COMANDO GENERAL
FUERZAS MILITARES DE COLOMBIA
UNIÓN - INTEGRIDAD - VICTORIA

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"

ADENDA No. 002
(5 DE AGOSTO DE 2026)

En uso de las facultades constitucionales y legales y en particular de las conferidas por el artículo 12 de la Ley 80 de 1993, Ley 1150 de 2007, Decreto 1082 de 2015, Resolución 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 destino al Ministerio de Defensa Nacional, unas funciones de carácter administrativo y se dictan otras disposiciones", Resolución No. 043 de 27 de marzo de 2025, expedida por el señor Comandante General de las Fuerzas Militares y demás normas reglamentarias, emanada del Ministerio de Defensa Nacional, en calidad de competente contractual delegado, teniendo en cuenta las observaciones presentadas dentro del traslado de la invitación, y conforme las consideraciones expuestas en el formulario de preguntas y respuestas del 5 de agosto de 2026, la administración procede a generar la presente adenda No. 2, en los siguientes términos:

PRIMERO: Modifíquese parcialmente numeral **2.3.1.3 ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO A ADQUIRIR,** en los numerales 1.1 y 1.2 el cual quedara así:

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.

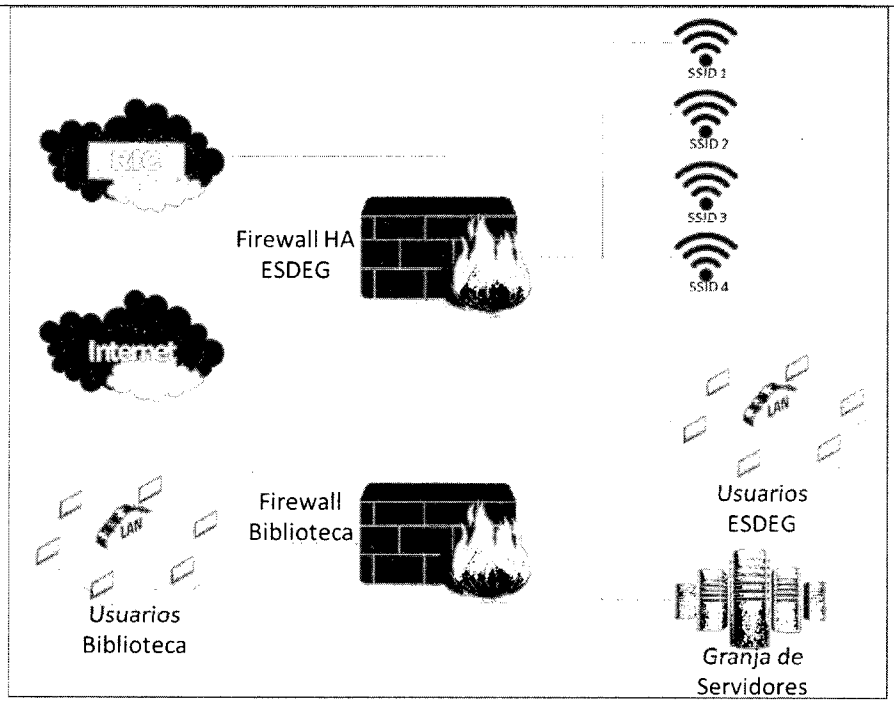
SEGUNDO: Modifíquese parcialmente numeral 2.3.1.4. ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO, en el ítem 1.34 y 5.1 literal b, el cual quedara así:

2.3.1.4. ESPECIFICACIONES TÉCNICAS DE OBLIGATORIO CUMPLIMIENTO

ITEM	ESPECIFICACIONES TECNICAS MINIMAS
1	**RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO 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: • 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.
1.5	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 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, 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, 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: 1. 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. 2. Verificar la configuración de las interfaces físicas, para que se optimice el uso de los puertos operativos de cada uno de los equipos instalados. 3. Garantizar y hacer pruebas de la infraestructura en alta disponibilidad que tiene configurada la escuela en el Firewall. 4. Realizar la evaluación y verificación de las reglas de filtrado configuradas en los equipos de aseguramiento Firewall. 5. 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. 6. Apoyar los procesos de gestión para optimizar el empleo de los canales de conectividad "internet" para cada uno de los segmentos. 7. Verificar que la plataforma de aseguramiento tecnológico permita la conectividad de la red, com mínimo con las siguientes características:

<table>
<tr>
<td></td>
<td>


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.
</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>1.36</td>
<td>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.</td>
</tr>
</table>

- 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 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 RENOVACIÓN DE LICENCIAMIENTO Y SOPORTE TÉCNICO 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. 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.
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.
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.
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
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:** 1. Primera capacitación en instalación, uso y administración de la herramienta Firewall y Fortianalyzer. 2. 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 Afinamiento Alta disponibilidad Excepciones Bloqueo de puertos Actualización de colectores Usuarios Grupos Debbuging **Nota:** 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.**

SEGUNDO: Modifíquese parcialmente numeral 3.1 FACTORES TÉCNICOS DE PONDERACIÓN – OPCIONAL-CONSOLIDADO FINAL, el cual quedara así:

CRITERIOS DE PONDERACIÓN			
		DESCRIPCIÓN	**PUNTAJE POR ASIGNAR**
Factor No. 1	**PONDERACIÓN TÉCNICA**	Se otorgarán veinte (20) 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. 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.	20

		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. 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. EL proponente deberá entregar Datsheet o ficha técnica que permita validar el cumplimiento de la solución ofertada.	
		Se otorgarán trece (13) 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.	13

Factor No. 2	**PONDERACIÓN ECONÓMICA**	Conforme se indicó en el pliego de condiciones (TRM)	50
TOTAL, PUNTAJE			83
Factor No. 3	**INDUSTRIA NACIONAL (LEY 816/03)**	Para aquellas propuestas presentadas por nacionales o extranjeros con trato nacional, que se encuentran enmarcados en el Artículo 1 del Decreto 680 de 2021 y se comprometa a que en el curso de la ejecución todo empleado o contratista sea colombiano y de aquellos países en los cuales a las ofertas de bienes y servicios colombianos se les conceda el mismo tratamiento otorgado a sus bienes y servicios nacionales.	16,6
		Para aquellas propuestas presentadas por oferentes extranjeros sin trato nacional de acuerdo con lo definido en el Artículo 1 del Decreto 680 de 2021, que se comprometa a que en el curso de la ejecución del contrato por lo menos el 40% de sus empleados o contratistas sean colombianos.	8,3
		Para aquellas propuestas presentadas en las cuales más del 60% de empleados o contratistas para la ejecución se encuentra integrado por personas de nacionalidad extranjera y más del 60% bienes necesarios para la ejecución no sean de producción nacional.	0
PUNTAJE TOTAL CALIFICACIÓN (MÁXIMO)		**PONDERACIÓN ECONÓMICA + PONDERACIÓN TÉCNICA + APLICACIÓN LEY 816/03**	**99,6**
PUNTAJE ADICIONAL (VERIFICACIÓN JURÍDICA) *		Cumplimiento Mipyme para puntaje adicional	0,20
		Cumplimiento emprendimiento y empresa de mujeres para puntaje adicional	0,20
REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS: -2 %		En cumplimiento del Artículo 58 de la Ley 2195 de 2022 (CUANDO APLIQUE)	-2
PUNTAJE TOTAL CALIFICACIÓN (MÁXIMO A OBTENER)			**100**

TERCERO: Los demás aspectos del proceso No. **126-MDN-COGFM-ESDEG-2026**, que no hayan sido modificados continúan vigentes y son de obligatorio cumplimiento.

CF. **CLAUDIA PATRICIA PÉREZ RODRIGUEZ**
Jefe Departamento Administrativo y Ordenador del Gasto
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Elaboró: PS MARTHA CECILIA JULIO CORTEZ
Comité Jurídico

Reviso:

TE. ENRIQUE RAMIREZ FLOR
Comité Técnico Estructurador

MY LORENA ROMERO CANO
Jefe Sección de Contratos

PS. ANDRES HERNANDEZ FANDIÑO
Estructurador Económico