Defensa

COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

CONTRATO DE SERVICIOS No. 259COGFM DIADF 2025
(19 DE SEPTIEMBRE DE 2025)

DEPENDENCIA SOLICITANTE	:	DEPARTAMENTO CONJUNTO DE COMUNICACIONES – CGDJ6
CONTRATISTA	:	UT 273COGFM H&Y 2025
NIT.	:	901988423-0
REPRESENTANTE LEGAL SUPLENTE:		JESÚS ALBERTO FRANCO ACOSTA
CEDULA DE EXTRANJERÍA No.	:	582.410
DIRECCIÓN	:	Calle 98 # 70 - 91 Ofc. 202-203
TELÉFONO	:	3229495938 - (601) 5804352
CORREO ELECTRÓNICO	:	Jbravo@heimcore.com.co
CIUDAD	:	Bogotá D. C.

Entre los suscritos a saber, señor Coronel GEOVANNY ANDRES SUAREZ PENAGOS, vecino de la ciudad de Bogotá D.C., identificado con la Cédula de Ciudadanía N° 80.177.974 expedida en Bogotá D. C., en su calidad de DIRECTOR ADMINISTRATIVO Y FINANCIERO DEL COMANDO GENERAL DE LAS FUERZAS MILITARES, designado mediante Resolución N° 3943 del 13 de septiembre de 2024, "*Por la cual se traslada a Oficial Superior del Ejercito Nacional*", debidamente posesionado como consta en Acta No. 645 del 16 de septiembre de 2024 y facultado para celebrar contratos conforme a lo dispuesto en la Ley 80 de 1993 y Resolución N° 4223 del 23 de junio de 2022, "*Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa Nacional, unas funciones de carácter administrativo y se dictan otras disposiciones.*", quien en adelante se denominará EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, por una parte y por la otra el señor JESÚS ALBERTO FRANCO ACOSTA, identificado con cedula de extranjería número 582.410, en calidad de Representante Legal de la UT 273COGFM H&Y 2025 con NIT. 901988423-0, conformada por conformada por medio de documento privado de fecha 20 de agosto de 2025 por las siguientes sociedades: 1) HEIMCORE S.A.S, con NIT 900425697 2, representada por el señor JESÚS ALBERTO FRANCO ACOSTA, identificado con cedula de extranjería número 582.410, con una participación del ochenta por ciento (80%); y 2) YEAPDATA S.A.S, con NIT 900311748-1, representada por la señora EDNNA CONSTANZA MARTINEZ, identificada con cedula de ciudadanía número 34.561.033 de Popayán, con una participación del veinte por ciento (20%); quién para efectos del presente contrato se denominará EL CONTRATISTA, hemos convenido celebrar el presente contrato, previos los siguientes considerandos: a) Que el estudio y documentos previos fueron elaborados por la DEPARTAMENTO CONJUNTO DE COMUNICACIONES (CGDJ6), de conformidad con lo establecido en el Decreto 1082 de 2015 y Ley 80 de 1993. b) Que el Proceso de Selección Abreviada de Menor Cuantía No. 273COGFM DIADF 2025, se adelantó atendiendo lo establecido en Ley 80 de 1993 y el Decreto No. 1082 de 2015. c) Que existen los recursos presupuestales necesarios para atender el pago del presente contrato. d) Que por medio de la Resolución No. 403 del 19 de agosto de 2025 se ordenó la apertura del Proceso de Selección Abreviada de Menor Cuantía No. 273COGFM DIADF 2025. e) Que el día 26 de agosto de 2025 se efectuó el Cierre y Recepción de ofertas. f) Que en sesión del día 10 de septiembre de 2025 por medio de Acta N° 670 el Comité de Adquisiciones recomendó al señor Director Administrativo y Financiero del COGFM y Ordenador del Gasto, adjudicar el Proceso de Selección Abreviada de Menor Cuantía No. 273COGFM DIADF 2025, a la UT 273COGFM H&Y 2025 para el LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF. g) Que por medio de la Resolución N° 440 del 10 de septiembre de 2025, se decide el Proceso de Selección Abreviada de Menor Cuantía No. 273COGFM DIADF 2025 y se ordena la adjudicación a la UT 273COGFM H&Y 2025 para el LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF. h) Que habiéndose dado cumplimiento a todos los trámites y requisitos legales que exige la Contratación Estatal, es procedente la celebración del presente contrato, el cual se regirá por las siguientes: CLAUSULA PRIMERA.- OBJETO.- EL CONTRATISTA se obliga para con el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA a prestar el servicio de mantenimiento, soporte, garantía y

renovación de las plataformas tecnológicas del CGDJ6 del COGFM para el LOTE 2: LICENCIAS PROXY WEB; LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS y LOTE 5: SUSCRIPCIÓN WAF, de conformidad con las especificaciones técnicas, aspectos técnicos ponderables, personal para la ejecución del contrato y cuadro de precios descritos en el Anexo Único, el cual forma parte integral del presente contrato. CLAUSULA SEGUNDA. - VALOR TOTAL DEL CONTRATO. - El valor total del presente contrato es por la suma de mil setecientos sesenta y nueve millones doscientos quince mil PESOS M/CTE. ($1.769.215.000,00) exento o excluido de IVA según aplique e incluidos demás impuestos, tasas y gravámenes que se causen por el hecho de su celebración, ejecución, liquidación. CLAUSULA TERCERA. – FORMA Y CONDICIONES DE PAGO.- El valor del contrato se pagará de forma parcial o total, dentro de los sesenta (60) días calendario siguientes, de conformidad con la Ley 2024 del 23 de julio de 2020 "por medio de la cual se adoptan normas de pago en plazos justos en el ámbito mercantil y se dictan otras disposiciones en materia de pago y facturación", al acta de recibo a satisfacción parcial o total del objeto del contrato, suscrita por el supervisor del contrato y el contratista o su delegado, presentación de la respectiva factura donde se registre: - fecha, valor de los bienes suministrados o de los servicios prestados IVA exento o excluido según aplique, y alta de entrada al almacén según aplique; asimismo, deberá acreditar el pago de los aportes a seguridad social, ARL y parafiscales mediante certificación expedida y soportada (planillas de pago) del pago de aportes parafiscales por el revisor fiscal o en su defecto por el representante legal a fecha 30 del mes vencido anterior a la fecha de pago, de acuerdo a la autorización de PAC, situación de recursos por la Dirección del Tesoro Nacional, (Ministerio de Hacienda) y cumplimiento de los demás trámites administrativos a que haya lugar. PARÁGRAFO PRIMERO: el pago se efectuará mediante consignación a la **Cuenta Ahorros No. 003334083 del Banco de Bogotá** o en otro banco o cuenta que el contratista designe con anterioridad al vencimiento del pago, con sujeción a lo previsto en las disposiciones cambiarias, por medio de aviso escrito con no menos de treinta (30) días calendario de anticipación, previa entrega de la certificación bancaria y activación de la cuenta en el SIIF. PARÁGRAFO SEGUNDO: El contratista en caso de estar obligado a facturar electrónicamente deberá enviar la facturación electrónica debidamente validada por la DIAN, conforme a lo estipulado en el Decreto 358 del 05 de marzo de 2020, la resolución 000042 del 05 de mayo de 2020 y la Directiva Presidencial No. 9 de 2020, al correo **siifnacion.facturaelectronica@minhacienda.gov.co** y cumplir con los lineamientos de elaboración de la facturación emitidos por SIIF Nación para la recepción de facturación electrónica así: Recepción centralizada por parte de la entidad PGN: Es responsabilidad del Contratista (Emisor FE, ND, DC) registrar en la factura, según sea el caso, los siguientes datos en los campos solicitados: a) Por regla general se debe diligenciar en la sección de la factura Notas u Observaciones, entre #$ el código de identificación de la entidad del Presupuesto General de la Nación (PGN) que está adquiriendo a la cual le va a enviar la factura, los datos del contrato o identificación de la caja menor y correo del supervisor o cuentadante o el correo que defina la Entidad que opte por recepción centralizada, finalizando con #$, debidamente separados por punto y coma, según los siguientes ejemplos: Para la recepción centralizada por parte de la entidad PGN: #$15-01-02-000; Contrato No 259COGFM DIADF 2025; **facturaciondiadf@cgfm.mil.co** #$. b) Si el contratista al elaborar y emitir la factura electrónica (FE), nota debito (ND), nota crédito (DC) mediante operador tecnológico autorizado, solución gratuita de la DIAN o software propio, tiene la posibilidad de definir el asunto del correo remisorio de los documentos electrónicos al adquiriente, debe registrar los siguientes datos: PCI; Identificación del contrato o caja menor; Correo del supervisor o cuentadante de caja menor que adquiera bienes y servicios o el correo que defina la entidad que opte por recepción centralizada, así: Para la recepción centralizada por parte de la entidad PGN: 15-01-02-000; Contrato No 259COGFM DIADF 2025; **facturaciondiadf@cgfm.mil.co**. Es obligatorio diligenciar en la sección de la factura datos del emisor, en el campo "correo" la dirección electrónica del proveedor o contratista, en donde le será notificado en caso de existir fallas en la validación del correo, se recuerda que si la factura no es recibida y registrada en el SIIF Nación no va a ser posible generar obligaciones a favor de los proveedores y contratistas que están obligados a facturar electrónicamente, por cuanto éstas son un requisito para su elaboración. PARÁGRAFO TERCERO: EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA no se responsabiliza por la demora presentada en el pago de las facturas al CONTRATISTA cuando ella fuere ocasionada por encontrarse incompleta la documentación de soporte o por no ajustarse a cualquiera de las condiciones establecidas en el presente contrato, o cuando presente errores matemáticos en la liquidación. CLAUSULA CUARTA – SUJECIÓN DE LOS PAGOS A LAS APROPIACIONES PRESUPUESTALES.- El valor del presente contrato se pagará con cargo al certificado de Disponibilidad Presupuestal N° 40325 de fecha 26 de mayo de 2025, con cargo a la Unidad Ejecutora 15-01-02-000, expedido por el Jefe de Presupuesto, para la vigencia fiscal 2025, distribuido de la siguiente manera:

RUBRO PRESUPUESTAL				**VALOR PRESUPUESTO DISPONIBLE**
CÓDIGO	**DESCRIPCIÓN**	**RECURSO**	**DEPENDENCIA**	
A-02-02-02-008-003	SERVICIOS PROFESIONALES	10	CGDJ6	294.000.000,00

	CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS SERVICIOS DE INVESTIGACIÓN, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)			
A-02-02-02-008-004	SERVICIOS DE TELECOMUNICACIONES, TRANSMISIÓN Y SUMINISTRO DE INFORMACIÓN			1.475.215.000,00
VALOR TOTAL PRESUPUESTO DISPONIBLE:				**1.769.215.000,00**

CLAUSULA QUINTA - PLAZO DE EJECUCIÓN. - El plazo de ejecución del presente contrato será hasta el 12 de diciembre de 2025, contado a partir del día hábil siguiente a la aprobación de la garantía por parte de la Dirección Administrativa y Financiera del Comando General FF.MM, previa expedición del registro presupuestal. CLAUSULA SEXTA. - PLAZO DE DURACIÓN.- El plazo de duración del contrato será de seis (6) meses adicionales al plazo establecido para la ejecución. Este plazo aplica únicamente para trámites administrativos y no cuenta para ejecución. CLAUSULA SÉPTIMA.- LUGAR DE EJECUCIÓN.- El lugar de ejecución y prestación de los servicios será en el MINISTERIO DE DEFENSA NACIONAL- COMANDO GENERAL DE LAS FUERZAS MILITARES, – Dirección Tecnologías de la Información –DITIN–, ubicada en la Avenida el Dorado Carrera 54 No. 26 – 25 CAN Edificio Fortaleza, de la ciudad de Bogotá D.C., previa coordinación con el supervisor del contrato. CLAUSULA 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 DE DEFENSA - COMANDO GENERAL – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, para el adecuado desarrollo del contrato. CLAUSULA NOVENA. - OBLIGACIONES DEL CONTRATISTA. – El contratista se obliga para con el MINISTERIO DE DEFENSA - COMANDO GENERAL – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, entre otras a: El contratista se obliga para con el MINISTERIO DE DEFENSA - COMANDO GENERAL – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, entre otras a: 1) Cumplir con las especificaciones técnicas, estudio previo, el pliego de condiciones y el presente Contrato, en particular, con los plazos máximos establecidos. 2) Proveer a su costo, todos los servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el presente contrato. 3) Garantizar que ningún funcionario suministrará ninguna clase de información o detalle a terceros y que mantendrá como documentación clasificada todos los aspectos relacionados con el presente contrato, así como los asuntos técnicos e instalaciones del Comando General de las Fuerzas Militares, conocidos por el Contratista, durante el desarrollo de este contrato y con posterioridad al mismo. 4) Asumir en su totalidad los gastos ocasionados como transporte, perdida del material o daños ocasionados, que cubra la garantía. 5) Informar oportunamente al supervisor del contrato cualquier novedad que se presente en el curso de la ejecución del mismo. 6) Obrar con lealtad y buena fe en las distintas etapas contractuales evitando dilaciones y trabas. 7) Entregar al supervisor del contrato el certificado de aportes parafiscales debidamente suscrito por el representante legal o Revisor Fiscal. 8) Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones derivadas del presente contrato. 9) Responder en los plazos que el MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA establezca en cada caso, los requerimientos de aclaración o de información que le formule. 10) Cumplir cabalmente con sus obligaciones frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por lo cual el incumplimiento de esta obligación será causal para la imposición de multas sucesivas hasta tanto se dé cumplimiento, previa verificación de la mora mediante liquidación efectuada por la entidad administradora. 11) Constituir en debida forma, dentro de los tres (03) días hábiles siguientes a la comunicación de la expedición del registro presupuestal, la garantía que ampara el presente contrato. 12) Una vez radicada en la Entidad la factura original y/o cuenta de cobro, según aplique, el contratista deberá cargarla en el SECOP II, diligenciando los campos de pago, número de factura, fecha de emisión, fecha de recepción, valor total de la factura y estado, en cumplimiento a lo previsto en la Guía rápida de Gestión contractual para Proveedores en el SECOP II. 13) Elaborar y suscribir conjuntamente con el supervisor el cronograma de actividades del contrato, dentro de los cinco (05) días calendario siguientes a la comunicación de inicio del plazo de ejecución. 14) Observar y cumplir con las disposiciones legales en general del ordenamiento jurídico colombiano y en todo caso tener especial cumplimiento con lo dispuesto en el Decreto 1072 de 2015 en su artículo 2.2.4.6.28. Contratación, la cual prescribe: "El empleador debe adoptar y mantener las disposiciones que garanticen el cumplimiento de las normas de seguridad y salud en el trabajo de su empresa, por parte de los proveedores, trabajadores dependientes, trabajadores cooperados, trabajadores en misión,

contratistas y sus trabajadores o subcontratistas, durante el desempeño de las actividades objeto del contrato. Para este propósito, el empleador debe considerar como mínimo, los siguientes aspectos en materia de seguridad y salud el trabajo: 1. Incluir los aspectos de seguridad y salud en el trabajo en la evaluación y selección de proveedores y contratistas; 2. Procurar canales de comunicación para la gestión de seguridad y salud en el trabajo con los proveedores, trabajadores cooperados, trabajadores en misión, contratistas y sus trabajadores o subcontratistas; 3. Verificar antes del inicio del trabajo y periódicamente, el cumplimiento de la obligación de afiliación al Sistema General de Riesgos Laborales, considerando la rotación del personal por parte de los proveedores contratistas y subcontratistas, de conformidad con la normatividad vigente; 4. Informar a los proveedores y contratistas al igual que a los trabajadores de este último, previo al inicio del contrato, los peligros y riesgos generales y específicos de su zona de trabajo incluidas las actividades o tareas de alto riesgo, rutinarias y no rutinarias, así como la forma de controlarlos y las medidas de prevención y atención de emergencias. En este propósito, se debe revisar periódicamente durante cada año, la rotación de personal y asegurar que dentro del alcance de este numeral, el nuevo personal reciba la misma información; 5. Instruir a los proveedores, trabajadores cooperados, trabajadores en misión, contratistas y sus trabajadores o subcontratistas, sobre el deber de informarle, acerca de los presuntos accidentes de trabajo y enfermedades laborales ocurridos durante el periodo de vigencia del contrato para que el empleador o contratante ejerza las acciones de prevención y control que estén bajo su responsabilidad; y 6. Verificar periódicamente y durante el desarrollo de las actividades objeto del contrato en la empresa, el cumplimiento de la normatividad en seguridad y salud el trabajo por parte de los trabajadores cooperados, trabajadores en misión, proveedores, contratistas y sus trabajadores o subcontratistas. PARÁGRAFO. Para los efectos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST, los proveedores y contratistas deben cumplir frente a sus trabajadores o subcontratistas, con las responsabilidades del presente capítulo". 15) Entregar al Supervisor del Contrato, dentro de los cinco (05) días siguientes al perfeccionamiento del mismo el certificado del curso virtual de cincuenta horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto 1072 de 2015), el cual deberá permanecer vigente durante el plazo de ejecución del contrato. 16) Cumplir con el protocolo de bioseguridad MDN-COGFMPROGESHU-DIPEC.GI.95.1-2 V. 05 de fecha 5 de mayo de 2022, expedido por el Comando General de las Fuerzas Militares y aquel que lo modifique o derogue. 17) 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. CLAUSULA DECIMA – DERECHOS DEL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA. - 1) Supervisar el desarrollo y ejecución del presente contrato, y acceder a los documentos e información que soportan la labor del Contratista. 2) Solicitar y recibir información técnica respecto de los servicios que preste, bienes y demás elementos que suministre el Contratista en desarrollo del objeto del presente contrato. 3) Rechazar los bienes o servicios cuando no cumplan con las Especificaciones Técnicas exigidas. 4) Tramitar diligentemente las apropiaciones presupuestales que requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo, como consecuencia de la suscripción del presente contrato. 5) Asignar al contrato un supervisor a través del cual la Dirección Administrativa y Financiera del COGFM mantendrá la interlocución permanente y directa con el interlocutor designado por el Contratista. CLAUSULA DECIMA PRIMERA - OBLIGACIONES DEL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA. - 1) Colocar a disposición del CONTRATISTA los bienes y lugares que se requieran para el cumplimiento de las obligaciones del CONTRATISTA. 2.) Recibir a satisfacción los bienes que sean entregados y servicios prestados por el CONTRATISTA, cuando estos cumplan con las condiciones establecidas en el presente contrato. 3.) Pagar al CONTRATISTA en la forma pactada y con sujeción a las disponibilidades presupuestales y de PAC previstas para el efecto. 4.) Tramitar diligentemente las apropiaciones presupuestales que requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo como consecuencia de la suscripción del presente contrato. 5.) Asignar al contrato un Supervisor, a través de quien EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA mantendrá la interlocución permanente y directa con el CONTRATISTA. CLAUSULA DECIMA SEGUNDA. - ACTAS DE RECIBO. - Cumplido el recibo del objeto del contrato, dentro de los tres (3) días siguientes se suscribirá entre las partes EL ACTA DE RECIBO A SATISFACCIÓN PARCIAL Y/O TOTAL, en la cual se manifestará la conformidad con las condiciones en las que se hace la entrega, precios y valor total de la factura. Dichas actas serán suscritas por el Supervisor del contrato y por el CONTRATISTA o su delegado y comprometerá en su contenido tanto al CONTRATISTA como al MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA siendo solo hasta ese momento cuando se consideran entregados los bienes y prestados los servicios contemplados en el objeto contractual. CLAUSULA DÉCIMA TERCERA. - SUPERVISIÓN. - El Supervisor del presente contrato será la señor Mayor JOSE FRANCISCO LOMBANA CARDONA, Director Tecnologías de la Información TI o QUIEN HAGA SUS VECES, Cel: 3165775377, correo electrónico: joselom@cgfm.mil.co; quien ejercerá las actividades de supervisión y control de la ejecución del contrato que les corresponden directamente y tendrán las siguientes funciones básicas: 1.) Exigir al CONTRATISTA la información que considere necesaria para verificar la correcta ejecución del presente contrato. El CONTRATISTA está obligado a suministrar la información

solicitada inmediatamente, a no ser que se convenga un plazo cuando la naturaleza de la información exigida así lo requiera. 2.) Verificar directamente que el CONTRATISTA cumpla las condiciones de ejecución del presente contrato según los términos en los que se ha convenido, y requerir al CONTRATISTA para que corrija los incumplimientos. 3.) Realizar las pruebas que considere necesarias para verificar que los bienes y servicios objeto del contrato, cumplan con las características técnicas y funcionales exigidas en el presente contrato. 4.) Aprobar o improbar, en los términos y con los efectos previstos en este contrato, que los bienes y servicios suministrados, mediante visitas o mediante el examen de los documentos y elementos que EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA considere pertinentes, cumplan con las condiciones de ejecución del contrato, y verificar que su resultado se adecue a los términos del presente contrato. 5.) En caso de terminación anticipada del contrato por mutuo acuerdo de las partes, adelantar las labores pertinentes para determinar el valor de las compensaciones mutuas. 6.) EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, no ejercerá funciones de control de las actividades de los subcontratistas, ni de aprobación del resultado de las mismas; sin embargo, en el caso en que el CONTRATISTA adelante actividades que le son propias a través de subcontratistas, deberá disponer, bajo su costo, de su propio equipo de control de calidad, que estará obligado a suministrar a satisfacción del MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA la información que le requiera. 7) 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. 8) En general, vigilar y controlar que el CONTRATISTA cumpla con sus obligaciones para el normal desarrollo y ejecución del presente contrato. 9) Y tendrá las siguientes facultades en particular. a.) Rendir mensualmente informe preciso y detallado por escrito al MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, sobre el avance y ejecución del contrato, tanto en los aspectos técnicos, económicos y jurídicos que le competen al CONTRATISTA. b.) Rechazar los bienes y los servicios que no cumplan con las especificaciones técnicas descritas en el Anexo Único. c) Verificar la correcta ejecución y cumplimiento del contrato. d.) Exigir el cumplimiento del contrato en todas y cada una de sus partes. e.) Atender y resolver en coordinación con EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, todas las consultas sobre omisiones, errores, discrepancias o aclaraciones y complemento en los aspectos técnicas, descritos en las especificaciones técnicas. f.) Verificar y dejar constancia del cumplimiento de las obligaciones parafiscales de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, en concordancia con lo dispuesto en la Ley 1150 de 2007. g.) Elaborar y suscribir conjuntamente con el contratista dentro de los tres días hábiles siguientes a la comunicación de inicio del contrato, el cronograma de actividades del contrato, cuando aplique; h) Elaborar y suscribir el acta de liquidación del contrato. i.) Todas las demás atribuciones que se contemplen en los documentos del contrato. El SUPERVISOR ejercerá las actividades de supervisión y control de la ejecución del contrato que le corresponden directamente y tendrá las facultades establecidas en los artículos 83 y SS., de la Ley 1474 de 2011 y Resolución N° 4130 del 16 de junio de 2022, "Por la cual se expide el Manual de Contratación y de Convenios". PARÁGRAFO PRIMERO. LIMITACIONES DEL SUPERVISOR: El Supervisor no está facultado en ningún momento para adoptar decisiones que impliquen la modificación de los términos y condiciones previstas en el presente contrato, las cuales únicamente podrán ser adoptadas por los representantes legales de las partes, mediante la suscripción de una modificación al contrato principal. PARÁGRAFO SEGUNDO. CAMBIO DE SUPERVISOR: Cuando el MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, lo requiera o estime conveniente, podrá sustituir el supervisor del contrato sin necesidad de suscribir un contrato modificatorio, El cambio de supervisor será comunicado al contratista mediante oficio en el cual realizara la nueva designación. El supervisor deberá entregar sus funciones al nuevo supervisor designado, mediante acta suscrita conjuntamente la cual deberá contener como mínimo la siguiente información: estado de ejecución del contrato, relación de documentos que entrega, y observaciones que considere pertinentes. CLAUSULA DECIMA CUARTA.- GARANTÍA A CARGO DEL CONTRATISTA.- Dentro de los tres (3) días hábiles siguientes a la comunicación de la expedición del registro presupuestal, EL CONTRATISTA deberá, a través de la plataforma del SECOP II, enviar la Garantía Única de Cumplimiento a favor del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, NIT No. 800.230.729-9, expedida por Compañía de Seguros o entidad bancaria legalmente constituida en Colombia, que cubra los siguientes amparos: a) CUMPLIMIENTO DEL CONTRATO: Por el VEINTE POR CIENTO (20%) del valor total del contrato, cuya vigencia será igual al plazo de duración del contrato y de las prórrogas si las hubiere. b) CALIDAD DEL SERVICIO: Por el TREINTA POR CIENTO (30%) del valor total del contrato, la cual permanecerá vigente durante el plazo de ejecución del contrato y dos (02) años más y de las prórrogas si las hubiere. c) PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES: Por el CINCO POR CIENTO (5%) del valor del contrato, con una vigencia igual a la ejecución del contrato y tres (3) años más y de las prórrogas si las hubiere. PARÁGRAFO PRIMERO: En la póliza deberá constar expresamente que se ampara el cumplimiento del contrato, el pago de las multas y de la penal pecuniaria convenidas y que la entidad aseguradora

renuncia al beneficio de excusión. En todo caso el CONTRATISTA deberá reponer la garantía, cuando el valor de la misma se vea afectado por razón de los siniestros presentados, dentro de los tres (3) días calendarios siguientes a la notificación del acto que deje en firme la sanción correspondiente. PARÁGRAFO SEGUNDO: Si el CONTRATISTA se negare a constituir póliza de garantía, así como no otorgarla en los términos, cuantía y duración establecidos en esta cláusula, EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA podrá declarar la caducidad del presente contrato. PARÁGRAFO TERCERO: Las pólizas no expirarán por falta de pago de la prima o revocatoria unilateral. PARÁGRAFO CUARTO: El CONTRATISTA se obliga para con EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a mantener vigente la garantía hasta la liquidación del contrato. CLAUSULA DECIMA QUINTA.- 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 1993. 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 servicios y/o bienes entregados por aquel y recibidos a satisfacción por el Ministerio - Comando General - Dirección Administrativa y Financiera 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. CLAUSULA DECIMA SEXTA. – FUERZA MAYOR O CASO FORTUITO. - Para efectos de este contrato fuerza mayor o caso fortuito son todos aquellos eventos imprevisibles e irresistibles tales como naufrago, terremoto, inundaciones, apresamiento por parte del enemigo, actos de autoridad ejercidos por un funcionario público, perturbaciones de orden público, amenazas de acto terrorista, actos mal intencionados de terceros, etc., según lo previsto en el Código Civil Colombiano. En caso de ocurrencia de una causal de fuerza mayor o caso fortuito, la parte afectada deberá dar aviso en el término de cinco (5) días hábiles, contados a partir de la ocurrencia de la causal, para que la otra califique si el hecho es constitutivo o no de fuerza mayor o caso fortuito. En caso de ser el hecho constitutivo de fuerza mayor o caso fortuito, la demora será justificada y se entenderá prorrogado el término de la duración del contrato, por un lapso igual a aquel en que fue suspendido. En todos los casos de suspensión se levantará un acta en la cual conste la fecha de la suspensión, las causas que la originaron y la fecha estimada de reanudación. Reiniciados los trabajos se levantará la respectiva acta en la que consten las consecuencias de la suspensión. PARÁGRAFO PRIMERO: En caso de presentarse un evento de fuerza mayor o caso fortuito, que no afecte la totalidad del objeto del presente contrato, es decir que solo lo afecte parcialmente, la fuerza mayor solo operará para los servicios y/o bienes a los cuales les sobrevino la causal de fuerza mayor o caso fortuito. PARÁGRAFO SEGUNDO: En caso de que se presente un evento constitutivo de fuerza mayor o caso fortuito, que impida a cualquiera de las partes cumplir con sus obligaciones, dicha parte deberá emplear esfuerzos razonables para minimizar o mitigar cualquier retraso que se presente. CLAUSULA DECIMA SÉPTIMA. – DEBIDO PROCESO. - Durante la ejecución del contrato, EL MINISTERIO DE DEFENSA – COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, podrá hacer uso de las acciones sancionatorias previstas en el presente contrato, las cuales se adelantarán respetando el derecho al debido proceso consagrado en el Artículo 29 de la Constitución Política y en cumplimiento del procedimiento regulado en el artículo 86 de la Ley 1474 de 2011. En todo caso, EL MINISTERIO DE DEFENSA – COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, en el proceso sancionatorio que se adelante, brindará todas las garantías constitucionales y legales al CONTRATISTA para que ejercite su derecho a la defensa en audiencia y tenga la oportunidad de exponer las razones y/o motivos sobre los hechos, generadores de la afectación de la ejecución, contractual. En ningún caso procederá la imposición de sanción sin haberse brindado la oportunidad al CONTRATISTA de explicar las Circunstancia que impiden la ejecución normal y oportuna, del contrato. CLAUSULA DECIMA OCTAVA. – MULTAS.- Previa aplicación del precepto Constitucional del Debido Proceso citado en la cláusula décima octava, El MINISTERIO con la acreditación de las pruebas correspondientes, podrá aplicar las siguientes: a) MULTA POR INCUMPLIMIENTO PARCIAL DE LAS OBLIGACIONES DEL CONTRATO.- En caso de mora o incumplimiento parcial de alguna de las obligaciones derivadas del presente contrato por causas imputables al CONTRATISTA, salvo circunstancias de fuerza mayor o caso fortuito, conforme a lo establecido en el artículo 86 de la Ley 1474 de 2011, EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA podrá imponer al CONTRATISTA multas, cuyo valor se liquidará con base en el punto cinco por ciento (0.5%) del valor de los bienes y servicios dejados de entregar y prestar respectivamente, según aplique, por cada día de retardo y hasta por quince (15) días calendario. Esta sanción se impondrá conforme a la Ley y se reportará a la Cámara de Comercio competente de conformidad con lo previsto en el artículo 6.2 de la Ley 1150 de 2007. b) MULTA POR LA MORA EN LA CONSTITUCIÓN DE LOS REQUISITOS DE EJECUCIÓN Y

LEGALIZACIÓN.- Cuando el contratista no constituya dentro del término y en la forma prevista en el contrato, o en alguno de sus modificatorios, cualquiera de las garantías y/o alguno de los requisitos de legalización, el MINISTERIO – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA mediante acto administrativo motivado, le impondrá al CONTRATISTA multas, cuyo valor corresponderá al 0.5% del valor del contrato, por cada día de retardo y hasta por diez (10) días calendario, al cabo de los cuales el MINISTERIO – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA podrá optar por declarar la caducidad del mismo. c) MULTAS POR INCUMPLIMIENTO AL SISTEMA DE SEGURIDAD SOCIAL Y PARAFISCALES.- En caso de mora o incumplimiento de las obligaciones frente al Sistema de Seguridad Social y/o Parafiscales (Cajas de compensación familiar, Sena e ICBF) EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA podrá imponer al CONTRATISTA multas, cuyo valor se liquidará con base en un cero punto dos por ciento (0.2%) del valor del contrato, por cada día de retardo en la presentación de la certificación que evidencie el cumplimiento de la presente obligación y hasta por quince (15) días calendario. Esta sanción se impondrá conforme a la Ley y se reportará a la Cámara de Comercio competente de conformidad con lo previsto en el artículo 6.2 de la Ley 1150 de 2007. CLAUSULA DÉCIMA NOVENA.- PENAL PECUNIARIA. - En caso de declaratoria de caducidad o de incumplimiento total de las obligaciones derivadas del presente contrato, EL CONTRATISTA pagará al MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a título de pena pecuniaria, una suma equivalente al veinte por ciento (20%) del valor total del contrato. La imposición de esta pena pecuniaria se considerará como pago parcial y definitivo de los perjuicios que cause al MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA. No obstante, EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA se reserva el derecho de cobrar perjuicios adicionales por encima del monto de lo aquí pactado, siempre que los mismos se acrediten. Tanto el valor de las multas, como el de la cláusula penal pecuniaria serán descontados de los pagos que se efectúen al CONTRATISTA. El pago de la cláusula penal pecuniaria estará amparado mediante póliza de seguros en las condiciones establecidas en el presente contrato. CLAUSULA VIGÉSIMA. – LEGALIDAD DE LAS MULTAS Y DE LA CLAUSULA PENAL PECUNIARIA. - Las MULTAS Y LA CLAUSULA PENAL PECUNIARIA establecidas en el presente contrato se pactan e imponen en desarrollo del 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. PARÁGRAFO PRIMERO. - APLICACIÓN DEL VALOR DE LAS SANCIONES PECUNIARIAS: El valor de las multas y de la cláusula penal pecuniaria se tomará del saldo a favor del CONTRATISTA si lo hubiere, o de la garantía constituida. Si esto último no fuere posible, se cobrará por vía ejecutiva. PARÁGRAFO SEGUNDO. En la imposición de las multas por parte del MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA se dará cumplimiento al principio señalado en el artículo 86 de la Ley 1474 de 2011 del debido proceso. PARÁGRAFO TERCERO. Las multas impuestas se harán efectivas directamente por EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA pudiendo acudir entre otros a los mecanismos de compensación de las sumas adeudadas al CONTRATISTA, cobro de la garantía o cualquier otro medio para obtener pago incluyendo la jurisdicción coactiva en los términos previstos en el artículo 17 de la Ley 1150 del 2007. PARÁGRAFO CUARTO. - 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 el Decreto 1082 de 2015. PARÁGRAFO QUINTO. - 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 SEXTO. - 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 de EL CONTRATISTA si lo hubiere. Si esto último no fuere posible, se cobrará por vía ejecutiva. CLAUSULA VIGÉSIMA PRIMERA – SOLUCIÓN DE CONFLICTOS. - Conforme a lo establecido en la Ley 80 de 1993, las partes se comprometen a utilizar los mecanismos de solución previstos en la mencionada Ley, para lo cual, cualquiera de ellas podrá solicitar reunión con el fin de solucionar directamente el conflicto, la cual se llevará a cabo dentro de los cinco (05) días hábiles al recibo de la solicitud presentada, de lo cual, se dejará constancia por escrito. En caso de no solucionarse dentro de dicho término se procederá a utilizar los mecanismos alternativos de solución de conflictos contemplados en la citada norma para lo cual se tendrán diez (10) días hábiles siguientes a la

terminación del primer término. Una vez agotadas las anteriores etapas sin que haya mediado acuerdo entre las partes se acudirá al juez natural del contrato. La administración podrá ampliar los términos anteriormente previstos hasta la mitad del término inicialmente pactado. 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 - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, pudiendo éste reservarse las razones que tenga para negar dicha autorización. Si la persona a la cual se le va a ceder el contrato es extranjera debe renunciar a la reclamación diplomática. La celebración de subcontratos no relevará al CONTRATISTA de las responsabilidades que asume en virtud del presente contrato. EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA no adquirirá relación alguna con los Subcontratistas. CLAUSULA VIGÉSIMA TERCERA. – CESIÓN DE DERECHOS PATRIMONIALES Y 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 - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, 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 4334/2008 en concordancia con el Decreto 1981 de 1998. CLAUSULA VIGÉSIMA CUARTA.- INHABILIDADES E INCOMPATIBILIDADES. - El Contratista declara bajo la gravedad del juramento, la cual se entenderá cumplida con la suscripción del presente Contrato, que no se halla incurso en ninguna de las causales de inhabilidad o incompatibilidad señaladas en la ley. PARÁGRAFO. - 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. CLAUSULA VIGÉSIMA QUINTA. – ANTISOBORNO Y ANTICORRUPCIÓN: 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. CLAUSULA VIGÉSIMA SEXTA. – PROTECCIÓN DE DATOS PERSONALES: Las partes declaran que conocen y cumplen con la Ley 1581 de 2012 y sus normas reglamentarias, incluyendo el Decreto 1074 de 2015 y aquellas normas que la modifiquen, complementen o sustituyan. PARÁGRAFO: En caso de presentarse por alguna de las partes incumplimiento a lo anterior descrito, será responsable ante las entidades competentes y/o terceros EL MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES DE COLOMBIA – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, según corresponda y de acuerdo con el régimen jurídico aplicable para las partes. CLAUSULA VIGÉSIMA SÉPTIMA. - OBLIGACIONES DE ÉTICA Y CUMPLIMIENTO CON EL COMPROMISO DE LA TRANSPARENCIA: EL CONTRATISTA, declara cero tolerancias frente a hechos constitutivos de fraude, corrupción, soborno, lavado de activos y la financiación del terrorismo, en cualquiera de las actividades en las que la REPÚBLICA DE COLOMBIA MINISTERIO DE DEFENSA NACIONAL participa, el CONTRATISTA de manera directa o en su relacionamiento con aliados, contratistas, proveedores y clientes. El CONTRATISTA y EL Ministerio de Defensa Nacional – Comando General – Dirección Administrativa y Financiera, se compromete a: i) Actuar en forma transparente en el desarrollo del contrato, sin desconocimiento de las normas que prohíben hechos de corrupción, soborno nacional e internacional, fraude, lavado de activos y financiación del terrorismo, así como a comunicarse entre sí y a reportar ante el CONTRATISTA o ante las autoridades judiciales y administrativas competentes cualquier información relacionada con presuntos hechos de fraude, corrupción, soborno nacional o transnacional, lavado de activos y financiación del terrorismo durante la ejecución del contrato; ii) A mantener registros de todas las transacciones y disposición de activos, de acuerdo con las normas contables y de control interno aplicables, y a realizar todos los pagos y desembolsos a través de transferencias bancarias, sin efectuar pagos en efectivo. De otra parte, 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 – Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, 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 la República de Colombia y especialmente de aquellas que rigen el presente contrato, y les impondrá la obligación de no ofrecer o pagar sobornos o cualquier halago corrupto, a los funcionarios del Ministerio de Defensa Nacional-Comando General de las Fuerzas Militares- Dirección Administrativa y Financiera. CLAUSULA VIGÉSIMA OCTAVA. – CLAUSULAS EXORBITANTES: DE LA TERMINACIÓN, MODIFICACIÓN E INTERPRETACIÓN UNILATERAL.- Las partes acuerdan pactar las siguientes clausulas exorbitantes, así: a) La interpretación Unilateral del contrato, se realizará según lo establecido en el artículo 15 de la ley 80 de 1993. b) La Modificación Unilateral del contrato se realizará según lo establecido en el artículo 16 de la Ley 80 de 1993. c) La Terminación Unilateral del Contrato, se realizará, según lo establecido en el artículo 17 de la ley 80 de 1993. La interpretación y terminación unilaterales, así como la caducidad se ordenarán mediante resolución motivada, contra la cual procederá el recurso de reposición. Una vez declarada la caducidad se dará por terminado el contrato y se ordenará su liquidación en el estado en que se encuentre, sin que haya lugar a indemnización alguna para EL CONTRATISTA. CLAUSULA VIGÉSIMA NOVENA – RESERVA DEL PRESENTE CONTRATO. - El CONTRATISTA, se obliga para con EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, a no suministrar ninguna clase de información o detalle a terceros y a mantener como documentación clasificada todos los aspectos relacionados de las Fuerzas Militares de la República de Colombia conocidos o que llegaren a ser conocidos por el CONTRATISTA durante el desarrollo de este contrato o con posterioridad. EL MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA no adquirirá relación alguna con los Subcontratistas. CLAUSULA TRIGÉSIMA. - IMPUESTOS. - El Contratista pagará todos los impuestos, tasas, contribuciones y similares que se deriven de la ejecución del contrato, de conformidad con la Ley Colombiana. CLAUSULA TRIGÉSIMA PRIMERA – LIQUIDACIÓN DEL CONTRATO. - El presente contrato se liquidará de conformidad con lo dispuesto en el artículo 60 de la Ley 80 de 1993, modificado por los artículos 11 y 32 de la Ley 1150 de 2007 y el artículo 217 del Decreto 019 de 2012. CLAUSULA TRIGÉSIMA SEGUNDA. – RÉGIMEN LEGAL. – Este contrato se regirá por el Estatuto General de Contratación Administrativa vigente y sus Decretos Reglamentarios, las leyes de presupuesto y 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. CLAUSULA TRIGÉSIMA TERCERA. – INDEMNIDAD. - CONTRATISTA se obliga a mantener al MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, libre de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes realizadas durante la ejecución del contrato. CLAUSULA TRIGÉSIMA CUARTA – DOMICILIO. - Para todos los efectos, las partes acuerdan como domicilio contractual las siguientes direcciones: MINISTERIO DE DEFENSA - COMANDO GENERAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA: Avenida el Dorado CAN Carrera 54 No 26 - 25, Área de Contratación del Comando General. EL CONTRATISTA: Calle 98 # 70 - 91 -202-203., Bogotá D. C. CLAUSULA TRIGÉSIMA QUINTA.- DOCUMENTOS.- Forman parte integral del presente contrato y se anexan al mismo los siguientes documentos: a) Certificado de Disponibilidad Presupuestal; b) Certificado de existencia y representación legal expedido por la Cámara de Comercio de Bogotá; c) Oferta presentada por el contratista y Anexo Único; d) Constancia de cumplimiento de aportes parafiscales; e) Actas de recibo parcial y/o final; y f) Demás documentos relacionados con el presente contrato. CLAUSULA TRIGÉSIMA SEXTA – REQUISITOS PARA EL PERFECCIONAMIENTO. - Para el perfeccionamiento se requiere acuerdo sobre el objeto y la contraprestación y que esta se eleve a escrito por los competentes contractuales. CLAUSULA TRIGÉSIMA SÉPTIMA. – REQUISITOS PARA LA EJECUCIÓN DEL CONTRATO. - Para la ejecución del contrato, se requiere: a) Expedición del Registro presupuestal por parte de la Entidad contratante, b) Presentación de las garantías a cargo del contratista. c) Acreditación que el contratista se encuentra al día en el pago de aportes parafiscales- sistema de seguridad social integral; y d) Aprobación de las garantías por parte del Director Administrativo y Financiero del Comando General de las Fuerzas Militares. Para constancia se firma en Bogotá a los XXXXX (XX) días del mes de XXXX del dos mil veinticinco (2025).

POR EL MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA,

Coronel GEOVANNY ANDRES SUAREZ PENAGOS
Director Administrativo y Financiero del COGFM

POR EL CONTRATISTA,

JESÚS ALBERTO FRANCO ACOSTA
C.E. 582.410
Representante Legal de UT 273COGFM H&Y 2025
NIT. 901988423-0

Vo. Bo. MY. ERIKA ANDREA RODRÍGUEZ SÁENZ
Jefe Área de Contratación

Elaboró: PS JONNATAN [illegible] GARCIA
Asesor ARCON

Revisó: PS. DIEGO HERNANDO PARDO G.
Comité Económico Evaluador

Vo. Bo. PD. ANDREA SOLANGE GONZALEZ
Abogada Área de Contratación

Reviso: PS. VIVIANA MARCELA PELÁEZ G.
Comité Jurídico Evaluador

ANEXO ÚNICO

ESPECIFICACIONES TÉCNICAS, PERFILES, CUADRO DE PRECIOS Y ASPECTOS TÉCNICOS PONDERABLES

- **LOTE 2: LICENCIAS PROXY WEB.**

1. ESPECIFICACIONES TÉCNICAS

ÍTEM No.	DESCRIPCIÓN DEL BIEN / SERVICIO *(1)*	MARCA / REFERENCIA OFERTADA
1	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM).	FPX2KET318000036 FORTINET
ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO		
1	RENOVACIÓN GARANTÍA Y SOPORTE TÉCNICO, LICENCIAS DE LA PLATAFORMA DE SEGURIDAD DE FILTRADO Y ANÁLISIS WEB/PROXY DEL FABRICANTE (FORTINET HERRAMIENTA PERTENECIENTE AL COGFM).	
La renovación del licenciamiento es requerida para los siguientes modelos de la solución de seguridad de filtrado web/proxy así: - FPX-2000E: FPX2KET321000015 - FortiAnalyzer VM-GB5 La vigencia de la renovación de las licencias y de la garantía deberá ser de dos (2) años contado a partir del 15 de noviembre de 2025 o fecha que indique la plataforma o documento de fabricante.		
Se debe brindar e instalar actualizaciones de la solución de seguridad de filtrado web/proxy descritas en el presente anexo, cada vez que se libere en el mercado una nueva versión de software, Upgrade, Update o parche. Lo anterior previa solicitud y aprobación del supervisor del contrato y una vez haya sido probada en laboratorio, asegurando la continuidad del servicio y funcionamiento de los sistemas.		
Se debe realizar entrega al COGFM, de los medios magnéticos o manuales si existen cambios de versión.		
El servicio de renovación de la solución debe incluir las siguientes actividades de configuración e implementación y puesta en funcionamiento: - Instalación de la última versión establecida por el fabricante - Configuración de la plataforma (direcciones de red, NTP, rutas y demás configuraciones) manualmente. - Aplicar los parches instalados en el equipo - actualizaciones, Upgrade, Update o parches. - Ajustes a las configuraciones filtros, políticas y excepciones de ser necesario. - Pruebas de identificación de usuarios y de navegación. - Aplicar los controles de navegación a los usuarios del comando general. - Afinamiento de políticas de ancho de banda y priorización de las aplicaciones críticas para el COGFM. - Revisión y afinamiento del control y bloqueo de las solicitudes de DNS contra destinos conocidos y maliciosos. - Afinamiento de la protección contra amenazas de contenido web malicioso como exploits del navegador, scripts e identifique y bloquee botnets y devoluciones de llamada de malware. - Activación de protección antivirus, antispyware y antimalware que se puede adquirir durante la navegación. O en línea. - Nuevas implementaciones.		
Las renovación y activación debe quedar en un esquema 7x24 ante fabricante con las mismas características de seguridad actuales de las plataformas que componen la solución de seguridad de filtrado web/proxy.		
Se debe entregar certificado donde se evidencien las licencias renovadas, con su respectiva clave y fechas de vigencia. (cuando ello hubiere lugar)		
2. SERVICIO DE SOPORTE DE LA SOLUCIÓN DE SEGURIDAD FILTRADO Y ANÁLISIS WEB/PROXY		
El Servicio de soporte para la solución de seguridad de filtrado web/proxy debe ser renovado en un esquema y horario 7x24 durante dos (2) años, contado a partir de la fecha de instalación y activación de las renovaciones; siempre y cuando el supervisor lo vea pertinente, cumpliendo las siguientes actividades:		

El servicio técnico debe incluir atención de incidentes y consultas de tipo telefónico, correo electrónico (e-mail), acceso remoto, plataforma de mesa de ayuda y atención en sitio (presencial) en la cuidad de Bogotá en caso de que así se requiera, en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado en la solución a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).
Al finalizar el caso reportado se generará un informe de servicio con las evidencias del antes, durante y después de estas actividades. De igual forma quedará constancia en el informe de servicio si hubo cambio de software y/o en alguna configuración.
El servicio prestado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket o casos reportados para los incidentes presentados en la mesa de ayuda).
Se debe tener una atención ilimitada a casos reportados por el administrador de la solución, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de la solución de filtrado web/proxy, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.
Durante el periodo de soporte técnico, se requiere un reporte mensual de verificación del correcto funcionamiento de la consola, componente principal de la solución de seguridad de filtrado web/proxy. Las cuales deben incluir como mínimo las siguientes actividades: - Actualizaciones (Upgrade, Update, parches críticos de Seguridad) - Revisión y solución de errores. - Realización y programación de copias de seguridad en la unidad de almacenamiento de la entidad. - Revisión logs - Revisión y Mejoramiento de espacio de disco, Utilización de CPU – RAM. - desinstalación de funcionalidades inoperativas. - Procedimientos de hardening. Una vez realizados los acompañamientos (remotos o en sitio), se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar: - Actividades realizadas. - Actualizaciones aplicadas. - Procedimientos preventivos y/o correctivos aplicados. - Recomendaciones. - Pendientes.
En caso de presentar fallas en el funcionamiento, continuidad de los procesos y servicios de cada uno de los elementos de software y hardware que componen la solución de seguridad de filtrado web/proxy, se deberán efectuar los soportes todas las veces que se requiera. Estos deben incluir como mínimo: - Instalación y/o reparación de software. - Configuraciones, puesta en producción y funcionamiento. - Cambio de partes y/o repuestos y/o equipos nuevos de ser requeridos de ser necesario. (Servicio que debe ser incluido como garantía extendida con el fabricante.) - Remplazo de equipos por otros de iguales o superiores características en caso de ser necesario. El tiempo máximo permitido para cambio de partes, repuestos o reparación del equipo es de 20 días calendario una vez sea reportado el incidente, en caso que la falla genere afectación de servicio el contratista deberá suministrar, instalar, configurar y poner en funcionamiento temporalmente un equipo, repuestos o partes de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para COGFM, con el fin de garantizar la continuidad en la prestación de los servicios. En caso de que el repuesto o reparación del equipo ocasione la reinstalación o reconfiguración de software, sistema operativo o firmware, estas labores deben ser realizadas sin costo adicional para COGFM, garantizando la continuidad de los servicios.
GARANTÍA TÉCNICA Y SERVICIO
• Se deberá brindar el acompañamiento de soporte con un horario 7x24 por el proveedor, por el término de veinticuatro (24 meses) contado a partir de la fecha de activación de la licencia o renovación cada vez que el supervisor del contrato lo requiera durante el término de la garantía. • Se debe brindar soporte técnico por medio telefónico o remoto de forma inmediata en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas

después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).

- El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá.
- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario
- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado son el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.

ALCANCE GARANTÍA TÉCNICA

El término de la garantía técnica (o garantía legal de conformidad con el art. 7º de la Ley 1480 de 2011), de conformidad con el art. 7, 8, 9 y 11 de la Ley 1480 de 2011. Para los servicios prestados será de veinticuatro (24 meses), contados a partir de la suscripción del acta de recibo a satisfacción de los servicios firmada por parte del representante de la empresa o su representante autorizado y el supervisor del contrato.

Es la obligación, en los términos de la ley 1480 de 2011 de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad, el buen estado y funcionamiento de los productos.

Se deberá garantizar las licencias que están respaldadas por la casa propietaria del software, de la última versión disponible en el mercado, de acuerdo con las especificaciones técnicas exigidas.

NOTA: entiéndase como fecha de inicio del contrato instalación, la fecha en que se realice y evidencie la renovación de las licencias, en la respectiva consola de gestión.
El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración y realizar pruebas exitosas de funcionalidad.
Dentro de los primeros cinco (05) días calendario al inicio del plazo de ejecución, el contratista deberá entregar al supervisor para la aprobación, el cronograma a desarrollar para el cumplimiento del objeto del contrato, donde incluya los recursos necesarios para la ejecución e implementación.
Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo son de referencia, en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

FUNCIONAMIENTO Y CONTINUIDAD

- Garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados por los sistemas y equipos descritos en este anexo, a partir de la fecha de activación del producto.

SEGURIDAD

- ACUERDO DE CONFIDENCIALIDAD: El Contratista y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista, lo cual será verificado por el supervisor del contrato.
- Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares.
- El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.

OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO

- El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.
- El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
- Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de

condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista deberá presentar el cronograma de actividades para la ejecución del objeto del contrato, previa aprobación del supervisor del contrato.

2. PERSONAL PARA LA EJECUCIÓN DEL CONTRATO

CARGO	DATOS DEL PERSONAL
INGENIERO DE SOPORTE	VÍCTOR MANUEL MENDOZA ANAYA CC. 80113599 Ingeniero de Sistemas Matricula Profesional: 25255-216835

- En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario.

Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa.

- La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto.

- La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado.

- El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.

NOTA: Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el Contratista debió efectuar el respectivo análisis del pliego de condiciones del presente proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato derivado del presente proceso.

Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato.

El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma.

3. CUADRO PRECIOS

No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR TOTAL INCLUIDO IVA
1	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM).(De acuerdo a las especificaciones técnicas del Anexo)	2	UND	147.000.000,00	294.000.000,00

NOTA: Teniendo la procedencia de los bienes, de conformidad con el Estatuto Tributario, artículo 476, Los servicios a adquirir se encuentran excluidos de IVA y artículo 477 los Bienes que se encuentran exentos del impuesto de IVA.

Los servicios a adquirir se encuentran excluidos de IVA:

Art. 476. Servicios excluidos del impuesto sobre las ventas

(...)

Numeral 20. Adquisición de licencias de software para el desarrollo comercial de contenidos digitales, de acuerdo con la reglamentación expedida por el Ministerio de Tecnologías de la Información y Comunicaciones.

Numeral 21. Suministro de páginas web, servidores (hosting), computación en la nube (cloud computing).

Que teniendo en cuenta la procedencia de los bienes se dará el siguiente trato tributario:

Art. 477. Bienes que se encuentran exentos del impuesto.

...3. Las municiones y material de guerra o reservado y por consiguiente de uso privativo y los siguientes elementos pertenecientes a las Fuerzas Militares y la Policía Nacional:

n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional.

(...)

4. ASPECTOS TÉCNICOS PONDERABLES

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN	
01	El Contratista ofrece sin costo adicional: la actualización del fortiAnalyzer a la versión VM y que cuente con una capacidad mínima de procesamiento de +100gb por día de logs, sin que este ofrecimiento genere costo adicional para el COGFM.
02	El Contratista ofrece sin costo adicional: 25 horas de transferencia de conocimiento en administración y configuración del Proxy para (02) dos funcionarios del CGDJ6 con Voucher incluido, sin que este ofrecimiento genere costo adicional para el COGFM.

- **LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.**

1. ESPECIFICACIONES TÉCNICAS

ÍTEM Nro.	DESCRIPCIÓN DEL BIEN O SERVICIO	MARCA / REFERENCIA OFERTADA
1	SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS	
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION & RESPONSE EDR	CrowdStrike Falcon® Endpoint Protection Enterprise
1.2	SUSCRIPCIÓN DE CACERÍA DE AMENAZAS ADMINISTRADA	CrowdStrike Threat Graph
1.3	SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES	CrowdStrike Falcon® Identity Protection

<table>
<tr><td>1.4</td><td>SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES</td><td>CrowdStrike Falcon® Spotlight</td></tr>
<tr><td>1.5</td><td>SUSCRIPCIÓN DE PROTECCIÓN DE DATOS</td><td>CrowdStrike
Falcon Data Protection for Endpoint</td></tr>
<tr><td>1.6</td><td>SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS</td><td>CrowdStrike
Falcon Search Retention.</td></tr>
<tr><td>1.7</td><td>SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA</td><td>CrowdStrike® Next-Gen SIEM</td></tr>
<tr><td colspan="3">ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO</td></tr>
<tr><td>1.2</td><td colspan="2">LICENCIAMIENTO</td></tr>
<tr><td>1.2.1</td><td colspan="2">El proveedor debe brindar la suscripción de toda la solución, este deberá ser un modelo por suscripción por un periodo de 24 meses a partir del 02 de noviembre del 2025 para todos los módulos; debe ser entregado al Comando General de las Fuerzas Militares-COGFM de acuerdo con los siguientes productos:
<table>
<tr><th>ítem</th><th>Descripción</th></tr>
<tr><td>1</td><td>SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR)</td></tr>
<tr><td>2</td><td>SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA</td></tr>
<tr><td>3</td><td>SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES</td></tr>
<tr><td>4</td><td>SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES</td></tr>
<tr><td>5</td><td>SUSCRIPCIÓN DE PROTECCIÓN DE DATOS</td></tr>
<tr><td>6</td><td>SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS</td></tr>
<tr><td>7</td><td>SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA</td></tr>
</table></td></tr>
<tr><td>1.2.2</td><td colspan="2">Se requiere que la solución sea cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, contenedores de nube, dispositivos OT inclusive si estos se encuentran distribuidos de forma remota. No se aceptan soluciones que involucren hardware o virtualización. La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía. En caso de que se requieran módulos o funcionalidades adicionales deberían activarse sobre la misma plataforma con el mismo sensor.</td></tr>
<tr><td>1.2.3</td><td colspan="2">El proveedor deberá rendir un informe en donde certifique la funcionabilidad de la plataforma, la activación de las suscripciones licencias con sus respectivos soportes; así mismo entregará los certificados de las licencias al Departamento Conjunto de Comunicaciones del COGFM.</td></tr>
<tr><td>1.3</td><td colspan="2">GENERALIDADES DE LA PLATAFORMA:</td></tr>
<tr><td>1.3.1</td><td colspan="2">La solución integral debe ser soportada sobre una plataforma en la cual se garanticen las siguientes generalidades:</td></tr>
<tr><td>1.3.2</td><td colspan="2">La solución debe contar con las siguientes condiciones generales para su operación y correcto desempeño:
- Consola única central 100% nube (cloud) para administración y operación de todos los módulos ofrecidos y futuros.
- Sensores/software que serán instalados en estaciones de trabajo, servidores, máquinas virtuales, contenedores o dispositivos OT.
- La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola por grupos de direcciones IP.</td></tr>
<tr><td>1.3.3</td><td colspan="2">En caso de requerir activación de funcionalidades adicionales no debe requerir nuevos despliegues de producto, ni de sensores o agentes en la infraestructura.</td></tr>
<tr><td>1.3.4</td><td colspan="2">Se requiere que se despliegue un sensor/agente único para realizar todas las funcionalidades solicitadas con las siguientes condiciones como mínimo:
- Sensor que NO requiera ser reiniciado en su instalación como desinstalación.
- El proceso de despliegue del sensor debe ser compatible y tener documentado el uso de plataformas de terceros como (SystemCenter / AWS automatic Deployment / GPO / PowerShell / PDQ) entre otros.
- El consumo de recursos del agente debe ser en promedio 1% de CPU, teniendo activas todas las capacidades de detección, prevención y riesgo. No debe tener requerimientos de hardware específicos para su funcionamiento.
- El sensor a desplegar en ambientes de OT de ser necesario deber ser el mismo que se utiliza en el ámbito OT.
- El sensor a desplegar debe convivir con cualquier otra solución de EPP existente en el ambiente sin causar ninguna incompatibilidad ni lentitud en el dispositivo.</td></tr>
</table>

	- El despliegue del sensor no debe requerir desinstalar las soluciones de EPP existentes en el ambiente y no debe crearse ninguna exclusión para su operación de detección de amenazas.		
1.3.5	- Los sensores a desplegar NO deben requerir actualizaciones de patrones/firmas/comportamientos de forma completa o parcial. - La solución debe estar basada en AI/ML (Inteligencia Artificial / Machine Learning), No se aceptan combinaciones de modelo de firmas/herística u otros mecanismos no especificados.		
1.3.6	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional. - La plataforma debe contar con un "Market Place" para poder realizar las integraciones con terceros mediante API y ver el estado de la integración. También disponer de la posibilidad de realizar la prueba o test de nuevos módulos sin necesidad de nuevos despliegues o autorizaciones de terceros.		
1.3.7	- La plataforma debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API.		
1.3.8	- La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días consulta en segundos.		
1.3.9	- La consola de gestión debe incluir capacidades de analítica mediante motores de AI, incluir para todos los módulos capacidades de SOAR que no implique un licenciamiento independiente y que no se limite su uso en la creación de playbooks de automatización.		
1.3.10	- La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, auto triage notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros.		
1.3.11	- La plataforma debe permitir la definición de roles personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que deben ingresar a la consola como permitir el acceso mediante MFA e integración con SSO.		
1.3.12	- La plataforma debe estar administrada por una única consola en un ambiente jerárquico basado en padres e hijos. En caso de que la entidad requiera, puede dividirse o ser parte de un sistema de CSIRT/SOC para poder ser gestionada de forma colaborativa delegada. Sin que esto impacte la operación y administración de la plataforma.		
1.3.13	- La plataforma debe contar con un portal de ayuda, webinar y base de conocimiento integrado a la consola para poder ampliar los conocimientos sobre los módulos o webinar para poder aplicar buenas prácticas en el desarrollo de la solución. Como también hacer el escalamiento de casos en caso de requerirse con el fabricante en modalidad 7x24. NO se aceptan plataformas o soluciones que tengan múltiples interfaces o múltiples consolas.		
1.3.14	- La consola debe incorporar un mecanismo de autodepuración para eliminar los dispositivos que no se gestionan en un periodo mayor a 45 días calendario o definir una política de retención para poder hacer procesos de autodepuración más acelerados.		
1.3.15	- El licenciamiento de la plataforma se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados.		
1.3.16	- Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes. Estos tokens deben ser de un único uso y deben ser generados de forma aleatoria para que solo los usuarios con el perfil asociado puedan hacer uso de este token de desinstalación.		
1.3.17	- La plataforma debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un arbol de procesos de forma: Gráfica, listado de actividades y líneas de tiempo.		
1.3.18	- La plataforma debe poder establecer control o comunicación directa por medio de línea de comandos con los sensores (win/linx/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros, estos accesos directos a los dispositivos se deben validar mediante un acceso de Multi factor conocido como MFA.		
2	**REQUISITOS ESPECÍFICOS DE LOS MÓDULOS**		
2.1	**SUSCRIPCIÓN DE ENDPOINT DETECTION & RESPONSE EDR, QUE INCLUYE:** - **Antivirus de nueva generación y EDR** - **Antimalware** - **Firewall Management** - **Control de dispositivos**	**(Número de endpoints)**	**1400**

2.1.1	- Uso de la inteligencia de amenazas basado en la identificación de como los adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques, como también sus asociaciones, IOCs y vulnerabilidades objetivo, detecciones asociadas en los EDR.
2.1.2	Capacidades de detección y prevención de: - Detección y prevención de virus/malware conocido y desconocido o día cero. - Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades. - Detección y prevención por indicadores de ataque (File-less attacks). - Capacidad de independizar la detección de la prevención por políticas. - Identificación y prevención de actividades sospechosas (procesos, registro, script, comandos, drivers). - Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usado por los ataques de Ransomware basado en comportamiento. - Identificación y prevención de movimientos laterales y Accesos a credenciales. - Identificación y prevención de ataques y explotación de vulnerabilidades día cero.
2.1.3	Capacidades de detección de TTPs en post ejecución como: - Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP). - Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos.
2.1.4	La plataforma debe tener capacidad de desarrollar actividades forenses como: - Contar con un acceso remoto (vía línea de comandos) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual. - Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos. Contar con comandos de colección de datos que permitan dar paso a investigaciones. Los comandos requeridos son: - Explorar el sistema de archivos y extraer archivos. - Lista de procesos en ejecución. - Extraer el registro de eventos de Windows. - Consultar registro de Windows. - Enumere las conexiones de red actuales y la configuración de la red. - Extraer la memoria de un proceso (memory dump). Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son: - Eliminar un archivo. - Terminar un proceso (Kill process). - Eliminar o modificar la clave o el valor del registro de Windows. - Enviar scripts programados. - Enviar y recibir archivos por demanda.
2.1.5	- La solución deberá contar con la capacidad de aislar una activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación externa a la computadora con excepción a la comunicación con la propia consola de gestión de la solución.
2.1.6	- La solución debe hacer un mapeo de alertas basado en el modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).
2.1.7	- La solución deber tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, estado de la conexión a la consola, tags predefinidos, roles de los dispositivos, esto basado en la meta data de los dispositivos registrados como mínimo. - La organización en grupos de forma automática o manual basado en reglas o filtros de acuerdo a los atributos de los dispositivos.
2.1.8	- La plataforma debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como Virus total vía API.
2.1.9	La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales. La solución debe contar como mínimo los siguientes elementos de análisis y características: - Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control. - Capacidad de protección aun cuando los equipos no cuenten con conectividad a la nube. - Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente.

	- Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS. - Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos. - Detección y prevención de explotaciones de tipo Force DEP (Data Execution Prevention), Heap Spray preallocation, Force ASLR (Address space layout randomization), SEH (Structured Exception Handling Ovewrite protection), NULL Page Allocation, Remote library Loading, Untrusted font. Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente: - Cadenas ejecutadas dinámicamente vía el cmdlet "invoke-expression". - Comandos vía –EncodedCommand. - Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware. - Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware. - Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware. - Detección y prevención de movimientos laterales. - Detección y prevención de intentos de robo de credenciales. - Detección y prevención de intentos de elevación de privilegios. - Detección y prevención de intentos de uso de "sticky keys". - Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés). Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe		
2.1.10	- El módulo de EDR debe tener una cuarentena de archivos el cual debe integrar un análisis de sandboxing automático sin límite de uso. Esto es cuando un archivo llegue a cuarentena se tenga un reporte de sanboxing con el análisis comportamental.		
2.1.11	- Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura, como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas Windows y MAC.		
2.1.12	- Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento.		
2.1.13	- Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.		
2.1.14	- Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.		
2.1.15	- Debe tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.		
2.1.16	- Se deben contar con dashboards para poder ver la actividad de dispositivos externos como: Audio/video, Imaging, Mass Storge, Mobiles (MTP/PTP), impresoras, Wireless (Bluetooth), Any Class.		
2.1.17	- Debe permitir configurar de forma personalizada la notificación que le aparece a los usuarios cuando se realizar alguna restricción en el acceso.		
2.1.18	- Capacidad de tomar el control del Firewall nativo de estaciones para sistemas Windows y MAC para la restricción o permisos de puertos, IPs y procesos.		
2.1.19	- Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de red, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.		
2.1.20	- Deberá utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall.		
2.1.21	- Debe tener la capacidad de poder identificar el tipo de conexión para poder hacer bloqueos de tráfico hacia redes wifi, por ejemplo, y con ello poder restringir de forma granular el acceso dependiendo de la política de la entidad.		
2.1.22	Las reglas de Firewall deben poder definir la localización del dispositivo con ello aplicar políticas de forma contextual, para identificar la ubicación se debe hacer con la definición de: - Tipo de conexión & SSID, IP Gateway, Servidor DHCP, Prueba de resolución DNS, Prueba de certificado Https, Prueba de ping, dirección IP.		
2.2	**SUSCRIPCIÓN DE CACERÍA DE AMENAZAS ADMINISTRADA que debe incluir:** **- Analítica de telemetría de comportamiento con IA - Inteligencia Artificial**	**(Número de endpoints)**	**1400**

	- **Servicio de cacería de amenazas administrada por parte del fabricante 7x24**		
2.2.1	- Sistema de detección y respuesta de puntos finales, identidad y nube con monitoreo continuo para poder tener visibilidad de actividad anómala, respuesta y desarrollo de actividad forense para evitar potenciales brechas o compromiso en las operaciones. Se deben integrar un sistema de analítica y correlación para realizar análisis retrospectivos.		
2.2.2	- Que permita acceso instantáneo al "quién, qué, cuándo, dónde y cómo" de un ataque.		
2.2.3	- Que la solución EDR permita detectar incidentes automáticamente sin requerir ningún ajuste o configuración antes de estar en pleno funcionamiento.		
2.2.4	- Que tenga la posibilidad de realizar búsquedas personalizadas sobre las detecciones que se remontan a 90 días para buscar amenazas de manera proactiva y que los resultados de las consultas se devuelvan en cinco segundos o menos.		
2.2.5	- Que brinde protección contra fallas silenciosas (que se producen cuando un ataque se desliza a través de las soluciones de seguridad sin que se active ninguna alarma) y que registre todas las actividades de interés de un equipo tanto en tiempo real como después del hecho.		
2.2.6	La plataforma debe permitir realizar investigaciones forenses en tiempo real y retrospectivos basado en (Para estos casos con menús dedicados para): - Host (actividad de procesos, actividad sospechosa, actividad de red, entre otros). - Usuarios (terminar donde ha registrado un usuario, que servicios accede, como y de que tipo fue el registro). - Hash (Búsquedas de ejecuciones de Hash, creaciones, modificaciones). - Direcciones IP. - Grupos de dominios. - Búsquedas por el identificador de sensor. - Búsquedas por contexto de procesos. - Contar con un buscador de consultas para identificar (dispositivos con riesgo, con detecciones críticas, con vulnerabilidades materializables entre otros). - Realizar cacería de amenazas en sensores windows, mac, linux, directorio activo y contenedores. - Realizar una evaluación de Mitre mediante mapas de calor, tácticas en el tiempo. - Líneas de comando y actividad ASEP(Aggregate System Entry Point). - Ejecutables que se ejecutan desde la papelera o carpetas temporales. - Actividad de logon, actividad de powershell, actividad de tareas registradas.		
2.2.7	- Debe realizar un diagnóstico de "Zero Trust Assessment (ZTA)" para determinar el estado del equipo en la organización. Es decir que evalué el nivel de seguridad en cuanto parámetros de seguridad del sistema operativo y políticas de seguridad de prevención.		
2.2.8	- Que permita desarrollar reglas o indicadores que identifican y previenen ataques sin archivos que aprovechan los malos comportamientos y que con el tiempo ajuste y amplíe los indicadores integrados.		
2.2.9	- Debe permitir la creación de Indicadores de Ataque por sus siglas IOA, incluso permita crear reglas de IOA personalizadas en la plataforma, Como bloqueos de procesos, archivos, dominios o IPs dependiendo ejecuciones de comandos archivos o procesos antecesores.		
2.2.10	- Para la creación de las reglas personalizadas deberá especificar el "tipo de regla" y seleccionar acciones como: operaciones de creación de procesos, creación de archivos, conexión de red y nombre de dominio.		
2.2.11	- Para las detecciones de dichas reglas de IOA, tenga la capacidad de buscar las detecciones provocadas por una regla específica.		
2.2.12	Tener la capacidad de realizar búsquedas proactivas (hunting) para eventos de cambios registrados por la telemetría de la plataforma, en un rango o periodo de tiempo específico ejemplos: - Realizar búsquedas de nuevos servicios o tareas programados a alrededor de un proceso de investigación. - Realizar búsquedas de cambios en llaves de registros, accesos remotos, logins alrededor de un proceso, equipo, IP o dominio específico.		
2.2.13	- Visualización de incidentes calificados por la plataforma que correlacione las detecciones y actividades asociadas a los incidentes, asignando el indicador de riesgo del impacto del incidente.		
2.2.14	- La plataforma debe mostrar en forma gráfica el incidente relacionando los dispositivos impactados, procesos y línea de tiempo en la que ocurren los eventos relacionados tanto bloqueados como observados que tiene relación con el incidente.		

2.2.15	- La solución debe permitir consultar información de telemetría relacionados con un proceso, tarea o comportamiento para ampliar el proceso de investigación y consulta con un alcance de 7 días historicos.		
2.2.16	- La plataforma debe incluir servicios de fábrica para actividades de threat hunting y MDR para tener búsquedas/investigaciones proactivas sobre detecciones y anomalías en el entorno del cliente.		
2.2.17	- La solución debe realizar el envío de la telemetría en tiempo real y consultada inclusive aun si los dispositivos están fuera de línea esto por un periodo de al menos 7 días.		
2.2.18	La información de telemetría debe ser colectada 7x24 y esta no debe ser mayor a 40MB por día por dispositivo, la información a tomar debe incluir como mínimo +1100 tipos de eventos entre ellos: - Process - Token info events, Creations, Injections, Grandparent, Parent, Child relationships. - Network - Close, Connect, Listen, Receive/Accept for IP4/IP6. - File - Writes, deleted, rename, open and info. - Registry - ASEP. Updates, Dumps, Impersonation. - User - Logon, Logoff, Failed attempts. - DLL - Injection and reflection attempts. - Detalle de los dispositivos incluido, pero no limitado a: - OS - OU Attributes, Hostname, Device type, OS Version, Manufacturer, Model. - Network - MAC, Local and External IP, Neighbors.		
2.2.19	- La solución debe permite la configuración de consultas personalizadas utilizando un lenguaje de consulta estándar y documentado, estas consultas pueden ser personalizadas y programadas para poder ser utilizadas como reportes vía correo electrónico.		
2.2.20	- Deberá ofrecer un servicio administrado de cacería de amenazas capaz de detectar intrusiones, actividades maliciosas y adversarios, realizado directamente por el fabricante por medio de un equipo capacitado y certificado sin necesidad de realizar ningún tipo de VPN o instalación de plataforma de terceros para obtener la información. Este servicio se debe prestar en modalidad 7x24x365.		
2.2.21	Como parte del servicio deberá buscar de manera proactiva campañas de malware sigilosas y en caso de existir alguna se notificar según corresponda. El proceso de notificación debe ser vía correo electrónico por medio de la misma consola de gestión y administración de los anteriores módulos presentar: - Reportes de cacería. - Librerías para cacería de amenazas. - Investigaciones documentadas. - Espacio para poder someter muestras para análisis.		
2.2.22	- El servicio deberá ir más allá de la detección pasiva y automatizada, deberá investigar e incluso responder a indicadores que apunten a ataques. Alertar con recomendaciones de remediación, con un análisis detallado que permita determinar ¿qué sucedió? y ¿cómo? responder al incidente.		
2.2.23	- Deberá contar con investigaciones retroactivas revisando datos históricos en busca de evidencia de una intrusión. Recopilar artefactos de investigación como direcciones IP, dominios, hashes y otros. Estos artefactos deberán ser cargados a una base de inteligencia propietaria del fabricante y generar alertas en la interfaz de usuario de la plataforma de seguridad ofertada.		
2.2.24	- El proceso de investigación debe contar con un playbook de investigación y análisis para poder clasificar las detecciones como mínimo: Falso positivo, verdadero positivo, indeterminado, sospechoso.		
2.2.25	- Se debe tener en la consola de gestión de EDR un dashboard que muestre el número de investigaciones realizadas por el equipo de cacería de amenazas.		
2.2.26	- Contar en el portal de gestión con una librería de cacería de amenazas, como: tips para hacer consultas, TTPs para ataques cloud, Exfiltración de datos, cacería de DLLs, credenciales no seguras, explotación Web, herramientas de acceso remoto, movimientos laterales en windows.		
2.3	**SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES, que debe incluir:** **- Diagnóstico continuo de riesgos del AD e Intra ID** **- Detección y prevención de ataques y anomalías de identidad con el uso de Inteligencia Artificial**	**(Número de usuarios endpoints)**	**1400**
2.3.1	- El sistema debe inspeccionar profundamente los protocolos de autenticación (NTLM, Kerberos, LDAP, etc.) para ayudar a controlar el uso inseguro de protocolos y reducir el riesgo de amenazas de seguridad, incluido el reenvío de credenciales y el análisis de hash de contraseñas con bases de datos de passwords expuestos, así como la detección de ataques como Kerberoasting, Pass-the-Hash y Golden Ticket.		
2.3.2	- El sistema debe unificar la visibilidad de las cuentas y las identidades en la nube (EntraID), remota (VPN) y local (Directorio activo local).		

2.3.3	- El sistema debe proporcionar una calificación del nivel de riesgo de detecciones, anomalías y auditoria del AD indicando niveles (alta, media, baja).
2.3.4	- El sistema debe perfilar el comportamiento de cada usuario y dispositivo en la red, incluidos los usuarios privilegiados y las cuentas de servicio y desarrollar una puntuación de riesgo para cada uno de ellos.
2.3.5	- El sistema debe descubrir todos los usuarios conectados al directorio activo, detectar y responder a las amenazas relacionadas con la identidad en tiempo real.
2.3.6	- El sistema debe ser capaz de descubrir continuamente todas las categorías de usuarios, incluidos los privilegiados, las cuentas de servicio, los usuarios regulares y las cuentas obsoletas.
2.3.7	- El sistema debe rastrear y hacer cumplir la política basada en la identidad del usuario para servidores y aplicaciones confidenciales. Debería descubrir, monitorear y administrar automáticamente las cuentas privilegiadas en la red.
2.3.8	- La plataforma debe permitir la definición de segmentos como VPNs, Contratistas, redes de servidores, DMZ para que con este contexto se pueda aumentar la visibilidad del tráfico de red que se debe monitorear para hacer la detección de amenazas y determinar su acción para protección, contención o solicitud de verificación de identidad.
2.3.9	- La plataforma debe mapear el proceso de "Kill Chain Attack & Defense" de Active Directory para proteger el entorno del AD.
2.3.10	- El sistema debe reducir la superficie de ataque mediante la identificación de administradores sigilosos, cuentas de servicio mal utilizadas y comportamiento anómalo de los usuarios.
2.3.11	- La plataforma debe incluir informes completos sobre riesgo y cumplimiento con ayudas gráficas.
2.3.12	- La plataforma debe utilizar ciencia de datos "Data Science" para la investigación de seguridad interna y para cuantificar el riesgo. Como también debe utilizar información basada en hechos (es decir, niveles de privilegio, alertas de seguridad o inteligencia de amenazas para generar una puntuación de riesgo.
2.3.13	- La plataforma sebe usar el mismo sensor de EDR para las capacidades de detección y análisis sobre la identidad del directorio activo (En los controladores de dominio).
2.3.14	- La plataforma debe responder proactivamente a las amenazas en tiempo real según las políticas preestablecidas sin interrumpir a los usuarios válidos. Debe evitar u orquestar aprobaciones cuando terceros, como proveedores, contratistas o socios, acceden a servidores confidenciales con el entorno del cliente, mediante integraciones con sistemas MFA.
2.3.15	- La plataforma debe tener la capacidad de forzar cambios de contraseña para sus usuarios, basado en el nivel de seguridad de las credenciales (como credenciales comprometidas, credenciales con bajos niveles de seguridad, credenciales sin rotación).
2.3.16	- La plataforma debe integrarse a una plataforma de protección EDR y gestión de vulnerabilidades nativa de forma que se pueda correlacionar amenazas desde la perspectiva de Endpoint, vulnerabilidades y la protección de la identidad usando una consola única.
2.3.17	- La plataforma debe tener la capacidad de tomar medidas de prevención en función de los umbrales de puntuación de riesgo.
2.3.18	- La plataforma debe entregar capacidades para definir políticas granulares sobre estado de seguridad de las entidades, tráfico de red de autenticación, estado de seguridad de los dispositivos, roles de las cuentas, orígenes, destino de las conexiones, protocolos, ubicaciones geográficas, riesgos, dispositivos que no se usan normalmente, entre los mínimos.
2.3.19	- El sistema debe informar sobre el estado de las contraseñas para todas las cuentas de usuario, identificará a los administradores ocultos, las cuentas obsoletas y otros problemas que tradicionalmente son difíciles de encontrar.
2.3.20	- la plataforma debe permitir realizar un desglose o "drill down" bajo demanda desde una búsqueda personalizada que coincida con una o más características de la sesión.
2.3.21	- La plataforma debe correlacionar y analizar automáticamente los eventos de seguridad, dentro del contexto de la sesión de un usuario.
2.3.22	- La plataforma debe almacenar información de telemetría de usuario para ser consultada sobre detalles tanto para auditoría como para cacería de amenazas usando un lenguaje para consulta de metadata y telemetría.
2.3.23	- La plataforma debe proporcionar capacidades de análisis privilegiado (calcular puntajes de riesgo para cuentas y usuarios privilegiados a través de análisis de comportamiento y correlación de actividad privilegiada con información de vulnerabilidad).
2.3.24	- La plataforma debe tener la capacidad de utilizar el aprendizaje automático (Machine Learning) no supervisado para crear y mantener modelos de datos de usuarios, grupos de pares de la

	organización y comportamiento de los activos utilizando funciones en datos de eventos históricos recopilados durante un período definido por el usuario.		
2.3.24	El módulo de detección prevención de ataques de identidad debe: - Detectar contraseñas codificadas utilizadas por aplicaciones que estén en las GPO. - Detectar la creación y eliminación de cuentas de usuario en un período de tiempo. - Admitir esquemas del AD de varios bosques/dominios. - Permitir agregar empleados ejecutivos, de alto privilegio o en riesgo en listas de seguimiento, como también la posibilidad de agregar password conocidos. - Tener la capacidad de crear flujos de trabajo para automatizar respuestas. - Detectar un cambio de credencial anómalo para un usuario. - Detectar una cantidad anómala de activos a los que se accede dentro de una sesión. - Detectar actividades de inicio de sesión de cuentas revocadas. - Detectar el inicio de sesión del usuario desde múltiples ubicaciones geográficas. - Detectar inicios de sesión exitosos desde cuentas no correlacionadas. - Detectar el inicio de sesión desde una ubicación geográfica rara. - Detectar la actividad de administración de DC (creación/eliminación de cuentas) usando VPN. - Detectar la conexión VPN por parte de un no usuario (cuenta de servicio). - Detectar la conexión VPN por cuenta deshabilitada. - Realizar un seguimiento de las actividades de los usuarios en sesiones desde el inicio hasta el cierre de sesión. - Identificar a los usuarios que realizan cambios de credenciales. - Identificar automáticamente cuentas de servicio mediante aprendizaje automático ML. - Detectar la conexión VPN por cuenta de servicio. - Detectar cuentas humanas que se comportan como cuentas de servicio. - Detectar anomalías de acceso por cuentas de servicio. - Detectar el inicio de sesión interactivo por parte de cuentas que no son de usuario (no correlacionadas). - Detectar el inicio de sesión de un usuario no ejecutivo en un activo ejecutivo.		
2.4	**SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES que debe incluir:** - **Descubrimiento de activos en la red con y sin sensor** - **Inventario de aplicaciones instaladas y usadas** - **Listado de accesos exitosos y fallidos a los dispositivos** - **Gestión de vulnerabilidades**	**(Número de endpoints)**	**1400**
2.4.1	- Módulo que deberá proporcionar la visibilidad el todo el entorno de tecnología de la organización, desde la consola central supervisar todo desde un panel de control para explorar aplicaciones, accesos y activos utilizando datos históricos y en tiempo real que tengan o no tengan el sensor instalado.		
2.4.2	- La herramienta deberá ofrecer inventario de aplicaciones instaladas y usadas, listados de extensiones usadas en los navegadores, las versiones que se están ejecutando para identificar aplicaciones sospechosas o no autorizadas. Adicionalmente deben brindar una clasificación y categorización de fábrica.		
2.4.3	- Se deberán definir grupos de aplicaciones para poder clasificar las aplicaciones como también se podrán crear IOCs para autorizar o bloquear aplicaciones basadas en hash mediante workflows de manera automática.		
2.4.4	- La herramienta deberá tener la capacidad de identificar todos los dispositivos en la red, incluso si están protegidos o no por la plataforma. Se deben tener 3 clasificaciones (Dispositivo gestionados, dispositivos no gestionados y candidatos a instalar el sensor, dispositivos no soportados entre ellos (impresoras, Routers, dispositivos OT)).		
2.4.5	- Sobre los dispositivos administrados se debe obtener información de estado de salud como uso de CPU, Memoria, espacio libre de disco, entre otros.		
2.4.6	- La herramienta deberá tener la capacidad de monitorear los logins de todos los usuarios activos en la red, con privilegios de administrador, locales o de dominio, historial de inicio de sesión e información de actualización de contraseña.		
2.4.7	- Cómo parte de la plataforma unificada, la plataforma de higiene de TI deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint.		
2.4.8	- La herramienta deberá proporcionar información contextual para todos los sistemas, utilizando cuadros de mando, gráficos y funciones de búsqueda para profundizar en los datos de apoyo. Los resultados deberán correlacionarse con los dispositivos que están en línea, fuera de línea o no conectados a la red corporativa.		
2.4.9	- La herramienta de higiene de TI, deberá utilizar la información de la solución de detección y respuesta de endpoints (EDR) para alimentar los datos de búsqueda.		
2.4.10	- La herramienta deberá tener la capacidad de minimizar el abuso de cuentas privilegiadas monitoreando el uso y creación de credenciales de administrador.		

2.4.11	- Las búsquedas de inventario deberán realizarse en la nube para no tener ningún impacto en el rendimiento de los equipos o en la red.		
2.4.12	- Solución de administración de vulnerabilidades automática sin escaneos y siempre activa con datos en tiempo real. Donde se pueda realizar análisis de impacto basado en la determinación de si se dispone de exploits o inclusive si se tienen exploits activos en la organización.		
2.4.13	- La herramienta deberá ofrecer la gestión unificada de amenazas y vulnerabilidades, como parte de una plataforma integral para prevenir vulnerabilidades y la actividad posterior a la explotación de las mismas.		
2.4.14	- La herramienta deberá permitir investigar vulnerabilidades y exposiciones comunes (CVE) para examinar los objetivos y perfiles de los actores de amenazas.		
2.4.15	- La herramienta no deberá realizar escaneos para su funcionamiento, lo cual permita la administración de vulnerabilidades automatizada y siempre activa con datos en tiempo real.		
2.4.16	- Cómo parte de la plataforma unificada, la plataforma de gestión de vulnerabilidades deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint EDR.		
2.4.17	- La herramienta deberá permitir supervisar continuamente el estado de vulnerabilidad de todos los equipos dondequiera que residan: en las instalaciones, fuera de las instalaciones o en la nube.		
2.4.18	- No debe requerir dispositivos de hardware ni infraestructura adicionales para su funcionamiento.		
2.4.19	- La herramienta deberá monitorear todos los equipos a través de un sensor ya sea dentro o fuera de la red, en la nube, en equipos físicos y virtuales.		
2.4.20	- Debe permitir que los datos estén disponibles a través de un dashboard intuitivo y búsqueda en tiempo real.		
2.4.21	- Deberá proporcionar el contexto de las amenazas para ver tanto la presencia de una vulnerabilidad como la evidencia de intentos de explotación.		
2.4.22	- Deberá permitir operar instantáneamente tan pronto como sea instalado, monitoreando e identificando las vulnerabilidades sin necesidad de reiniciar o realizar una configuración compleja.		
2.4.23	- Desarrollar por medio del SOC el programa de gestión de vulnerabilidades a lo largo de todo el ciclo de vida, desde el aspecto fundamental del descubrimiento de activos, pasando por la evaluación y priorización de vulnerabilidades y exposiciones, hasta la corrección eficaz.		
2.5	**SUSCRIPCIÓN DE PROTECCIÓN DE DATOS que debe incluir:** **- Clasificación de información en tiempo real** **- Detección y prevención de salida de información sensible** **- Analítica y correlación de eventos con el uso de Inteligencia Artificial**	**(Número de endpoints)**	**1400**
2.5.1	- Se debe proveer funciones de protección de datos para evitar su fuga utilizando el mismo sensor de EDR, con la misma consola de gestión y sin requerir hacer un nuevo despliegue para activar esta funcionalidad.		
2.5.2	- El módulo de protección de datos debe identificar información sensible por medio de patrones de contenido, expresiones regulares o etiquetas de Microsoft y Google.		
2.5.3	- El módulo debe poder identificar y mostrar los flujos de información por volumen de datos o por número de eventos que coinciden con políticas de protección de datos. Esto de forma gráfica para los vectores de salida tanto web como Dispositivos de almacenamiento USB y uso del copiar en el portapapeles.		
2.5.4	- Los eventos de salida de información deben indicar el archivo que se detecta en la salida, vector de salida, política, usuario donde se debe llevar al perfil de usuario mediante la protección de identidad, el dispositivo donde se debe llevar a la descripción y detalles del dispositivo.		
2.5.5	- Las políticas se deben asignar a los dispositivos, se debe hacer la asignación varios tipos de clasificaciones, debe tener la posibilidad de hacer identificación por porcentaje de similaridad, bloquear el uso de browsers en caso de tener coincidencia con datos sensibles salientes, personalizar las notificaciones de alertamiento a los usuarios.		
2.5.6	- Las políticas podrán ser configuradas en modo simulación para realizar entrenamiento de reglas antes de activar la prevención.		
2.5.7	- Se podrán crear patrones de contenido por medio de expresiones regulares, como también indicar la cantidad de veces que puede repetirse una coincidencia.		
2.5.8	- Se podrá crear grupos de aplicaciones web para poder ser granular en las políticas de protección de datos.		
2.5.9	- La solución debe tener la capacidad para inspeccionar nuevos formatos de archivos cifrados y detectar intentos de exfiltrar archivos cifrados.		

2.5.10	- Las reglas de protección de información deben tener la opción de creación de detecciones indicando el tipo de criticidad y este debe ser procesado y analizado por Inteligencia artificial para poder generar detecciones de anomalías por volumetría y estado de criticidad.		
2.5.11	- Las reglas de protección de datos deben tener la opción de almacenar la evidencia de los archivos que coinciden con los patrones de detección de salida de datos, definiendo la cantidad de espacio para evidencias en cada uno de los dispositivos y el porcentaje mínimo de ocupación del disco duro.		
2.5.12	- La solución de protección de datos debe tener un panel de control para poder ver los flujos de datos, esto es: origen de la información, medio de salida y canal de salida, indicando por colores las acciones tomadas en volumen de eventos o tamaño de datos.		
2.5.13	- Por medio de políticas se podrá definir que dispositivos se activa la protección de datos, con esto logrando ser selectivos en dispositivos que no lo requieran.		
2.6	**SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS que debe incluir:** **- Indicadores de compromisos en tiempo real IOCs,** **- Análisis de Sandboxing automático** **- Perfiles de grupos o actores de ataques y campañas de ciberseguridad**	**(Número de endpoints)**	**1400**
2.6.1	- Protección de dispositivos, protección de Identidad y protección de nube al siguiente nivel que combine sandboxing de malware, la búsqueda de malware y la inteligencia de amenazas en una solución integral. Además, que tenga la capacidad de producir un indicador de Compromiso (por sus siglas IOC) tanto para la amenaza que encontró como para todas sus variantes conocidas.		
2.6.2	- Inteligencia de amenazas tipo TIP (Threat inteligence Platform) que permita la consulta e inyección de IOCs (Indicadores de compromiso) vía API manual o automáticamente. Con actualización en tiempo real.		
2.6.3	- Debe tener Sandbox en nube, capacidad de enviar muestras para análisis por demanda o automáticamente desde los endpoints para complementar el análisis de muestras desconocidas, al menos 100 muestras mensuales por demanda.		
2.6.4	- Tener disponible una base de datos de archivos de malware al menos los últimos 5 años para poder hacer consulta y descarga de muestras de malware para estudio e ingeniería inversa por parte del equipo de la organización.		
2.6.5	- La plataforma debe entregar reportes de inteligencia al menos semanales programados sobre amenazas, campañas y ataques más reconocidos para preparación y conocimiento centralizado en la consola de administración.		
2.6.6	- Se debe contar con un panel que permita consultar inteligencia de Vulnerabilidades para brindar información sobre nuevas vulnerabilidades con una descripción de su impacto en la plataforma y vinculación a campañas de adversarios en ciberseguridad.		
2.6.7	- Se deben contar con una sección de servicios para poder tener: resúmenes, violaciones, eventos, fuentes de datos, temas y consultas, integraciones API e interfaces, despliegues, dependencias, librerías, Modelos o Frameworks, datos recolectados.		
2.6.8	- El módulo de inteligencia debe contar con el listado de actores o grupos para ser analizados de forma continua en la cual se pueda definir IOCs, vulnerabilidades, TTPs de mitre de forma gráfica.		
2.7	**SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA**	**UNIDAD**	**01**
2.7.1	El módulo debe incluir como mínimo las siguientes funcionalidades: - Analítica y correlación automática de EDR, ITDR, Data Protection, inteligencia de manera integrada XDR - Sistema de SOAR nativo integrado - Analítica de ciberseguridad BOT de Inteligencia Artificial Capacidad por día de 75GB de ingesta adicional a la que ya se cuenta por identidad y el EDR y tiempo de retención de 3 meses (90 días). En la misma plataforma de administración de EDR/protección identidad/ gestión de riesgo, XDR se debe tener la capacidad de ingestión de cualquier tipo de dato/logs sin limitación en el uso de conectores OnPremise o conectores cloud para desarrollar las capacidades de SIEM de nueva generación desarrollando a profundidad las siguientes características en una sola plataforma y en una única consola: - Monitoreo y gestión de Incidentes basado en los diferentes vectores usando AI/ML sin configuración de reglas. - Configuración de reglas de correlación personalizadas clasificando los resultados en detecciones y tipificando de acuerdo al modelo de MITRE Attack (Enterprise o Mobile).		

	- Gestión de eventos para hacer consultas avanzadas, dashbboards mediante operaciones condiciones para poder fortalecer los procesos de cacería de amenazas. - Ingesta de datos por medio de conectores que puedan personalizarse o tenerse configurados para poder parametrizar cualquier fuente de información. - Ingesta de datos con capacidad de respuesta orquestada para los vectores de: EDR / Cloud / Identidad / correo / Navegación Web /Red y/o Firewall con el objetivo de mitigar el impacto de incidentes de seguridad. - Se requiere que se puedan crear flujos de trabajo o "playbooks" de respuesta en un SOAR nativo para poder automatizar acciones. - Integrar una plataforma de inteligencia de amenazas "TIP" (Threat Intelligence Platform) Nativa para enriquecer y tener el contexto de amenazas cibernéticas en las investigaciones, detecciones y correlaciones.
2.7.2	- La plataforma de SIEM debe tener la capacidad de activar capacidades nativas de detección y respuesta que no requieran configuración para su integración, pero se requiere que se tengan una o más de las siguientes funcionalidades nativas: EDR / ITDR - Identitity Detection & Response del mismo fabricante que ofrece el SIEM.
2.7.3	La plataforma de SIEM debe tener la capacidad de poder integrar de manera nativa las siguientes capacidades, de acuerdo a la solicitud del presente proyecto: - Inteligencia de amenazas reconocida como lider en el mercado (TIP - Threat Intelligence Platform). - Administración de logs sin usar bases de datos estándares ni bases de datos indexadas, para retención de datos de 3 meses. - Investigación en profundidad basado en telemetría, comportamientos o funciones lógicas como funciones de inteligencia Artificial. - Módulo de reportería personalizada con detalles avanzados para tener filtros gráficos (Mapas de calor, ubicación geográfica, pipes, tendencias, barras, tablas,) que se actualicen en tiempo real en segundos y puedan exportarse en documentos pdf. - Incorporar parámetros para realizar una gestión de incidentes (Delegación de casos, seguimientos, escalamientos, documentación específica de cada situación, triage) - Correlación avanzada y personalizada. - Capacidad de desarrollar casos de uso de cumplimiento mediante personalización de correlación e ingesta de datos personalizados. - Entregar capacidades para realizar cacería de amenazas para extrapolar procesos, tareas, dependencias a partir de artefactos o actividades de comportamiento sobre todo el ambiente. - Basado en lago de Datos flexible y de crecimiento adaptable. - Capacidades de UBEA - User Behavior & Entity Analytics por medio de la protección de identidad solicitado anteriormente. - Conectores y capacidades XDR - Extended Detection and response. - Capacidades de SOAR para orquestación y automatización.
2.7.4	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional.
2.7.5	- La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.
2.7.6	- La plataforma de SIEM debe tener la capacidad de crear gráficos de tendencia o de observación de datos que pueda visualizarse en: Tablas, pipes, columnas, mapas de calor, mapas de ubicación geográfica, "sandkey", para poder tener el análisis gráfico los cuales se deben actualizar en tiempo real. También en los gráficos se debe tener opción de hacer consultas y filtros para poder hacer profundización en los eventos.
2.7.7	- Los gráficos deben exportarse en formato PDF, pueden exportarse para poder convertirse en un formulario o clonarse o eliminarse.
2.7.8	La plataforma debe permitir la creación de tableros de control que permita: - Realizar seguimiento a tendencias, búsquedas de IOCs. - Seguimiento a las operaciones de seguridad para determinar: Tiempos promedio de detección, tiempos promedio de diagnóstico, tiempos promedio de cierre de incidentes. - Tableros de control de mapas de calor con las TTPs de Mitre para determinar frecuencias, impactos sobre la organización.
2.7.9	- La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, "autotriage", notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros.
2.7.10	El módulo de SOAR debe ser parte de la plataforma en la misma consola de SIEM integrada de manera nativa, debe contar con un tablero de gestión para ver las ejecuciones de playbooks de los últimos 30 días que muestre: - Cantidad de ejecuciones de playbooks provenientes de alertas, detecciones o incidentes. - Cantidad de ejecuciones que provengan de aprobaciones de usuarios.

	- Tendencia de ejecuciones de playbooks completas y fallidas. - Top de ejecuciones por tipo de disparo o iniciación de los playbooks. - Listado de la ejecuciones más recientes y listado de ejecuciones que corren por demanda.
2.7.11	- El módulo de SOAR debe contar con una biblioteca de playbooks para poder incorporar sin necesidad de construirlos de cero estos, como también debe tener la opción de importar playbook de objetos .yaml provenientes de comunidades y colaboración del ecosistema.
2.7.12	El módulo de SOAR debe permitir la creación de playbooks como mínimo: - A partir de un evento, alerta, detección, incidente, estado de un dispositivo, detección de una instalación de aplicación, cambios de políticas o auditoria de sistema, estado de seguridad de los dispositivos o de la nube, un evento de identidad como mínimo. - A partir de una tarea programada la cual puede ejecutarse de forma recurrente definiendo una fecha, hora, día, mes. - Por demanda, donde un administrador puede iniciar para poder automatizar una tarea. En este caso se puede crear un esquema de variables para poder personalizar las consultas al sistema.
2.7.13	- El módulo de SOAR debe contar con información de la ejecución de cada playbook para entender que actividades desarrolló, comprender los procesos de decisión y poder determinar errores para mejorar en el diseño y respuesta de los mismos. Como también deben contar con un módulo de auditoria para determinar quién o cuando se cambió, modificó, Guardando las versiones de cambio y permitiendo volver a versiones anteriores de playbooks.
2.7.14	La plataforma debe contar con capacidades de establecer conversaciones en lenguaje natural mediante motor de Inteligencia artificial para: - Hacer consultas para buscar información en la plataforma (ej: listados de dispositivos con características específicas, búsquedas de aplicaciones de riesgo, vulnerabilidades, consultas de IOCs, que permiten reducir el tiempo de investigación de los analistas). - Consultar sobre ejecuciones de scripts y explicación en lenguaje natural sobre significados de códigos. - Consultas para poder solicitar las consultas a realizar para acelerar la cacería de amenazas. - Consultas para solicitar apoyo en la creación de flujos de automatización. Esta funcionalidad debe estar disponible para poder ser agregada como apoyo a los consultores de SOC, CSIRT o encargados de analizar o investigar incidentes de seguridad.
2.7.15	- El módulo de SOAR debe tener la capacidad de tomar medidas de corrección inmediatas desde el gráfico/ árbol de procesos de incidentes activando un flujo de trabajo SOAR por demanda esto puede ser: Aislamiento de dispositivos, bloqueo de autenticación de usuarios, deshabilitación de usuarios, envío de artefactos al sandboxing, captura de datos de análisis forense, entre otros los cuales pueden ser personalizados o creados de acuerdo a las necesidades.
2.7.16	- La plataforma debe contar con un BOT que tenga el rol de analista de ciberseguridad que apoye los equipos de investigación, cacería de amenazas y administradores de seguridad para poder acelerar las actividades de su día a día. - El BOT debe simplificar el proceso de determinar riesgos y actividad maliciosa en el entorno y reducir la necesidad de revisar y filtrar manualmente grandes cantidades de datos. Puede generar avisos o registros de avisos para determinar rápidamente qué adversarios se han detectado en la organización o han atacado a otras organizaciones del sector, encontrar endpoints afectados por vulnerabilidades de alto riesgo y mucho más.
2.7.17	- La interacción con el BOT debe ser por medio del establecimiento de conversaciones introduciendo una consulta en la barra de conversaciones o ejecutando un libro de indicaciones (conjunto de preguntas), la plataforma debe mantener el contexto de varias preguntas para llegar a la respuesta. la información consultada debe corresponder únicamente a los datos alojados por la plataforma y sus módulos activos únicamente.
2.7.18	- Las respuestas se deben generar en el orden en que las solicitudes se encuentran en la cola. El formato y la cantidad de información de una respuesta pueden variar según la solicitud. De acuerdo a las consultas deben incluir en su mayoría tablas de resultados y un resumen general que los describe, con un concepto de seguridad y análisis. Según los datos de la tabla, puede copiar los datos JSON generados o descargar un CSV, si está disponible. Siempre utilizando lenguaje natural.
2.7.19	El analista BOT debe tener integraciones con el sistema para tener un uso adicional para: - Crear y correr consultas (queries) sobre los datos y datos crudos recopilados sobre la plataforma. - Analizar líneas de comando ejecutados en las cargas de trabajo sin límite de uso: Esto es decodificar, desofuscar y explicar el propósito de una línea de comando o script que se capture en una detección de EDR (ej. Comandos vía powershell). - Crear diagnósticos de detecciones indicando un Score de evaluación de impacto vía AI, explicando porque puede ser potencialmente peligroso y teniendo un concepto para acelerar el proceso de diagnóstico de detecciones, esto por medio del uso de lenguaje natural.

2.7.20	La capacidad de que el analista BOT haga el diagnóstico de detecciones (triage) debe presentar un tablero de control que muestre en un rango de tiempo desde 1 hora, un día, una semana, 30 días, o 90 días: - Cantidad total de diagnósticos y diagnóstico en el tiempo. - Tiempo promedio que toma hacer los diagnósticos. - Tiempo ahorrado en esta actividad. - Detecciones más recientes. - Cantidad de veredictos realizados: Verdaderos positivos, Falsos positivos o sin veredicto.
2.7.21	- El consumo de este servicio de BOT debe basar en el número de consultas ejecutadas por mes con el objetivo de tener una consulta de su consumo, teniendo en cuenta que si se realiza una consulta que se ha realizado en los últimos 30 días la plataforma no debe considerarlo una nueva consulta ejecutada.
3	**SERVICIO DE SOPORTE Y GARANTÍA TÉCNICA**
3.1	**SOPORTE DE FÁBRICA**
3.1.1	**SOPORTE DEL FABRICANTE:** El fabricante debe brindar un soporte en horario de 24x7 (Las 24 horas del día, los 7 días a la semana) desde la firma del contrato, por una vigencia de 24 meses. - Acceso al portal de soporte (base de conocimiento, Escalamiento de Tickets). - 7x24x365 soporte telefónico. - Priorización de Caso. - Asignación de un TAM (especialista de producto) para revisión y evaluación periódica. - Healthcheck de la solución de forma trimestral. - Reportes trimestrales. - Gestión de casos proactivos. - Acompañamiento en nuevas funcionalidades y actualizaciones. - Acompañamiento en el Kick Off del proyecto.

3.1.2	**SOPORTE DEL PROVEEDOR:**
	- El proveedor debe brindar un soporte en horario de 24x7 (24 horas del día, los 7 días de la semana) remoto o presencial según lo solicite la entidad a partir de la firma del contrato, o cada vez que el supervisor lo requiera, por una vigencia de 24 meses.
	- El proveedor debe brindar un soporte presencial dos días a la semana en horario de 8x2 (8 horas del día, 2 días de la semana) presencial, a partir de la firma del contrato, por una vigencia de 24 meses, los días se programarán previa coordinación con el supervisor del contrato.
	- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario.
	- El proponente debe garantizar que las actividades propias de soporte no afecten la continuidad de la operación y funcionamiento de los equipos o herramientas que requieran intervención.
	- Las ventanas de mantenimiento, actualizaciones, deben ser programados en horarios no hábiles, previas coordinaciones con el Supervisor del contrato y de acuerdo con las necesidades del COGFM.
	- El proponente debe contar con una mesa de ayuda para atención de incidentes disponible para el COGFM 7x24 durante la vigencia del contrato, esta mesa debe contar con una herramienta de atención de incidentes que cumpla con mínimo 12 procesos de ITIL certificados; esta mesa será la encargada de gestionar todos los incidentes y requerimientos reportados durante la vigencia del contrato.
	- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket de servicio para los incidentes presentados).
	- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado son el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.
	
	- **Tiempos de respuesta**: El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el supervisor del contrato.
	  - Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente.
	  - De ser necesario el proveedor deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas.
	  - El tiempo máximo permitido para restablecer el servicio es de 4 horas.
	
	- **Tipo De Atención:**
	  - Soporte Nivel 1: De manera presencial dos días a la semana con duración de 8 horas laborales (2x8) en las instalaciones del Comando General de las Fuerzas Militares Centro Administrativo Nacional CAN edificio Fortaleza Carrera 54 # 26-25 en la ciudad de Bogotá, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato.

	- Soporte Nivel 2: Cuando se requiera por medio telefónico o de manera remota a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato, y de acuerdo con los términos y tiempos de respuesta especificados.
4	**OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO**
4.1	**GARANTÍA DE SOPORTE**
4.1.1	- El Contratista deberá garantizar el normal funcionamiento después de la implementación y puesta en marcha de la solución, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. - Soporte disponible los 365 días del año en horario 7x24 (7 días a la semana las 24 horas del día). - El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica gratuita, servicio de correo electrónico o en forma remota de acuerdo a los niveles de servicio. En un lapso de cuatro (04) horas después de haber reportado el incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas.
4.1.2	El proponente debe integrar a su propuesta los siguientes servicios: - Servicio por parte del fabricante para poder hacer al menos 02 workshops durante el despliegue de la plataforma (Taller de buenas prácticas de despliegue y análisis de detecciones para una correcta comprensión). - Servicio de asignación de un TAM - Tecnical account manager por parte del fabricante para que realice una evaluación continua de la configuración de la plataforma y apoyo en la gestión de casos de soporte cuando se hace el escalamiento con fábrica. - Se debe tener acceso a entrenamientos en línea por parte del fabricante sin límite para los funcionarios de la entidad durante la vigencia del contrato.
4.2	**TRASFERENCIA DE CONOCIMIENTO**
4.2.1	- El Contratista debe realizar transferencia de conocimiento para el personal que administra la solución, de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica. - Debe incluir material técnico, en la ciudad de Bogotá en Idioma español; se debe ofrecer una metodología teórica y práctica con laboratorios de cómputo debidamente configurados, en instalaciones dispuestas por el contratista que incluya equipos de cómputo, material impreso, digital, de software y hardware. - El contratista debe disponer de aulas completamente dotadas que cubran todos los aspectos logísticos para la ejecución de los entrenamientos requeridos, igualmente proveer instructores idóneos, calificados y certificados, con experiencia en la ejecución de capacitación. - El Contratista deberá entregar el material de clases necesario para desarrollar el entrenamiento de acuerdo a cada uno de los módulos. Así mismo, se deberán entregar las presentaciones utilizadas por los instructores. - El Contratista deberá emitir un certificado a cada uno de los estudiantes que aprueben la transferencia tecnológica. <u>**LA CAPACITACIÓN DEBERÁ ESTAR ENFOCADA EN:**</u> - Configurar la solución la solución adquirir. - Crear políticas para la protección dentro de la organización. - Gestión de hosts. - Respuesta de incidentes. - Caza de Amenazas. - Despliegue del Agente. - Protección de datos. - Detención y respuesta EDR-XDR. - Antivirus y Antimalware. - El objetivo de esta transferencia de conocimiento es capacitar al personal de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares para que puedan gestionar, instalar, configurar y analizar los productos adquiridos de manera efectiva y adecuada. El certificado emitido por el fabricante y/o distribuidor autorizado servirá como evidencia de la participación y aprobación de la capacitación por parte de los funcionarios.
4.3	**CONFIDENCIALIDAD DE LA INFORMACIÓN**

4.3.1	- El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción **"acuerdo de confidencialidad".** - La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización. - A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento. - Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. - El contratista y los recursos humanos que formarán parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, **el acuerdo de confidencialidad** donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.
4.4	**CRONOGRAMA**
4.4.1	Dentro de los primeros cinco (05) días calendario del plazo de ejecución, el contratista deberá presentar el cronograma para la ejecución del objeto del contrato, para aprobación del supervisor del contrato, que incluya el proceso y actividades de: - Planeación (requerimientos y preparación) - Despliegue (Posibles esquemas de despliegue de sensores, como puede acelerar el proceso), proceso de implementación para minimizar la fricción o interrupciones con la plataforma actual. - Post-Implementación (se debe indicar como es el proceso de escalamiento de nuevos requerimientos, atención de solicitudes de soporte - portales/teléfono/equipo encargado, apoyo en la revisión del estado de la plataforma como informar las nuevas funcionalidades que son importantes incorporar, durante la ejecución del contrato).
5	**Servicio de ingeniera soporte e implementación y puesta en funcionamiento de la solución de acuerdo a documento de especificaciones técnicas.**
5.1	**<u>Implementación del Proyecto</u>** - El contratista junto con el supervisor del contrato debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con la seguridad perimetral. - El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones. - Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Comando General de las Fuerzas Militares. - El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Comando General que sean necesarias para el óptimo funcionamiento de todas las tecnologías.

- El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de la solución a adquirir con sus correspondientes integraciones, con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Comando General de las Fuerzas Militares.

- Las soluciones a implementar deben ser compatibles con las plataformas actuales del Comando General y cumplir con el protocolo IPv4 e IPV6.

- Toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato.

Caso de Fallas:

- Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad.

- En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo:
  - ✓ Implementación de software.
  - ✓ Configuraciones, puesta en producción y funcionamiento.

Integración:

- Realizar una correcta implementación:
  Es importante realizar una correcta implementación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware y software.

- Configuración adecuada:
  La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red.

- Pruebas de integración:
  El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.

Herramienta o software de implementación y despliegue masivo de agentes:

Deberá suministrarse una herramienta licenciada para el proceso de implementación de la solución que permita automatizar la instalación, actualización y desinstalación de los agentes en múltiples equipos de cómputo al mismo tiempo que cumpla con las siguientes especificaciones:

- Descubrimiento de activos: Acceder fácilmente a los datos de sus dispositivos locales, incluidas las versiones de software antiguas.
- Sincronización automática con AD: Sincronizar con Active Directory para importar registros de computadoras automáticamente.
- Se requiere de un software que se pueda instalar en cualquier dispositivo PC o servidor Windows para poder realizar procesos de despliegue masivos de software, No debe requerir un servidor dedicado y puede ser también desplegado de forma distribuida para mayores capacidades de despliegue.
- Este software debe ser de un fabricante independiente.
- La herramienta de despliegue debe poder realizar identificación de dispositivos como:
  - ✓ Dispositivos pertenecientes al directorio activo, donde se pueda definir cuentas de administración generales o parciales para hacer despliegues de software, como también selección granular de dispositivos objetivo como grupos del directorio activo.
  - ✓ Dispositivos windows donde se puede hacer despliegues vía powershell por medio de scripts.
  - ✓ Dispositivos linux donde se pueden hacer despliegues vía SSH por medio de scripts
  - ✓ Listas de dispositivos por medio de la importación de listados.

- La herramienta de despliegue debe tener la capacidad de personalizar tareas y paquetes para poder lanzar tareas en paralelo sin afectar despliegues anteriores.

	- La herramienta de despliegue debe permitir un seguimiento detallado del proceso de despliegue indicando errores en el proceso para poder remediar de forma adecuada.

. ESTUDIO DE SEGURIDAD PERSONAL: El contratista debe aceptar y permitir que el COGFM efectúe un Estudio de Seguridad Personal (ESP) a los funcionarios designados para el desarrollo del proyecto, a fin de comprobar datos y establecer antecedentes disciplinarios; que garanticen la seguridad de la información. Los formatos de seguridad personal (ESP), deberán ser entregados al supervisor del contrato, debidamente diligenciados a más tardar pasados 15 días calendario de la firma y perfeccionamiento del contrato, cuando ello hubiere lugar.
. El contrato debe ejecutarse a todo costo, el contratista se compromete a prestar el servicio con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.
. El contratista deberá garantizar el personal suficiente, idóneo con profesionales calificados necesarios para la completa ejecución y cumplimiento del contrato, sin que esto genere costo adicional para el Comando General de las Fuerzas Militares, de igual manera disponga de instalaciones y equipos de cómputo propias para la ejecución del proyecto.
. Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
. El Comando General de las Fuerzas Militares no asumirá ninguna responsabilidad contractual ni laboral con los funcionarios que la empresa contratista asigne para el cumplimiento del contrato.

2. PERSONAL PARA LA EJECUCIÓN DEL CONTRATO

CARGO	DATOS DEL PERSONAL
GERENTE DE PROYECTO	RONALD ALEXANDER CASTAÑEDA OLARTE CC. 80.195.893 de Bogotá Ingeniero electrónico Matricula Profesional: CN206-47243
INGENIERO IMPLEMENTADOR	EDGAR ALFONSO GODOY LOPEZ CC. 79.906.707 de Bogotá Ingeniero de Sistemas Matricula Profesional: 25255-088953CND

- En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario.

Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa.

- La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto.

- La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado.

- El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.

NOTA: Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el Contratista debió efectuar el respectivo análisis del pliego de condiciones del presente proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y

cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato derivado del presente proceso.

Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato.

El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma.

3. CUADRO PRECIOS

No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR UNITARIO CON IVA
1	**SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS**				
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	237.780.000,00	237.780.000,00
1.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	189.820.000,00	189.820.000,00
1.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	151.664.000,00	151.664.000,00
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	67.540.000,00	67.540.000,00
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	47.069.000,00	47.069.000,00
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	13.642.000,00	13.642.000,00
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	380.000.000,00	380.000.000,00
VALOR TOTAL LOTE No. 3					**1.087.515.000,00**

NOTA: Teniendo la procedencia de los bienes, de conformidad con el Estatuto Tributario, artículo 476, Los servicios a adquirir se encuentran excluidos de IVA y artículo 477 los Bienes que se encuentran exentos del impuesto de IVA.

Los servicios a adquirir se encuentran excluidos de IVA:

Art. 476. Servicios excluidos del impuesto sobre las ventas

(...)

Numeral 20. Adquisición de licencias de software para el desarrollo comercial de contenidos digitales, de acuerdo con la reglamentación expedida por el Ministerio de Tecnologías de la Información y Comunicaciones.

Numeral 21. Suministro de páginas web, servidores (hosting), computación en la nube (cloud computing).

Que teniendo en cuenta la procedencia de los bienes se dará el siguiente trato tributario:

Art. 477. Bienes que se encuentran exentos del impuesto.

...3. Las municiones y material de guerra o reservado y por consiguiente de uso privativo y los siguientes elementos pertenecientes a las Fuerzas Militares y la Policía Nacional:

n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional.

(...)

4. ASPECTOS TÉCNICOS PONDERABLES

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN
El contratista ofrece sin costo adicional: transferencia de conocimiento de la solución de protección de datos ofertada con certificación de Voucher para cuatro (04) funcionarios del Comando General de las Fuerzas Militares – CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.

- **LOTE 5: SUSCRIPCIÓN WAF.**

1. ESPECIFICACIONES TÉCNICAS

ÍTEM No.	**DESCRIPCIÓN**	**MARCA / REFERENCIA OFERTADA**
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF).	F5- Distributed Cloud Services Base Package F5- Distributed Cloud Mesh – Globally Distributed Load Balancer with Threat Campaigns Distributed Cloud Mesh – Additional Anycast VIP

GENERALIDADES

La solución de seguridad deberá proporcionar una plataforma unificada de seguridad que integre servicios de protección contra ataques de denegación de servicios distribuida, firewall de aplicaciones web (WAF), seguridad para APIs y detección y prevención de bots maliciosos y usuarios reales comprometidos.

La solución de seguridad deberá ofrecer estos servicios en la nube del fabricante no se aceptarán despliegues en nube pública.

La solución de seguridad deberá incluir al menos dos balanceadores de carga, cada uno con soporte para un mínimo de 32 aplicaciones web, y al menos dos direcciones IP ANYCAST distribuidas en todos los centros de datos de la solución de seguridad para la publicación de los servicios web de la entidad. Estas aplicaciones podrán estar asociadas a un mínimo de 200 nombres de dominio raíz diferentes.

La solución de seguridad deberá realizar el enforcement de políticas de seguridad para las aplicaciones WEB y APIs, tanto en los nodos regionales o puntos de presencia, como en los múltiples proveedores de nube o en las premisas.

Esta solución de seguridad deberá contar con soporte y garantía por parte del fabricante. La vigencia de la suscripción soporte y garantía deberá ser de dos (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante.

CARACTERÍSTICAS TÉCNICAS

REQUERIMIENTOS ESPECÍFICOS

FUNCIONALIDAD	**DESCRIPCIÓN**
SaaS	La solución deberá soportar una arquitectura Software as a Servicie (SaaS), donde la manera de consumo de los servicios sea dentro

	de su propio cloud, incluyendo todos los puntos de presencia distribuidos de manera global.
	La solución deberá ofrecer disponibilidad de ancho de banda limpio en su servicio WAF o protección de aplicaciones web, sin limitación en el volumen de datos por solicitud inspeccionada o mitigada, garantizando la protección para todo el tráfico que llegue a la Entidad, hasta un máximo de treinta (30) millones de requests mensuales como parámetro de dimensionamiento y control operativo.
	La solución deberá incluir al menos dos balanceadores de carga, cada uno con soporte para un mínimo de 32 aplicaciones web, y al menos dos direcciones IP ANYCAST distribuidas en todos los centros de datos de la solución para la publicación de los servicios web de la entidad. Estas aplicaciones podrán estar asociadas a un mínimo de 200 nombres de dominio raíz diferentes.
ADMINISTRACIÓN	
Gestor Centralizado / Consola Central	La solución deberá proporcionar una consola central SaaS para la administración centralizada de las configuraciones de red y seguridad, así como también acceso a herramientas de troubleshooting y dashboard donde se visualice la disponibilidad y el estado de los servicios. Además, debe permitir que la gestión se realice mediante clickops, API requests, Terraform o integrandose al pipeline CI/CD de la organización
API de la solución	La solución deberá ser full RESTful-API o API first: - permitiendo realizar todas las configuraciones a través de su API, así como también, la petición de información de los dashboards. .- debe estar bien documentada y proveer de las configuraciones en JSON y YAML de cualquiera de los objetos que se definan. .- debe permitir la creación de credenciales por usuario, el uso de API token, certificados, así como la creación de usuarios API con RBAC.
Usuarios Admin	La solución deberá soportar la creación de múltiples usuarios, así como roles de acceso como read only, SecOps, DevOps, NetOps, SuperUser, Billing User entre otros.
RBAC	La solución deberá permitir el uso de RBAC para el control de acceso de los usuarios al gestor centralizado, permitiendo la delimitación de las APIs/recursos que se pueden visualizar y/o administrar.
Self Service	La solución deberá proporcionar al usuario del gestor centralizado la posibilidad de administrar sus servicios dentro de una consola unificada y donde se permita la colaboración de distintos equipos (SecOps,DevOps,entre otros)
Servicio Administrado	La solución deberá contemplar la opción de incluir un servicio administrado para WAAP, operado por personal especializado y certificado por el fabricante, el cual será presentado como un componente opcional y evaluado de forma independiente a la solución principal
Soporte	La solución deberá contar con soporte 24x7, ya sea por medio de Teléfono, Mail u otros medios de contacto. Asimismo, el servicio de soporte deberá permitir la interacción con el Centro de Soporte en idioma español en el uso horario de la región (Colombia) durante horario laboral.
Capacitación	La solución deberá contar con capacitación onDemand a través de videos y/o documentación que ejemplifiquen configuraciones básicas y que sean accesible desde la plataforma o página web del fabricante
VISIBILIDAD	
Integración con SIEM	La solución deberá proporcionar integración con herramientas de logging de terceros.
Dashboard de Performance	La solución SaaS deberá proporcionar visibilidad acerca de: .- Salud de la aplicación .- Alertas activas .- Origin Servers/Backends .- Latencia de fin a fin .- Visitantes únicos .- Tipo de dispositivo

	.- Peticiones (Request Rate, Total Request, Error rate, total errors, drop rate, drop count) .- Throughput .- ASN .- TLS Fingerprint .- TLS Ciphers y protocolos .- Códigos de error de HTTP .- Localización de clientes .- Top URLs
Dashboard de Seguridad	La plataforma SaaS deberá proporcionar visibilidad sobre: .- Eventos de seguridad por aplicación (WAF, APISec, DDoS, Anti-Bot entre otros) .- Top ten de las firmas con más hits .- Eventos localizados geográficamente .- Tipos de ataques .- Score de usuarios maliciosos .- Clasificación de bots (humano, malicioso, Sospechoso) Asimismo, la solución deberá proporcionar filtros para búsquedas utilizando el identificador asociado con el evento de seguridad.
Auditoria	La plataforma SaaS deberá proporcionar visibilidad sobre los cambios de configuración realizados por los usuarios del gestor centralizado durante un periodo de tiempo de 30 días
CERTIFICACIONES	
California Consumer Privacy Act (CCPA)	Deberá estar en cumplimiento con lo dispuesto por California Consumer Privacy Act (CCPA)
General Data Protection Regulation (GDPR)	Deberá estar en cumplimiento con lo dispuesto por General Data Protection Regulation (GDPR)
System and Organization Controls (SOC) Type 2	La solución deberá contar con la certificación System and Organization Controls (SOC) Type 2
SLAs	
Disponibilidad	La plataforma SaaS deberá proporcionar un 99.99% de disponibilidad
Tiempo de Respuesta	El servicio de Soporte técnico de la solución propuesta deberá tener un tiempo de respuesta de 30min para el primer contacto
Analisis deCausa Raiz	El servicio de Soporte técnico de la solución debe cumplir con el siguiente SLA relacionado con el análisis de causa raíz de un incidente: Incidente de severidad crítica: proporcionar un draft a las 24 hrs y el análisis final en 7 días

WEB SECURITY	
Funcionalidad	**Descripción**
Web Application & API Security	1.- La solución propuesta deberá emplear una combinación de técnicas algorítmicas, basadas en firmas, utilización de bases reputacionales y machine learning para identificar ataques a nivel de aplicación y API, proporcionando una solución holística de firewall aplicativo de próxima generación. 2.- La solución deberá contar con un motor de machine learning para determinar de manera automática todos los API endpoints que son accedidos a través de cualquiera de los servicios virtuales publicados. Además, deberá permitir que la información aprendida pueda ser utilizada para la definición de políticas por aplicación
Web Application Firewall	La solución deberá proporcionar una plataforma SaaS con motor de Machine Learning y firmas para la detección de ataques a nivel de capa de aplicación, que incluya la detección de ataques del OWASP TOP 10 así como los últimos ataques conocidos con actualización automática en valores de firmas, así como la utilización de una base de datos asistida de campanas de amenazas para detección de ataques específicos alrededor del mundo.
Detección de Usuarios Maliciosos	La solución deberá contar con la capacidad de detectar usuarios maliciosos mediante el análisis de su comportamiento utilizando técnicas y modelos avanzados, tal como Machine Learning.
Supresión de falsos positivos	La solución deberá utilizar un modelo de Machine Learning para el perfilamiento del tráfico dentro del WAF que permita la supresión de falsos positivos.

Tuning de la base de firmas	La solución deberá contar con un mecanismo automático que permita el tuning de las firmas de ataques
DDoS L3/L4	La solución deberá contar con la capacidad de detección y mitigación automática de ataques volumétricos de denegación de servicio, sin límite en la cantidad de este tipo de eventos y sin ancho de banda mínimo para la mitigación.
DDoS L7	La solución deberá permitir el bloqueo de clientes/usuarios de la aplicación basándose en su comportamiento. La solución deberá permitir la definición de políticas de retos de identificación de usuario de la aplicación utilizando JavaScript y CAPTCHA
Antibot	La solución deberá contar con la funcionalidad de Anti-Bot permitiendo la categorización de bots en buenos, sospechosos y malos y, por ende, su mitigación.
Servicio de reputación de IP	La solución deberá contar con la funcionalidad de bloqueo automático de conexiones desde IPs consideradas maliciosas, mediante la utilización de una base dinámica de reputación de IPs.
Bloqueo de peticiones no deseadas	La solución deberá permitir el bloqueo de clientes basándose en su comportamiento, el ASN, la red, la dirección IP y el país desde donde se generó la conexión
Cifrado	La solución deberá permitir la configuración de Cifrados de acuerdo a diferentes perfiles: alto, medio o bajo, así como la creación de políticas personalizadas para utilización de ciphers y protocolos específicos por aplicación. **High:** TLS 1.2 y 1.3 TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Generación Automática de Certificados Digitales	La solución deberá permitir la configuración de certificados públicos firmados de manera automática y controlados de manera automática a través de alguna delegación de dominio o validación de registros de DNS
Reescrituras HTTP	La solución deberá permitir la configuración de reescrituras HTTP. Asimismo, deberá permitir el tratamiento tanto de las peticiones HTTP hacia las aplicaciones, como de respuestas personalizadas según los diferentes códigos de HTTP.
Balanceo de cargas	La solución deberá permitir la configuración de origen servers/backend servers y sus correspondientes monitores de salud de manera ilimitada. Asimismo, la solución deberá permitir el uso de los siguientes métodos de balanceo: .- RoundRobin .- Least Active Request .- Random .- Persistencia por dirección IP .- Persistencia basada en cookie .- Ring Hash Así como crear pesos sobre los orígenes que se deseen y asignar esquemas activo-pasivo.
Analítica de Comportamiento de Usuario	La solución deberá contar con mecanismos que permitan el análisis de comportamiento utilizando métricas y logs. El análisis de comportamiento debe incluir: .-Detección de anomalías por petición, utilizando métricas como tamaño de la petición, tamaño de la respuesta, latencia. .-Lógica de Negocio, utilizando los logs de peticiones, por cliente por servidor y el host virtual para aprender: elementos dinámicos, probabilidad de función, tiempos y anomalías analiza esto utilizando redes neuronales.
Control sobre el número de peticiones (Rate Limit L7 DoS)	La solución deberá permitir controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre API endpoints específicos.
CSRF	La solución deberá controlar los subdominios permitidos en las peticiones cruzadas dentro de un Load Balancer/Proxy

Manejo de Información sensible	La solución deberá permitir controlar la información a visualizar de las respuestas del servidor, permitiendo enmascarar la información considerada como sensible, como, por ejemplo: datos de tarjeta de crédito
Client Side Defense	La solución debe proveer de un sistema de protección multifase a las aplicaciones Web, contra Formjacking, Magecart-style, y otros ataques de JavaScript. La protección multifase debe incluir detección, alertamiento y mitigación
Identificación del usuario	La solución deberá identificar usuarios teniendo en consideración los siguientes parámetros: ClientIP, TLSFingerprint, Cookie, HTTP Header, Client ASN, Client City, Client Region, Query Parameter Key.
Engine de WAF unificado	La solución deberá utilizar el mismo motor de WAF cualquiera sea la arquitectura implementada: SaaS, On-Premise, Hibrido, permitiendo la extensión de las políticas o servicios de seguridad a los diferentes ambientes que la constituyen.
Mutual TLS	La solución deberá permitir la utilización de MTLS para comunicación hacia los clientes y hacia los servidores.
Cookie Protection	La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticacion.
GraphQL Inspection	La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando instrospeccion, de los recursos, disponibles en el esquema actual.
Ruteo de requests HTTP	La solución deberá permitir la redirección de peticiones a distintos grupos de origen servers/backend servers dependiendo de: .- prefijo de URI .- HTTP header .- cookie .- método HTTP aplicando reglas de WAF por cada ruta, así como reglas de seguridad específicas.
Mitigación de Usuarios Maliciosos	La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos: low, medium, high. Dependiendo del puntaje por los eventos de seguridad de un usuario, la solución debe contar con la capacidad de mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.
Errores de Respuesta Personalizados	La solución deberá permitir crear un mensaje de respuesta personalizado por cada código de error HTTP
Tamaño de los headers	La solución deberá permitir limitar el tamaño de los headers HTTP de los requests/peticiones de los usuarios
Manipulación de Headers	La solución deberá permitir la eliminación o adición de nuevos headers HTTP en las respuestas o peticiones entre el cliente y servidor. Por ejemplo: la solución deberá ser capaz de insertar el header X-Forwarded-For HTTP Header para informar al origen server/backend server de la dirección IP original del request del cliente
CORS	La solución deberá tener la capacidad de proteger contra CORS
GeoIP protection	La solución deberá permitir el control de acceso de los usuarios a la aplicación según el país de origen, permitiendo reglas de allow o deny desde países en específico; por ejemplo: que se permita el acceso solo a un país, y se bloquee el resto.
Service Policies	La solución deberá permitir la creación de reglas de L3, L7 para permitir o negar el acceso a recursos, así como el manejo de los diferentes motores de seguridad para la creación de excepciones.
Protección contra ataques sofisticados o campañas activas	La solución deberá contar con la capacidad de proteger a las aplicaciones contra ataques sofisticados o ataques "In-the-wild" con gran precisión, de manera que la información contextual de esos ataques reales utilizados alrededor del mundo sea empleada para la creación de firmas de WAF en tiempo real.

API Security	
Funcionalidad	**Descripción**

Monitoreo y Protección de APIs	La solución deberá tener la capacidad de monitorear y proteger las APIs tan cerca del origen como sea posible. Además, la solución debe brindar esta capacidad utilizando el mismo motor de protección tanto en el propio cloud, como en clouds públicos/privados y en las premisas.
API Anomaly Detection	La solución deberá contar con un mecanismo de análisis de comportamiento de las peticiones/request hacia cualquier de los API endpoints definidos, permitiendo la detección de anomalías por petición/request.
API Discovery	La solución deberá contar con la capacidad de aprender/determinar los API endpoints que son accedidos, incluyendo petición y respuesta, y detectar información sensible. Además, debe proveer la vista de API endpoints en inventario, shadow y descubiertas, y generar un Probability Distribution Function (PDF) para las métricas relacionadas a cada endpoint, con actualización periódica. Esta funcionalidad aplicará para un (1) API, con un máximo de quinientos mil (500.000) requests mensuales en protección.
Sensitive Data	La solución deberá contar con la capacidad de identificar y localizar la información sensible en las peticiones desde los clients y en las respuestas de los API endpoints. Deberá identificar PII, tal como números de tarjeta de crédito y numero de seguridad social e indicar el parámetro/campo donde la información esta localizada.
API Endpoint Learning	La solución deberá contar con un mecanismo que permita el descubrimiento dinámico de las APIs, determinar cuáles endpoints deberían ser utilizados y permitir únicamente estos API endpoints, obtener información de la utilización, como tamaño de las peticiones y frecuencia. Asimismo, la solución deberá proporcionar las siguientes métricas: tamaño de la petición/respuesta, latencia con datos y latencia sin datos, frecuencia de peticiones, frecuencia de errores, troughput de las respuestas.
API Schema Learning	La solución deberá aprender la estructura del esquema de las APIs, analizando los requests/peticiones y respuestas para cada una de ellas. Asimismo, deberá permitir la descarga del swagger file aprendido.
Importación de especificación (Swagger file)	La solución deberá permitir la importación de las especificaciones del API contenidas en un archivo Swagger.
API Authentication Discovery	La solución debe contener sensores integrados para la detección de tipos de autenticación, y localización en las llamadas API. Una vez detectados, se deben asociar con un edpoint y mostrar un estado de autenticación.
JSON Web Token Discovery	La solución deberá ser capaz de descubrir el header, payload y firma de JWTs así como la identificación de campos utiles para el cliente, permitiendo la identificación de datos sensibles en los payloads de JWT así como la definición del score de riesgo.
Detección de Usuarios Maliciosos	La solución debe contar con un motor de WAF que permita realizar un perfilamiento de usuarios, utilizando: la cantidad de firmas identificadas, cantidad de accesos prohibidos, errores de login, tasa de errores.
Mitigación de Usuarios Maliciosos	La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos, low, medium, high y dependiendo del puntaje por los eventos de seguridad de un usuario, realizar una mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.
Control sobre el número de peticiones Rate Limit L7	La solución deberá controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre endpoints específicos.
API Security	La solución deberá permitir la carga de archivos Swagger para cada versión de la API, controlando el modo de consumo de los endpoints por frecuencia o método HTTP. Donde todo lo que no se encuentra dentro de la definición de Open API (swagger file) (o explícitamente permitido) sea bloqueado. La solución deberá permitir la creación de políticas de seguridad, donde se contemplen excepciones que permitan el acceso a usuarios específicos dentro de API end points o grupos de API.

Manejo versionamiento de definición de APIs	La solución deberá permitir la carga de distintos archivos Swagger, dependiendo de la versión de la API a proteger, y añadir la definición en distintos segmentos dentro del balanceador.
Cookie Protección	La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticación.
GraphQL Inspection	La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando introspección, de los recursos, disponibles en el esquema actual.
API Discovery	La solución debe disponer de una función de descubrimiento de API que lea e identifique los API endpoints en el repositorio de código.
	La solución debe tener una función de descubrimiento de API que lea e identifique los puntos finales de API de dominios externos, rastreando los dominios externos.

HERRAMIENTA DE PENTEST AUTOMATIZADA	
Funcionalidad	**Descripción**
Prueba de penetración automatizada	La solución debe contar con una solución Dynamic Application Security Testing(DAST) en la nube para aplicaciones web y API. La prueba de penetración puede configurarse en minutos y solo requiere la URL de su aplicación web/API junto con las credenciales de uno o más usuarios de prueba que pueden utilizar para iniciar sesión en su aplicación de destino automáticamente.
Tipo de vulnerabilidades	El servicio Scan debe identificar vulnerabilidades en sus aplicaciones web y APIs. Estas pruebas se basan en el OWASP Top 10, un documento de concienciación estándar para desarrolladores y seguridad de aplicaciones web. El servicio Scan también debe incluir pruebas propias y pruebas curadas por la comunidad. Estas son algunas de las pruebas que debería realizar Scan: Broken Access Control Business Logic Attacks SQL Injection (incl. Blind SQL Injection): Cross-Site Request Forgery (CSRF): Cross-Site Scripting (XSS) (Stored, Reflected, DOM-based) Insecure Direct Object References (IDOR) Security Misconfiguration Vulnerable and Outdated Components Identification and Authentication Failures Software and Data Integrity Failures Security Logging and Monitoring Failures Server-Side Request Forgery (SSRF)
Tipos de servicios	La solución de seguridad debe realizar scans y servicios de recon.

GARANTÍA TÉCNICA Y SERVICIO

- Garantizar soporte del fabricante 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante.
  . El soporte del fabricante deberá incluir:
  - Soporte vía correo electrónico
  - Soporte vía telefónica
  - Recepción de alertas, mensajes o noticias sobre las actualizaciones del servicio durante el periodo contratado.
  - Ningún límite en la cantidad de apertura de casos, incidentes, solicitudes, requerimientos, consultas, soporte técnico, resolución de problemas.
- Soporte 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante.
  . El soporte debe incluir:
  - Apoyo en nuevas configuraciones.

- Atención de incidentes (correo electrónico, teléfono, mesa de ayuda).
- Instalación de nuevas actualizaciones (si aplica)
- Un mantenimiento general en el año.
- Atención de casos de carácter técnico en temas funcionales de las diferentes aplicaciones las cuales estén siendo protegidas en la presente solución.

Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al mismo, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).

- El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá.
- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se *llevará a cabo por medio de un Ticket de servicio para los incidentes presentados).*
- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.

ALCANCE GARANTÍA TÉCNICA

GARANTÍA: El término de la garantía técnica o garantía legal de conformidad con los artículos No. 7, 8, 9 y 11 de la Ley 1480 de 2011, será de dos (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante

Aspectos incluidos en la garantía legal. Corresponden a la garantía legal las siguientes obligaciones:

- Se debe efectuar como mínimo dos (02) mantenimientos preventivos a la solución descrita en el presente anexo, por el término de la garantía.

Estos mantenimientos deben incluir como mínimo las siguientes actividades:

- Actualizaciones y Parches de Seguridad
- Aplicación de actualizaciones y parches de seguridad críticos en el WAF.
- Revisión periódica de las nuevas versiones del WAF y su impacto en la configuración actual.
- Revisión y Solución de Errores
- Monitoreo y resolución de errores o fallos en las reglas de seguridad.
- Identificación y mitigación de falsos positivos y falsos negativos en la protección del WAF.
- Copias de Seguridad y Recuperación
- Programación y validación de copias de seguridad de configuraciones y reglas de seguridad.
- Plan de recuperación en caso de incidentes o errores de configuración.
- Monitoreo y Análisis de Logs
- Revisión periódica de logs de actividad y eventos de seguridad.
- Generación de reportes sobre ataques detectados y acciones de mitigación aplicadas.
- Optimización de Recursos
- Análisis del consumo de recursos en la nube y optimización de configuraciones.
- Ajustes en las reglas de caching y mitigación de ataques para mejorar la disponibilidad y rendimiento del servicio.
- Desactivación de Funcionalidades Inoperativas
- Identificación y eliminación de reglas o configuraciones obsoletas o ineficaces.
- Mantenimiento de una configuración optimizada basada en buenas prácticas.
- Procedimientos de Hardening
- Implementación de medidas de refuerzo de seguridad recomendadas por los principales proveedores de WAF en la nube.
- Configuración avanzada de mitigación de amenazas (Rate Limiting, Bot Management, Geo-blocking, etc.).
- Nuevas implementaciones.

Las ventanas de mantenimiento deben ser programados en horarios no hábiles, previas coordinaciones con el Supervisor del contrato y de acuerdo con las necesidades del COGFM.

- En caso de presentarse fallas en la solución de seguridad descrita en el presente anexo, se deberán efectuar los acompañamientos todas las veces que se requiera. Estos deben incluir como mínimo:
- Remplazo de la solución de seguridad por otra de iguales o superiores características.
- Instalación y/o reparación de software.
- Configuraciones, puesta en producción y funcionamiento.

- El servicio será brindado en sitio en la ciudad de Bogotá de acuerdo con los tiempos de respuesta establecidos.
- El tiempo máximo permitido para cambio o reparación de la solución de seguridad es de 20 días calendario una vez sea reportado el incidente, en caso que la falla genere afectación de servicio el contratista deberá suministrar, configurar y poner en funcionamiento temporalmente, una solución, de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para COGFM, con el fin de garantizar la continuidad en la prestación de los servicios.
- El contratista deberá suministrar, configurar y poner en perfecto funcionamiento la solución de seguridad,
  después de realizar el mantenimiento (cuando aplique), garantizando la continuidad de los servicios.
- En caso de que la solución de seguridad genere la reinstalación o reconfiguración de software, sistema operativo o firmware, estas labores deben ser realizadas por el contratista sin costo adicional para el COGFM.
- Todos los gastos que se ocasionen por concepto de transporte y otros gastos a fin de cumplir con los mantenimientos preventivos y correctivos correrán por cuenta del contratista.

FUNCIONAMIENTO Y CONTINUIDAD

- Garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados por la solución de seguridad descrita en este anexo, a partir de la fecha de activación del producto.
- Se debe garantizar el funcionamiento de cada uno de los elementos de software del SISTEMA DE SEGURIDAD, mínimo durante el tiempo de la garantía técnica, reemplazando durante dicho periodo, cualquier elemento del software en falla o mal funcionamiento.

ACTUALIZACIONES

- Durante el tiempo de la garantía se debe brindar e instalar actualizaciones a la solución de seguridad descrita en el presente anexo, cada vez que se libere en el mercado una nueva versión de software, upgrade, o parche. Lo anterior previa solicitud y aprobación del supervisor del contrato y una vez haya sido probada en laboratorio, asegurando la continuidad del servicio y funcionamiento de los sistemas.
- Se debe realizar entrega al COGFM, de los medios magnéticos y/o manuales si existen cambios de versión.

REPORTES E INFORMES TÉCNICOS

Una vez realizados los acompañamientos *(remotos o en sitio)*, se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar:

- Actividades realizadas.
- Actualizaciones aplicadas.
- Procedimientos preventivos y/o correctivos aplicados.
- Recomendaciones.
- Pendientes.

SEGURIDAD

ACUERDO DE CONFIDENCIALIDAD: El Contratista y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista, lo cual será verificado por el supervisor del contrato.

Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares.

El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.

OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO

El contrato debe ejecutarse a todo costo, el contratista se compromete a realizar la suscripción con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.

El contratista deberá realizar transferencia de conocimiento y entrenamiento como mínimo de 20 horas, en el manejo y administración de la plataforma de protección de aplicaciones web, Adicionalmente suministrar el respectivo voucher para presentar examen de certificación como técnico especialista ante el fabricante de la solución de seguridad, para tres (03) funcionarios del CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.

Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia

deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista deberá presentar el cronograma de actividades para la ejecución del objeto del contrato, para aprobación del supervisor del contrato.

2. PERSONAL PARA LA EJECUCIÓN DEL CONTRATO

CARGO	DATOS DEL PERSONAL
INGENIERO DE SOPORTE E IMPLEMENTADOR DE LA SOLUCIÓN DE SEGURIDAD	JUAN PABLO MACÍAS VARGAS CC. 1032363649 Ingeniero Telecomunicaciones Matricula Profesional: CN290-76534

- En el evento que el contratista requiera cambiar el personal propuesto, deberá tramitar a través del supervisor y allegar copia de la hoja de vida y de todos los documentos exigidos en el proceso, experiencia del nuevo personal, para aprobación por parte de la Entidad; éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado y cumplir con los requerimientos estipulados en esta ficha técnica. Se deberá reemplazar en un periodo máximo de tres (3) días calendario.

Deberá informarse al supervisor, de tal situación, con mínimo diez (10) días calendario de antelación, anexando la hoja de vida del nuevo funcionario. Así mismo los recursos asignados para el presente contrato, solo podrá ser cambiados a solicitud de supervisor del contrato en el caso que este sea desvinculado de la empresa.

- La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto.

- La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que la supervisión haya fijado.

- El supervisor evaluará el desempeño laboral del profesional asignado y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.

NOTA: Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el Contratista debió efectuar el respectivo análisis del pliego de condiciones del presente proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato derivado del presente proceso.

Con la presentación de la propuesta, el Contratista acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

El Contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato.

El Contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de la misma.

3. CUADRO PRECIOS

No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR TOTAL INCLUIDO IVA
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	387.700.000,00	387.700.000,00

NOTA: Teniendo la procedencia de los bienes, de conformidad con el Estatuto Tributario, artículo 476, Los servicios a adquirir se encuentran excluidos de IVA y artículo 477 los Bienes que se encuentran exentos del impuesto de IVA.

Los servicios a adquirir se encuentran excluidos de IVA:

Art. 476. Servicios excluidos del impuesto sobre las ventas

(...)

Numeral 20. Adquisición de licencias de software para el desarrollo comercial de contenidos digitales, de acuerdo con la reglamentación expedida por el Ministerio de Tecnologías de la Información y Comunicaciones.

Numeral 21. Suministro de páginas web, servidores (hosting), computación en la nube (cloud computing).

Que teniendo en cuenta la procedencia de los bienes se dará el siguiente trato tributario:

Art. 477. Bienes que se encuentran exentos del impuesto.

...3. Las municiones y material de guerra o reservado y por consiguiente de uso privativo y los siguientes elementos pertenecientes a las Fuerzas Militares y la Policía Nacional:

n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional.

(...)

4. ASPECTOS TÉCNICOS PONDERABLES

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN
El contratista ofrece sin costo adicional: Terminal para administración y gestión de la solución de seguridad que debe incluir como mínimo Intel® Core™ Ultra 7 265KF, Windows 11 Pro, NVIDIA® GeForce RTX™ 5080, 32 GB DDR5, SSD de 2 TB, Con periféricos incluidos y 02 dispositivos de visualización de 25" que permitan visualización y monitoreo de datos críticos, sin que este ofrecimiento genere costo adicional para la entidad.

POR EL MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA,

Coronel GEOVANNY ANDRES SUAREZ PENAGOS
Director Administrativo y Financiero del COGFM

Teniente Coronel JULIAN ANDRES QUIÑONES LONDOÑO
Gerente de Proyecto

POR EL CONTRATISTA,

JESUS ALBERTO FRANCO ACOSTA
C.E. 582.410
Representante Legal Suplente de UT 273COGFM H&Y 2025
NIT. 901988423-0

Vo. Bo. MY. ERIKA ANDREA RODRÍGUEZ SÁENZ
Jefe Área de Contratación

Elaboró: PS JONNATAN F. PUERTO GARCIA
Asesor ARCON

Revisó: PS. DIEGO FERNANDO PARDO G.
Comité Económico Evaluador

Vo. Bo. PD. ANDREA SOLAQUE GONZALEZ
Abogada Área de Contratación

Reviso: PS. VIVIANA MARCELA PELÁEZ G.
Comité Jurídico Evaluador