el contratista a través de la Plataforma SECOP II.**