COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

CONTRATO DE PRESTACION DE SERVICIOS No. 144-MDN-COGFM-ESDEG-2026

CONTRATISTA	HEIMCORE S.A.S
NIT No.	900425697-2
REPRESENTANTE LEGAL	JESUS ALBERTO FRANCO ACOSTA
IDENTIFICACIÓN	C.E No. 582410
DIRECCIÓN	Calle 98 # 70 - 91 Of 202 Edificio Vardi Centro Empresarial Ponte de Bogotá D.C.
TELÉFONO CELULAR	5804352
CORREO ELECTRÓNICO	acabello@heimcore.com.co
OBJETO	RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIANALIZER 200F Y ACTUALIZACIÓN DEL EDR CON XDR (EXTENDED DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO.
VALOR DEL CONTRATO	CUATROCIENTOS VEINTE CINCO MILLONES CIEN MIL PESOS M/CTE ($425.100.000,00,00) IVA incluido para cada uno de los ítems incluye impuestos, tasas, contribuciones y otros conceptos que genere la ejecución del futuro contrato. (si aplica)
CIUDAD	Bogotá D.C

Entre los suscritos a saber: Capitán de Fragata **CLAUDIA PATRICIA PEREZ RODRIGUEZ**, mayor de edad, vecino de Bogotá, D.C, identificada con la cedula de ciudadanía No. 22.732.677 expedida en Barranquilla, quien actúa en su condición de Jefe del Departamento Administrativo de la Escuela Superior de Guerra "General Rafael Reyes Prieto", NIT. 830.002.634-1 cargo para el cual fue encargado mediante Resolución No. 043 del 27 de marzo de 2025, expedida por el Comandante General de las Fuerzas Militares, debidamente facultado para celebrar contratos según Resolución de Delegación No. 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 destine al Ministerio de Defensa Nacional, una funciones de carácter administrativo y se dictan otras disposiciones", expedida por el Ministerio de Defensa Nacional, y quien en consecuencia representa por la delegación conferida MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - ESCUELA SUPERIOR DE GUERRA – DEPARTAMENTO ADMINISTRATIVO, por una parte y por la otra el señor **JESUS ALBERTO FRANCO ACOSTA,** identificado con C.E No. 582410 de Venezuela, representante legal suplente de la firma HEIMCORE S.A.S, identificada con NIT. No. 900425697-2, quien para efectos del presente documento se denominará EL CONTRATISTA, hemos convenido celebrar el presente Contrato de Servicios previas las siguientes consideraciones: **a)** Que se elaboró el estudio previo de conformidad con la modalidad de Selección Abreviada Menor Cuantía cuyo fundamento jurídico se encuentra previsto en el numeral literal b numeral 2º del artículo 2° de la Ley 1150 de 2007, reglamentado por el artículo 2.2.1.2.1.2.20 del Decreto 1082 del 26 de mayo de 2015. **b)** Que al momento de la apertura del proceso de selección, se contó con la respectiva apropiación presupuestal que respalda el presente compromiso, como da cuenta el Certificado de Disponibilidad Presupuestal No. 15826 del 04 de junio de 2026, expedido por el Jefe de Presupuesto de la ESDEG. **c)** Que el Jefe del Departamento de Administrativo y Ordenador del Gasto mediante Resolución No. 089 del 14 de julio de 2026, SE ordenó la Apertura del proceso de contratación bajo la modalidad de Selección abreviada de Menor Cuantía **No. 126-MDN-COGFM-ESDEG-2026, RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD**

Scanned with CamScanner

PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIANALIZER 200F Y ACTUALIZACIÓN DEL EDR CON XDR (EXTENDED DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" d) Que el cierre y recepción de ofertas del proceso se realizó el día 10 de agosto de 2026, como consta en la plataforma de SECOP II y se recibieron las siguientes ofertas:



LISTA DE OFERTAS

Abrir Panel | Opciones

Referencia de oferta	Entidad	Evaluación	Presentada	Oferta
oferta_126-MDN-COGFM-ESDEG-2026	Heimcore SAS	Oferta en evaluación	10/08/2026 3:49 PM	425.100.000 COP
Renovacion Licenciamiento- Oferta redneet 2026	REDNEET SAS	Oferta en evaluación	10/08/2026 3:26 PM	469.511.710 COP

e) Que de acuerdo con el cronograma establecido en el pliego de Condiciones y la Resolución de Apertura el Comité Evaluador presentó su informe de evaluación. **f)** Que el día 14 de agosto de 2026, la Entidad publicó el primer informe de evaluaciones. **g)** Que el día 31 de agosto de 2026, la Entidad publicó el segundo informe de evaluaciones. **h)** Que durante el término del traslado de los informes de evaluaciones no se presentaron observaciones a los mismos. **i)** Que el día 27 de agosto de 2026 se reunió el comité de adquisiciones, se instaló la Audiencia de Adjudicación del proceso, tal como consta en Acta 297 MDN-COGFM-JEMCO-ESDEG-SBESG-VIADM-DEADM-SESCO de la misma fecha. **j)** Que la Adjudicación fue ordenada en la Resolución No. 113 de 31 de agosto de 2026, mediante la cual se adjudicó el proceso de Menor Cuantía **No. 126-MDN-COGFM-ESDEG-2026, CUYO OBJETO ES "RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIANALIZER 200F Y ACTUALIZACIÓN DEL EDR CON XDR (EXTENDED DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO",** por la suma de CUATROCIENTOS VEINTE CINCO MILLONES CIEN MIL PESOS M/CTE ($425.100.000,00,00) IVA incluido para cada uno de los ítems incluye impuestos, tasas, contribuciones (si aplica) y otros conceptos que genere la ejecución del futuro contrato a la firma HEIMCORE SAS, con NIT. 900.425.697-2, representada legalmente por el suplente de la empresa señor JESUS ALBERTO FRANCO ACOSTA C.E. No. 582410, teniendo en cuenta que cumple con las mismas obligaciones del representante, legal principal y teniendo en cuenta certificación de ausencia temporal acreditada dentro del proceso del proceso. O) Que EL CONTRATISTA ha manifestado bajo la gravedad de juramento no encontrarse dentro de las causales de inhabilidad e incompatibilidad consagradas en la Constitución y la ley. **p)** Que habiéndose dado cumplimiento a todos los trámites y requisitos legales que exige la Contratación Administrativa, es procedente la celebración del presente contrato, el cual se regirá por las siguientes:

CLÁUSULAS CONTRACTUALES

CLÁUSULA PRIMERA. - OBJETO: **"RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIANALIZER 200F Y ACTUALIZACIÓN DEL EDR CON XDR (EXTENDED DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"**

CLÁUSULA SEGUNDA. – VALOR DEL CONTRATO: Para efectos legales, fiscales y presupuestales, el valor total del presente contrato asciende a la suma de CUATROCIENTOS VEINTE CINCO MILLONES CIEN MIL PESOS M/CTE ($425.100.000,00,00) IVA incluido para cada uno de los ítems incluye impuestos, tasas, contribuciones (si aplica) y otros conceptos que genere la ejecución del futuro contrato, para cada uno de los ítems, incluye impuestos, tasas, contribuciones (si aplica) y otros conceptos que genere la ejecución de presente contrato, discriminados en las cantidades y valores, discriminados de la siguiente forma:

Scanned with CamScanner

No.	Código UNSPSC	Descripción	Cantidad	Unidad	PRECIO DE REFERENCIA	PRECIO OFERTADO	PRECIO TOTAL
1	43222502	Firewall 600E; De acuerdo con las especificaciones tecnicas del anexo.	2,00	UN	85.448.517,50	72.448.517,50	144.897.035,00
2	43222502	FortiAnalyzer 300G; De acuerdo con las especificaciones tecnicas del anexo.	1,00	UN	69.448.750,00	55.202.965,00	55.202.965,00
3	43231500	Renovación de licenciamiento para la solución de seguridad de usuario final bajo la arquitectura de Detección y Respuesta de Puntos Finales (EDR) y Detección y respuesta extendidas (XDR) de acuerdo con las especificaciones técnicas) de acuerdo con las especificaciones técnicas.	500,00	UN	464.000,00	450.000,00	225.000.000,00
TOTAL							425.100.000,00

Notal: Se encuentra excluido del IVA De acuerdo con lo indicado en el Estatuto Tributario Art. 476 - EXCLUIDO DE IVA Numeral 21 (suministro de paginas WED, servidores (hosting) computación en la nube (cloud computing) y Art. 477 ET- Literal n equipos de software y demás implementos de sistemas y comunicaciones para el uso de la fuerzas militares y la policía Nacional

AFECTACIÓN PRESUPUESTAL:

RUBRO PRESUPUESTAL	PRESUPUESTO ASIGNADO	PRESUPUESTO A ADJUDICAR	SOBRANTES NO COMPROMETIDO
A-02-02-01-004-007 – EQUIPOS Y APARATOS DE RADIO TELEVISIÓN Y COMUNICACIONES	$ 520.720.000.00	$425.100.000,00,00	$ 95.620.000.00
TOTAL	$ 520.720.000.00	$425.100.000,00,00	$ 95.620.000.00

CLÁUSULA CUARTA. - FORMA Y CONDICIONES DE PAGO: El valor total del contrato se cancelará en un ÚNICO PAGO correspondiente al cumplimiento de la totalidad del objeto del presente proceso y la entrega de los bienes instalados, configurados y puestos en funcionamiento, dentro de los sesenta (60) días calendario siguientes al acta de recibo a satisfacción suscrita por el supervisor del contrato y el contratista o su delegado y presentación de la respectiva factura, entrada al almacén (cuando aplique); previa disponibilidad de PAC (disponibilidad de recursos); y cumplimiento de los demás trámites administrativos a que haya lugar, 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”.

Si la factura no ha sido correctamente elaborada, no cumple con las normas aplicables o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de interés o compensación de naturaleza alguna.

Scanned with CamScanner

Las PERSONAS JURÍDICAS al momento de presentar la factura deben acreditar el pago de los Aportes Parafiscales (si están obligados a ello), el de Seguridad Social Integral (salud y pensión) de conformidad con lo preceptuado en el artículo 23 de la Ley 1150 de 2007 modificatorio del inciso 2 y Parágrafo 1 del artículo 41 de la Ley 80 de 1993 y riesgos laborales de los empleados a cargo, en los términos y porcentajes establecidos en la Ley (artículo 2 de la Ley 1562 de 2012), mediante certificación expedida y soportada (planillas de pago) por el Revisor Fiscal cuando este exista de acuerdo con los requerimientos de Ley o en su defecto por el Representante Legal.

Las PERSONAS NATURALES, al momento de presentar la factura deberán acreditar el pago de los Aportes Parafiscales mediante certificación suscrita por el contratista, soportada con la copia de la planilla de pago de aportes a salud, pensión y riesgos laborales como trabajador independiente, con el respectivo comprobante de pago. El ingreso base de cotización debe ser sobre el 40% del valor mensualizado de sus ingresos, sin incluir el valor total del Impuesto al Valor Agregado (IVA), conforme a lo establecido en el Artículo 244 de la Ley 1955 del 25 de mayo de 2019.

PARAGRAFO 1: El contratista deberá tener en cuenta que 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 y la Resolución 042 del 05 de mayo 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 Proveedor o Contratista (Emisor FE, ND, NC) registrar en la factura, según sea el caso, los siguientes datos en los campos solicitados:

I. 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: #$15-01-02-001; Contrato No XXX;facturacionelectronica@esdegue.edu.co#$,

II. Si el proveedor o contratista al elaborar y emitir la factura electrónica (FE), nota debito (ND), nota crédito (NC) 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: 15-01-02-001; Contrato No XXX; facturacionelectronica@esdegue.edu.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.

NOTA 1: La certificación suscrita por (revisor fiscal o representante legal) el contratista (persona natural o jurídica) deberá contener como mínimo la siguiente información: Si cuenta o no con personal a cargo y que el personal que prestó el servicio se encuentra al día con los aportes al sistema de seguridad social.

NOTA 2: La facturación debe ser presentada redondeando todos los valores a dos (2) decimales.

NOTA 3: El contratista deberá elaborar y emitir nota debito (ND) o nota crédito (NC) mediante el operador tecnológico autorizado, solución gratuita de la DIAN o software propio, teniendo en cuenta la parametrización del software utilizado.

PARÁGRAFO 1.- Los pagos se efectuarán mediante consignación a la empresa HEIMCORE S.A.S identificado(a) con NIT. 900425697-2, en la CUENTA CORRIENTE No. 009384553 del BANCO DE BOGOTÁ o en otro banco o

Scanned with CamScanner

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.

CLÁUSULA QUINTA. - SUJECIÓN DE LOS PAGOS A LAS APROPIACIONES PRESUPUESTALES: El Gobierno Nacional mediante Decreto No. 1477 del 30 de diciembre de 2025 *"Por el cual se liquida el Presupuesto General de la Nación para la vigencia fiscal de 2026, se detallan las apropiaciones y se clasifican y definen los gastos"* liquidó el Presupuesto General de la Nación para la vigencia fiscal de 2026.

RUBRO	DESCRIPCIÓN	REC	PRESUPUESTO ASIGNADO
A-02-02-01-004-007	EQUIPOS Y APARATOS DE RADIO, TELEVISION Y COMUNICACIONES	10 CSF	520.720.000,00

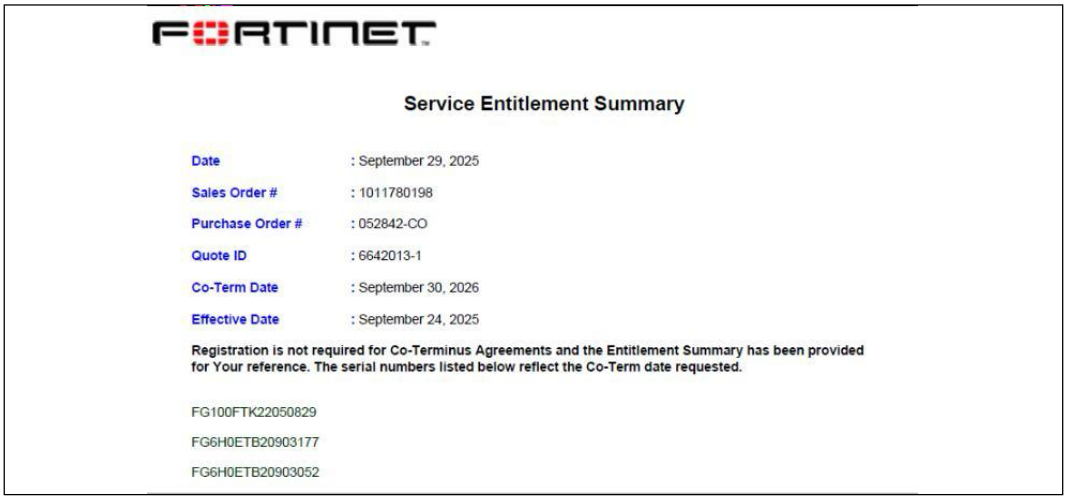
El valor total del Certificado de Disponibilidad Presupuestal es por la suma de **QUINIENTOS VEINTE MILLONES SETECIENTOS VEINTE MIL PESOS M/CTE ($520.720.000,00)**, así mismo se cuenta con Certificado Plan Adquisición, bienes y/o Servicios de Planeación Estratégica y Certificado de Disponibilidad Presupuestal No. 15826 del 04 de junio de 2026.

CLÁUSULA SEXTA. - PLAZO DE EJECUCIÓN: De conformidad con la necesidad planteada y avalada con la suscripción del presente, el plazo de ejecución será a partir del día hábil siguiente al perfeccionamiento del contrato y el cumplimiento de los requisitos de ejecución (aprobación de la póliza de cumplimiento), hasta el 30 de noviembre de 2026.

Las licencias deberán ser renovadas una vez finalice la vigencia actual de cada licencia, así:

No. CONTRATO	OBJETO	FINALIZACIÓN LICENCIMIENTO ACTUAL
CONTRATO DE PRESTACION DE SERVICIOS No. 173-MDN-COGFM-ESDEG-2025	CONTRATAR LA RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIGATE 100F, FORTIANALYZER 300G, FORTISWITCH 148E POE, ACCES POINT FORTIAP 320C Y EDR (ENDPOINT DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" (FORTIGATE 600E, FORTIGATE 100F, FORTIANALYZER 300G)	30 de septiembre de 2026
CONTRATO DE PRESTACION DE SERVICIOS No. 173-MDN-COGFM-ESDEG-2025	CONTRATAR LA RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO DE LA PLATAFORMA DE ASEGURAMIENTO TECNOLÓGICO COMPUESTA POR LOS EQUIPOS DE SEGURIDAD PERIMETRAL Y CONECTIVIDAD FORTIGATE 600E, FORTIGATE 100F, FORTIANALYZER 300G, FORTISWITCH 148E POE, ACCES POINT FORTIAP 320C Y EDR (ENDPOINT DETECTION AND RESPONSE), PARA LA ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" (EDR (ENDPOINT DETECTION AND RESPONSE)	30 de septiembre de 2026
Lo anterior conforme se puede verificar en el siguiente certificado:		

Scanned with CamScanner



FORTINET

Service Entitlement Summary

Date	: September 29, 2025
Sales Order #	: 1011780198
Purchase Order #	: 052842-CO
Quote ID	: 6642013-1
Co-Term Date	: September 30, 2026
Effective Date	: September 24, 2025

Registration is not required for Co-Terminus Agreements and the Entitlement Summary has been provided for Your reference. The serial numbers listed below reflect the Co-Term date requested.

FG100FTK22050829

FG6H0ETB20903177

FG6H0ETB20903052

Cabe resaltar que las licencias tienen una vigencia en la prestación del servicio de doce (12) meses contados a partir de su actualización.

Se permite aclarar que para los trámites administrativos y de pagos el plazo de ejecución será hasta el 30 de noviembre de 2026.

NOTA 01: Una vez se cumplan los requisitos del art. 41 de la ley 80 de 1993, el supervisor del contrato deberá elaborar acta de inicio la cual deberá contener los datos indicados en las especificaciones técnicas adicionales del presente documento. La omisión en la inclusión de algún dato no eximirá la responsabilidad de las funciones que son inherentes al supervisor del contrato de realizar el seguimiento del contrato.

CLÁUSULA SÉPTIMA. - PLAZO DE DURACIÓN: La vigencia del presente contrato será igual al plazo de ejecución del contrato y seis (6) meses más para efectos de su liquidación bilateral. Si el objeto del contrato está cubierto con garantía técnica que implique a su vez la prestación de servicios de forma posterior al vencimiento del plazo de ejecución del contrato, en el acta de terminación o de liquidación de común acuerdo del contrato o en el acto de liquidación unilateral se dejará constancia de esta circunstancia. Los amparos de la garantía única que se constituyan relacionados con las obligaciones a cargo del CONTRATISTA, que quedan pendientes a la fecha de suscripción del acta de liquidación, deberán estar vigentes hasta la satisfacción total de las mismas.

CLÁUSULA OCTAVA. - LUGAR DE PRESTACIÓN DEL SERVICIO: El lugar de entrega de los servicios objeto del presente proceso será: El servicio de licenciamiento será instalado y registrado en la plataforma tecnológica de aseguramiento de la Escuela Superior de Guerra, para lo cual el proponente podrá realizar esta actividad de manera remota; para efectos de soporte presencial, este se realizará en las instalaciones de la ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” en la Carrera 11 No. 102 – 50 de la ciudad de Bogotá D.C.

NOTA:

Las licencias serán actualizadas en el portal de Fortinet para el ITEM 1
Las licencias serán actualizadas en el portal de la herramienta adquirida para el ITEM 2

CLÁUSULA NOVENA. - OBLIGACIONES DEL CONTRATISTA: El contratista se obliga con el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES- ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” entre otras: **a) OBLIGACIONES GENERALES** El contratista se obliga con el Ministerio de Defensa Nacional-COGFM-ESDEG a: 1)Mantener la debida reserva frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del contrato, de conformidad con el compromiso de confidencialidad presentado junto con la oferta y que hace parte integral del contrato. 2) Informar oportunamente al supervisor del contrato, sobre la imposibilidad o dificultades que se presenten en la ejecución de este y ofrecer alternativas para

Scanned with CamScanner

garantizar su correcta ejecución. 3)Mantener los precios presentados junto con la oferta durante el plazo de ejecución del contrato. 4)Atender los requerimientos efectuados directamente por el contratante o por conducto del supervisor. 5)Proveer a su costo todos los bienes y/o servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el presente contrato. 6)Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones que le corresponden en los términos del presente contrato. 7)Asistir a las reuniones programadas por el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES- ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO". 8)Suscribir las modificaciones acordadas entre las partes, para efectos de garantizar la ejecución y el cumplimiento idóneo y oportuno del objeto contratado, dentro de los cinco (5) días siguientes al requerimiento por parte de la Escuela Superior de Guerra "General Rafael Reyes Prieto". 9)Constituir la garantía única dentro del plazo establecido en el cronograma del proceso y/o en la comunicación de aceptación de oferta/contrato. 10)Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad. Por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno del CONTRATISTA con el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES- ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO". 11)Obrar con lealtad y buena fe en la ejecución contractual evitando dilaciones y entrabamientos que afecten el debido desarrollo, responder por sus actuaciones y omisiones derivadas de la celebración del presente contrato y en general se obliga a cumplir con lo establecido en las leyes 80 de 1993, 1150 de 2007, 1474 de 2011, sus Decretos Reglamentarios y demás normatividad aplicable. 12)Mantener actualizado su domicilio durante la vigencia del contrato y seis (6) meses más y presentarse al MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES- ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" en el momento en que sea requerido por el mismo para la suscripción de la correspondiente acta de liquidación. 13)Guardar confidencialidad y reserva sobre la información y documentos que por razón de este contrato llegue a conocer. 14)Realizar el servicio objeto del presente contrato al Comando General de las Fuerzas Militares - Escuela Superior de Guerra "General Rafael Reyes Prieto", de conformidad con las especificaciones Técnicas contratadas y dentro del plazo establecido para la ejecución. 15)Rendir los informes relacionados con las actividades desarrolladas en relación con el objeto contratado, que le sean solicitados por el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES- ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO", a través del supervisor del contrato, cuando a ello hubiere lugar.16)Presentar oportunamente la factura correspondiente adjuntando el certificado de cumplimiento de Aportes Parafiscales (si está obligado a ello), el de Seguridad Social Integral (salud y pensión) de conformidad con lo preceptuado en el artículo 23 de la Ley 1150 de 2007 modificatorio del inciso 2 y Parágrafo 1 del artículo 41 de la Ley 80 de 1993 y riesgos laborales de los empleados destinados para la ejecución del contrato, en los términos y porcentajes establecidos en la ley (artículo 2 de la Ley 1562 de 2012).17)Contratar al personal necesario para la perfecta ejecución del contrato. 18)Cumplir con la garantía técnica y el término de respuesta a la garantía técnica. **b) OBLIGACIONES ESPECÍFICAS**: **1.** 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

Scanned with CamScanner

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.

CLÁUSULA DÉCIMA. -OBLIGACIONES DE LA ENTIDAD: 1. Pagar al Contratista los compromisos adquiridos en la forma pactada con sujeción a las disponibilidades presupuestales previstas para el efecto. 2. Recibir a satisfacción los servicios, cuando este cumpla con las condiciones establecidas en el presente contrato. 3. Verificar que el contratista realice el pago de aportes al sistema de seguridad social integral, parafiscales, ICBF, SENA y cajas de compensación familiar (cuando a ello haya lugar), en las condiciones establecidas por la normativa legal vigente. 4. Verificar a través del supervisor del contrato, que el contratista realice el cargue oportuno en la plataforma SECOP II, de toda la documentación relacionada en el numeral FORMA Y CONDICIONES DE PAGO durante la ejecución del contrato.

CLÁUSULA DÉCIMA PRIMERA.- GARANTÍA: El artículo 7 de la Ley 1150 de 2007, señala que los contratistas prestarán garantía única para el cumplimiento de las obligaciones surgidas del contrato. Los proponentes prestarán garantía de seriedad en los ofrecimientos hechos. De conformidad con el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015 las garantías que los proponentes o contratista pueden otorgar son: contrato de seguro contenido en una póliza, patrimonio autónomo y garantía bancaria. Las garantías deberán cubrir los riesgos establecidos en los Art. 2.2.1.2.3.1.7 del Decreto 1082 del 2015, de acuerdo con el objeto del proceso. Las suficiencias de las garantías se aplicarán conforme lo estipulado en los Artículos 2.2.1.2.3.1.10 hasta el 2.2.1.2.3.1.16 del Decreto 1082 de 2015, en lo que respecta a cada amparo solicitado.

Conforme lo anterior EL MINISTERIO DE DEFENSA- COMANDO GENERAL FUERZAS MILITARES - ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”- DEPARTAMENTO ADMINISTRATIVO, teniendo en cuenta el objeto contractual, para el presente proceso se establecerán los siguientes tipos de riesgos:

AMPARO	COBERTURA Y VIGENCIA
CUMPLIMIENTO DEL CONTRATO	EQUIVALENTE AL VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO, CUYA VIGENCIA SERÁ IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y UN (1) AÑO MÁS MÁS Y DE LAS PRÓRROGAS SI LAS HUBIERE, CONTADOS A PARTIR DE LA FECHA DEL PERFECCIONAMIENTO.
CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES	EQUIVALENTE AL VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO, CUYA VIGENCIA SERÁ IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y UN (1) AÑO MÁS Y DE LAS PRÓRROGAS SI LAS HUBIERE. PARA EFECTOS DE LA VIGENCIA DE LAS GARANTÍAS, ESTA IRÁ DESDE EL PERFECCIONAMIENTO DEL CONTRATO.
CALIDAD DEL SERVICIO	EQUIVALENTE AL VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO, CUYA VIGENCIA SERÁ IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y SEIS (6) MESES MÁS Y DE LAS PRÓRROGAS SI LAS HUBIERE. PARA EFECTOS DE LA VIGENCIA DE LAS GARANTÍAS, ESTA IRÁ DESDE EL PERFECCIONAMIENTO DEL CONTRATO.
PAGO SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES INDEMNIZACIONES LABORALES.	EQUIVALENTE AL CINCO POR CIENTO (5%) DEL VALOR TOTAL DEL CONTRATO, CUYA VIGENCIA SERÁ IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y TRES (3) AÑOS MÁS, CONTADOS A PARTIR DE LA FECHA DEL PERFECCIONAMIENTO DEL CONTRATO.

Beneficiario: MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO NIT. 830.002.634-1.

EL CONTRATISTA deberá cumplir con todos los requisitos para mantener vigente la garantía o seguros a que se refiere esta cláusula. Estará a cargo del CONTRATISTA el pago de la prima y demás erogaciones de constitución y mantenimiento de la garantía mencionada. Sin embargo, EL CONTRATISTA autoriza a la Entidad para que con cargo a las sumas que éste le adeude, se descuente el valor de la prima del seguro cuando por cualquier circunstancia EL CONTRATISTA no las constituyere.

Scanned with CamScanner

De conformidad con el artículo 2.2.1.2.3.1.18 del Decreto 1082 de 2015, en caso de que el presente contrato sea modificado para incrementar su valor o prorrogar el plazo, EL CONTRATISTA se obliga a ampliar el valor de la garantía otorgada o ampliar su vigencia, según el caso, so pena de tipificar un incumplimiento a las obligaciones del contrato.

Una vez perfeccionado el contrato, dentro de los tres (3) días hábiles siguientes a la firma del mismo, el contratista para la ejecución del contrato deberá constituir garantía única que avalará el cumplimiento de las obligaciones surgidas del presente contrato, para lo cual constituirá un mecanismo de cobertura de riesgo expedido por una entidad legalmente autorizada para funcionar en Colombia a favor del MINISTERIO DE DEFENSA- COMANDO GENERAL FUERZAS MILITARES - ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”- DEPARTAMENTO ADMINISTRATIVO.

Las vigencias de los amparos de la garantía única iniciarán con la fecha de la firma del comunicado de aceptación de la oferta. El hecho de la constitución de estos amparos no exonera al CONTRATISTA de las responsabilidades legales en relación con los riesgos asegurados. Dentro de los términos estipulados en el contrato, ninguno de los amparos otorgados podrá ser cancelado o modificado sin la autorización expresa del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”- DEPARTAMENTO ADMINISTRATIVO.

EL CONTRATISTA deberá mantener vigente las garantías, amparos y pólizas a que se refiere esta cláusula y serán de su cargo el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan.

Si el CONTRATISTA no modifica las garantías, éstas podrán variarse por la aseguradora o banco a petición del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZASMILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” y a cuenta del CONTRATISTA quien por la firma del contrato que se le adjudique autoriza expresamente al MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZASMILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” - DEPARTAMENTO ADMINISTRATIVO para retener y descontar los valores respectivos de los saldos que hubiere a su favor, sin que por ello se entienda que el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” , asume la responsabilidad de la ampliación de los amparos y pago de las primas, los cuales son responsabilidad del contratista.

En la Garantía debe quedar expresamente consignado que se ampara el cumplimiento del contrato, el pago de las multas y de la penal pecuniaria convenidas. Así mismo deberá constar que la aseguradora renuncia al beneficio de excusión.

Estos mecanismos de cobertura son requeridos por el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” – DEPARTAMENTO ADMINISTRATIVO, teniendo en cuenta que el objeto de las mismas, sirven para respaldar el cumplimiento de todas y cada una de las obligaciones que surgen a cargo del contratista frente a la administración y /o terceros, por razón de la celebración, ejecución y liquidación del contrato.

NOTA 1: el artículo 2.2.1.2.3.1.4 dispone Garantía del oferente plural. Cuando la oferta es presentada por un proponente plural, como unión temporal, consorcio o promesa de sociedad futura, la garantía debe ser otorgada por todos sus integrantes.

NOTA 2: En el caso que se constituya una garantía bancaria, para respaldar el contrato como garantía única, se deberá aportar correo electrónico institucional del banco emisor en el que se pueda constatar la siguiente información: beneficiario, valor, fecha de expedición, vigencia. En caso de que el banco no suministre la información de los datos o la suministre de forma parcial, la ESDEG, dará inicio al correspondiente debido proceso.

NOTA 3: Para el caso de garantías bancarias, contratos de seguro de cumplimiento (Pólizas de seguros)

Scanned with CamScanner

y los patrimonios autónomos otorgados como garantías, estas deberán permitir la verificación en línea o por Internet, con el propósito de verificar la validez, idoneidad y suficiencia de los documentos, y/o un punto de contacto telefónico o virtual (en idioma castellano) para solicitar cualquier requerimiento orientado a absolver las consultas que sobre el particular sean pertinentes. Lo anterior por disposición de la Circular conjunta No. 001 del 20 de agosto de 2021, sobre los mecanismos para fortalecer la debida diligencia de los beneficiarios de pólizas de seguros, garantías y avales bancarios y patrimonios autónomos.

NOTA 4: Dando aplicación del artículo 2.2.1.2.3.4.1. del Decreto 1082 de 2015, en el caso de garantía bancaria, y las cartas de crédito STAND BY, solo se aceptarán siempre y cuando la garantía conste en documento expedido por una entidad financiera autorizada por la Superintendencia Financiera o quien haga sus veces otorgado de acuerdo con las normas del Estatuto Orgánico del Sistema Financiero. En el documento debe constar expresamente que:

1. La garantía será efectiva a primer requerimiento o primera demanda de la Entidad Estatal.
2. La garantía bancaria será irrevocable
3. Se indique la suficiencia (amparos y vigencia establecidos)
4. Que se renuncia al beneficio de excusión
5. Que “la garantía será pagada por el garante dentro de los treinta (30) días siguientes a la fecha del acto administrativo que declare el incumplimiento del oferente”
6. Indicar la dirección electrónica para notificaciones

CLÁUSULA DÉCIMA SEGUNDA. – 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 la República 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-Comando General Fuerzas Militares – Escuela Superior de Guerra “General Rafael Reyes Prieto”.

CLÁUSULA DÉCIMA TERCERA. – SUPERVISIÓN: La supervisión del presente contrato estará a cargo del TE ENRIQUE RAMIREZ FLOR, OFICIAL GESTION GOBIERNO DETIC de la Escuela Superior de Guerra “General Rafael Reyes Prieto”, o quien haga sus veces, cuyo correo electrónico es enrique.ramirez@esdeg.edu.co quien deberá velar por los intereses del CONTRATANTE y en especial tendrá las siguientes: FUNCIONES GENERALES. FUNCIONES GENERALES. 1. La revisión de los antecedentes del contrato suscrito, de los derechos y obligaciones de las partes y de los mecanismos pactados para el reconocimiento de los derechos de contenido económico. 2. La intervención formal en la coordinación, vigilancia y control de la ejecución del objeto contratado, para garantizar que las obligaciones contractuales se han cumplido y que permita a la entidad tramitar los pagos al contratista. 3. La presentación periódica de informes sobre la ejecución del contrato, cuando suceda algo que amerite ser informado (pagos, entregas, demoras, etc.), en especial, el informe anexo al acta de recibo parcial y/o final que sustente el pago de las obligaciones cumplidas por el contratista. La presentación de informes deberá ser con cada pago. 4. La elaboración y envió del proyecto de Acta de Liquidación de los contratos acompañada de sus documentos soporte, dejando constancia sobre los acuerdos, conciliaciones y transacciones a que llegaren las partes en caso de divergencias presentadas. 5. En caso de no lograrse la liquidación el contrato o convenio en la oportunidad legal establecida y por ende perderse la competencia legal para llevar a cabo la liquidación, el Supervisor será responsable por el Cierre del Expediente Contractual, a través de un Acta, para efectos de establecer dentro de la entidad estatal el estado final del contrato celebrado. 6. Así mismo, conforme al Artículo 2.2.1.1.2.4.3. del Decreto 1082 de 2015, Obligaciones posteriores a la liquidación, y una vez “Vencidos los términos de las garantías de calidad, estabilidad y mantenimiento, o las condiciones de disposición final o recuperación ambiental de las obras o bienes”, el Supervisor del Contrato o Convenio será responsable del cierre del expediente del Proceso de Contratación, a través del Acta respectiva. 7. En los contratos en que se realicen mantenimiento, renovaciones y mejoras a los bienes, se debe determinar por el supervisor si los trabajos realizados al bien generan un mayor valor del mismo, toda vez que amplíen su vida productiva, su utilidad y su eficiencia operativa. El Supervisor deberá en el Acta de Liquidación expresar

Scanned with CamScanner

técnicamente si hubo un aumento del valor del bien, toda vez que ese mayor valor deberá reflejarse por la entidad en su balance contable. 8. La información del proceso podrá consultarse en la Dirección de Contratación Estatal o quien haga sus veces, o en el Sistema Electrónico de Contratación Pública SECOP I o II, según corresponda. 9. El supervisor del contrato vigilará su ejecución y cumplimiento del objeto durante todo el tiempo que esté vigente y su función termina cuando se suscriba el acta de liquidación. 10 Salvo instrucción en contrario que emane de la Dirección de Contratación Estatal del Ministerio de Defensa Nacional o quien haga sus veces en la respectiva Unidad Ejecutora o Dependencia Delegataria, los Supervisores de los contratos o convenios adelantados transaccionalmente a través de la plataforma SECOP II deberán realizar el cargue de sus informes de supervisión en dicha plataforma, junto con los demás trámites contractuales, siendo responsables por la calidad y oportunidad en el cargue y/o reporte de la información o trámites que correspondan en ejecución de los contratos. 11. Cuando el supervisor del contrato manifieste su desacuerdo con la ejecución de un contrato o con la forma de los actos, documentos o circunstancias examinadas, formulará sus reparos por escrito. 12. Los reparos serán motivados en hechos, circunstancias y normas y abarcarán las observaciones y objeciones correspondientes. 13. El supervisor comunicará al competente contractual, a la dependencia interesada en el contrato y/o a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o Dependencia Delegataria, los resultados más relevantes de su actuación y recomendará las actuaciones para su normal ejecución. 14. El supervisor podrá solicitar al competente contractual la revisión de los actos que considere perjudiciales para los intereses de la Nación – Ministerio de Defensa Nacional. 15. Cuando se aprecien graves irregularidades en la ejecución de un contrato que amenace su paralización, es obligación del supervisor informar por escrito dentro de los cinco (5) días hábiles siguientes a la ocurrencia de los hechos al competente contractual y al Director de la dependencia que ha contratado el bien o servicio, para que estos inicien las acciones correspondientes. 16. Los supervisores de los contratos suscritos por Ministerio de Defensa Nacional – Unidad Ejecutora y Dependencias Delegatarias están obligados a acatar las observaciones y decisiones del competente contractual, en los eventos de discrepancias en su ejecución y no están autorizados a expedir cumplidos para pagar obligaciones, hasta tanto no se pronuncie favorablemente el competente contractual. 17. Los supervisores de los contratos suscritos por el Ministerio de Defensa Nacional – Unidades Ejecutoras y Dependencias Delegatarias, están obligados a entregar debidamente liquidadas todas las cuentas contractuales con sus respectivos soportes, utilizando el formato implementado por la Dirección de Contratación Estatal del Ministerio de Defensa Nacional. En este momento quedará documentalmente acreditado el cumplimiento de todos los requisitos necesarios para cumplir la obligación a cargo del Ministerio y del cumplimiento de las obligaciones del contratista. 18. Dar a conocer al CONTRATISTA la Política de Antisoborno implementada por el Ministerio de Defensa Nacional y los distintos canales dispuestos por el Ministerio -Unidad Ejecutora o Dependencia Delegataria para denunciar cualquier acto de soborno o de corrupción. **PARÁGRAFO PRIMERO: En el aspecto Técnico – Administrativo:** 1. Verificar que las especificaciones y condiciones particulares de los bienes o servicios contratados, correspondan a las solicitadas, definidas y aceptadas en el contrato. De presentarse dudas sobre este particular se formularán por escrito dentro de los tres (3) días hábiles siguientes a su ocurrencia, a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o Dependencia Delegataria. La Dirección de Contratación del MDN, o quien haga sus veces, responderá este requerimiento dentro de los tres (3) días hábiles siguientes a su recibo clarificando la situación. 2. En los eventos que así lo determine el contrato o si la naturaleza del mismo lo requiere, el supervisor suscribirá conjuntamente con el contratista las actas de iniciación o de recibo de bienes y/o servicios, dentro del término establecido en el contrato. Copia de estas actas se enviarán dentro de los cinco (5) días hábiles siguientes a su firma, a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o Dependencia Delegataria para su publicación en la plataforma SECOP II o su incorporación en la carpeta del contrato, según corresponda. 3. Cuando se requieran cronogramas o programación de actividades al contratista para ejecutar el objeto contratado, el supervisor los exigirá y recibirá para su revisión y control, dentro de los plazos estipulados en el contrato. Copia de estos cronogramas se remitirán dentro de los tres (3) días hábiles siguientes a su recibo, a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia para su publicación en la plataforma SECOP II o su incorporación en la carpeta del contrato, según corresponda. 4. Cuando se trate de la supervisión o interventoría de contratos de obras, las personas naturales o jurídicas o los funcionarios designados para este efecto, abrirán y llevarán conjuntamente con el contratista, o la persona delegada por éste, una memoria diaria de la obra, en donde constarán las acciones realizadas diariamente en ella, así como las actas de los comités técnicos de obra o administrativos que periódicamente deban

Scanned with CamScanner

realizarse y las observaciones que se consideren pertinentes. Este documento formará parte integral del contrato y la copia mensual del documento se remitirá al área de contratos del Ministerio o quien haga sus veces en la Unidad Ejecutora para que repose en la carpeta del contrato. Los mismos serán publicados en la plataforma SECOP II, siempre y cuando el contrato no esté amparado por alguna causal de reserva de información. 5. El supervisor podrá citar o convocar a reuniones al contratista, al competente contractual, a quienes tengan interés directo en la ejecución del contrato, a quienes participaron en la elaboración del pliego o solicitud de oferta y en la elaboración de la minuta del contrato, cuando tenga dudas sobre los términos del contrato y/o se considere necesario para su normal ejecución. 6. De estas reuniones levantará un acta suscrita por los que en ella intervinieron y la misma contendrá como mínimo los asuntos discutidos, las decisiones, acciones y compromisos a ejecutar. Copia de ella se enviará a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia, dentro de los tres (3) días hábiles siguientes a su suscripción, para su correspondiente archivo o publicación en SECOP II según corresponda. 7. Los supervisores de los contratos, si la naturaleza del mismo lo requiere y así se ha estipulado en la minuta del contrato, elaborarán actas de recibo parcial de bienes o servicios, las cuales suscribirá conjuntamente con el contratista. El valor de los bienes o servicios que por estas actas se recibe no será inferior al porcentaje estipulado en el contrato. Copia de estas actas se remitirá al área de contratos del Ministerio o quien haga sus veces en la Unidad Ejecutora para lo de su competencia. 8. El supervisor exigirá la buena calidad y correcto funcionamiento de los bienes y servicios contratados y se abstendrá de dar el respectivo cumplido si éstos no corresponden a las calidades, cantidades y especificaciones técnicas exigidas. El supervisor mantendrá el control y coordinación permanente sobre la ejecución del contrato, de tal manera que implemente actividades, tales como, reuniones con el comité evaluador y contratista, visitas que sean pertinentes a las empresas y las que se estimen necesarias. 9. El supervisor verificará que el contratista entregue los bienes y/o servicios que ofertó. En el evento que, por concepto técnico, algunos de los bienes y/o servicios no sean acordes con el contrato y la oferta, éste exigirá al contratista su modificación en el menor tiempo posible, o en el indicado en el contrato. En este evento se procederá así: a) Si el bien y/o servicio es entregado por el contratista con algún defecto menor, el supervisor podrá devolverlo para que aquel corrija o subsane los defectos, en un término que el supervisor considere perentorio sin afectar el plan logístico de la Fuerza. b) Si el bien entregado presenta un defecto que no afecte su funcionalidad, o que disminuya su durabilidad, pero que no sea susceptible de corrección, el supervisor los recibirá y autorizará su distribución, conservando las muestras defectuosas del total de muestras evaluadas según el plan de muestreo previsto en la norma técnica o especificación técnica o dejando cinco (5) muestras de los bienes recibidos, recolectadas al azar las cuales serán marcadas y etiquetadas de manera que se identifiquen suficientemente, para practicar sobre las mismas las pruebas que el comité técnico del material considere procedentes e iniciar las acciones legales a que haya lugar. c) Si el bien entregado presenta defectos mayores será rechazado por el supervisor, conservando las muestras defectuosas del total de muestras evaluadas según el plan de muestreo previsto en la norma técnica o especificación técnica, dejando cinco (5) muestras de los bienes recibidos, recolectadas al azar las cuales serán marcadas y etiquetadas de manera que se identifiquen suficientemente para efectos de practicar sobre las mismas las pruebas que el comité técnico del material considere procedentes y determinar las acciones legales a que haya lugar. d) Para todos los eventos, el supervisor se apoyará en los conceptos emitidos por los comités del bien (técnico), quienes se pronunciarán sobre sus defectos indicando si son mayores o menores, o si afectan su durabilidad, funcionalidad, o el aspecto que resulte pertinente. 10. El supervisor verificará conforme con la naturaleza jurídica y tipo del contrato suscrito, que el contratista tenga previstos todos los medios y recursos para mantener la seguridad e integridad de las personas que laboran en el Ministerio. 11. El supervisor exigirá el total cumplimiento de los cronogramas pactados en los contratos y sólo podrá recomendar su modificación cuando por razones técnicas o dada la naturaleza del contrato, esto se haga necesario. Cualquier modificación que afecte el plazo de ejecución del contrato será previamente autorizada por el competente contractual. 12. El supervisor resolverá todas las consultas presentadas por el contratista y hacer las observaciones que estime conveniente. Si durante la ejecución del contrato se presentan dudas o diferencias que no puedan resolverse por el supervisor, éste las remitirá dentro de los tres (3) días hábiles siguientes a su ocurrencia, al competente contractual para su consulta y decisión. 13. El supervisor, si es necesario, puede solicitar por escrito la suspensión temporal de la ejecución de un contrato por circunstancias de fuerza mayor o caso fortuito, justificando las circunstancias de tiempo, modo y lugar que originan tales hechos, ante el competente contractual para que éste emita su autorización. Si el competente contractual aprueba y suscribe la suspensión del contrato, la Dirección de Contratación Estatal o quien haga sus

Scanned with CamScanner

veces en la Unidad Ejecutora o dependencia, elaborará el acta de suspensión, copia de la cual se remitirá supervisor del contrato dentro de los tres (3) días hábiles siguientes a su suscripción, para lo de su competencia. El supervisor para todos los eventos de suspensión de un contrato, al desaparecer los hechos que originaron su suspensión, solicitará su reiniciación, dejando constancia del tiempo total de la suspensión temporal y del vencimiento final del contrato. 14. El Supervisor constatará a la fecha de vencimiento del contrato su total cumplimiento. Si llegare a tener dudas sobre la ejecución del mismo no podrá expedir el acta de recibo final, hasta no clarificar las dudas. 15. Para que el supervisor expida el acta de recibo final del contrato verificará que todas las obligaciones estén cumplidas y procede el pago final. Esta acta contendrá como mínimo la descripción de los bienes y/o servicios recibidos, el valor final del contrato, incluyendo reajustes si proceden. Copia del acta se enviará a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia para su respectivo archivo. En los casos que corresponda, se hará su publicación en SECOP II. 16. Los supervisores de los contratos suscritos por el Ministerio de Defensa Nacional – Unidad Ejecutora o Dependencias Delegataria, al finalizar el contrato y emitir el último cumplido de recibo a satisfacción de los bienes y/o servicios contratados, elaborarán dentro del mes siguiente a su terminación un acta de liquidación final del contrato, acompañada de los documentos soportes siguiendo el formato entregado por la Dirección de Contratación Estatal del Ministerio o quien haga sus veces en las Unidades Ejecutoras o Dependencias Delegatarias. 17. El supervisor elaborará el acta de liquidación la cual deberá comprender la siguiente información: Datos generales sobre el contrato principal, sus adiciones y modificatorios (si los hay), datos sobre los certificados de disponibilidad y registro correspondientes al contrato principal, sus adiciones y modificaciones, se hará referencia a la Garantía - incluyendo la extensión de las mismas si a ello hubiere lugar, Garantía técnica indicada en el contrato (si aplica). Las prestaciones y obligaciones cumplidas por el contratista, relacionando las actas de recibo, número de elementos, cantidades recibidas y entrada al almacén (si aplica), el Cumplimiento de las obligaciones por la Entidad Estatal, esto es el corte de cuentas sobre el estado económico del contrato, adjuntado: Para los contratos suscritos en pesos la(s) obligación(es) y orden(es) de pago(s) debidamente suscritos por el ordenador del gasto y demás documentos que respalden dicho pago. b) Para los contratos suscritos en moneda extranjera la(s) obligación(es) y orden(es) de pago debidamente suscritos por el ordenador del gasto (sin ajuste y con ajuste), el reporte SWIFT y demás documentos que respalden los pagos de divisas. Si el contrato proyecta gastos de nacionalización, deberá anexar copia de las declaraciones de importación debidamente canceladas y copia de la(s) obligación(es) y orden(es) de pago debidamente suscritos por el ordenador del gasto. c) Es pertinente indicar, si el contrato se celebró en moneda extranjera, el balance del acta de liquidación será en pesos colombianos y en la moneda contratada. Lo anterior de conformidad con lo establecido con el inciso 6 del artículo 25 de la Ley 80 de 1993, que señala que las entidades estatales ejecutoras de los presupuestos públicos solo pueden iniciar procedimientos de selección de contratistas si se cuenta con disponibilidad presupuestal, las multas debidas o canceladas (si aplica) y finalmente la verificación del cumplimiento de las obligaciones con el sistema de seguridad social integral, así como el pago de las obligaciones fiscales y parafiscales a cargo del contratista, adjuntando certificación emitida por el revisor fiscal del contratista. (Si aplica). 18. El supervisor remitirá el acta con el lleno de los requisitos enunciados en el numeral anterior dentro del plazo estipulado para la liquidación a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia, para revisión, aceptación y trámite de firmas. o La obligación atrás establecida sólo se entenderá cumplida por el supervisor cuando esté suscrita el acta de liquidación por el contratista y el competente contractual. Si el contratista no acude a suscribirla, la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia, procederá mediante acto administrativo motivado a liquidar unilateralmente el contrato. 19. Si el contratista no está de acuerdo con el contenido del acta de liquidación, se le remitirá nuevamente al supervisor dentro de los tres (3) días hábiles siguientes al recibo de las observaciones o reparos del contratista. En este evento el supervisor no podrá tomarse más de un (1) mes en informar al jefe del área de contratos sobre los resultados del nuevo análisis, para que este realice los trámites que considere pertinentes. **PARÁGRAFO SEGUNDO: En el aspecto Legal:** 1.Cumplir todas y cada una de las cláusulas contractuales. 2. Solicitar a la dependencia de contratos, si las requiere, copia de las garantías constituidas por el contratista y de su aprobación por el Ministerio de Defensa Nacional o quien haga sus veces en la Unidad Ejecutora y de las modificaciones exigidas a éstas durante la ejecución del contrato. Las mismas se pueden consultar igualmente a través de SECOP II. En cumplimiento de esta obligación verificará que las vigencias de las garantías y de sus modificaciones estén dentro de los términos del contrato. 3. Informar por escrito a la dependencia de contratos del Ministerio o quien haga sus veces en la Unidad Ejecutora si el contratista omite alguna o

Scanned with CamScanner

algunas de sus obligaciones, para que la dependencia de contratos decida si procede o no aplicar sanciones y/o declarar la caducidad. La omisión o el retardo injustificado al deber de informar oportunamente los incumplimientos, acarreará para el supervisor acción disciplinaria y las demás que para el efecto concurran. 4. Solicitar al competente contractual, en los eventos contemplados en el contrato y en la Ley, con copia a la Dirección de Contratación Estatal o quien haga sus veces en la Unidad Ejecutora o dependencia, la aplicación de la terminación, modificación e interpretación unilateral, o cuando se pretenda su terminación por mutuo acuerdo. 5. El Supervisor tiene la obligación legal de remitir a la dependencia de contratos del Ministerio, dentro de los términos aquí establecidos, copia de todos los documentos soporte de la supervisión y los conceptos y observaciones de las modificaciones al mismo, para garantizar que se realicen los trámites a que haya lugar en el menor tiempo posible. **PARÁGRAFO TERCERO: Funciones particulares de los Supervisores: Entre otras, se encuentran las siguientes:** 1. Elaborar y suscribir el acta de iniciación del contrato, cuando sea del caso. 2. Suscribir las actas de recibo parcial y final de los bienes y servicio del contrato. 3. Verificar la correcta ejecución del contrato. 4. Exigir el cumplimiento del contrato. 5. Atender y resolver, en coordinación con el Ministerio de Defensa Nacional, todas las consultas sobre omisiones, errores, discrepancias o aclaraciones y complemento en los aspectos técnicas, descritos en las normas técnicas que rigieron el proceso de contratación. 6. Verificar y dejar constancia del cumplimiento de las obligaciones parafiscales de conformidad con el artículo 50 de la Ley 789 de 2002, así como el cumplimiento del sistema de gestión en seguridad y salud en el trabajo, en caso contrario avisará de esta circunstancia al área de contratos del Ministerio o quien haga sus veces en la Unidad Ejecutora y dependencia. 7. Para material de Intendencia: verificar y seguir el cumplimiento de las actividades descritas en el cronograma de entregas, conforme con la reglamentación expedida por la Oficina de Investigación y Normalización del Ministerio de Defensa Nacional. 8. Verificar que las garantías que ampara el cumplimiento del contrato estén vigentes e informar en su oportunidad al Ministerio sobre los inconvenientes presentados. 9. Todas las demás atribuciones contempladas en el contrato. **PARÁGRAFO CUARTO: CAMBIO SUPERVISOR: Cuando el MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" - DEPARTAMENTO ADMINISTRATIVO**, lo requiera o estime conveniente, podrá sustituir el supervisor sin necesidad de suscribir un contrato modificatorio. El cambio de supervisor será comunicado al contratista mediante oficio. El supervisor deberá entregar sus funciones al nuevo supervisor designado, mediante acta suscrita conjuntamente y deberá contener como mínimo la siguiente información: estado de ejecución del contrato, relación de documentos. **PARÁGRAFO SEGUNDO. PROCEDIMIENTO EN CASO DE INCONFORMIDAD DEL SUPERVISOR CON RELACIÓN A LA EJECUCIÓN DEL CONTRATO**. Cuando el supervisor del contrato se encuentre en desacuerdo con la ejecución y desarrollo de las obligaciones pactadas en el contrato, o con la forma de los actos, documentos o circunstancias examinadas, deberá sin excepción llevar a cabo el procedimiento establecido de conformidad con lo dispuesto en el Manual de contratación del Ministerio Defensa Nacional. **CLÁUSULA DÉCIMA CUARTA - LIMITACIONES DEL SUPERVISOR:** El Supervisor no estará facultado, en ningún momento, para adoptar decisiones que impliquen la modificación de los términos y condiciones previstos en el presente contrato, las cuales únicamente podrán ser adoptadas por los representantes legales de las partes, mediante la suscripción de modificaciones al contrato principal. **CLÁUSULA DÉCIMA QUINTA. - 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 de 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 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 a los cuales les sobrevino la causal de fuerza mayor o caso fortuito. **PARÁGRAFO SEGUNDO:** En caso de que se presente el evento constitutivo de fuerza mayor o caso

Scanned with CamScanner

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. **CLÁUSULA DÉCIMA SEXTA. - ACTAS DE RECIBO.-** Cumplido el recibo del objeto del contrato, se suscribirán entre las partes LAS ACTAS DE RECIBO A SATISFACCIÓN PARCIAL Y/O TOTAL, en las cuales se manifestará la conformidad con las condiciones en las que se hace la entrega, precios y valor total de la factura. Dichas serán suscritas por el supervisor del contrato y por el representante legal del CONTRATISTA y comprometerá en su contenido tanto al CONTRATISTA como al MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO siendo solo hasta ese momento cuando se consideran entregados los servicios contemplados en el objeto contractual. **CLÁUSULA DÉCIMA SÉPTIMA. - SANCIONES.-** EL CONTRATANTE podrá sancionar al CONTRATISTA por los incumplimientos parciales en sus obligaciones. Previa aplicación del precepto Constitucional del Debido Proceso citado en la siguiente clausula, MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO con la acreditación de las pruebas correspondientes, podrá aplicar las siguientes sanciones: **a) MULTAS:** En el evento en que EL CONTRATISTA incurra en mora o en incumplimiento parcial de cualquiera de las obligaciones, condiciones y especificaciones contraídas en el Contrato por causas imputables al CONTRATISTA, y con el fin de garantizar la correcta ejecución del contrato, EL CONTRATANTE impondrá multas cuyo valor se liquidará con base en el cero punto cinco por ciento (0.5%) del valor total del contrato por cada día de retardo y hasta por un plazo máximo de quince (15) días calendario en calidad de sanción, salvo circunstancias de fuerza mayor o caso fortuito, conforme a las definiciones del artículo 1º de la Ley 95 de 1.890. Lo anterior sin perjuicio que EL CONTRATANTE, haga efectiva la cláusula penal pecuniaria y/o declare la Caducidad del contrato. Esta suma podrá ser tomada de la garantía constituida o descontada de las cuentas que por cualquier concepto EL CONTRATANTE le adeude al CONTRATISTA. Con la suscripción del Contrato, El CONTRATISTA renuncia a los requerimientos judiciales o privados para constituirlo en mora; **b) 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 Familia, SENA e ICBF) el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO 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 retraso 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; **c) 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 NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO, a título de pena pecuniaria, una suma equivalente al diez por ciento (10%) 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 NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO. No obstante, el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" – DEPARTAMENTO ADMINISTRATIVO 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 amparada mediante póliza de seguros en las condiciones establecidas en el presente contrato. **PARÁGRAFO 1: 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 2**.- 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 3:** Las multas impuestas se harán efectivas directamente por EL MINISTERIO DE DEFENSA-COMANDO GENERAL-DIRECCIÓN

Scanned with CamScanner

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 4:** 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 5:** 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 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 6: - 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. **CLÁUSULA DÉCIMA OCTAVA. CLAUSULAS EXORBITANTES: DE LA TERMINACIÓN, MODIFICACIÓN E INTERPRETACIÓN UNILATERALES**. - 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. **CLÁUSULA DÉCIMA NOVENA - 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 DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO por medio de acto administrativo debidamente motivado podrá decretar la caducidad y ordenar la liquidación en el estado en que se encuentre, todo de conformidad con lo previsto en el artículo 18 de la Ley 80 de 1.993. Ejecutoriada la resolución de caducidad, el contrato quedará definitivamente terminado y el CONTRATISTA no tendrá derecho a reclamar indemnización alguna. El MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, hará efectiva la garantía pactada en el mismo, así como el valor de la penal pecuniaria, y procederá a su liquidación. Para efectos de esta liquidación, el CONTRATISTA devolverá los dineros que hubiere recibido por concepto del presente contrato, previa deducción del valor de los elementos entregados por aquel y recibidos a satisfacción. En el acta de liquidación se determinarán las obligaciones a cargo de las partes, teniendo en cuenta el valor de las sanciones por aplicar o las indemnizaciones a cargo del CONTRATISTA, si a esto hubiere lugar, y la fecha de pago. **CLÁUSULA VIGÉSIMA. - INDEMNIDAD:** El CONTRATISTA se obliga a mantener al MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, 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. **CLÁUSULA VIGÉSIMA PRIMERA.- RESERVA DEL PRESENTE CONTRATO.-** El CONTRATISTA se obliga para con EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, 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. **CLÁUSULA VIGÉSIMA SEGUNDA. - CESIONES Y SUBCONTRATOS:** El CONTRATISTA no podrá ceder el presente contrato a persona alguna natural o

Scanned with CamScanner

jurídica o extranjera, sin previa autorización escrita del CONTRATANTE, pudiendo 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 CONTRATANTE no adquirirá relación alguna con los subcontratistas. **CLÁUSULA 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 EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, 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 1988. **CLÁUSULA VIGÉSIMA CUARTA. -SUJECIÓN A LA LEY COLOMBIANA:** Para todos los efectos este contrato se somete a la ley colombiana y a las autoridades legalmente establecidas en el país. **CLAUSULA VIGÉSIMA QUINTA - APLICACIÓN DE PRINCIPIOS GENERALES: -** De conformidad con lo establecido en el Artículo 40 de la Ley 80 de 1993, el presente contrato, además de sus estipulaciones, se rige por los principios previos de las normas civiles, comerciales y las consagradas en esta ley que corresponde a su esencia y naturaleza. **CLAUSULA VIGÉSIMA SEXTA – DEBIDO PROCESO:** Durante la ejecución del contrato, EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, 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 NACIONAL - COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA - DEPARTAMENTO ADMINISTRATIVO, 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. **CLÁUSULA VIGÉSIMA SÉPTIMA. - DECLARACIÓN EXPRESA INHABILIDADES E INCOMPATIBILIDADES:** El CONTRATISTA declara bajo la gravedad del juramento que no se halla incurso en ninguna de las causales de inhabilidad e incompatibilidad contempladas en el artículo 127 de la Constitución Política y 8° de la Ley 80 de 1993 y que no se encuentra en proceso de concordato o acuerdo de recuperación o concurso liquidatario, según Leyes 222/95 y 550 de 1999. **PARÁGRAFO PRIMERO**. - INHABILIDADES E INCOMPATIBILIDADES SOBREVINIENTES-. Si llegare a sobrevenir inhabilidad e incompatibilidad en el CONTRATISTA, este cederá el contrato previa autorización escrita el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” – DEPARTAMENTO ADMINISTRATIVO o si ello no fuere posible, renunciará a su ejecución. **CLAUSULA VIGÉSIMA OCTAVA – PROPIEDAD INTELECTUAL:** La información, los contenidos y materiales suministrados a el MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” – DEPARTAMENTO ADMINISTRATIVO que hacen parte del objeto del contrato, son propiedad del CONTRATISTA o se encuentra debidamente autorizado por el titular para su utilización, en ninguna instancia podrán ser utilizados ni comercializados directamente por MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO” – DEPARTAMENTO ADMINISTRATIVO sin autorización previa y por escrito de EL CONTRATISTA. Las partes se reservan todos los derechos

Scanned with CamScanner

exclusivos que recaen sobre su capital intelectual y en general sobre cualquier otra creación que hayan desarrollado con anterioridad a la suscripción del presente contrato o por fuera de su objeto, por lo cual su utilización o implementación no se entenderá en ningún momento como una cesión sobre los mismos. **CLAUSULA VIGÉSIMA NOVENA - 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. - DOMICILIO**. - Las partes declaran que para todos los efectos legales judiciales y extrajudiciales que se deriven del presente contrato fijan su domicilio legal en la ciudad de Bogotá D.C., en las siguientes direcciones: CONTRATISTA: Calle 98 # 70 - 91 Of 202 Edificio Vardi Centro Empresarial Ponte de Bogotá D.C. CONTRATANTE: Carrera 11 No. 102-50 ciudad de Bogotá, D.C. **CLAUSULA TRIGÉSIMA PRIMERA -DOCUMENTOS**. - Forman parte integral del presente contrato los siguientes documentos: a) Certificado de Disponibilidad Presupuestal. b) Certificado de existencia y representación legal expedido por el Ministerio de Educación. c) Oferta del contratista y d) Demás documentos relacionados con el presente contrato. **CLAUSULA TRIGÉSIMA SEGUNDA - REQUISITOS PARA EL PERFECCIONAMIENTO**: Para el perfeccionamiento se requiere de la firma de las partes. **CLAUSULA TRIGÉSIMA TERCERA - 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 la garantía a cargo del contratista, y c) Aprobación de la garantía por parte del Jefe del Departamento Administrativo y Ordenador del Gasto de la Escuela Superior de Guerra “General Rafael Reyes Prieto”.

Para constancia se firma en Bogotá, conforme aprobación de las partes en plataforma SECOP II

POR EL MINISTERIO DE DEFENSA NACIONAL- COMANDO GENERAL DE LAS FUERZAS MILITARES – ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”- DEPARTAMENTO ADMINISTRATIVO

CF CLAUDIA PATRICIA PEREZ RODRIGUEZ
No. 22.732.677 expedica en Barranquilla
Jefe Departamento Administrativo y Ordenadora del Gasto
Escuela Superior de Guerra “General Rafael Reyes Prieto”
CONTRATANTE

POR EL CONTRATISTA,

JESUS ALBERTO FRANCO ACOSTA
CC No. C.E No. 582410 de Venezuela
Representante legal de HEIMCORE S.A.S
900425697-2

MY. GISELLE LORENA ROMERO CARO
Jefe Sección Contratos

ING YESSID CACERES
Comité técnico Evaluador

PS. MARTHA CECILIA JULIO ORTEZ
Integrante Comité Jurídico

PS. MARCELA ZABALETA IDARRAGA
Comité Jurídico Evaluador

PS. ZULMA COBOS CHICO
Integrante Económico Comité Evaluador

TC JULIAN JAIMES DELGADO
Gerente de proyecto

Scanned with CamScanner

ANEXO NO. 1

"ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO"

2.3.1.3 ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO A ADQUIRIR

ITEM No.	ESPECIFICACIONES TECNICAS MINIMAS	CANTIDAD DE EQUIPOS	UNIDAD DE MEDIDA	CANTIDAD
1	**RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO**			
1.1	Firewall 600E	2	Licencia	2
1.2	FortiAnalyzer 300G	1	Licencia	1
ITEM No.	**ESPECIFICACIONES TECNICAS MINIMAS**	**CANTIDAD DE DISPOSITIVOS**	**UNIDAD DE MEDIDA**	**CANTIDAD REQUERIDA**
2	**RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO EDR**			
2.1	Renovación de licenciamiento para la solución de seguridad de usuario final bajo la arquitectura de (Detección y Respuesta de Puntos Finales (EDR) y "Detección y respuesta extendidas – (XDR)" de acuerdo con las especificaciones técnicas	500	Licencia	500

La suscripción del licenciamiento será por un (01) año a partir de la fecha de finalización del soporte con que cuenta la ESDEG. Además, el licenciamiento deberá incluir el soporte técnico (preventivo y correctivo en cuanto a hardware y software) de los equipos mencionados.

ITEM	ESPECIFICACIONES TECNICAS MINIMAS
1	**RENOVACION DE LICENCIAMIENTO Y SOPORTE TECNICO FIREWALL 600E, FORTIANALYZER 300G**
1.1	Se deberá proveer la renovación del licenciamiento y soporte técnico para los equipos que se relacionan a continuación, así: Dos (02) FortiGate 600E Un (01) Fortianalyzer 300G La renovación del licenciamiento que se indica anteriormente deberá comprender al menos, sin limitarse a ellos, los componentes que se indican a continuación: FortiGate 600E y 100E: 24x7 Comprehensive Support Advanced Hardware Replacement Firmware & General Updates AntiVirus IPS Botnet/IP Domain Mobile Malware Cloud Sandboxing Application Control Web & Video Filtering AntiSpam FortiAnalyzer 300G: 24x7 FortiCare Contract Subscription license for theFortiGuard Indicator of Compromise (IOC). La renovación debe tener una vigencia de un (01) año ante fabricante a partir del acta de recibo a satisfacción por parte del Supervisor del contrato, y según la vigencia del actual licenciamiento.
1.2	Se deberán instalar las actualizaciones a la última versión liberada en el mercado por el fabricante, previa aprobación del administrador de la herramienta y del soporte técnico durante la ejecución del contrato y garantía técnica del mismo, sin generar costos adicionales para la ESDEG.
1.3	El licenciamiento debe quedar registrado a nombre de La ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO" y deberá ser entregado en el Almacén por parte del supervisor del contrato.
1.4	El contratista debe garantizar el registro de las licencias, y en caso de presentar algún error en dicho registro, el mismo, contará con un día (1) día hábil a partir de la notificación por parte del administrador de la herramienta de la ESDEG el cual dará a conocer al supervisor del contrato para realizar las correcciones del caso.
	El licenciamiento debe ser instalado por personal altamente capacitado con conocimiento de la herramienta como se indica en el ítem (4.4 ASPECTOS TÉCNICOS HABILITANTES), y debe quedar listo en perfecto uso y funcionamiento a partir del

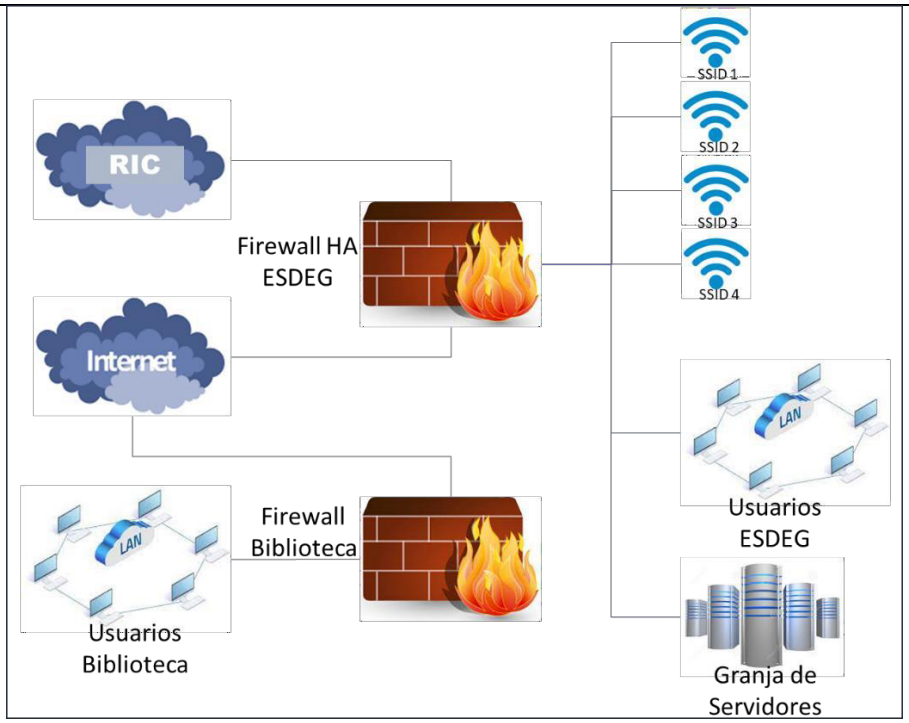
Scanned with CamScanner

1.5	cumplimiento de los requisitos de ejecución del contrato, en el evento que ocurra alguna falla o indisponibilidad del servicio tendrá como plazo máximo 4 horas para dejarlo en correcto funcionamiento, esto debe quedar documentado y aprobado por el administrador de la herramienta de la ESDEG y el supervisor del contrato quienes dan el aval del funcionamiento de la Plataforma y el licenciamiento instalado.
1.6	El contratista debe verificar el estado funcional del firewall, en el que registre los cambios que se requieran, evidenciando los posibles intentos de fugas de información que el firewall bloqueó y/o contuvo en su momento.
1.7	Soporte Preventivo Lógico: Realizar actividades de cuatro (04) soportes preventivos lógicos durante la ejecución del contrato más el término de garantía del contrato, previa coordinación con el supervisor del contrato y el administrador de la herramienta en la ESDEG., el cual consistirá en realizar labores preventivas para asegurar el buen funcionamiento, minimizar problemas y mantener los siguientes equipos: Dos (02) Fortigate 600E Un (01) Fortianalyzer 300G Las actividades que debe desarrollar en el soporte preventivo se encuentran enumeradas en el item 1.8 al item 1.21
1.8	Debe llevar a cabo rutinas de actualización mensual durante la ejecución del contrato más el término de garantía de este; de igual forma realizará acciones de actualización de firmware de la infraestructura, a fin de garantizar el correcto funcionamiento de todos los equipos.
1.9	Debe realizar el seguimiento, validación, verificación y depuración de las políticas implementadas, según recomendación el contratista y aprobación del supervisor del contrato.
1.10	Realizar la revisión y seguimiento a los archivos log de los eventos registrados en el sistema, con el fin de detectar y evaluar los errores no reportados.
1.11	Debe realizar backup al iniciar y al finalizar la revisión y control de acuerdo con los soportes planteados en el cronograma de soportes emitidos por el supervisor del contrato en el acta de inicio del contrato.
1.12	Debe realizar una depuración del sistema, eliminación de logs, verificación del funcionamiento de bases de datos, pruebas (internas y externas) control de acceso, de acuerdo con solicitud y aprobación del supervisor del contrato.
1.13	Debe realizar las actualizaciones de las versiones de sistema operativo (software) previa autorización del Administrador de la herramienta y el supervisor del contrato, así como todos los updates, upgrades y demás actualizaciones al momento de considerarse versiones estables liberadas por el fabricante y/o ser un requerimiento por parte de la Escuela Superior de Guerra.
1.14	Debe garantizar el funcionamiento del sistema en alta disponibilidad de los FortiGate 600E, el cual será verificado por el administrador de la herramienta.
1.15	Debe hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma.
1.16	En caso de identificar alguna anomalía con alguno de los equipos, Emitir recomendaciones temporales y definitivas para errores identificados y notificados al fabricante.
1.17	Incluir en el servicio de soporte las correcciones de configuración, incluso reinstalación de la solución de seguridad para garantizar su correcto funcionamiento.
1.18	Será necesario realizar las actividades inherentes a los respaldos de configuración y sistema operativo de todos los equipos. Dichos respaldos deberán ser entregados para su resguardo al personal que designe el supervisor del contrato al menos un día hábil antes de realizar el soporte preventivo lógico.
1.19	El contratista debe entregar en medio escrito y digital la topología de configuración de los equipos instalados en el datacenter HA.
1.20	Informar oportunamente al supervisor del contrato sobre las imposibilidades o dificultades que se presenten en la ejecución de este y ofrecer alternativas para garantizar la buena ejecución del contrato.
1.21	El contratista debe aplicar medidas correctivas de acuerdo con las recomendaciones emitidas por el CCOCI (Comando Conjunto Cibernético).
1.22	Soporte Preventivo Hardware: Realizar actividades de dos (02) soportes preventivos hardware durante la ejecución del contrato más el término de garantía del contrato, previa coordinación con el supervisor del contrato y administrador de la herramienta, el cual consistirá en realizar labores preventivas para asegurar el buen funcionamiento, minimizar problemas y mantener los siguientes equipos: Dos (02) Fortigate 600E Un (01) Fortianalyzer 300G Las actividades que debe desarrollar en el soporte preventivo hardware se encuentran enumeradas en el item 1.23 al item 1.26.
1.23	Revisión y limpieza externa de los equipos.
1.24	Verificación funcionamiento y limpieza externa de cables de conexión y poder.
1.25	Revisión de la instalación eléctrica de los equipos (chequeo de conectores entre otros).
1.26	Verificación de funcionamiento de todos los componentes del Firewall Fortinet 600E, Fortigate 100F, Fortianalyzer 300G. Así mismo se deberá realizar pruebas de diagnóstico del funcionamiento y rendimiento del equipo.
1.27	Soporte Correctivo Hardware: Corresponde a las actividades de soporte correctivo en sitio necesarios y/o requeridos por la Escuela Superior de Guerra cada vez que se presente una falla o mal funcionamiento propio de la solución, para asegurar el buen funcionamiento,

Scanned with CamScanner

	minimizar problemas y mantener los siguientes equipos: Dos (02) Fortigate 600E Un (01) Fortianalyzer 300G
1.28	El contratista deberá realizar las acciones necesarias para que la configuración de los equipos de aseguramiento tecnológico, se ajusten a las mejores prácticas y recomendaciones que sobre el manejo de mecanismos de aseguramiento tecnológico se han emitido.
1.29	El contratista deberá realizar la verificación de la configuración de conectividad de la plataforma HA de aseguramiento tecnológico, emitiendo y en coordinación con el supervisor, aplicando las recomendaciones que considere deben ser tenidas en cuenta por la Escuela Superior de Guerra.
1.30	El contratista deberá realizar verificación y actualización de las políticas de filtrado que se tienen definidas en la plataforma de aseguramiento firewall, realizando, en coordinación con el supervisor del contrato, los ajustes y configuraciones que sean requeridos.
1.31	El contratista deberá verificar las políticas y configuraciones realizadas sobre la plataforma de firewall, que están siendo aplicadas dentro de los procesos de filtrado y enrutamiento de navegación; dentro de estas actividades deberá evaluar la efectividad de la configuración del componente IPS e IDS de la plataforma UTM.
1.32	El contratista deberá realizar la evaluación y configuraciones indicadas en el numeral anterior, para los protocolos IPV4 e IPV6 en caso de que se requiera para su correcto funcionamiento
1.33	Debe considerar los soportes correctivos necesarios en caso de falla en alguna de las tarjetas, chasis, componente o cualquiera de las partes (hardware/software) de la solución Fortinet 600E, Fortianalyzer 300G, FortiSwitch 148E PoE, FortiAp 320C. Sin cargo adicional para la Escuela Superior de Guerra.
1.34	Debe suministrar en un 100% todos los repuestos que sean necesarios durante el término de la vigencia del contrato y garantía técnica, para remplazar las partes dañadas de la solución Fortinet 600E, Fortianalyzer 300G, FortiSwitch Sin cargo alguno para la Escuela Superior de Guerra, cuando se evidencie que el daño fue realizado por el contratista al realizar los soportes.
1.35	El proponente deberá adelantar las acciones necesarias para verificar la configuración de los equipos de aseguramiento perimetral (Firewall), de acuerdo con la infraestructura tecnológica que tiene implementada la institución, para lo cual deberá tener en cuenta las siguientes actividades: Verificar que la actividad de movimiento de los equipos de aseguramiento perimétrico FIREWALL al nuevo centro de cableado principal de la Escuela Superior de Guerra ubicado en el primer piso, ala occidental del edificio de aulas. Verificar la configuración de las interfaces físicas, para que se optimice el uso de los puertos operativos de cada uno de los equipos instalados. Garantizar y hacer pruebas de la infraestructura en alta disponibilidad que tiene configurada la escuela en el Firewall. Realizar la evaluación y verificación de las reglas de filtrado configuradas en los equipos de aseguramiento Firewall. Garantizar la interconectividad de las redes y servicios de la escuela, de acuerdo con las reglas definidas por el equipo de TIC de la Escuela Superior de Guerra. Apoyar los procesos de gestión para optimizar el empleo de los canales de conectividad “internet” para cada uno de los segmentos. Verificar que la plataforma de aseguramiento tecnológico permita la conectividad de la red, como mínimo con las siguientes características:

Scanned with CamScanner

	 Reglas básicas: Los servicios que llegan por la RIC, deberán ser accequibles a través de las redes de los usuarios de la ESDEG, usuarios biblioteca, SSID1 y SSID2. Desde la red RIC, no se debe poder acceder a la granja de servidores. Desde Internet no se debe permitir protocolo ICMP Se deben configurar las buenas prácticas de navegación en la plataforma de aseguramiento tecnológico (Proxy). El firewall ESDEG y el Firewall Biblioteca, deberán quedar configurados de tal manera que se visualice la red de la biblioteca como una extensión de la red ESDEG (Site to Site o MPLS o SD-WAN). El SSID 4 no deberá tener acceso por la LAN a la granja de servidores, RIC, redes WiFi ni redes de usuarios ESDEG y Biblioteca. La granja de servidores deberá estar asegurada de tal manera que se reduzca al mínimo, la posibilidad de acceder con ataques de cualquier nivel (Aseguramiento por Firewall). En la granja de servidores se encuentra el servicio de control de dominio y autenticación. En la granja de servidores se encuentra el servicio de DNS. En la granja de servidores se encuentra el servicio de plataforma académica. La plataforma académica y el servidor de aplicaciones deberán poderse acceder desde cualquier parte de la red e internet.
	El Contratista deberá contar con una mesa de servicio para apoyo a las solicitudes de soporte realizadas a fabrica con software certificado en mínimo 11 procesos ITIL, deberá suministrar certificación del software utilizado en la presentación de la propuesta.
1.36	ENTREGABLES CUANDO SE REQUIERA: Siempre, antes de realizar cualquier cambio en el Firewall, se debe realizar backup al iniciar y al finalizar la revisión y control de acuerdo con los soportes planteados en el cronograma de soportes emitidos por el supervisor del contrato. Debe garantizar el funcionamiento del sistema en alta disponibilidad de los FortiGate 600E, el cual será verificado por el administrador de la herramienta, el contratista debe emitir un informe después de cada verificación y será aprobado y entregado al supervisor del contrato. Soportes preventivos lógicos y hardware: Al finalizar cada soporte correctivo (cuando haya lugar) deberá entregar un informe detallado reportando de manera inmediata las acciones ejecutadas (antes, durante y después), así como las recomendaciones al final del soporte preventivo según aplique: lógico o hardware. Será necesario realizar las actividades inherentes a los respaldos de configuración y sistema operativo de todos los equipos. Dichos respaldos deberán ser entregados para su resguardo al personal que designe el supervisor del contrato al menos un día hábil antes de realizar el soporte preventivo según aplique: lógico o hardware. Al finalizar cada soporte correctivo (cuando haya lugar) deberá entregar un informe detallado reportando de manera

Scanned with CamScanner

	inmediata las acciones ejecutadas (antes, durante y después) en el soporte. Informe de entrega única: Al finalizar la instalación del licenciamiento por parte del contratista, este debe entregar un informe donde garantice que no hay sublicenciamiento. Además, el contratista debe certificar en el informe que las licencias fueron renovadas y activadas en los equipos objetos del contrato, con el aval del Administrador de la Herramienta de la ESDEG. Informes de seguimiento para conocimiento del supervisor: El contratista debe entregar un informe mensual con el aval del Administrador de la Herramienta de la ESDEG, al supervisor del contrato donde se evidencie e indique el estado funcional del firewall, en el que registre los cambios que se requieran, evidenciando los posibles intentos de fugas de información que el firewall bloqueó y/o contuvo en su momento, ese informe debe contener un reporte estadístico, eventos de seguridad generados de estado crítico, una estadística de funcionabilidad y disponibilidad del servicio. Debe entregar al administrador de la herramienta y al supervisor del contrato un informe gerencial mensualmente en el que contenga la eliminación y depuración del sistema, eliminación de logs, verificación del funcionamiento de bases de datos, pruebas (internas y externas) control de acceso. Debe entregar bimestralmente un informe gerencial para la toma de decisiones sobre el seguimiento y validación, verificación y depuración de las políticas implementadas. Realizar la revisión y seguimiento a los archivos log de los eventos registrados en el sistema, con el fin de detectar y evaluar los errores no reportados esta revisión deberá estar acompañada de un informe al supervisor del contrato. Debe hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en un informe trimestral. El contratista debe entregar un informe trimestral donde se apliquen medidas correctivas de acuerdo con las recomendaciones emitidas por el CCOCI (Comando Conjunto Cibernético) Este informe se entregará al supervisor del contrato y al administrador de la herramienta.
ÍTEM 2	ESPECIFICACIONES TECNICAS MINIMAS RENOVACION DE LICENCIAMIENTO Y SOPORTE TECNICO DE EDR - XDR (ADVANCED MALWARE PREVENTION, DLP, APPLICATION CONTROL, DEVICE CONTROL, FW, VULNERABILITY PROTECTION, WEB REPUTATION, XDR)
1	La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, análisis de archivos adjunto de correo POP3, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).
2	La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.
3	La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.
4	La solución ofertada deberá proporcionar un único agente de seguridad para Endpoints, que ofrezca todas las funcionalidades de control y protección.
5	La solución ofertada deberá permitir la activación o desactivación de módulos o configuraciones (Análisis de comportamiento, Control de Aplicaciones, Firewall, HIPS, DLP, etc), de manera granular y particular en los agentes de seguridad.
6	La solución ofertada deberá estar en capacidad de detectar y eliminar códigos maliciosos (Rootkits, Gusanos, Troyanos, Spyware, Malware Fileless, Virus, Ransomware, Crypto Miners (Monederos), etc.
7	La solución debe proporcionar protección de la exploración de la memoria y estar en capacidad de terminar procesos maliciosos en ejecución.
8	La solución debe proporcionar protección contra de exploits mediante el análisis de comportamiento de aplicaciones, archivos maliciosos y vulnerabilidades conocidas.
9	La solución debe tener capacidades de aprendizaje automático mediante el uso de algoritmos que permitan identificar amenazas de día cero.
10	La solución deberá ofrecer mecanismos de autenticación de múltiple factor (MFA) para usuarios administradores.
11	La solución debe contar con capacidades de detección y análisis de comportamiento malicioso
12	La solución deberá estar en capacidad de identificar vulnerabilidades conocidas sobre el sistema operativo y aplicaciones instaladas, y proporcionar los controles de mitigación inmediata para la prevención de exploits.
13	La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.
14	La solución debe poder ser instalada o administrada en la nube, on-premise o hibrida
15	La solución debe tener la capacidad de brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos.
16	La solución deberá incluir módulos de Firewall, prevención de Intrusiones en host y protección de vulnerabilidades
17	La solución debe permitir la integración con Active Directory.
18	La solución debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.
19	La solución debe permitir recuperar los archivos que sean enviados a cuarentena.
20	Debe permitir genera investigaciones detalladas que permitan realizar una investigación sobre el estado actual del sistema.

Scanned with CamScanner

	Las investigaciones detalladas se pueden configurar para que se ejecuten en períodos específicos y también admiten un conjunto más amplio de criterios mediante el uso de las reglas de OpenIOC y YARA.
21	La solución debe permitir el análisis de comportamiento de un malware, actividades específicas de IoC, conexiones de comando a control
22	La interfaz debe estar integrada con la consola de administración de las soluciones de seguridad para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los sucesos
23	La solución debe permitir realizar el monitoreo de comportamiento avanzado y debe estar basado en la información que es capturada, IoC externos o internos
24	La consola de análisis debe permitir la visualización de la siguiente información: - comunicación: IP, Puerto, Dominio, DNS - Malware o cualquier archivo: SHA1 hash, nombre de archivo, ruta del archivo, tipo del archivo - Registro de actividad - Procesos ejecutando -Actividad de cuenta de usuario
25	Análisis de comportamiento IOA examinando un elemento desconocido mientras se está cargando y busca comportamientos sospechosos o indicadores de ataques (IOA) en el sistema operativo, las aplicaciones, los scripts y cómo interactúan para bloquearlos.
26	Protección de Exploración de la memoria: identificando procesos en ejecución a medida que se ejecuta en la memoria para determinar si es malicioso. Permite terminar el proceso en ejecución dependiendo de la configuración de la acción.
27	La solución debe contar con fuentes de inteligencia del fabricante que permita tener información sobre amenazas, para correlacionar registros de Internet, emails, archivos, dominios y muchas otras fuentes de amenazas para identificar las infraestructuras del atacante antes de que se ejecuten.
28	Protección contra ataques de exploits: controla los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
29	Protección de exploits de documentos: escanee documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas
30	Aprendizaje automático: analiza archivos desconocidos de baja prevalencia al extraer características de los archivos para examinarlos utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso (es decir, malware / ransomware / amenazas de dia 0).
31	Protección contra ransomware: busca la ofuscación / cifrado rápido de archivos mediante un proceso desconocido, elimina ese proceso y restaura los archivos cifrados.
32	La solución debe proporcionar protección a los agentes contra Ramsomware.
33	La solución debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tenre la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.
34	La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.
35	La solución debe tener la capacidad de analizar la reputación de archivos y URL
36	La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de esta.
37	La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella.
38	La solución debe tener la capacidad de programar la sincronización de los equipos para horas y fechas específicas.
39	La solución debe permitir la configuración de SNMP traps
40	La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas a la administración, cuando una amenaza sea detectada.
41	La solución debe permitir la configuración de la plantilla del correo para él envió de notificaciones.
42	La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.
43	La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)
44	La solución debe permitir la configuración de proxy tanto para los agentes como para el servidor de administración.
45	La solución debe permitir proteger los equipos frente a vulnerabilidades no conocidas presentes en los equipos
46	Los agentes de protección de los equipos deben tener la capacidad de protegerse contra intentos de desinstalación o cancelación de los procesos por los usuarios o por una aplicación de terceros.
47	La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad.
48	La solución debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint
49	La solución debe permitir generar control de aplicaciones, de forma granular y por categorías y permitir o bloquear por HASH, ruta de instalación, nombre de programa además de generar alerta o eventos de los cambios no autorizados
50	La solución debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el tráfico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)
51	La solución provee una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.
52	La solución debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de informacion sensible de la organización ya sea de forma accidental o deliberada.
53	La solución debe permitir la creacion de politicas que limiten la trasmision o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).
54	La solución debe tener la capacidad de igualmente brindar protección y aplicar politicas para transferencia de activos digitales mediante cliente de correo ya sera software o web.
55	La solución debe permitir que la organización haga cumplir con las normas de privacidad establecidas.
56	La solución debe tener la capacidad de brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo configurar reglas o políticas para ser aplicadas a grupos o agentes individuales.

Scanned with CamScanner

57	La solución debe proporcionar identificadores de datos y/o plantillas para la creación de políticas.
58	La solución debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, gráficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de cálculo, presentación, archivos vinculados e incrustados, y/o archivos encriptados.
59	La solución debe tener la capacidad de localizar activos digitales almacenados en portátiles, equipos de escritorio, y servidores.
60	La solución debe tener la capacidad de proporcionar filtros de protección para canales de red como FTP o HTTP, canales de aplicaciones o periféricos.
61	La solución debe tener la capacidad de detectar datos estructurados y no estructurados.
62	La solución debe mantener un monitoreo constante.
63	La solución debe permitir generar un control de dispositivos externos al equipo, generando bloqueos y alertas, pero permitir dispositivos por su ID,
64	La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o SB-1386.
65	La solución debe estar en la capacidad de generar registros de infección o software mal intencionado que genere cambios en el sistema con el fin de generar investigaciones para respuesta a incidentes, verificando los procesos tareas archivos creados o modificados al igual que las rutas del sistema, generando así reporte grafico o eventos para estudiar los incidentes
66	La solución debe tener la capacidad de hacer Rollback de las actualizaciones de los componentes.
67	La solución debe contar con cifrado basado en hardware y en software para entornos mixtos
68	La solución debe permitir la administración de las claves de cifrado, y la sincronización de políticas con todos los equipos
69	La solución debe garantizar el cifrado de archivos, carpetas y medios extraíbles.
70	La solución debe tener capacidad de implementar comandos remotos, recuperar datos perdidos y una sincronización de políticas en tiempo real
71	La solución debe tener integración con UEFI (Unified Extensible Firmware Interface), responsable de inicializar el hardware de los equipos antes de dar el control al sistema operativo.
72	La solución debe cifrar todas las unidades de disco físicas que tenga disponibles el equipo.
73	La solución debe contar con varios metodos de autenticación para el inicio de sesión en los equipos. ColorCode: Una secuencia única de colores. Domain Authentication: Sincronización LDAP de Active Directory para inicio de sesión único (SSO). Fixed Password: Una cadena de caracteres, números y símbolos. PIN: Un número de identificación personal estándar. Remote Help: Autenticación interactiva para usuarios que olvidan sus credenciales o dispositivos que no tienen políticas sincronizadas dentro de un período de tiempo predeterminado. Self Help: Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el Soporte técnico. Smart Card: Una tarjeta física utilizada junto con un PIN o una contraseña fija.
74	La solución debe asegurar que los dispositivos perdidos o robados puedan ser borrados o bloqueados de forma remota antes de que puedan iniciar usando redes (WiFi y Ethernet).
75	La consola debe proporcionar la capacidad de administrar los usuarios para agregar o eliminar cuentas, restablecer contraseñas, cambiar permisos, configurar prioridad de políticas, importar usuarios desde Active Directory y buscar cuentas de usuario específicas.
76	La consola debe mostrar un estado actual de los discos cifrados de cualquier equipo con las fechas de última sincronización y política aplicada.
77	La consola debe brindar la posibilidad de mostrar en todos los dispositivos los intentos fallidos de inicio de sesión.
78	La consola debe mostrar los dispositivos que se encuentran bloqueados debido a restricciones de políticas.
79	La consola cuenta con una lista de políticas donde muestra la información y el estado de las políticas creadas para todos los usuarios.
80	La solución debe permitir el cifrado completo de disco incluyendo aplicaciones, configuraciones de registro, archivos temporales, archivos de intercambio, spoolers de impresión y archivos eliminados.
81	La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica.
82	La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.
83	La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de estos.
84	La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de estos.
85	La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
86	La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.
87	La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.
88	La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, Reputación web, conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.
89	La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.

Scanned with CamScanner

90	La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.
91	Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.
92	Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.
93	Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.
94	Los agentes deben ser agrupados por NetBios, Directorio Activo, DNS y/o grupos personalizados.
95	El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.
96	Los agentes de instalación deberán permitir desinstalar un antimalware anterior.
97	Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc), si alguna de estas es inaccesible para el agente.
98	La solución debe tener reconocimientos en cuanto a protección de Vulnerabilidades para endpoints
99	La solución debe estar ubicada en el cuadrante de lideres de Gartner y Forrester
100	La solución debe contar con certificación de AV-Test en cuanto al rendimiento, protección y usabilidad.
101	XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.
102	Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.
103	La Plataforma de XDR debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.
104	Debe proveer una vista de alertas (llamadas workbenches) con la capacidad de investigar más a fondo.
105	Las alertas deben permitir ver un análisis de causa raíz (también llamado Execution Profile) identificar el alcance del impacto y permitir tomar acciones de respuesta.
106	Debe contar con un dashboard de risk visibility que permita visibilidad centralizada y una visión holística ver lo que está sucediendo en el entorno, incluido un resumen de detecciones clave, puntos finales con técnicas de ataque observables, listas priorizadas de dispositivos y usuarios de riesgo, junto con visibilidad de uso de aplicaciones en la nube aprobadas y no aprobadas y los riesgos asociados a esto
107	Integración con Azure AD para una estrategia de Zero trust identificando usuarios con comportamiento anómalo y permitiendo tomar acciones como cambios de contraseña o inactivar usuarios.
108	Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).
109	Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
110	XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.
111	Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.
112	Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducir las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.
113	Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.
114	Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.
115	Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.
116	Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico.
117	Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor
118	La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.
119	Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK.
120	En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.
121	Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.
122	Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence.
123	Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.
124	Debe proveer un conector para Splunk, Qradar, Soluciones de terceros como Paloalto panorama, Broadcom, Checkpoint, para compartir objetos sospechosos
125	Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud
126	XDR debe analizar la data recolectada por los sensoress para proveer alertas inteligentes, y detecciones de alta fidelidad.
127	Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK
128	El contratista debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos to improve.
129	Los modelos deben priorizar la respuesta del administrador en base a puntajes (score).
130	El aplicativo de Detection Model Management debe permitir controlar el tipo de alertas que se disparan y se envían a Workbench.
131	Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE.
132	Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen.
133	High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen
134	Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen.

Scanned with CamScanner

135	Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting.
136	Los modelos deben especificar para que productor en específico (Workstation/Server/Email/Network) aplica una alerta
137	Los modelos deben especificar y permitir modificar “status”: encendido/apagado
138	Los modelos deben especificar la última vez que se actualizó
139	Debe hacer una sección de excepciones dentro de la App de Model Management que despliegue todas las excepciones que se añadieron.
140	La excepción debe ser granular y debe mostrar lo siguiente:
141	Object: El objeto que se ha añadido como excepción en una investigación
142	Filter: El filtro que identificó el objeto como un indicador de amenaza
143	Type: El atributo del objeto añadido
144	Data field: Log definido por el objeto
145	Match type: Exacto o Parcial (soporta wildcards)
146	Description: Información definida por el usuario para la excepción
147	Created: Fecha y hora en que se añadió la excepción
148	Created by: Usuario que creó la excepción
149	Debe permitir añadir excepciones durante la investigación de una alerta.
150	En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción.
151	Debe integrar inteligencia al minuto con reportes del contratista y terceras partes confiables para ayudar a identificar amenazas
152	Debe poder analizar los logs, comparar la data contra los reportes de Threat Intelligence automáticamente, y generar alertas basadas en indicadores sospechosos o maliciosos detectados
153	La App de Workbench debe mostrar alertas por los modelos de detección y permitir investigar a más detalle.
154	La data del Workbench debe incluir:
155	Status: New/In Progress/Closed/Closed – False Positive
156	Score: basado en la severidad del modelo de detección y el impacto de la alerta.
157	Workbench ID: identificador único para la alerta
158	Model: Modelo que disparó la alerta
159	Model severity: Severidad asignada al modelo que disparó la alerta
160	Impact scope: Número de entidades afectadas por Servers/Workstations/Users/Cuentas de correo
161	Created: Fecha y Hora que XDR generó la alerta
162	Detailed Profile:
163	Endpoint Profile: Debe incluir Hostname/IPv4/GUID/MAC Address/OS version/Producto/Último usuario que inció sesión.
164	Email Profile: debe incluir: Asunto del correo/Message ID/Risk level/Fecha y hora del correo/Dirección de remitente/dirección de destinatarios/Información de cada adjunto al correo/URLs embebidas/Cabecera del correo.
165	Analysis Chain
166	Despliega el análisis de causa raíz y provee información adicional que puede ser útil para la investigación.
167	Debe desplegar un análisis visual de los objetos envueltos en un evento
168	Debe resaltar los objetos en la cadena que son posiblemente maliciosos
169	Debe desplegar el objeto o la lista de objetos que coinciden con los criterios de investigación definidos
170	Debe resaltar el objeto “más probable” que creó el objeto que coincidió con el criterio de investigación.
171	Debe desplegar detalles del endpoint que fue investigado
172	La cadena de análisis debe usar íconos para los distintos tipos de objetos (servidor/endpoint/url/archivos, etc…). La descripción debe estar directamente en la ventana de investigación para entender rápidamente la relación entre los distintos objetos.
173	Network Analytics
174	Debe poder obtenerse una representación visual de correlación de eventos de la perspectiva de la red y no del endpoint.
175	Network Analytics debe usar como sensor al BDS (Breach Detection System) y debe proveer integración nativa para compartir no solo eventos sino el contexto entero (toda la telemetría posible).
176	Debe tener una barra de reproducción (play/pause) con un “time slider” para ver eventos correlacionados vs tiempo
177	Cada gráfica de correlación debe tener 1 o más líneas de correlación que muestran actividad maliciosa o sospechosa entre un origen y destino.
178	Cada línea de correlación representa 1 o más transacciones entre 2 hosts.
179	El grosor de la línea es proporcional al número de transacciones entre los hosts. Al colocar el mouse sobre la línea debe mostrar el número de transacciones para esa línea de correlación
180	La línea de correlación debe poder ser entre host interno y externo. También debe poder ser entre 2 hosts internos (para identificar movimientos laterales).
181	Cada línea de correlación debe indicar los protocolos usados. Y debe existir una flecha para indicar direccionalidad de la comunicación.
182	Debe identificar actividades claves para hosts internos y externos en la gráfica.
183	Debe incluir actividades similares a: Machine Learning, Lateral Activity, Detected Event, C&C Activity, and Malicious Download.
184	Correlation Information Pop-up Window: Debe incluir los siguientes campos: Source IP/Destination IP/Severity/URLs/Hashes/Protocols/Number of transactions/Reason/Earliest date/Latest date
185	Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.
186	Debe responder a amenazas sin dejar la consola de XDR.
187	Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos
188	Añadir a lista de bloqueo
189	Eliminar de lista de bloqueo
190	Terminar procesos en endpoints

Scanned with CamScanner

191	Recolectar archivos en endpoints
192	Bloquear remitente de correo
193	Poner en cuarentana un correo
194	Borrar un correo
195	Aislar un equipo
196	Restaurar la conexión en equipos aislados
197	After triggering a response to an event or object, you must view the response task status and command details in the Response Management table
198	Search app enables sweeping across applicable product data lakes (email, endpoint, and network) via the XDR console
199	It must allow perform IoC sweeps, customize searches by specifying parameters, filters, and other criteria, and search for multiple events that occurred on the same endpoint
200	A query builder must allow to combine search attributes, operators, and specified values into a single search query
201	Debe listar búsquedas previas
202	Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.
203	El administrador debe poder ver los queries guardados
204	Debe ser fácil limpiar los criterios de búsqueda
205	Los resultados deben ser exportables a CSV o JSON
206	Los resultados deben mostrar origen de los datos (workstation/servidor/email/network)
207	El administrador debe ser capaz de ver los logs en RAW
208	XDR debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado en Kibana para identificar, categorizar y obtener los resultados de búsqueda.
209	La configuración administrativa de XDR debe brindar a los usuarios la capacidad de configurar cuentas de usuario, roles y configuraciones, conectar productos adicionales y configurar opciones de monitoreo adicionales. Las siguientes opciones deben estar disponibles:
210	SAML Single Sign-On: Debe soportar inicio de sesión SAML, single sign-on (SSO) utilizando las credenciales corporativas.
211	Account Management: Debe permitir crear usuarios locales y usuarios para aplicaciones de terceros que se conectan a la API.
212	Role Management: Debe permitir ver y configurar el acceso basado en roles que se aplican a los usuarios aplicativos de terceros que se conectan a través de la API
213	Product Connector: Debe permitir conectar correo, endpoint, servidor, cloud, y productos de red nativamente para proveer un mejor contexto y una perspectiva más amplia para identificar amenazas fácilmente y contenerlas de forma efectiva.
214	Alert Notifications: Debe proveer formas de notificación externas como correo e incluir una app de splunk.
215	Audit Logs: Debe proveer logs de auditoría que provee un resumen de acceso de usuario, acciones relacionadas con las Apps, cambio de configuraciones, y otras modificaciones que ocurran usando la consola XDR o las APIs.
3	RESPONSABILIDAD AMBIENTAL
3.1	El proponente garantiza la manipulación y manejo responsable conforme a las disposiciones legales vigentes, de desechos y residuos de componentes electrónicos o informáticos, lo anterior por políticas ambientales y sistema de gestión ambiental del MDN. La Escuela Superior de Guerra no se hace responsable por las prácticas de eliminación de desechos y residuos de componentes electrónicos o informáticos será responsabilidad del contratista.
4	CAPACITACION
4.1	Suministrar dos (02) transferencias de conocimiento ocho (08) horas cada una, en sitio o en los laboratorios del contratista adjudicatario, hasta cuatro (04) funcionarios orgánicos del Departamento TIC que designe el Supervisor del contrato. Las capacitaciones serán: Primera capacitación en instalación, uso y administración de la herramienta Firewall y Fortianalyzer. Segunda capacitación en instalación, uso y administración de la herramienta EDR - XDR, con sus licencias o la tecnología ofertada. Esto en horario de lunes a viernes de 9:00 a 16:00 horas de acuerdo con la necesidad y de común acuerdo con el supervisor del contrato. Las transferencias de conocimiento serán en administración y configuración de los equipos soportados, en horario de lunes a viernes de 9:00 a 16:00 horas de acuerdo con la necesidad y de común acuerdo con el supervisor del contrato. Temas de la capacitación: Introducción Configuraciones Administración Comunicación Reglas Directivas Logs Reportes Políticas Perfiles VPN

Scanned with CamScanner

	Afinamiento Alta disponibilidad Excepciones Bloqueo de puertos Actualización de colectores Usuarios Grupos Debbuging ta: Se debe otorgar a los asistentes Certificado Digital de asistencia generado por el contratista.
5	DOCUMENTACION CONTRATISTA
5.1	El Contratista al inicio de la ejecución deberá entregar al supervisor del Contrato: a. Certificación vigente emitida por el fabricante de los equipos para que posea la Entidad relacionados en el ítem 1, que lo acredite como Partner o distribuidor o comercializador autorizado para suministrar la renovación de garantía y soporte para el presente proceso. b. Certificación vigente emitida directamente por el fabricante de los equipos relacionados en el ítem 2, mediante la cual se acredite que el oferente posee la autorización para suministrar la renovación de garantía y soporte del fabricante para el presente proceso.

2.3.1.5 GARANTÍA TÉCNICA Y TERMINO DE RESPUESTA

GARANTÍA TÉCNICA	El contratista deberá anexar a la propuesta documento debidamente suscrito por el representante legal en donde se compromete que en caso de detectarse fallas en el servicio deberá brindar soporte técnico en el siguiente sentido: • El soporte telefónico para problemas técnicos menores debe ser atendido por el proveedor, los cuales no tendrán limitación en cantidad, estarán cubiertos dentro del valor del servicio contratado. Un problema técnico "menor" corresponde a solicitudes que tienen las siguientes características: 1) Tiempo de atención inferior a treinta (30) minutos contabilizados luego de la descripción o explicación que se haga de un problema o consulta de acuerdo con la severidad y 2) Consultas de tipo informativo. • Brindar el soporte técnico a los funcionarios designados por el encargado de ejercer el control por parte de la ESDEG, con un tiempo de respuesta no mayor a cuatro (4) horas contadas a partir del momento en que se solicite el soporte servicio. • Proveer el servicio de soporte técnico telefónico, remoto y/o en sitio, durante el término de la vigencia de las licencias. Así mismo, contar con una línea de soporte telefónico local y una mesa de servicio para creación de casos, atención de requerimientos y solución de dudas. • Atender todos los requerimientos técnicos a que haya lugar, durante el término de vigencia de las licencias, bien sean consultas técnicas sobre funcionamiento de las herramientas, reconfiguración de la solución y atención a los requerimientos técnicos. Durante el término de la vigencia de las licencias. • Atender los requerimientos del supervisor del contrato en el plazo que para tal efecto se defina. Durante el término de la vigencia de las licencias. • El término de la garantía es por doce (12) meses contados a partir de la activación de las licencias adquiridas por parte del supervisor del contrato. • Que ampare la prestación normal del servicio contratado. • La garantía implica que las licencias suministradas serán reparadas y ajustados cuantas veces sea necesario hasta alcanzar su óptimo funcionamiento. • Se está en la obligación de realizar los trámites pertinentes ante fábrica cuando se presente algún daño de equipo durante el tiempo de la garantía y/o cuando se presente una nueva tecnología que obligue a la entidad a la compra de un nuevo equipo por obsolescencia tecnológica.
TERMINO DE GARANTÍA TÉCNICA	El contratista deberá anexar a la propuesta documento debidamente suscrito por el representante legal en donde se compromete con este término de respuesta a la garantía técnica. En caso de detectarse fallas en el licenciamiento contratado, el CONTRATISTA deberá concurrir a cumplir con su deber de garantía, en un tiempo máximo de cuatro (4) horas luego del reporte efectuado por el CONTRATANTE. Si dentro de este tiempo no se soluciona el problema y/o continua la novedad por la cual se reportó el incidente y/o es reiterativo, es decir se ha presentado la falla en tres (3) ocasiones en el mismo equipo, el CONTRATISTA se compromete a reemplazarlo por uno de iguales o superiores especificaciones técnicas a las contratadas. Estarán a cargo del CONTRATISTA todos los costos en que deba incurrir en el cumplimiento de su deber de garantía.

2.3.1.6. PERFIL PROFESIONAL

Scanned with CamScanner

REQUERIMIENTOS DE PERSONAL REQUERIDO Y EXPERIENCIA ESPECIFICA:

Es fundamental contar con personal capacitado y con la experiencia necesaria para llevar a cabo la ejecución del presente proceso contractual. Esto asegura una correcta implementación, cumpliendo con los estándares y normas de la industria, contar con personal calificado contribuye a la eficiencia, seguridad y éxito del proyecto, reduciendo riesgos y costos asociados, el proponente junto con su oferta deberá acreditar y adjuntar hojas de vida y certificaciones para el siguiente personal:

ÍTEM	CARGO	CANT	PERFIL ACADÉMICO	EXPERIENCIA GENERAL	EXPERIENCIA ESPECIFICA
1	**INGENIERO DE SEGURIDAD**	1	Un ingeniero de sistemas, telecomunicaciones, electrónico o afines Con especialización en seguridad informática o seguridad de redes. Certificado por el fabricante del equipo ofertado, en los niveles FCP-NS y FCSS para administrar, configurar e instalar equipos de seguridad Firewall y Analizador de trafico de red.	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional, así: Minino de 02 años con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante. (FIREWALL)	Experiencia certificada, como mínimo debe haber participado en 1 proyecto de seguridad. Deberá adjuntar certificado del fabricante vigente, con fecha de expedición menor a 2 años a partir de la presentación de la oferta, con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante.
2	**INGENIERO DE IMPLEMENTACIÓN**	1	Un ingeniero de sistemas, telecomunicaciones, electrónico o afines Certificado por el fabricante de la solución ofertada, con curso en implementación y configuración de la solución de XDR de la marca ofertada y/o nivel profesional en ciberseguridad.	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional, así: Minino de 01 año con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante.	Experiencia certificada, como mínimo debe haber participado en 1 proyecto de seguridad. Deberá adjuntar certificado del fabricante vigente, con fecha de expedición menor a 2 años a partir de la presentación de la oferta, con el fin de garantizar que está vigente y que el personal tiene los conocimientos sobre las últimas versiones, equipos y funcionalidades liberadas por el fabricante.

2.3.1.5. DOCUMENTOS.

ÍTEM	ASPECTOS SG-SST	AFECTACIONES	OBLIGACIONES PARA EL CONTROL DE LOS ASPECTOS Y AFECTACIONES
1	Para la ejecución de contratos no se identificaron aspectos ambientales	Para la ejecución de contratos no se identificaron aspectos ambientales	Al no identificarse aspectos ni impactos ambientales, no se requieren controles operacionales; no obstante, se recomienda que el oferente debe velar por la protección y conservación del medio ambiente durante la ejecución del

Scanned with CamScanner

ÍTEM	ASPECTOS SG-SST	AFECTACIONES	OBLIGACIONES PARA EL CONTROL DE LOS ASPECTOS Y AFECTACIONES
			contrato y el cumplimiento de la normatividad ambiental vigente.

4.1.2 CUMPLIMIENTO DE LAS DISPOSICIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO

ÍTEM	ASPECTOS SG-SST	AFECTACIONES	OBLIGACIONES PARA EL CONTROL DE LOS ASPECTOS Y AFECTACIONES
1	Prevención de Riesgo en actividades generales	Afectaciones a la salud por los diferentes riesgos al que el personal está expuesto, como físico, mecánico, fenómenos naturales, locativos, condiciones de salud, biomecánico, entre otros.	Durante la ejecución del contrato el contratista debe garantizar la señalización y demarcación de todas las áreas de trabajo intervenidas para evitar que personas ajenas a la actividad ingresen a las áreas, todas las sustancias químicas deben estar etiquetadas según el sistema globalmente armonizado dando cumplimiento a la resolución 773 del 2021. Nota: El contratista remitirá un certificado de compromiso al cumplimiento de las normas, al supervisor del contrato la primera semana de inicio de ejecución del contrato
2	Cumplimiento de normas	Sanciones.	El oferente JUNTO CON LA OFERTA deberá allegar certificado emitido por la ARL con valoración moderadamente aceptable de implementación del Sistema de Gestión de Seguridad y Salud en el Trabajo, correspondiente a la autoevaluación de los estándares mínimos del año 2025. Nota 1: En caso de existir un consorcio o unión temporal, cada uno de sus miembros deberá adjuntar el certificado emitido por la ARL. Nota 2: La documentación anteriormente indicada, deberá expresar de manera clara que la evaluación se realizó en el mes de febrero, marzo, independiente de la fecha de expedición de la certificación, de acuerdo con la Circular No. 027 de 2026. Nota 3: Si la empresa o entidad es creada durante la respectiva anualidad, se admitirá que la aplicación de la evaluación se realice en cualquier fracción del año 2025.
3	Cumplimiento de normas	Afectaciones a la salud por los diferentes riesgos al que el personal está expuesto, como físico, mecánico, fenómenos naturales, locativos, condiciones de salud, biomecánico, entre otros..	En caso de requerir realizar actividades con energía dar cumplimiento a las medidas de prevención de Seguridad y Salud en el Trabajo estipuladas en el RETIE
4	Cumplimiento de normas	Sanciones.	El contratista debe garantizar el cumplimiento de la normatividad legal vigente de Seguridad y Salud en el Trabajo.

PONDERABLE:

Se incluye en el contrato, ponderable ofertado por el contratista en su ofrecimiento.

FACTOR PONDERABLE	CANTIDAD
Se otorgarán treinta (30) puntos al contratista que ofrezca sin costo adicional para la entidad una herramienta de Ciberinteliegencia de amenazas que se integre de forma nativa con la solución de seguridad perimetral con que cuenta la entidad, la herramienta debe tener mínimo las siguientes características: La entidad requiere una solución de Ciberinteliegencia de amenazas que ayude a dar un mejor manejo y visibilidad del riesgo digital en la misma. La solución debe estar licenciada para el monitoreo y gestión de riesgo de 200 activos de la entidad, por un período de 1 año. La solución debe recopilar inteligencia de varias fuentes, como Darkweb, Open Source e Investigación técnica.	1

Scanned with CamScanner

La inteligencia debe tener una calificación de confianza basada en el estándar de la industria, como (Admiralty System) para todos los informes publicados. Todos los informes de inteligencia deben calificarse según los criterios de relevancia específicos para el panorama de amenazas del cliente. La Inteligencia de amenazas presentada debe cubrir todas las amenazas relevantes para el Cliente. La inteligencia de amenazas presentada debe cubrir amenazas relevantes para el sector de la industria y los ataques más relevantes a organizaciones pares del cliente. La solución debe supervisar e informar sobre amenazas en nuevas vulnerabilidades y exploits que se discuten activamente en Dark web y fuentes abiertas La inteligencia de amenazas debe estar asignada al marco MITRE ATT&CK La inteligencia debe proporcionarse y actualizarse en tiempo real a medida que se recopila nueva información o contexto de diversas fuentes. La solución debe proporcionar inteligencia sobre fugas de credenciales a través de infracciones de terceros en una vista de línea de tiempo limpia La solución debe tener una fuerte presencia en los sitios de darknet examinados y solo por invitación, como foros y mercados. La solución debe hacer monitoreo extensivo de Dark Web para inteligencia específica de la organización mediante el monitoreo de salas de chat ocultas, sitios web privados, redes punto a punto, plataforma de redes sociales, sitios del mercado negro y botnets. La solución debe hacer descubrimiento de datos filtrados en la dark web, incluidos archivos confidenciales, datos financieros/de tarjetas de crédito, PII, etc. La solución debe poder demostrar la capacidad de interactuar con actores en Dark Web y recopilar inteligencia a través de HUMINT La solución debe tener la habilidad de pivotar hacia la inteligencia en términos de varios filtros tales como: - Nombre del adversario, - Motivación adversaria, - Industria de destino, - Geografía objetivo - Tipos de informes, - Calificaciones de relevancia La solución debe tener capacidad para producir informes de alerta temprana basados en ataques iniciales y futuros y nuevos TTP La solución debe tener capacidad para informar exclusivamente sobre ataques de Ransomware y TTP relacionados. La solución debe tener capacidad para realizar una investigación inicial dentro del sistema utilizando enriquecimientos en tiempo real para buscar IOC La solución debe tener la capacidad de seguimiento y monitoreo de marca como: - Detectar credenciales violadas, es decir, correos electrónicos. (En caso de clientes Bancarios también se pueden incluir los datos de la Tarjeta) - Monitorear posibles infecciones de Stearler Infection - Identifique las credenciales filtradas que están disponibles en la dark web - Identificar la fuente de la violación de datos (incluidos terceros) - Detectar información filtrada y datos confidenciales - Capacidad de monitorear al Cliente como marca para cualquier ataque de phishing inminente - Hacer detección de sitios de phishing mediante el uso de marcas de agua digitales. - Identificar la dirección IP y los correos electrónicos de los usuarios phishing a través de campañas de phishing - Capacidad de identificar dominios similares basados en el uso del logo de la marca - Capacidad para identificar nombres de dominio de apariencia similar que coincidan estrechamente con el Cliente - Identificar informacion alojada en Buckets de internet tales como AWS S3, Azure, Digital Ocean, entre otros - Identificar codigo fuente con informacion sensible en repositorios de codigo tales como GitHub - Realizar monitoreo de VIP, donde se evaluen meciones tales como menciones en telegram, en darknet, en stealer infections y dox sites - Evaluacion de riesgos de Proveedores, donde se debera evaluar, nivel de riesgo dle proveedor, superficie de ataques del proveedor, menciones en la darknet del proveedor, brechas de seguridad del proveedor, incidentes de ransomware del proveedor, distribucion geografica de activos del proveedor, etc - Servicio de eliminación: eliminación de contenido sospechoso (sitios/perfil/etc.) La solución debe hacer exposición y escaneo de Shadow IT: escaneos de puertos, dispositivos mal configurados, escaneos de certificados SSL, etc.	

Scanned with CamScanner

La solución debe tener soporte para categorizar los hallazgos de inteligencia de amenazas a través de MITRE ATT&CK Framework, etc. La solución debe mostrar vulnerabilidades o configuraciones incorrectas del servidor (nube/en premisas) La solución debe contar con informes de activos vulnerables y activos de shadow IT La solución deberá tener integración con proveedores de nube pública para la identificación de activos La solución debe tener la capacidad para escanear y monitorear la infraestructura de Internet del Cliente para: - Identificación de Activos - Identificar el cambio en los activos frente a Internet - Identificación de Cambios en Puertos abiertos - Identificar cualquier certificado SSL caducado o a punto de caducar La solución debe tener las siguientes características de administración: Debe tener funciones para analizar e investigar los IOC a pedido, como búsquedas de reputación de IP/Dominio/Hash/CVE para varios parámetros, como - Información básica - Búsqueda de listas negras - Ubicación geográfica - Información de la red - Informes de inteligencia previos La plataforma debe tener características para integrarse con plataformas de colaboración como Microsoft Teams o Slack para el envío de notificaciones La plataforma debe tener funciones para proporcionar acceso basado en roles, alertas personalizadas, alertas de flash, etc. Debe tener la capacidad de proporcionar analista y reportes por demanda para cualquier requerimiento de aclaración e investigación personalizada La solución debe poder ser administrada vía portal Web y vía API Rest La solución deberá disponibilizar toda la información vía API REST con la intención de que la empresa pueda tener capacidades de SecOps incluyendo la superficie de ataque externa, Inteligencia de amenzas centradas en el advesario y protección de marca. La solución deberá ser 100% SaaS, por lo que no se debe requerir la implementación de Hadrware para su puesta en producción Menú tipo dropdown para navegar por la información Mostrar los orígenes del tráfico o usuarios que generan tráfico. Interface gráfica de usuario (GUI), vía Web por HTTPS e interfaz de línea de comando (CLI) para hacer administración de la solución, ya sea de manera centralizada o descentralizada en cada dispositivo. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones que pueden modificar o visualizar. La solucion debe tener la capacidad de crear reglas tipo ZTNA para permitir o denegar accesos con base a cumplimiento La solucion debe tener la capacidad de crear reglas con base a TAGS Los equipos deben ser capaces de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, prevención de Fuga de Información, Antivirus e IPS. Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la Compañia. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS y FTPS. El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión. Debe ser posible seleccionar el sistema operativo, protocolo, severidad y objetivo para la configuración de perfiles IPS. Debe ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv4 e IPv6. Debe basarse en categorías de aplicaciones que permitan seleccionar grupos de firmas basados en un tipo de categoría. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. Autenticación basada en contraseña y en doble factor de autenticación (certificado, correo, SMS y tokens). Las soluciones deben estar en capacidad de integrarse con el Directorio Activo de la Organización. Soporte de VPNs IPSec sitio a sitio y cliente – sitio. Soporte para IKEv2 e IKE Configuration Method Soporte de VPNs con algoritmos de cifrado: AES256, AES192, AES128. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5, 14, 21 y 32.	

Scanned with CamScanner

EL proponente deberá entregar Datsheet o ficha técnica que permita validar el cumplimiento de la solución ofertada.	
Se otorgarán veinte (20) puntos al contratista que ofrezca sin costo adicional para la entidad 10 licencias para el doble factor de autenticación para usar las VPN generando seguridad para la entidad de la misma marca fortinet.	
TOTAL, PUNTOS PONDERABLES	

CONTRATANTE

CF CLAUDIA PATRICIA PEREZ RODRIGUEZ
No. 22.732.677 expedida en Barranquilla
Jefe Departamento Administrativo y Ordenadora del Gasto
Escuela Superior de Guerra "General Rafael Reyes Prieto"

POR EL CONTRATISTA,

JESUS ALBERTO FRANCO ACOSTA
CC No. C.E No. 582410 de Venezuela
Representante legal de HEIMCORE S.A.S
900425697-2

MY. GISELLE LORENA ROMERO CARO
Jefe Sección Contratos

ING YESSID CACERES
Comité técnico Evaluador

PS. MARTHA CECILIA ULLOA CORTEZ
Integrante Comité Jurídico

PS. MARCELA ZABALETA IDARRAGA
Comité Jurídico Evaluador

PS. ZULMA COBOS CHICO
Integrante Económico Comité Evaluador

TC JULIAN JAIMES DELGADO
Gerente de proyecto

Archivado en: 15103.12.3 Contratos de Bienes y Servicios 2026

Scanned with CamScanner