I. FECHA DEL ESTUDIO PREVIO.

AGOSTO DE 2025

II. DEPENDENCIA SOLICITANTE

DEPARTAMENTO CONJUNTO DE COMUNICACIONES - CGDJ6 DEL COGFM.

III. DESCRIPCIÓN DE LA NECESIDAD.

Antecedentes:

Los avances en informática e internet han transformado el panorama global, eliminando las fronteras entre países y utilizando el espectro electromagnético para la transmisión de datos e información a altas velocidades. Esta interconexión ha generado una dependencia constante de la tecnología, aumentando la exposición a riesgos cibernéticos que buscan vulnerar infraestructuras críticas.

Las Fuerzas Armadas han tenido que adaptarse a este nuevo contexto, donde las amenazas ya no solo provienen del campo físico, sino también del ámbito virtual. Esto ha implicado un ajuste en las políticas y estrategias de seguridad, especialmente en la protección de redes y sistemas informáticos. En Colombia, las Fuerzas Militares han dado prioridad a esta adaptación sin descuidar los desafíos internos.

En este contexto, la seguridad perimetral, y en particular el uso de firewalls se ha vuelto esencial para proteger la infraestructura tecnológica del Comando General de las Fuerzas Militares. Las herramientas de seguridad, como los firewalls, actúan como una barrera de protección que filtra el tráfico entrante y saliente, bloqueando accesos no autorizados y resguardando los sistemas ante posibles ciberamenazas.

Aunque el Comando General de las Fuerzas Militares ya dispone de estas herramientas, es necesario fortalecerlas continuamente, ya que tanto la tecnología como las amenazas cibernéticas avanzan rápidamente. La seguridad perimetral debe mantenerse actualizada para enfrentar nuevas vulnerabilidades, asegurando la confidencialidad, integridad y disponibilidad de la información institucional.

El constante desarrollo tecnológico ha incrementado la sofisticación de las amenazas, que incluyen intentos de infiltración por parte de actores malintencionados. Los firewalls deben adaptarse y reforzarse frente a nuevas tácticas utilizadas para comprometer la infraestructura tecnológica, protegiendo la información sensible y evitando el acceso no autorizado a sistemas estratégicos.

El ciberespacio se ha convertido en una plataforma empleada por grupos ilegales para llevar a cabo actividades delictivas, como terrorismo, narcotráfico y espionaje, lo que representa un riesgo para la seguridad nacional. Por ello, la seguridad perimetral, especialmente a través de firewalls avanzados, es crucial para enfrentar estas amenazas y salvaguardar la integridad de las Fuerzas Militares.

La evolución de los riesgos cibernéticos requiere que las herramientas de seguridad perimetral del COGFM sean actualizadas y fortalecidas de manera constante, garantizando la protección ante nuevas formas de ataque y asegurando la continuidad operativa de la institución. Esto implica contar no solo con firewalls robustos, sino también con estrategias que permitan adaptarse rápidamente a las amenazas emergentes.

El correo electrónico sigue siendo una de las principales vías de comunicación, pero también es uno de los canales más explotados por los ciberdelincuentes y los anunciantes no deseados. Según diversos estudios, el 50-60% de los correos electrónicos que se envían a diario son spam. Al reducir el spam y los correos no deseados, se puede garantizar que los correos legítimos sean entregados de manera eficiente. Esto es crucial ya que los retrasos o la pérdida de correos importantes pueden resultar en problemas legales para la entidad. Las organizaciones deben estar preparadas para gestionar esta avalancha de mensajes. El uso de spam para ejecutar fraudes o hacer daño a la reputación de las organizaciones es una amenaza constante, las herramientas antispam también ayudan a reducir el riesgo de que los funcionarios caigan en estafas que puedan perjudicar tanto a la empresa como a su imagen.

Actualmente, el COGFM cuenta con diversas soluciones de seguridad, con un enfoque prioritario en la seguridad y disponibilidad de los servicios y por lo tanto requieren de un mecanismo que permita fortalecer la red y la gestión centralizada de los servicios expuestos. En este contexto, la seguridad para el Correo Electrónico Institucional es una necesidad crítica para garantizar que la infraestructura digital del COGFM continúe operando bajo los más altos estándares de ciberseguridad.

El Comando General de las Fuerzas Militares enfrenta desafíos crecientes en la gestión de seguridad para el acceso remoto a sistemas críticos desde dispositivos móviles. La digitalización de las operaciones y el uso extendido de tablets y smartphones han expuesto la necesidad de adoptar una solución que garantice la

protección de la información sin comprometer la movilidad y la operatividad de los usuarios. Actualmente, la organización no cuenta con un sistema de Acceso a la Red de Confianza Cero (ZTNA), lo que genera riesgos en la integridad y confidencialidad de los datos estratégicos.

La falta de un modelo de seguridad basado en Zero Trust ha generado vulnerabilidades significativas, aumentando la exposición del Comando a accesos no autorizados, suplantaciones de identidad y ataques dirigidos a dispositivos móviles. En un entorno donde la conectividad remota es esencial para las operaciones militares, la ausencia de una solución ZTNA amplifica los riesgos asociados con el acceso a redes externas, dejando la información institucional susceptible a ataques de phishing móvil, malware dirigido y exfiltración de datos sensibles.

El acceso a aplicaciones alojadas en el DataCenter on-premise se realiza sin una validación continua de identidad ni segmentación avanzada de accesos, lo que incrementa la posibilidad de accesos indebidos y movimientos laterales dentro de la red. La falta de controles específicos para dispositivos móviles expone a la organización a amenazas avanzadas que comprometen la seguridad de los datos, afectando la toma de decisiones estratégicas y la operatividad de las Fuerzas Militares.

El modelo de seguridad basado en perímetro ha demostrado ser insuficiente ante las exigencias actuales de protección en entornos móviles. La necesidad de aplicar controles granulares sobre los accesos y un monitoreo continuo de la actividad en los dispositivos conectados se ha convertido en un requisito crítico para garantizar la seguridad y confidencialidad de la información institucional. Sin una solución ZTNA optimizada para dispositivos móviles, el Comando General de las Fuerzas Militares enfrenta una creciente exposición a ciberamenazas que pueden comprometer la integridad de sus activos digitales y afectar la eficacia operativa de sus misiones estratégicas.

La implementación de una solución de Acceso a la Red de Confianza Cero permitiría minimizar los riesgos asociados al acceso remoto desde dispositivos móviles, garantizando un control estricto sobre la autenticación de usuarios, la segmentación de acceso y la visibilidad del tráfico. Esto facilitaría la adopción de mecanismos de seguridad adaptativa, alineando la infraestructura del Comando con estándares internacionales de ciberseguridad y asegurando una gestión eficiente y resiliente ante escenarios de riesgo cibernético.

El Departamento Conjunto de Comunicaciones del Comando General de las Fuerzas Militares tiene a su cargo la administración de la Red Integrada de Comunicaciones (RIC), considerada uno de los activos más estratégicos y valiosos del sector defensa colombiano. Esta red constituye la columna vertebral tecnológica para el mando y control de las operaciones militares, tanto de forma individual por cada Fuerza como en acciones conjuntas, en cumplimiento de su misión constitucional de defensa de la soberanía, la integridad territorial y el orden institucional.

La RIC integra el Sistema de Comunicaciones Unificadas, una plataforma robusta que proporciona servicios de videoconferencia con disponibilidad 24/7, permitiendo una comunicación segura, continua y de alta calidad. Este servicio está disponible para entidades como:

- El Ministerio de Defensa Nacional
- Las Fuerzas Militares de Colombia (Ejército Nacional, Armada Nacional y fuerza aeroespacial Colombiana).
- Agregados militares acreditados en el país
- Entidades internacionales como la OTAN y el Comando Sur de los Estados Unidos.

Gracias a esta infraestructura, se eliminan los costos logísticos asociados a desplazamientos, viáticos y tiempos improductivos, optimizando la coordinación operativa y administrativa. Además, se fortalece la capacidad de respuesta ante situaciones críticas, se mejora la interoperabilidad con aliados estratégicos y se garantiza la continuidad del mando en escenarios de alta exigencia.

La confiabilidad, seguridad y disponibilidad de la RIC la posicionan como una herramienta esencial para la defensa nacional, alineada con los más altos estándares internacionales en comunicaciones de misión crítica.

Siendo usuarios de la Red Integrada de Comunicaciones (RIC) del Comando General de las Fuerzas Militares las siguientes entidades:

- **Unidades militares** del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.
- **Policía Nacional de Colombia**.
- **Grupo Social y Empresarial del Sector Defensa (GSED)**.
- **Entidades civiles** como la Aeronáutica Civil, gobernaciones, alcaldías y otras instituciones del Estado.
- **Medios públicos** como Radio Televisión Nacional de Colombia (RTVC).

Estas entidades se benefician de los servicios de la RIC, que incluyen **comunicaciones de voz, datos y videoconferencias**, a través de medios de transmisión seguros y eficientes. Dichos servicios se prestan **sin actividades de tarifación ni facturación**, lo que garantiza una comunicación continua, estratégica y sin restricciones económicas entre los actores clave del sector defensa y otras entidades del Estado.

Actualmente, el Comando General de las Fuerzas Militares dispone de equipos de videoconferencia (Cámaras Cisco Room Kit Mini), asignados a las distintas Fuerzas (Ejército Nacional, Armada Nacional y Fuerza Aérea Colombiana), así como a jefaturas, subjefaturas y departamentos que requieren interacción mediante videoconferencia segura. Esta capacidad es provista por el Sistema de Comunicaciones Unificadas del Departamento Conjunto de Comunicaciones (CGDJ6).

- LOTE 1: LICENCIAS FIREWALL + VPN.

Definición de la necesidad:

La plataforma de seguridad perimetral Firewall del Comando General de las Fuerzas Militares, adquirida en 2016, ha sido esencial para proteger la infraestructura tecnológica y la información clasificada. Sin embargo, el avance de las amenazas cibernéticas requiere su renovación y actualización para enfrentar nuevos riesgos.

Actualizar esta solución es clave para mitigar riesgos y garantizar protección frente a amenazas actuales, mejorando la capacidad de respuesta ante incidentes futuros. Además, es necesario renovar el licenciamiento del firewall + VPN y contratar el servicio de garantía para asegurar la continuidad operativa.

El uso de tecnologías como inteligencia artificial y big data por actores malintencionados ha incrementado la sofisticación de los ataques cibernéticos, lo que hace urgente la actualización del firewall. La creciente conectividad y el uso de tecnologías emergentes amplían las superficies de ataque, reforzando la necesidad de fortalecer la seguridad perimetral.

En resumen, estas actualizaciones son vitales para mantener una postura de seguridad cibernética efectiva y proteger los activos digitales del COGFM en un entorno tecnológico en constante cambio.

La preocupación actual de las Fuerzas Militares está enfocada en buscar los métodos adecuados para implementar una cultura organizacional relacionada con el uso y la prevención y empleo de las herramientas informáticas que le permitan minimizar los riesgos ante los ataques ocasionados por la inseguridad informática y el crimen cibernético, motivo por el cual es necesario proponer alternativas de prevención ante el ciberterrorismo y los ciberataques en esta Institución.

Por lo anterior el Comando General de las Fuerzas Militares en cumplimiento de su misión institucional y con el fin de facilitar la consecución de su gestión, cuenta con herramientas de seguridad informática las cuales a la fecha han brindado protección a la infraestructura tecnológica del Comando General de las Fuerzas Militares. No obstante, y teniendo en cuenta el tiempo en servicio de estas herramientas y que la tecnología, junto con sus vulnerabilidades avanza a pasos agigantados, es necesario fortalecer la plataforma de seguridad informática del COGFM con el fin de minimizar los riesgos de ocurrencia de eventos y/o incidentes de seguridad informática así mismo preservar los tres pilares fundamentales de la información que son:

- La Confidencialidad
- La Integridad
- La Disponibilidad

Los avances tecnológicos a nivel de la información han requerido que día a día se implementen esquemas más fuertes de seguridad para proteger la información institucional de amenazas cada vez más especializadas, como los ataques de piratas informáticos y ataques denegación de servicios entre otros; los cuales causan traumatismos considerables no sólo en el intercambio de información, sino también en detrimento de la imagen institucional en caso de que se logre vulnerar la infraestructura tecnológica de la institución.

El empleo de Internet y de las herramientas tecnológicas especializadas, les permiten a los grupos al margen de la ley el aprovechamiento del ciberespacio para el desarrollo de posibles amenazas (delictivas, terrorismo, espionaje) y/o que constituyen un riesgo de la seguridad y desarrollo Nacional, entre otras, consolidándose en una amenaza potencial externa e interna. Este escenario de guerra es utilizado, como la plataforma de coordinación, difusión y ataque por parte de las amenazas actuales y futuras para realizar acciones de narcotráfico, terrorismo, espionaje, trata de personas, comercialización robo de secretos de estado, desinformación o grupos que delinquen en forma transnacional.

Las amenazas constituyen un riesgo a la Seguridad y Defensa Nacional y a todos los intereses que Corresponden al Comando General de las Fuerzas Militares. La realización de actividades y operaciones

especializadas de la Jefatura de Comunicaciones y Tecnologías de la información para proteger y enfrentar las amenazas, retos y objetivos a través del ciberespacio, son insuficientes comparadas con los riegos actuales, teniendo en cuenta la evolución permanente y el desarrollo de factores potenciales de amenazas externas.

- LOTE 2: LICENCIAS PROXY WEB.

Definición de la necesidad:

La renovación de las licencias de Proxy Web es esencial para controlar y monitorear el tráfico web, filtrando contenido malicioso y restringiendo el acceso a sitios no autorizados.

Por otra parte el Analizador de eventos del proxy es fundamental para la recopilación, análisis y correlación de registros y eventos de seguridad, permitiendo una visibilidad detallada del tráfico de red y el comportamiento de los usuarios. Su importancia radica en la capacidad de centralizar logs, generar informes personalizados y detectar anomalías en tiempo real, facilitando la toma de decisiones y el cumplimiento de normativas de seguridad. Además, ayuda a identificar patrones de amenazas, mejorar la respuesta ante incidentes y optimizar las políticas de seguridad mediante análisis forense, proporcionando una gestión eficiente y proactiva de la infraestructura de ciberseguridad.

El proxy permite la creación de reglas o políticas, administradas por los siguientes perfiles.

Perfil de Antivirus (AntiVirus Profile) herramienta esencial para la seguridad de la red, ya que protege contra malware, troyanos, spyware y otras amenazas al analizar en tiempo real los archivos transmitidos a través del proxy. Su importancia radica en la detección y bloqueo de contenido malicioso antes de que llegue a los dispositivos finales, minimizando riesgos de infección. Utiliza bases de datos de firmas de malware actualizadas y análisis heurístico para identificar amenazas nuevas o desconocidas. Además, permite inspeccionar tráfico cifrado (SSL/TLS) para detectar archivos peligrosos ocultos en conexiones seguras, fortaleciendo la seguridad sin comprometer el rendimiento de la red.

Perfil de Filtro Web (Web Filter) es una función clave para controlar y proteger el acceso a sitios web dentro de la red, permitiendo bloquear contenido malicioso, restringir el acceso a categorías no deseadas y prevenir ataques basados en la web. Su importancia radica en la capacidad de aplicar políticas de navegación según usuarios, grupos o dispositivos, asegurando cumplimiento normativo y mejorando la productividad al evitar distracciones. Además, contribuye a la seguridad al impedir el acceso a sitios de phishing, malware y contenido inapropiado, utilizando bases de datos constantemente actualizadas y filtrado dinámico basado en reputación.

Perfil de Control de Aplicaciones (Application Control) es fundamental para gestionar y supervisar el uso de aplicaciones dentro de la red, permitiendo restringir, priorizar o bloquear programas y servicios no autorizados que puedan comprometer la seguridad o el rendimiento. Su importancia radica en la capacidad de prevenir el uso de aplicaciones de alto riesgo, como proxies anónimos, redes P2P o herramientas de evasión, reduciendo la exposición a amenazas y fugas de datos. Además, mejora la productividad al limitar el acceso a aplicaciones no esenciales y de esta manera, optimiza el ancho de banda al controlar el tráfico generado por aplicaciones de alto consumo.

Perfil de Prevención de Intrusiones (IPS - Intrusion Prevention System) es esencial para la detección y mitigación de ataques en la red, ya que analiza el tráfico en busca de patrones maliciosos y vulnerabilidades explotables. Su importancia radica en la capacidad de identificar y bloquear intentos de intrusión, como ataques de fuerza bruta, exploits de software y tráfico anómalo, antes de que afecten los sistemas. Además, utiliza firmas actualizadas y técnicas de detección heurística para proteger contra amenazas emergentes, reduciendo el riesgo de compromisos de seguridad y fortaleciendo la postura defensiva de la organización sin afectar el rendimiento de la red.

Perfil de Inspección SSL (SSL Inspection) es crucial para analizar el tráfico cifrado y detectar amenazas ocultas en conexiones seguras sin comprometer la privacidad ni el rendimiento. Su importancia radica en la capacidad de interceptar y desencriptar comunicaciones HTTPS, inspeccionando contenido en busca de malware, ataques de phishing y otras amenazas que podrían evadir los controles de seguridad tradicionales. Además, permite aplicar políticas de acceso y filtrado a sitios web cifrados, garantizando el cumplimiento normativo y la protección de datos sensibles, al tiempo que optimiza la seguridad de la red al evitar el tráfico malicioso que usa cifrado como método de ocultación.

En resumen, la renovación del proxy web es esencial para mantener la robustez y la efectividad de la postura de seguridad cibernética del Comando General de las Fuerzas Militares, asegurando así la protección continua de sus activos digitales y la capacidad para cumplir con sus responsabilidades operativas y estratégicas.

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

Definición de la necesidad:

La ciberseguridad tradicional implementa una variedad de herramientas independientes para cada vector de ataque, como son: antivirus, detección y respuesta de endpoints, búsqueda de amenazas, inteligencia de amenazas, etc. Este funcionamiento genera una complejidad al interior de un SOC, quienes se ven obligados a invertir una cantidad significativa de tiempo en la administración y correlación de datos provenientes de múltiples fuentes diferentes.

Sin embargo, con los avances tecnológicos se han permitido optimizar esta complejidad y realizar una protección contra amenazas mediante la integración de varias capacidades en una sola herramienta de ciberseguridad la cual se basa en comportamientos y no en firmas. Este avance en la industria de ciberseguridad facilita el análisis de amenazas y ayuda a una defensa eficiente y efectiva. Por ello, la Dirección de Tecnologías de la Información del Departamento Conjunto de Comunicaciones, requiere una herramienta de protección de datos que integre las siguientes capacidades en un solo sensor para ser instalado en todos los equipos de cómputo institucionales del Comando General de las Fuerzas Militares así:

- Antivirus
- Detección y respuesta de endpoints
- Búsqueda de amenazas
- Inteligencia de amenazas
- Protección de datos
- Cacería de Amenazas administradas
- Control de acceso de dispositivos
- Telemetría y almacenamiento para el análisis de incidentes
- Protección de Amenazas sobre la identidad
- Descubrimiento de los Activos en la Red
- Firewall Management
- Repositorios y Almacenamiento de Logs

Actualmente, la integración de un único agente de ciberseguridad optimiza la eficiencia de los equipos de cómputo en una institución, especialmente las limitaciones en los recursos tecnológicos disponibles. Esta solución integrada no solo mejora el rendimiento, sino que también garantiza la detección efectiva de infracciones, ransomware y ataques cibernéticos. Es importante destacar que esta solución incorpora tecnologías avanzadas de Machine Learning e Inteligencia Artificial, esto significa que la protección de los activos tecnológicos de la institución no dependerá exclusivamente de las firmas de actualización tradicionales, en lugar de eso, el sistema actuará de forma proactiva y efectiva ante comportamientos anómalos, ofreciendo una defensa robusta contra amenazas emergentes.

En resumen, la suscripción de herramientas de seguridad informática es esencial para mantener la robustez y la efectividad de la postura de seguridad cibernética del Comando General de las Fuerzas Militares, asegurando así la protección continua de sus activos digitales y la capacidad para cumplir con sus responsabilidades operativas y estratégicas.

Basado en lo anterior se requiere realizar un proceso de contratación para la "SUSCRIPCIÓN E IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA HERRAMIENTA PARA LA PROTECCIÓN DATOS PARA EL COMANDO GENERAL DE LAS FUERZAS MILITARES; de acuerdo con la descripción, requisitos, especificaciones y demás condiciones las cuales se describen en la especificación técnicas del anexo

Los avances tecnológicos han transformado los escenarios de guerra, con la ciberdelincuencia y el ciberterrorismo surgiendo como nuevas amenazas críticas. En este contexto, es crucial para el Comando General de las Fuerzas Militares adaptarse y fortalecer sus capacidades en seguridad informática. La adquisición de herramientas para protección de datos no solo garantiza dicha protección contra ciberamenazas en constante evolución, sino que también salvaguarda la integridad de las operaciones militares en un entorno digital cada vez más complejo y dinámico.

Las últimas tendencias tecnológicas, como la inteligencia artificial, el aprendizaje automático y el análisis de big data, están siendo aprovechadas tanto por actores estatales como no estatales para perpetrar ataques cibernéticos sofisticados. En este sentido, la actualización de las herramientas de seguridad informática del Comando General de las Fuerzas Militares es esencial para mantenerse al día con estas amenazas emergentes y proteger proactivamente sus activos digitales.

Además, con el aumento de la conectividad y la adopción de tecnologías emergentes como el Internet de las cosas (IoT) y el cómputo en la nube, se amplían las superficies de ataque potenciales y se multiplican los puntos de vulnerabilidad en la infraestructura digital. La adquisición de herramientas de seguridad proporciona una defensa robusta y adaptable contra estas amenazas, asegurando la continuidad operativa y protegiendo la integridad de los datos críticos del Comando General de las Fuerzas Militares.

En resumen, estas herramientas son indispensables para mantener la efectividad de la postura de seguridad cibernética del Comando General de las Fuerzas Militares en un entorno tecnológico en constante evolución, y para proteger proactivamente sus activos digitales de las amenazas emergentes en el ciberespacio.

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

Definición de la necesidad:

El Comando General de las Fuerzas Militares requiere la suscripción de una Herramienta de filtrado y protección de Correo (Antispam) para proporcionar una capa esencial de seguridad a todas las aplicaciones de su red. Este software controla la entrada y salida de información, monitorea ciberamenazas, y gestiona el acceso a internet y aplicativos por diferentes puertos, facilitando la identificación, estudio, neutralización y contraataque de amenazas informáticas generadas a través del ciberespacio.

Con esta suscripción se garantiza la protección de todas las cuentas de correo del COGFM, incluyendo herramientas fundamentales para salvaguardar la integridad, confidencialidad y disponibilidad de la información crítica y los recursos digitales de la institución realizando el filtrado y bloqueo de correos no deseados y potencialmente peligrosos.

Además, la suscripción, garantía y soporte de este tipo de herramientas en el área de seguridad informática del Comando General de las Fuerzas Militares es imprescindible para asegurar el acceso continuo a actualizaciones críticas de software y parches de seguridad, garantizando así la estabilidad y la protección de los sistemas contra posibles vulnerabilidades, y asegurando la continuidad operativa de las funciones críticas de seguridad informática del Comando.

El Comando General de las Fuerzas Militares debe contar con herramientas de seguridad informática debido a la naturaleza crítica y sensible de la información que manejan y la necesidad de salvaguardarla de posibles amenazas y ataques cibernéticos.

Aquí hay algunas razones clave para implementar estas medidas de filtrado y protección de correo electrónico:

1. **Protección contra amenazas externas:** Las entidades de defensa nacional pueden ser blanco de ataques cibernéticos provenientes de actores maliciosos, como hackers, grupos terroristas o países hostiles. Las herramientas de protección de correo ayudan a detectar y bloquear intentos no autorizados de acceder a la red desde el exterior.

2. **Seguridad de información clasificada:** Las redes de defensa nacional a menudo manejan información altamente clasificada y confidencial. Por lo cual se debe garantizar que solo las personas autorizadas puedan acceder a esta información, evitando fugas y filtraciones no deseadas.

3. **Detección de malware:** Los correos electrónicos spam pueden ser un vehículo para ataques de phishing, malware o ransomware. A menudo, los mensajes fraudulentos intentan engañar a los empleados para que hagan clic en enlaces maliciosos o descarguen archivos infectados. Esto pone en riesgo la seguridad de la información sensible, así como la integridad de los sistemas de TI de la entidad.

4. **Control de tráfico y políticas de seguridad:** Las soluciones de protección de correo electrónico permiten implementar políticas de seguridad específicas, como bloqueo o limitación de ciertos servicios, lo que ayuda a reducir la superficie de ataque y mejorar la seguridad general de la red.

5. **Respaldo de controles internos:** Aunque también es importante tener medidas de seguridad en la capa interna de la red, contar con una protección de correo sólida es una primera línea de defensa eficaz, reduciendo la exposición de la red a amenazas externas.

6. **Soporte técnico**: Las herramientas de protección de correo electrónico a menudo incluyen acceso a soporte técnico del fabricante. Si surgen problemas técnicos o preguntas, la entidad de defensa puede recibir asistencia oportuna y eficiente para resolver los problemas.

7. **Continuidad operativa:** son componentes críticos de la infraestructura de seguridad de la red de una entidad de defensa nacional. Su suscripción oportuna asegura que siga funcionando sin interrupciones, lo que es esencial para mantener la seguridad y la continuidad operativa.

- LOTE 5: SUSCRIPCIÓN WAF.

Definición de la necesidad:

El Comando General de las Fuerzas Militares cuenta actualmente con una solución de seguridad de aplicaciones web WAF (Web Application Firewall) on-premise, cuyo licenciamiento ha sido renovado anualmente para proteger los activos estratégicos, incluyendo aplicaciones web expuestas en internet, contra una amplia gama de ciberataques. Sin embargo, esta tecnología ha alcanzado el final de su vida útil dentro de la institución, lo que hace necesario un cambio estratégico hacia una solución más moderna, escalable y eficiente.

Con el constante avance tecnológico, las amenazas cibernéticas han evolucionado considerablemente, incrementando la frecuencia e intensidad de ataques como los DDoS (Distributed Denial of Service), que buscan saturar los servidores mediante tráfico masivo, afectando la disponibilidad de los sistemas. Además, ataques avanzados a la capa de aplicación, como inyección SQL (SQLi), cross-site scripting (XSS) y cross-site request forgery (CSRF), representan un riesgo significativo para la integridad y confidencialidad de los datos. Estos ataques se han vuelto más automatizados e inteligentes, haciendo insuficiente la protección de soluciones on-premise tradicionales.

Ante este panorama, la migración a una solución de seguridad en la nube representa la mejor alternativa para fortalecer la ciberseguridad institucional. Los WAF basados en la nube ofrecen múltiples ventajas sobre las soluciones locales, incluyendo escalabilidad automática para mitigar ataques volumétricos sin afectar el rendimiento, actualización constante de reglas de seguridad mediante inteligencia artificial, machine learning, y una infraestructura distribuida que reduce los puntos únicos de falla.

Además, los proveedores de seguridad en la nube cuentan con redes globales de distribución de tráfico (CDN) y sistemas avanzados de detección de amenazas en tiempo real, lo que permite una respuesta inmediata ante ataques emergentes. También facilitan la integración con plataformas de seguridad Zero Trust, protegiendo no solo las aplicaciones web, sino también accesos y comunicaciones dentro de la organización.

La adopción de un WAF en la nube reducirá la carga operativa y los costos asociados a la administración de infraestructura física, al tiempo que mejorará la capacidad de respuesta ante incidentes de seguridad. Adicionalmente reduce la superficie de ataque y minimiza nuevos vectores emergentes.

Esta transición garantizará una protección más robusta y dinámica para los sistemas estratégicos del Comando General de las Fuerzas Militares, asegurando su disponibilidad, integridad y resiliencia ante la creciente sofisticación de las amenazas cibernéticas.

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

Definición de la necesidad:

El Comando General de las Fuerzas Militares requiere fortalecer la seguridad en el acceso remoto a sus aplicaciones institucionales, especialmente desde dispositivos móviles. Actualmente, la organización no cuenta con una solución de Acceso a la Red de Confianza Cero (ZTNA) que garantice un acceso seguro y controlado a los sistemas alojados en su DataCenter on-premise, lo que expone a la institución a riesgos de accesos no autorizados, vulnerabilidades de autenticación y posibles brechas de seguridad.

Para mitigar estos riesgos, se hace necesaria la implementación de una solución que integre mecanismos avanzados de autenticación, segmentación de acceso y monitoreo continuo del tráfico. Este enfoque permitirá proteger los datos sensibles y evitar la fuga de información mediante controles que restrinjan la descarga, copia o compartición no autorizada de archivos desde dispositivos móviles. La aplicación de un modelo Zero Trust garantizará que cada acceso sea validado y monitoreado en tiempo real, eliminando privilegios implícitos y reforzando la seguridad en cada conexión.

La solución ZTNA deberá incorporar los siguientes elementos clave:

Autenticación adaptativa y multifactor, asegurando la validación continua de identidad a través de biometría, tokens dinámicos y políticas de acceso contextual.

Segmentación y microsegmentación de acceso, limitando la exposición de recursos críticos y previniendo movimientos laterales dentro de la red.

Monitoreo del tráfico móvil, con análisis en tiempo real para detectar anomalías y prevenir incidentes de seguridad.

Protección contra fuga de información, con restricciones sobre la descarga, copia y compartición de datos sensibles.

Seguridad en redes públicas y externas, mediante cifrado avanzado y mecanismos de protección contra ataques en conexiones no seguras.

La implementación de esta solución permitirá al Comando operar bajo un esquema de seguridad Zero Trust, mejorando la capacidad de respuesta ante amenazas dirigidas a dispositivos móviles y asegurando la continuidad operativa sin comprometer la confidencialidad de la información institucional. Además, alineará la infraestructura de seguridad con estándares internacionales de ciberseguridad, garantizando un acceso remoto seguro y eficiente en el entorno militar.

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

Definición de la necesidad:

El Departamento Conjunto de Comunicaciones del Comando General de las Fuerzas Militares tiene como objetivo implementar el licenciamiento del software Webex de forma nativa en los dispositivos Cisco Room Kit Mini, así como en una amplia gama de equipos móviles y de escritorio. Esta implementación contempla:

Dispositivos móviles: iPhone, iPad y equipos con sistema operativo Android.
Plataformas de escritorio: PC con Windows, Apple Mac, y Chromebook.
Navegadores web compatibles: Google Chrome, Mozilla Firefox, Apple Safari y Microsoft Edge, en sistemas operativos Windows, macOS y Linux.

Esta iniciativa es crucial debido a la necesidad de integrar Webex con la infraestructura actual de videoconferencia y telefonía, garantizando la interoperabilidad y continuidad del servicio. Además, cumple con estrictos estándares de seguridad y encriptación, lo que asegura comunicaciones protegidas y confiables.

La implementación del licenciamiento Webex permitirá:

- Optimizar el rendimiento de los equipos existentes.
- Ampliar las capacidades de comunicación y colaboración.
- Prevenir la obsolescencia tecnológica.
- Garantizar un servicio eficiente, seguro y de alta disponibilidad.

La necesidad previamente descrita y su respectivo presupuesto se encuentran dentro del Plan Anual de Adquisiciones para la vigencia 2025.

Perspectiva legal

Comercialmente está permitido y regulado por el Código de Comercio, por cuanto se establecen características especiales para el cumplimiento del objeto del presente proceso y son bienes y/o servicios que se encuentran en el mercado regulado por las normas de comercio colombiano. El MDN – Comando General Fuerzas Militares tiene la capacidad jurídica para adquirir estos bienes y/o servicios, ésta en capacidad de contraer derechos y obligaciones y hacerlos exigibles dentro del proceso.

Analizado el objeto del presente proceso, legalmente es viable, ya que el objeto que sustenta el desarrollo del proceso contractual es de carácter lícito, y desarrolla los preceptos que incorporan los artículos 1518 y 1519 del Código Civil, y la normatividad contractual, contribuye a la aplicación del principio de transparencia, establecido en el artículo 24 de la Ley 80 de 1993, además el objeto está conforme al desarrollo de los procesos y procedimientos que permiten en forma continua y eficiente el cumplimiento de la misión institucional, en satisfacción del interés general y la continua prestación del servicio.

En el régimen de contratación estatal colombiano (Ley 80 de 1993 y Decreto 1150 de 2007), establece que las entidades estatales deberán seleccionar los contratistas por norma general bajo las modalidades de Licitación Pública, entre otras Selección Abreviada, Subasta inversa electrónica o presencial, Concurso de Méritos y por Contratación Directa; aplicando en igual de condiciones los principios de transparencia, economía, responsabilidad, selección objetiva, buena fe, planeación, publicidad e igualdad, con el objeto de cumplir los fines propios de la Contratación Estatal. La aplicación de los principios en materia contractual va

más allá de la mera selección objetiva del contratista, es decir, los principios generales del derecho, los que hagan parte de la Constitución o de una ley, han de ser apreciados en todas las etapas de la contratación estatal y no solo en el momento de la selección del contratista. Es decir que, postulados como la buena fe, la prevalencia del interés general, el debido proceso, la transparencia y la responsabilidad, entre otros, deben ser desplegados en cada una de las etapas del trámite contractual. Desde el punto de vista legal se puede determinar cómo viable la realización del presente proceso contractual, toda vez que el objeto a desarrollar es lícito dado que no contraviene la normatividad vigente colombiana.

Al hablar del Contrato Estatal, el cual es definido como aquel que celebran las entidades estatales; en el que se busca el cumplimiento de los fines del Estado, la continua y eficiente prestación de los servicios públicos y la efectividad de los derechos e intereses de los administrados que colaboran por medio de relaciones contractuales no laborales con las entidades públicas en la consecución de tales fines. (Artículo 3° de la Ley 80 de 1993).

En desarrollo de lo señalado en los numerales 7 y 12 del artículo 25 de la Ley 80 de 1993, del Artículo 2.2.1.1.2.1.1 del Decreto 1082 del 26 de mayo de 2015, los estudios y documentos previos estarán conformados por los documentos definitivos que sirvan de soporte para la elaboración del contrato, de manera que el eventual contratista pueda valorar adecuadamente el alcance de lo requerido por la entidad, así como el de la distribución de riesgos que la entidad propone.

La presente contratación se desarrolla atendiendo los principios constitucionales que en materia contractual no son otros distintos que los consagrados en el artículo 209 de la Carta Política, en el que se hace alusión a los principios de la función pública (artículo 3 de la Ley 489 de 2008), entre los cuales se encuentra la igualdad, la moralidad, la economía, la celeridad, la imparcialidad, la publicidad y la eficacia; los principios orientadores de lo contencioso administrativo, contenidos en el artículo 3 de la Ley 1437 de 2011, en donde se consagra que “Las actuaciones administrativas se desarrollarán, especialmente, con arreglo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad”; y a los principios rectores de la contratación pública contemplados en los artículos 24, 25 y 26 del estatuto contractual, Ley 80 de 1993, en los que se enuncian los principios de transparencia, economía y responsabilidad, así como a la normatividad legal vigente.

Análisis del sector

En junio de 2025 la variación mensual del IPC fue 0,10%, la variación año corrido fue 3,74% y la anual 4,82%.

En junio de 2025 la variación anual del IPC fue 4,82%, es decir, 2,36 puntos porcentuales menor que la reportada en el mismo periodo del año anterior, cuando fue de 7,18%.

Información junio 2025

Índice de Precios al Consumidor (IPC)

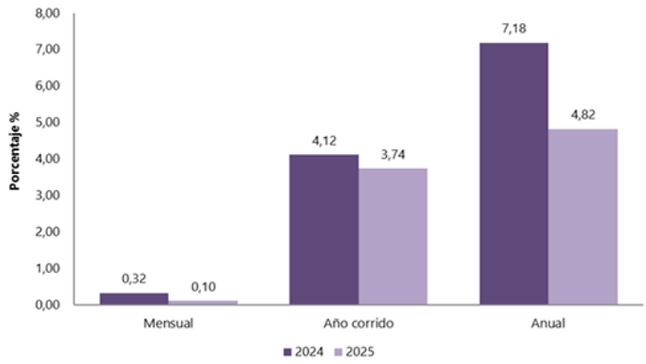
Variación mensual, año corrido y anual
Total nacional
2024 - 2025 (junio)

IPC	Junio					
	Variación mensual		Variación Año corrido		Variación Anual	
	2024	2025	2024	2025	2024	2025
IPC total	0,32	**0,10**	4,12	**3,74**	7,18	**4,82**

Fuente: DANE, IPC

El comportamiento mensual del IPC total en junio de 2025 (0,10%) se explicó principalmente por la variación mensual de las divisiones Restaurantes y hoteles y Transporte. Las mayores variaciones se presentaron en las divisiones Restaurantes y hoteles (0,42%) y Salud (0,36%).

Índice de Precios al Consumidor (IPC) Junio 2025
IPC Variaciones
Total Nacional Junio 2024 - 2025



Fuente: DANE, IPC.

RESULTADOS DEL MES DE JUNIO 2025

Comportamiento de la variación mensual del IPC según divisiones y subclases

Variación y contribución mensual por divisiones de gasto

En el mes de junio de 2025, el IPC registró una variación de 0,10% en comparación con mayo de 2025, ocho divisiones se ubicaron por encima del promedio nacional (0,10%): Restaurantes y hoteles (0,42%), Salud (0,36%), Bebidas alcohólicas y tabaco (0,27%), Bienes y servicios diversos (0,23%), Bienes y servicios para el hogar y para la conservación ordinaria del hogar (0,20%), Transporte (0,20%), Prendas de vestir y calzado (0,16%) y por último, Información y comunicación (0,12%). Por debajo se ubicaron: Educación (0,01%), Alojamiento, agua, electricidad, gas y otros combustibles (0,01%), Recreación y cultura (0,00%) y por último, Alimentos y bebidas no alcohólicas (-0,08%).

Variación y contribución mensual

Según divisiones de gasto

Junio 2024 – 2025

Divisiones de Gasto	Peso (%)	2024 Variación (%)	2024 Contribución Puntos Porcentuales	2025 Variación (%)	2025 Contribución Puntos Porcentuales
Restaurantes y hoteles	9,43	0,39	0,04	0,42	0,05
Salud	1,71	0,49	0,01	0,36	0,01
Bebidas alcohólicas y tabaco	1,70	0,08	0,00	0,27	0,00
Bienes y servicios diversos	5,36	0,14	0,01	0,23	0,01
Bienes y servicios para el hogar y para la conservación ordinaria del hogar	4,19	0,07	0,00	0,20	0,01
Transporte	12,93	0,19	0,03	0,20	0,03
Prendas de vestir y calzado	3,98	0,09	0,00	0,16	0,00
Información y comunicación	4,33	0,08	0,00	0,12	0,00
TOTAL	100,00	0,32	0,32	0,10	0,10
Alojamiento, agua, electricidad, gas y otros combustibles	33,12	0,58	0,18	0,01	0,00
Educación	4,41	-0,18	-0,01	0,01	0,00
Recreación y cultura	3,79	0,10	0,00	0,00	0,00
Alimentos y bebidas no alcohólicas	15,05	0,30	0,06	-0,08	-0,01

Fuente: DANE, IPC
Nota: La diferencia en la suma de las variables obedece al sistema de aproximación en el nivel de dígitos trabajados en el índice.

RESULTADOS AÑO CORRIDO

Comportamiento de la variación año corrido del IPC según divisiones y subclases

Variación y contribución año corrido por divisiones de gasto

En lo corrido del año, (enero - junio), cinco divisiones de bienes y servicios se ubicaron por encima del promedio nacional (3,74%): Educación (5,69%), Alimentos y bebidas no alcohólicas (4,80%), Restaurantes y hoteles (4,80%), Transporte (4,38%) y por último, Salud (3,77%). El resto de las divisiones se ubicaron por debajo del promedio: Alojamiento, agua, electricidad, gas y otros combustibles (3,39%), Bebidas alcohólicas y tabaco (3,27%), Bienes y servicios diversos (2,85%), Bienes y servicios para el hogar y para la conservación ordinaria del hogar (2,70%), Prendas de vestir y calzado (1,53%), Recreación y cultura (0,87%) y por último, Información y comunicación (-0,64%).

Variación y contribución año corrido
Según divisiones de gasto

Junio 2024 - 2025

Divisiones de Gasto	Peso (%)	2024 Variación (%)	2024 Contribución Puntos Porcentuales	2025 Variación (%)	2025 Contribución Puntos Porcentuales
Educación	4,41	8,70	0,33	5,69	0,23
Alimentos y bebidas no alcohólicas	15,05	3,79	0,72	4,80	0,90
Restaurantes y hoteles	9,43	5,21	0,56	4,80	0,53
Transporte	12,93	4,30	0,58	4,38	0,59
Salud	1,71	4,11	0,07	3,77	0,06
TOTAL	100,00	4,12	4,12	3,74	3,74
Alojamiento, agua, electricidad, gas y otros combustibles	33,12	5,09	1,56	3,39	1,06
Bebidas alcohólicas y tabaco	1,70	3,70	0,06	3,27	0,06
Bienes y servicios diversos	5,36	2,57	0,14	2,85	0,15
Muebles, artículos para el hogar y para la conservación ordinaria del hogar	4,19	1,97	0,08	2,70	0,11
Prendas de vestir y calzado	3,98	1,49	0,05	1,53	0,05
Recreación y cultura	3,79	-1,01	-0,03	0,87	0,03
Información y comunicación	4,33	-0,10	0,00	-0,64	-0,02

Fuente: DANE, IPC.
Nota: La diferencia en la suma de las variables obedece al sistema de aproximación en el nivel de dígitos trabajados en el índice.

RESULTADO ANUAL

Comportamiento de la variación anual del IPC según divisiones y subclases

Variación y contribución anual por divisiones de gasto

En el mes de junio de 2025, el IPC registró una variación de 4,82% en comparación con junio de 2024. En el último año, las divisiones Educación (7,56%), Restaurantes y hoteles (7,44%), Transporte (5,27%), Alojamiento, agua, electricidad, gas y otros combustibles (5,23%), Salud (5,20%) y por último, Bebidas alcohólicas y tabaco (5,14%) se ubicaron por encima del promedio nacional (4,82%). Entre tanto, las divisiones Alimentos y bebidas no alcohólicas (4,31%), Bienes y servicios diversos (3,61%), Bienes y servicios para el hogar y para la conservación ordinaria del hogar (2,92%), Prendas de vestir y calzado (2,10%), Recreación y cultura (1,68%) y por último, Información y comunicación (-1,46%) se ubicaron por debajo del promedio nacional.

Junio 2024 - 2025

Divisiones de Gasto	Peso (%)	2024 Variación (%)	2024 Contribución Puntos Porcentuales	2025 Variación (%)	2025 Contribución Puntos Porcentuales
Educación	4,41	11,21	0,43	7,56	0,30
Restaurantes y hoteles	9,43	9,57	1,02	7,44	0,81
Transporte	12,93	8,10	1,08	5,27	0,71
Alojamiento, agua, electricidad, gas y otros combustibles	33,12	9,25	2,81	5,23	1,62
Salud	1,71	6,78	0,11	5,20	0,09
Bebidas alcohólicas y tabaco	1,70	8,15	0,14	5,14	0,09
TOTAL	100,00	7,18	7,18	4,82	4,82
Alimentos y bebidas no alcohólicas	15,05	5,27	1,02	4,31	0,82
Bienes y servicios diversos	5,36	5,18	0,28	3,61	0,19
Bienes y servicios para el hogar y para la conservación ordinaria del hogar	4,19	3,17	0,13	2,92	0,12
Prendas de vestir y calzado	3,98	3,06	0,10	2,10	0,07
Recreación y cultura	3,79	2,00	0,07	1,68	0,05
Información y comunicación	4,33	-0,15	0,00	-1,46	-0,04

Fuente: DANE, IPC.

Fuente: https://www.dane.gov.co/files/operaciones/IPC/jun2025/bol-IPC-jun2025.pdf

Análisis de composición de software Análisis de participación y tamaño del mercado tendencias de crecimiento y pronósticos (2024-2029)

El Informe de análisis de composición de software está segmentado por componente (soluciones, servicios), modo de implementación (nube, local), industria vertical (TI y telecomunicaciones, BFSI, venta minorista y comercio electrónico) y geografía (América del Norte, Europa, Asia Pacífico, América Latina, Medio Oriente y

África). Los tamaños de mercado y las previsiones se proporcionan en términos de valor (millones de dólares) para todos los segmentos anteriores.

Análisis de composición de software Tendencias del mercado

El segmento de la nube es uno de los factores que impulsan el mercado

- Debido a la creciente aceptación del software y las soluciones basadas en la nube en todas las industrias, la implementación de la nube está experimentando la tasa de crecimiento más rápida durante el período previsto. Debido a la rentabilidad de la implementación, las pequeñas y medianas empresas (PYME) son donde la adopción prevalece. La opción de implementación en la nube facilita que varios sitios trabajen juntos sin tener que instalar software ni mantenerse al día con hardware adicional.
- Se espera que la computación en la nube controle una cuota de mercado considerable e incluso acelere el crecimiento. Se espera que los costos y beneficios operativos que ofrece el modo de implementación cambien la tendencia del modelo de implementación local durante el período previsto. Por ejemplo, según el estudio de NTT Ltd., más de la mitad de los encuestados (52%) mencionaron que la nube tendría el mayor impacto transformador en las operaciones comerciales de su organización.
- La nube ha demostrado su eficacia económica y operativa al permitir que organizaciones de todos los tamaños se concentren en sus competencias principales y, al mismo tiempo, transfieren la infraestructura de TI, la conectividad y la responsabilidad de gestión a proveedores de la nube que se destacan en el desarrollo y la prestación de estos servicios. Además, la industria de las telecomunicaciones está cambiando. Esto se debe a la rápida expansión de la tecnología, el aumento de la demanda, la diversificación de la base de clientes, la necesidad de productos y servicios actuales a tarifas bajas y la integración de varios sectores, como el satélite y el cable, con las telecomunicaciones existentes. Por lo tanto, se prevé que la implementación de software integrado en la empresa ayude a los CSP (proveedores de servicios en la nube) a gestionar y administrar varios sistemas y aplicaciones a través de múltiples funciones, permitiéndoles lograr una integración lógica de procesos de negocios entre diferentes sistemas de aplicaciones independientes.
- Además, Prisma Cloud ha agregado Análisis de composición de software (SCA) a su plataforma de protección de aplicaciones nativa de la nube para ayudar a los equipos a obtener seguridad de código que esté tan estrechamente vinculada como las aplicaciones que necesitan proteger. Este desarrollo se basa en nuestras capacidades de seguridad básicas de IaC líderes en la industria y hace posible la primera solución SCA consciente del contexto que puede incluir el contexto de la infraestructura en la seguridad de las aplicaciones.
- Además, el gasto en la nube pública es una partida importante en los presupuestos de TI. El uso cada vez mayor de la nube pública está elevando el gasto en la nube para organizaciones de todos los tamaños. Según una encuesta realizada por Flexera, el 37 por ciento de las empresas dijo que su gasto anual en TI superó los 12 millones de dólares, y el 80% informó que su gasto en la nube superó los 1,2 millones de dólares al año.

Descripción general de la industria del análisis de composición de software

El mercado de análisis de composición de software es moderadamente competitivo y está formado por varios actores importantes. En términos de cuota de mercado, algunos de estos actores dominan actualmente el mercado. Para mantenerse por delante de la competencia y ampliar su alcance global, las empresas influyentes utilizan fusiones y adquisiciones, así como la innovación de productos.

Segmentación de la industria del análisis de composición de software

El análisis de composición de software (SCA) es una herramienta de software que se utiliza para brindar seguridad frente a posibles amenazas cibernéticas. El software es responsable de realizar un análisis completo de seguridad del código de software y monitorear los contenidos de código abierto en cada etapa del ciclo de vida de desarrollo de software (SDLC). Existe una amplia gama de herramientas SCA en el mercado que se pueden utilizar para gestionar los riesgos de calidad, seguridad y cumplimiento de licencias que surgen del uso de código abierto y de terceros en aplicaciones.

El mercado de análisis de composición de software se divide por componente (soluciones, servicios), modo de implementación (nube, local), industria vertical (TI y telecomunicaciones, BFSI, venta minorista y comercio electrónico) y geografía (América del Norte, Europa, Asia Pacífico). , América Latina, Oriente Medio y África).

Los tamaños de mercado y las previsiones se proporcionan en términos de valor (millones de dólares) para todos los segmentos anteriores.

FUENTE:https://www.mordorintelligence.com/es/industry-reports/software-composition-analysis-market

Mercado de Software en Colombia – Por Tipo de Producto (Software de Aplicación, Software de Infraestructura de Sistemas, Software de Desarrollo e Implantación, Software de Productividad); Por Despliegue (On-Premises, En la Nube); Por Tamaño de la Empresa (Pequeñas y Medianas Empresas, Grandes Empresas); Por Vertical de la Industria (BFSI, Minoristas, Salud, Gobierno, TI y Telecomunicaciones, Otros); Dinámica del Mercado (2025-2034) y Panorama Competitivo

El mercado de software en Colombia creció sustancialmente en 2024. Se espera que el mercado crezca a una tasa de crecimiento anual compuesta (CAGR) del 7,70% entre 2025 y 2034.

El software se refiere a un conjunto de instrucciones que permiten a las computadoras realizar tareas específicas o ejecutar programas. Incluye aplicaciones, sistemas operativos y otros programas que facilitan diversas funciones, desde el tratamiento de textos a la gestión de sistemas. El software sirve como medio que permite la comunicación entre los componentes de hardware y los usuarios.

El tamaño del mercado de software en Colombia está aumentando rápidamente debido a la creciente transformación digital, el aumento de la adopción de soluciones basadas en la nube, y el crecimiento del comercio electrónico en la región. El software permite a las personas obtener soluciones personalizadas que satisfacen sus requisitos comerciales, lo que lleva a una rápida transformación digital y a la necesidad de software personalizado. El 63 % de la población colombiana utiliza Internet y más de la mitad de los colombianos de 15 años o más realizan y reciben pagos digitales, lo que lleva al uso creciente de software de pago digital.

El crecimiento del sector del comercio electrónico es otro factor clave que incrementa la cuota del mercado de software en Colombia. Los consumidores están cambiando cada vez más hacia las compras en línea, lo que lleva a la rápida adopción de plataformas digitales, que, resulta en un aumento de la demanda de soluciones de software especializadas para facilitar su experiencia de compra. Del mismo modo, la expansión de los sistemas de pago digitales y la necesidad de transacciones en línea seguras impulsan la demanda de aplicaciones de software avanzadas centradas en el procesamiento de pagos y la prevención del fraude en el sector del comercio electrónico. Junto con esto, las demandas de gestión de la cadena de suministro y cumplimiento de pedidos en el sector impulsan la adopción de soluciones de software diseñadas para agilizar las operaciones logísticas, llevando colectivamente al crecimiento del mercado de software en Colombia.

Tendencias Clave que Apoyan la Expansión del Mercado de Software en Colombia

Creciente adopción de software por parte de las pequeñas y medianas empresas

La creciente adopción de software por parte de las pequeñas y medianas empresas es una tendencia notable del mercado de software en Colombia. Las PYMES han cambiado rápidamente hacia la incorporación de tecnologías digitales en sus operaciones, impulsadas por la necesidad de aumentar la eficiencia, la rentabilidad, y la competitividad. Las PYMES están optando por soluciones de software para diversos fines como la contabilidad, la gestión de relaciones con los clientes (CRM), y la planificación de recursos empresariales (ERP). La accesibilidad del software ha facilitado a las PYME la implantación de herramientas avanzadas sin los elevados costes asociados a las soluciones tradicionales in situ. Además, las iniciativas gubernamentales y los programas de apoyo destinados a promover la transformación digital entre las pymes en Colombia impulsan aún más el mercado. Entidades como el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) han introducido iniciativas para facilitar la integración de soluciones de software, creando un impacto positivo en las perspectivas del mercado de software en Colombia.

Integración de tecnologías modernas como IA y Machine Learning

Las empresas en Colombia están utilizando cada vez más IA y ML para optimizar los procesos y mejorar la toma de decisiones. Las tareas repetitivas en todos los sectores se están automatizando mediante soluciones basadas en IA, lo que aumenta la eficiencia y la productividad. Desde los chatbots inteligentes que gestionan las consultas de atención al cliente hasta el análisis automatizado de datos en finanzas, los algoritmos de ML están agilizando las operaciones. Según el pronóstico del mercado de software en Colombia, el uso extensivo de estas tecnologías en los sectores de fabricación, TI y telecomunicaciones, y salud tendrá un impacto positivo en el crecimiento del mercado.

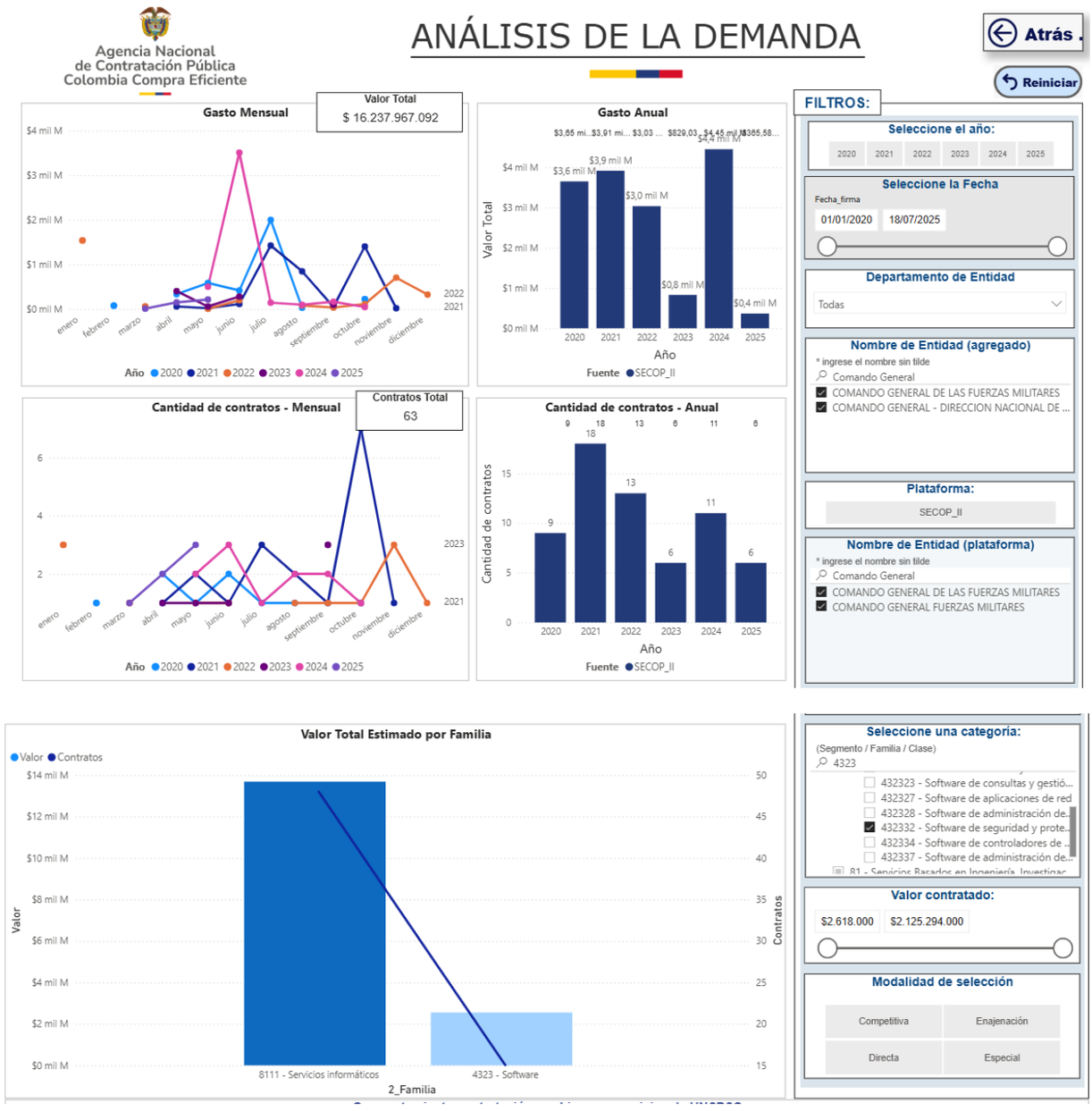
Por tipo de producto, el mercado se divide en:

- Software de Aplicación

- Software de Infraestructura de Sistemas
- Software de Desarrollo e Implantación
- Software de Productividad

El software de aplicación se subdivide en software de planificación de recursos empresariales (ERP), software de gestión de relaciones con los clientes (CRM), software de gestión de contenidos empresariales (ECM), software de gestión de la cadena de suministro (SCM), software de colaboración empresarial, y software educativo, entre otros. Mientras tanto, el software de infraestructura de sistemas se clasifica en sistemas de gestión de redes (NMS), software de almacenamiento, y software de seguridad. El software de desarrollo y despliegue se segrega en gestión de datos empresariales (EDM), herramientas de análisis e informes empresariales, servidores de aplicaciones, middleware de integración y orquestación, y herramientas de calidad de datos, y el software de productividad se divide en software de oficina y software creativo, entre otros.

Fuente:https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.informesdeexpertos.com%2Finformes%2Fmercado-de-software-en-colombia&psig

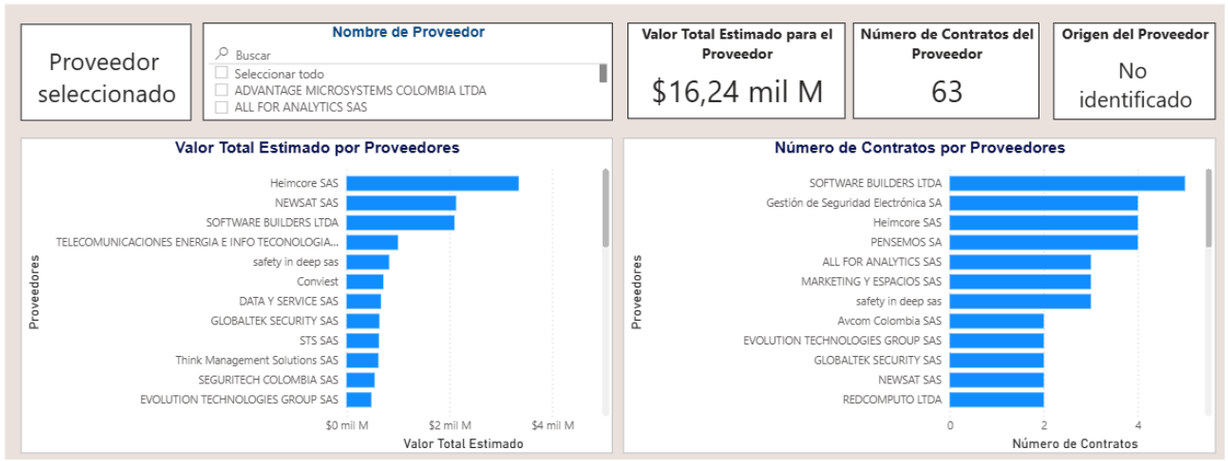


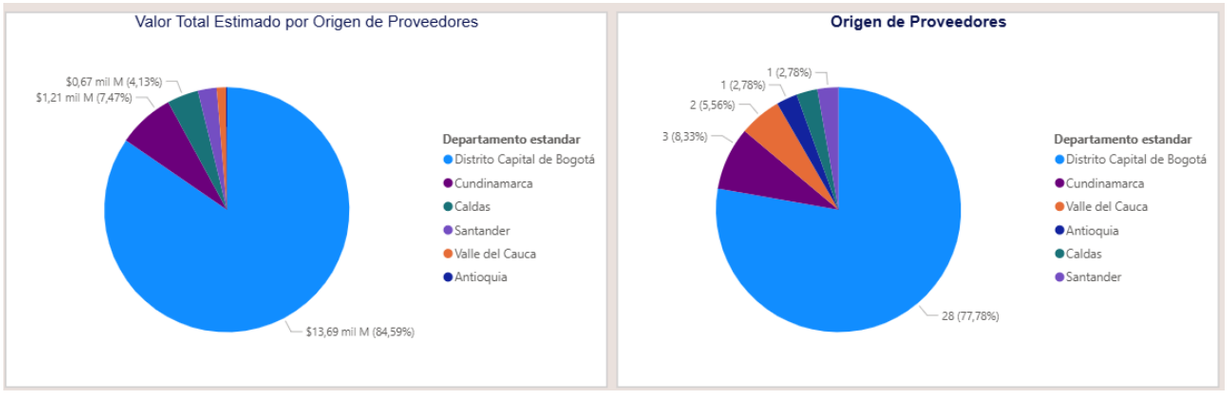
Comportamiento contratación por bienes y servicios de UNSPSC

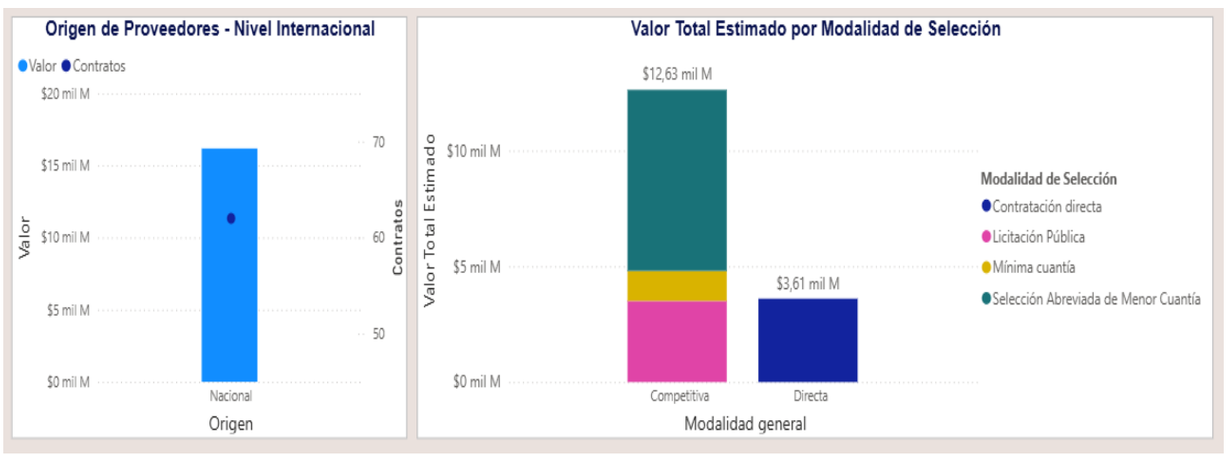
Año	2020			2021			2022			2023	
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor
8111 - Servicios informáticos	7	$3.162.960.015	19,48%	13	$2.775.424.136	17,09%	9	$2.221.718.153	13,68%	5	$825.749.674
4323 - Software	2	$485.060.703	2,99%	5	$1.138.856.660	7,01%	4	$811.748.500	5,00%	1	$3.279.632
Total	9	$3.648.020.718	22,47%	18	$3.914.280.796	24,11%	13	$3.033.466.653	18,68%	6	$829.029.306

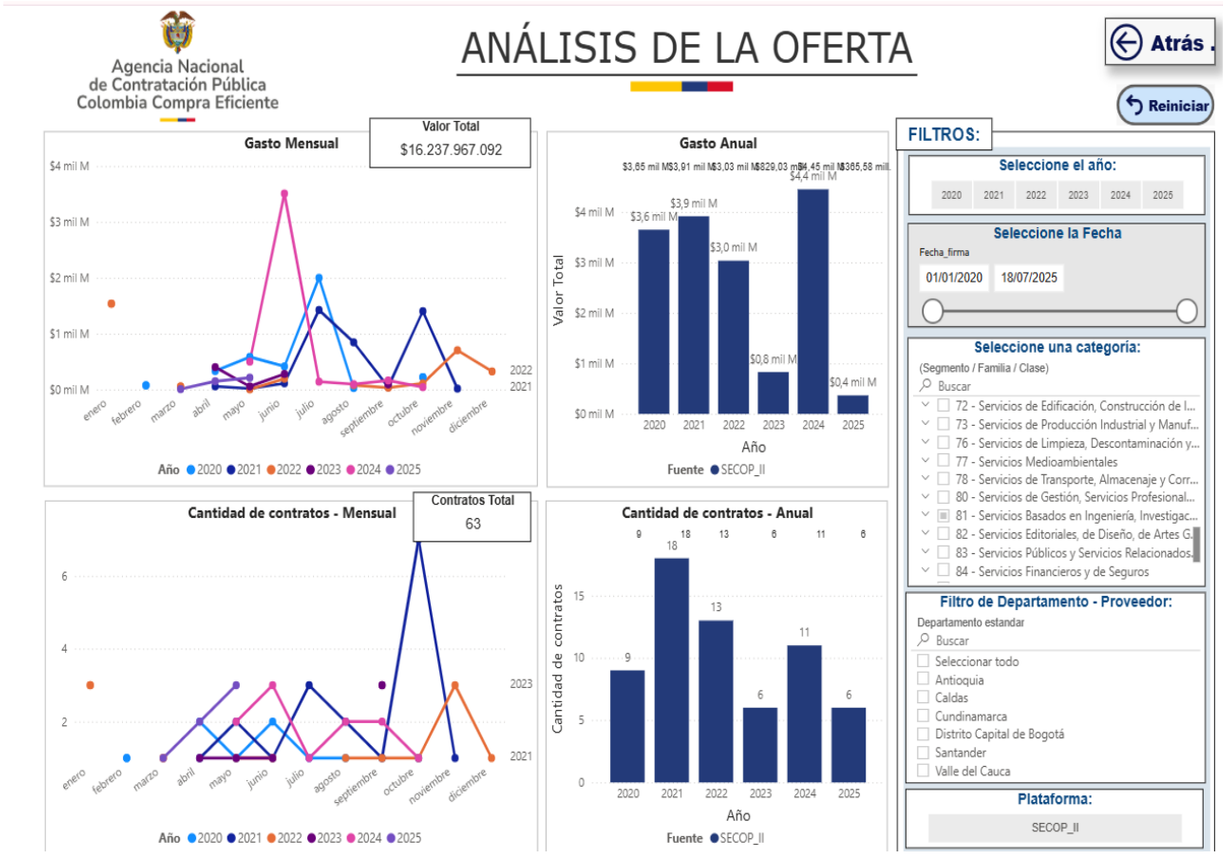
Comportamiento contratación por bienes y servicios de UNSPSC

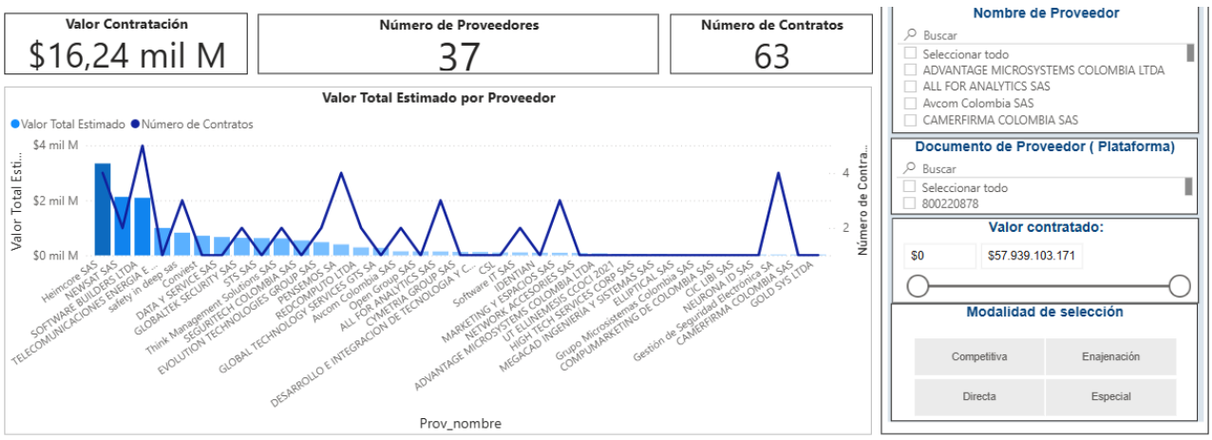
Año	2023		2024			2025			Total		
Clasificador de Bienes y Servicios - Familia	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación
8111 - Servicios informáticos	$825.749.674	5,09%	9	$4.343.945.519	26,75%	5	$359.550.800	2,21%	48	$13.689.348.297	84,30%
4323 - Software	$3.279.632	0,02%	2	$103.640.000	0,64%	1	$6.033.300	0,04%	15	$2.548.618.795	15,70%
Total	$829.029.306	5,11%	11	$4.447.585.519	27,39%	6	$365.584.100	2,25%	63	$16.237.967.092	100,00%

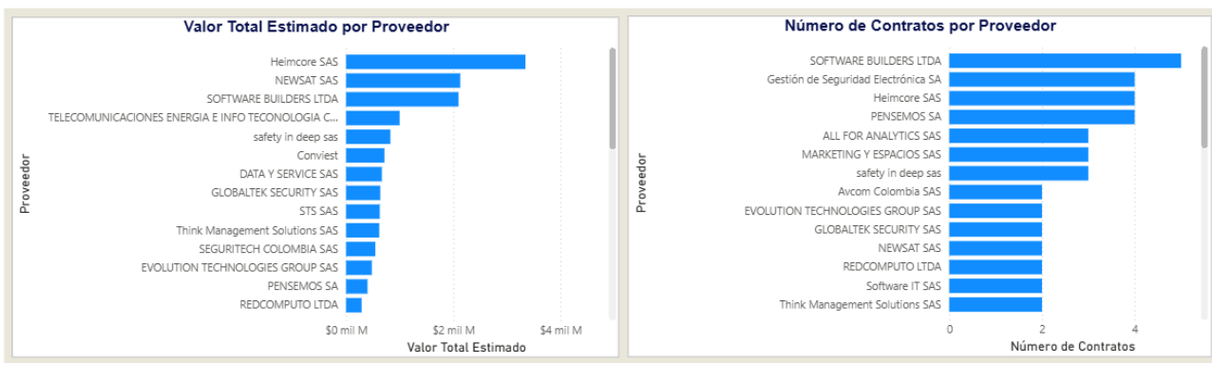


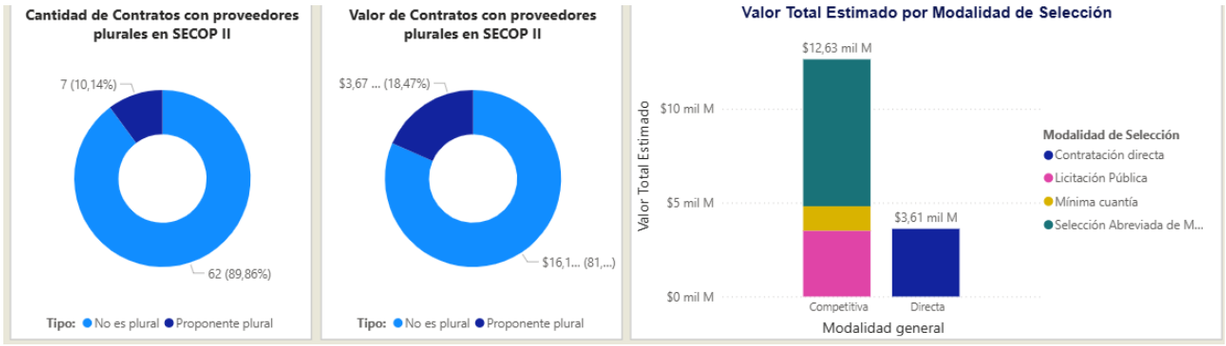


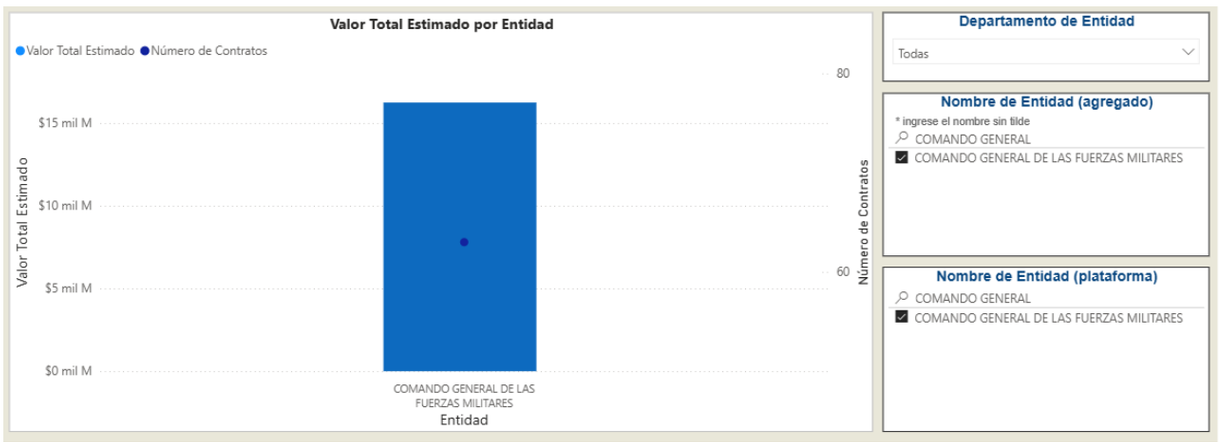



Agencia Nacional de Contratación Pública Colombia Compra Eficiente
ANÁLISIS DE LA OFERTA
Atrás
Reiniciar
Gasto Mensual
Valor Total
$16.237.967.092
Gasto Anual
Cantidad de contratos - Mensual
Contratos Total
63
Cantidad de contratos - Anual
FILTROS:
Seleccione el año:
2020 2021 2022 2023 2024 2025
Seleccione la Fecha
Fecha_firma
01/01/2020
18/07/2025
Seleccione una categoría:
(Segmento / Familia / Clase)
Buscar
72 - Servicios de Edificación, Construcción de I...
73 - Servicios de Producción Industrial y Manuf...
76 - Servicios de Limpieza, Descontaminación y...
77 - Servicios Medioambientales
78 - Servicios de Transporte, Almacenaje y Corr...
80 - Servicios de Gestión, Servicios Profesional...
81 - Servicios Basados en Ingeniería, Investigac...
82 - Servicios Editoriales, de Diseño, de Artes G...
83 - Servicios Públicos y Servicios Relacionados
84 - Servicios Financieros y de Seguros
Filtro de Departamento - Proveedor:
Departamento estandar
Buscar
Seleccionar todo
Antioquia
Caldas
Cundinamarca
Distrito Capital de Bogotá
Santander
Valle del Cauca
Plataforma:
SECOP_II
Año
Fuente SECOP_II


Valor Contratación
$16,24 mil M
Número de Proveedores
37
Número de Contratos
63
Valor Total Estimado por Proveedor
Valor Total Estimado
Número de Contratos
Prov_nombre
Nombre de Proveedor
Buscar
Seleccionar todo
ADVANTAGE MICROSYSTEMS COLOMBIA LTDA
ALL FOR ANALYTICS SAS
Avcom Colombia SAS
CAMERFIRMA COLOMBIA SAS
Documento de Proveedor (Plataforma)
Buscar
Seleccionar todo
800220878
Valor contratado:
$0
$57.939.103.171
Modalidad de selección
Competitiva
Enajenación
Directa
Especial


Valor Total Estimado por Proveedor
Proveedor
Valor Total Estimado
Heimcore SAS
NEWSAT SAS
SOFTWARE BUILDERS LTDA
TELECOMUNICACIONES ENERGIA E INFO TECONOLOGIA C...
safety in deep sas
Conviest
DATA Y SERVICE SAS
GLOBALTEK SECURITY SAS
STS SAS
Think Management Solutions SAS
SEGURITECH COLOMBIA SAS
EVOLUTION TECHNOLOGIES GROUP SAS
PENSEMOS SA
REDCOMPUTO LTDA
Número de Contratos por Proveedor
Proveedor
Número de Contratos
SOFTWARE BUILDERS LTDA
Gestión de Seguridad Electrónica SA
Heimcore SAS
PENSEMOS SA
ALL FOR ANALYTICS SAS
MARKETING Y ESPACIOS SAS
safety in deep sas
Avcom Colombia SAS
EVOLUTION TECHNOLOGIES GROUP SAS
GLOBALTEK SECURITY SAS
NEWSAT SAS
REDCOMPUTO LTDA
Software IT SAS
Think Management Solutions SAS





Comportamiento contratación por bienes y servicios de UNSPSC

Año	2020			2021			2022			2023	
Clasificador de Bienes y Servicios - Familia	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor
4323 - Software	2	$485.060.703	2,99%	5	$1.138.856.660	7,01%	4	$811.748.500	5,00%	1	$3.279.632
8111 - Servicios informáticos	7	$3.162.960.015	19,48%	13	$2.775.424.136	17,09%	9	$2.221.718.153	13,68%	5	$825.749.674
Total	**9**	**$3.648.020.718**	**22,47%**	**18**	**$3.914.280.796**	**24,11%**	**13**	**$3.033.466.653**	**18,68%**	**6**	**$829.029.306**

Comportamiento contratación por bienes y servicios de UNSPSC

Año	2023		2024			2025			Total		
Clasificador de Bienes y Servicios - Familia	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación	Contratos	Valor	Participación
4323 - Software	$3.279.632	0,02%	2	$103.640.000	0,64%	1	$6.033.300	0,04%	15	$2.548.618.795	15,70%
8111 - Servicios informáticos	$825.749.674	5,09%	9	$4.343.945.519	26,75%	5	$359.550.800	2,21%	48	$13.689.348.297	84,30%
Total	**$829.029.306**	**5,11%**	**11**	**$4.447.585.519**	**27,39%**	**6**	**$365.584.100**	**2,25%**	**63**	**$16.237.967.092**	**100,00%**

Fuente: https://www.colombiacompra.gov.co/analisis-de-datos-de-compra-publica/modelo-deabastecimiento-estrategico

Acuerdo Marco Vigente

En cumplimiento del parágrafo 5 del artículo 2 de la Ley 1150 de 2007, se deja constancia que una vez verificados los Acuerdos Marco de precios vigentes, a la fecha no existe Acuerdo Marco que abarque los servicios objeto de la presente contratación, por lo tanto y, de acuerdo a las características técnicas de los servicios a contratar, el proceso de adquisición se adelantará a través de la plataforma del SECOP II mediante la modalidad de selección abreviada de menor cuantía.

Perspectiva Organizacional:

En busca de la solidez, la experiencia y la legalidad con que debe contar el contratista seleccionado por el Ministerio de Defensa Nacional – Comando General de las FFMM para la adquisición de los bienes o servicios se debe asegurar la calidad de estos y el respaldo en condiciones óptimas, se considera necesario que cumpla con los siguientes aspectos a nivel organizacional:

- Poseer una amplia trayectoria y experiencia en el sector.
- Contar con la infraestructura y logística necesarias para efectuar el suministro de los bienes o la prestación de los servicios.

- Tener los medios tecnológicos necesarios, para dar respuesta de manera inmediata a los requerimientos de la institución.
- Dar respuesta oportuna a las solicitudes del Ministerio de Defensa, para así garantizar el óptimo desarrollo del contrato.

IV. DESCRIPCIÓN DEL OBJETO A CONTRATAR.

A. Objeto:

EL MINISTERIO DE DEFENSA NACIONAL - COMANDO GENERAL DE LAS FUERZAS MILITARES - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, requiere contratar el mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 del COGFM, de acuerdo con las especificaciones técnicas del ANEXO, así:

- LOTE 1: LICENCIAS FIREWALL + VPN.
- LOTE 2: LICENCIAS PROXY WEB.
- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.
- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).
- LOTE 5: SUSCRIPCIÓN WAF.
- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.
- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

B. Clasificador de bienes y servicios:

APLICA PARA CADA UNO DE LOS LOTES.

De conformidad al decreto 1082 de 2015, por el cual se reglamenta el sistema de compras y contratación pública, se deberá incluir la descripción del objeto a contratar identificado con el cuarto nivel del clasificador de Bienes y Servicios el cual es el sistema de codificación de las Naciones Unidas para estandarizar productos y servicios, así:

CÓDIGO ONU *(Segmento/Familia/Clase/Producto)*	**DESCRIPCIÓN**
43222501	Equipo de seguridad de red cortafuegos (firewall)
43232600	Software específico para la industria
43233205	Software de seguridad de transacciones y de protección contra virus
81111805	Mantenimiento o soporte de sistemas patentados o autorizados.
81112204	Mantenimiento de software de sistemas operativos.
81112208	Mantenimiento de software de protección y seguridad.
81112501	Servicio de licencias del software del computador.
81161500	Servicios de administración de acceso

C. Especificaciones técnicas:

De acuerdo con las especificaciones técnicas establecidas en el ANEXO del presente estudio.

V. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL.

De acuerdo con el certificado de disponibilidad No. 40325 de fecha 26 de mayo del 2025 con cargo a la Unidad Ejecutora 15-01-02-000, por valor total de **DOS MIL NOVECIENTOS SETENTA Y CINCO MILLONES NOVECIENTOS NOVENTA Y NUEVE MIL NOVECIENTOS NOVENTA Y NUEVE PESOS ($2.975.999.999,00), M/CTE.,** expedido por el jefe de Presupuesto del COGFM para la vigencia 2025; distribuido de la siguiente manera:

RUBRO PRESUPUESTAL				**VALOR PRESUPUESTO DISPONIBLE**
CÓDIGO	**DESCRIPCIÓN**	**RECURSO**	**DEPENDENCIA**	
A-02-02-02-008-003	SERVICIOS PROFESIONALES CIENTÍFICOS Y TÉCNICOS (EXCEPTO	10	CGDJ6	1.000.000.000,00

	LOS SERVICIOS DE INVESTIGACIÓN, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)			
A-02-02-02-008-004	SERVICIOS DE TELECOMUNICACIONES, TRANSMISIÓN Y SUMINISTRO DE INFORMACIÓN			1.975.999.999,00
VALOR TOTAL PRESUPUESTO DISPONIBLE:				**2.975.999.999,00**

VI. PRESUPUESTO OFICIAL ESTIMADO PARA EL PROCESO, SEGÚN ANÁLISIS DE MERCADO.

El presupuesto oficial para el presente proceso, según análisis de mercado, se estableció en la suma de **DOS MIL NOVECIENTOS CINCUENTA Y DOS MILLONES SETECIENTOS TREINTA Y CUATRO MIL SEISCIENTOS OCHENTA Y OCHO PESOS ($2.952.734.688,00) M/CTE**., exento o excluido de IVA según aplique e incluidos demás impuestos, tasas y gravámenes que se causen por el hecho de su celebración, ejecución, liquidación; distribuidos por lote de la siguiente manera:

No. LOTE	RUBRO	DESCRIPCIÓN DEL LOTE	PRESUPUESTO POR LOTE
1	A-02-02-02-008-003	LICENCIAS FIREWALL + VPN	697.553.650,00
2		LICENCIAS PROXY WEB.	294.620.000,00
3	A-02-02-02-008-004	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS	1.097.781.664,00
4		SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).	199.910.464,00
5		SUSCRIPCIÓN WAF.	387.730.210,00
6		SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.	199.738.700,00
7		SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.	75.400.000,00
VALOR TOTAL			**2.952.734.688,00**

A continuación, se detalla el presupuesto oficial, para cada uno de los ÍTEMS para cada Lote.

VALOR PRESUPUESTO DEL LOTE						**697.553.650,00**
	LOTE No. 1 LICENCIAS FIREWALL + VPN					
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	Renovación y actualización del licenciamiento de la solución de seguridad perimetral del COGFM y garantía técnica por un (01) año. (De acuerdo a las especificaciones técnicas del Anexo)	5	UND	139.510.730,00	EXENTO	697.553.650,00
VALOR TOTAL LOTE No. 1						**697.553.650,00**

VALOR PRESUPUESTO DEL LOTE						**294.620.000,00**
LOTE No. 2 LICENCIAS PROXY						
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM).(De acuerdo a las especificaciones técnicas del Anexo)	2	UND	147.310.000,00	EXENTO	294.620.000,00
VALOR TOTAL LOTE No. 2						**294.620.000,00**

VALOR PRESUPUESTO DEL LOTE	**1.097.781.664,00**
LOTE No. 3 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS	

No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA
1	**SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS**					
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	237.789.104,00	EXENTO	237.789.104,00
1.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	189.820.365,00	EXENTO	189.820.365,00
1.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	151.664.800,00	EXENTO	151.664.800,00
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	67.541.902,00	EXENTO	67.541.902,00
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	47.069.300,00	EXENTO	47.069.300,00
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	13.642.293,00	EXENTO	13.642.293,00
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	390.253.900,00	EXENTO	390.253.900,00
VALOR TOTAL LOTE No. 3						**1.097.781.664,00**

VALOR PRESUPUESTO DEL LOTE						**199.910.464,00**
LOTE No. 4 SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).						
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	SUSCRIPCIÓN FILTRADO Y PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM). (De acuerdo a las especificaciones técnicas del Anexo)	1.600	UND	124.944,04	EXENTO	199.910.464,00
VALOR TOTAL LOTE No. 4						**199.910.464,00**

VALOR PRESUPUESTO DEL LOTE						**387.730.210,00**
LOTE No. 5 SUSCRIPCIÓN WAF.						
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)	1	UND	387.730.210,00	EXENTO	387.730.210,00
VALOR TOTAL LOTE No. 5						**387.730.210,00**

VALOR PRESUPUESTO POR LOTE						**199.738.700,00**
LOTE No. 6 SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.						
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	Suscripción de licenciamiento SASE, incluyendo (acceso de red de zero confianza (ZTNA), protección de amenazas sobre dispositivos móviles (MTD), acceso seguro para dispositivos no gestionados (Enterprise Browser) por un periodo de tiempo de 2 años. (De acuerdo a	100	UND	1.997.387,00	EXENTO	199.738.700,00

	las especificaciones técnicas del Anexo					
VALOR TOTAL LOTE No. 6						**199.738.700,00**

VALOR PRESUPUESTO POR LOTE						**75.400.000,00**
LOTE No. 7 SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.						
No.	**DESCRIPCIÓN DEL ELEMENTO O SERVICIO**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**VALOR UNITARIO**	**VALOR IVA (*)**	**VALOR TOTAL INCLUIDO IVA**
1	Suscripción del Licenciamiento de videoconferencia cisco Webex para equipos con aplicación en dispositivos móviles.	13	UND	5.800.000,00	EXENTO	75.400.000,00
VALOR TOTAL LOTE No. 7						**75.400.000,00**

NOTA 1: Teniendo la procedencia de los bienes, de conformidad con el Estatuto Tributario, artículo 476, Los servicios a adquirir se encuentran excluidos de IVA y artículo 477 los Bienes que se encuentran exentos del impuesto de IVA.

Los servicios a adquirir se encuentran excluidos de IVA:

Art. 476. Servicios excluidos del impuesto sobre las ventas

(…)

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

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

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

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

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

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

(…)

NOTA 2: Los proponentes interesados en presentar propuesta para el presente proceso deberán tener en cuenta lo siguiente:

a. En el cuestionario económico del SECOP II, PROPUESTA ECONÓMICA DE PRECIOS UNITARIOS, deberá incluir el valor (precio) unitario exento o excluido IVA según aplique de los ítems requeridos **POR LOTE.** El oferente que en su propuesta económica de precios unitarios sobrepase cualquiera de los valores (precios) unitarios de referencia excluido IVA según aplique, de cualquiera de los ítems requeridos **POR LOTE**, incurrirá en causal de rechazo.

b. En la pregunta No. 4.1 del cuestionario económico del SECOP II, PROPUESTA ECONÓMICA DE PRECIOS UNITARIOS deberá incluirse el valor (precio) unitario exento o excluido IVA según aplique de todos los ítems requeridos **POR LOTE**. ***Cuenta para evaluación.***

c. Los valores unitarios ofertados por ítem deberán contener máximo dos (2) decimales. En caso necesario, la entidad procederá a hacer corrección aritmética partiendo del precio unitario sin IVA del respectivo ítem y usará la función de Excel *"=redondear (valor unitario sin IVA;2")*.

d. Cuando la propuesta económica sobrepase el precio de referencia unitario por ítem IVA exento o excluido, y/o efectuada la corrección aritmética por el comité económico evaluador lo supere estará incurso en causal de rechazo.

e. Ninguno de los valores (precios) unitarios ofrecidos IVA excluido según aplique por ítem, podrá ser igual cero (0), estar vacío o estar en blanco.

Nota 3**:** El Comando General de las Fuerzas Militares, no asumirá costos de ningún tipo, que no contemple el proponente dentro de su análisis de precios para presentar la oferta económica que permita la ejecución idónea del contrato resultante del presente proceso de contratación. Por lo tanto, el oferente debe contemplar todos los costos o gastos en que deba o pueda incurrir, para llevar a cabo la ejecución del proceso.

VII. EJECUCIÓN.

APLICA PARA CADA UNO DE LOS LOTES.

A. Plazo de ejecución:

El plazo de ejecución del contrato será hasta el 12 de diciembre de 2025, contado a partir del día hábil siguiente a la aprobación de la garantía por parte de la Dirección Administrativa y Financiera del Comando General FF.MM, previa expedición del registro presupuestal.

B. Plazo de duración:

El plazo de duración del contrato será de seis (6) meses adicionales al plazo establecido para la ejecución. Este plazo aplica únicamente para trámites administrativos y no cuenta para ejecución.

C. Lugar de ejecución y entrega:

El lugar de ejecución y prestación de los servicios será en el MINISTERIO DE DEFENSA NACIONAL-COMANDO GENERAL DE LAS FUERZAS MILITARES, – Dirección Tecnologías de la Información –DITIN–, ubicada en la Avenida el Dorado Carrera 54 No. 26 – 25 CAN Edificio Fortaleza, de la ciudad de Bogotá D.C., previa coordinación con el supervisor del contrato.

VIII. FORMA DE PAGO.

APLICA PARA CADA UNO DE LOS LOTES.

El MINISTERIO DE DEFENSA NACIONAL- COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA se obliga para con el CONTRATISTA a que el valor del contrato se pagará parcial o total dentro de los sesenta (60) días calendario siguientes de conformidad con la ley 2024 del 23 de julio de 2020 “por medio de la cual se adoptan normas de pago en plazos justos en el ámbito mercantil y se dictan otras disposiciones en materia de pago y facturación”, siguientes:

1. Al recibo a satisfacción parcial o total del objeto del contrato previa acta de recibo parcial y/o final suscrita por el supervisor del contrato y el contratista o su delegado

2. Presentación de la respectiva factura o documento equivalente donde se registre: - fecha, valor de los bienes suministrados o de los servicios prestados IVA exento o excluido según aplique, y alta de entrada al almacén según aplique.

3. Certificación expedida y soportada (planillas de pago) del pago de aportes parafiscales por el revisor fiscal o en su defecto por el representante legal a fecha 30 del mes vencido anterior a la fecha de pago.

4. Cupo de PAC asignado, situación de los recursos por parte del Tesoro Nacional y cumplimiento de los demás trámites administrativos a que haya lugar.

En caso de PERSONA JURÍDICA, deberá acreditar el pago de los aportes a seguridad social, ARL y parafiscales 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.

La PERSONA NATURAL deberá allegar, adicional a lo exigido para persona jurídica, 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 bruto mensual facturado, conforme a la Circular 00001 del 6 de diciembre de 2004 expedida por el Ministerio de Hacienda y Crédito Público y de la Protección Social. Igualmente deberá tener en cuenta lo establecido en la Resolución No. 209 del 12 de febrero de 2020 “Por la cual se adiciona el esquema de presunción de costos para los trabajadores independientes por cuenta propia y los trabajadores independientes con contratos diferentes a prestación de servicios personales conforme a su actividad económica”.

En caso de que la PERSONA NATURAL O JURÍDICA esté obligada a facturar electrónicamente, deberá enviar la facturación electrónica debidamente validada por la DIAN, conforme a lo estipulado en el decreto 358 del 5 de marzo de 2020 y en la resolución 000042 del 5 de mayo de 2020; al correo facturaciondiadf@cgfm.mil.co adjuntando copia en PDF de la respectiva resolución de facturación.

Nota:

"PARÁGRAFO 1°: El futuro proveedor o contratista deberá tener en cuenta que en caso de estar obligado a facturar electrónicamente deberá enviar la facturación electrónica debidamente validada por la DIAN, conforme a lo estipulado en el Decreto 358 del 05 de marzo de 2020, la resolución 000042 del 05 de mayo de 2020 y la Directiva Presidencial No. 9 de 2020 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, DC) registrar en la factura, según sea el caso, los siguientes datos en los campos solicitados:

a. Por regla general se debe diligenciar en la sección de la factura Notas u Observaciones, entre #$ el código de identificación de la entidad del Presupuesto General de la Nación (PGN) que está adquiriendo a la cual le va a enviar la factura, los datos del contrato o identificación de la caja menor y correo del supervisor o cuentadante o el correo que defina la entidad que opte por recepción centralizada, finalizando con #$, debidamente separados por punto y coma, según los siguientes ejemplos:

Para la recepción centralizada por parte de la entidad PGN: #$15-01-02-000; Contrato No XXX; facturaciondiadf@cgfm.mil.co #$

b. Si el proveedor o contratista al elaborar y emitir la factura electrónica (FE), nota debito (ND), nota crédito (DC) mediante operador tecnológico autorizado, solución gratuita de la DIAN o software propio, tiene la posibilidad de definir el asunto del correo remisorio de los documentos electrónicos al adquiriente, debe registrar los siguientes datos: PCI; Identificación del contrato o caja menor; Correo del supervisor o cuentadante de caja menor que adquiera bienes y servicios o el correo que defina la entidad que opte por recepción centralizada, así:

Para la recepción centralizada por parte de la entidad PGN: 15-01-02-000; Contrato No XXX; facturaciondiadf@cgfm.mil.co

Es obligatorio diligenciar en la sección de la factura datos del emisor, en el campo "correo" la dirección electrónica del proveedor o contratista, en donde le será notificado en caso de existir fallas en la validación del correo, se recuerda que si la factura no es recibida y registrada en el SIIF Nación no va a ser posible generar obligaciones a favor de los proveedores y contratistas que están obligados a facturar electrónicamente, por cuanto éstas son un requisito para su elaboración.

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."

IX. REGISTRO ÚNICO DE PROPONENTES.

Teniendo en cuenta el Artículo 6 de la Ley 1150 de 2007, modificado por el artículo 221 del Decreto 19 de 2012 que establece:

"(…) ARTÍCULO 6o. DE LA VERIFICACIÓN DE LAS CONDICIONES DE LOS PROPONENTES. <Artículo modificado por el artículo 221 del Decreto 19 de 2012. El nuevo texto es el siguiente:> Todas las personas naturales o jurídicas nacionales o extranjeras domiciliadas o con sucursal en Colombia, que aspiren a celebrar contratos con las entidades estatales, se inscribirán en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio con jurisdicción en su domicilio principal.

No se requerirá de este registro, ni de clasificación, en los casos de contratación directa; contratos para la prestación de servicios de salud; contratos de mínima cuantía; enajenación de bienes del Estado; contratos que tengan por objeto la adquisición de productos de origen o

destinación agropecuaria que se ofrezcan en bolsas de productos legalmente constituidas; los actos y contratos que tengan por objeto directo las actividades comerciales e industriales propias de las empresas industriales y comerciales del Estado y las sociedades de economía mixta y los contratos de concesión de cualquier índole. En los casos anteriormente señalados, corresponderá a las entidades contratantes cumplir con la labor de verificación de las condiciones de los proponentes.

En dicho registro constará la información relacionada con la experiencia, capacidad jurídica, financiera y de organización del proponente y su clasificación. (…)"

El artículo 2.2.1.1.1.5.1 del decreto 1082 del 2015, señala:

"(…) INSCRIPCIÓN, RENOVACIÓN, ACTUALIZACIÓN Y CANCELACIÓN DEL RUP. Las personas naturales y jurídicas, nacionales o extranjeras, con domicilio en Colombia, interesadas en participar en Procesos de Contratación convocados por las Entidades Estatales, deben estar inscritas en el RUP, salvo las excepciones previstas de forma taxativa en la ley.

La persona inscrita en el RUP debe presentar la información para renovar su registro a más tardar el quinto día hábil del mes de abril de cada año. De lo contrario cesan los efectos del RUP. La persona inscrita en el RUP puede actualizar la información registrada relativa a su experiencia y capacidad jurídica en cualquier momento.

Los inscritos en el RUP pueden en cualquier momento solicitar a la cámara de comercio cancelar su inscripción. (…)"

Los proponentes singulares y cada uno de los integrantes de proponente plural, deberán allegar junto con la propuesta, original del Registro Único de Proponentes expedido por la Cámara de Comercio.

X. TIPO DE CONTRATO:

Contrato de servicios.

XI. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN.

A. La modalidad de selección.

Teniendo en cuenta el principio de legalidad, la escogencia del contratista será a través de la Licitación Pública que es la regla general. Sin embargo, dentro del Estatuto de Contratación, existen algunas excepciones a esta regla, razón por la cual corresponde determinar si el objeto del presente proceso de selección se encuadra dentro de una de las denominadas excepciones legales.

De acuerdo con lo anterior, tenemos que el Estatuto General de Contratación de la Administración Pública contempla ciertas excepciones a la regla general como lo es SELECCIÓN ABREVIADA DE MENOR CUANTÍA cuando se trate de la contratación de bienes y servicios que se requieran para la defensa y seguridad nacional.

Dicha modalidad a aplicar es la contemplada en el Título I, Artículo 2, Numeral 2, literal i de la Ley 1150 de 2007, y el Título I, artículo 2.2.1.1.2.1.1 Estudios Previos y Artículos 2.2.1.2.1.2.20 y 2.2.1.2.1.2.26 del Decreto 1082 de 2015, como a continuación se transcribe:

*"**ARTÍCULO 2o. DE LAS MODALIDADES DE SELECCIÓN**. La escogencia del contratista se efectuará con arreglo a las modalidades de selección de licitación pública, selección abreviada, concurso de méritos y contratación directa, con base en las siguientes reglas:*
(…)

2. Selección abreviada. La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

El Gobierno Nacional reglamentará la materia.

Serán causales de selección abreviada las siguientes:

(…)

i) La contratación de bienes y servicios que se requieran para la defensa y seguridad nacional. (…)" (Subrayas fuera del texto original)

A su turno, el Decreto 1082 de 2015, establece lo siguiente:

*"**Artículo 2.2.1.2.1.2.20. Procedimiento para la selección abreviada de menor cuantía**. Además de las normas generales establecidas en el presente título, las siguientes reglas son aplicables a la selección abreviada de menor cuantía:*

1. En un término no mayor a tres (3) días hábiles contados a partir de la fecha de apertura del Proceso de Contratación los interesados deben manifestar su intención de participar, a través del mecanismo establecido para el efecto en los pliegos de condiciones.

2. Si la Entidad Estatal recibe más de diez (10) manifestaciones de interés puede continuar el proceso o hacer un sorteo para seleccionar máximo diez (10) interesados con quienes continuará el Proceso de Contratación. La Entidad Estatal debe establecer en los pliegos de condiciones si hay lugar a sorteo y la forma en la cual lo hará.

3. Si hay lugar a sorteo, el plazo para la presentación de las ofertas empezará a correr el día hábil siguiente a la fecha en la cual la Entidad Estatal informe a los interesados el resultado del sorteo.

4. La Entidad Estatal debe publicar el informe de evaluación de ofertas durante tres (3) días hábiles."

*"**Artículo 2.2.1.2.1.2.26. Selección Abreviada para la adquisición de Bienes y Servicios para la Defensa y Seguridad Nacional**. Las Entidades Estatales que requieran contratar Bienes y Servicios para la Defensa y Seguridad Nacional deben hacerlo a través del procedimiento para la selección abreviada de menor cuantía señalado en el artículo 2.2.1.2.1.2.20 del presente decreto.*

Si los bienes y servicios que se requieran para la defensa y seguridad nacional son Bienes y Servicios de Características Técnicas Uniformes en los términos del artículo 2.2.1.1.1.3.1 del presente decreto, la Entidad Estatal debe utilizar el procedimiento de subasta inversa, compra por Catálogo derivado de la celebración de Acuerdos Marco de Precios o a través de bolsa de productos.

Las Entidades Estatales deben consignar en los Documentos del Proceso las razones por las cuales los bienes o servicios objeto del Proceso de Contratación son requeridos para la defensa y seguridad nacional."

De acuerdo con lo anterior, tenemos que cuando se trate de la contratación de bienes y servicios que se requieran para la defensa y seguridad nacional, sin consideración de la cuantía, el procedimiento a seguir será el indicado en el Artículo 2.2.1.2.1.2.20 del Decreto 1082 de 2015.

Sobre este punto debemos definir y entender la connotación y alcance de los "*bienes y servicios que se requieran para la defensa y seguridad nacional*", por lo que nos remitimos a lo indicado por el H. Consejo de estado Sección Tercera (Rad. 36805 de julio 23 de 2015) donde sostuvo:

"(…) a diferencia de normativas anteriores al EGCAP, en este los conceptos de "defensa nacional" y "seguridad nacional" no se circunscribieron al "material de guerra", aseveración que fue justificada, de una parte, en que se trata de conceptos normativos indeterminados, naturaleza en virtud de la que adquieren significación de conformidad con el contexto social, cultural y económico que refleja las necesidades de una colectividad en una circunstancia espacio-temporal definida» y agregó que «la "defensa y seguridad nacional" constituye una expresión medular del Estado como pacto político garante de la vida, honra y bienes de las personas, sirve como instrumento para buscar obtener el bienestar de los ciudadanos y la estabilidad misma del Estado, propósito que rebasa en forma considerable el plano estrictamente bélico o armamentista y que puede estar referido inclusive a asuntos económicos, energéticos, ambientales y hasta de salud pública (…)".

La Ley 1150 de 2007 al consagrar la modalidad de Selección Abreviada Menor Cuantía, bienes y servicios para la defensa y seguridad nacional, adoptó un criterio finalístico, es decir, aquel que obliga a desentrañar la finalidad, el propósito o el móvil del objeto contractual, independientemente de la Entidad estatal, que acuda a la esta modalidad de selección, lo importante es enmarcar el objeto dentro de ese concepto, y que sirvan o coadyuven a la defensa y seguridad nacional.

Siguiendo el mimo hilo conductor, es a lugar citar los artículos 2 y 217 de la Constitución Política de la República de Colombia, en donde se consagra los fines del Estado y la finalidad de las Fuerzas Militares, situaciones que guardan relación directa con el citado artículo de contratación que se ha venido predicando para la adquisición de Bienes y Servicios para la Defensa y Seguridad Nacional así:

> *"ARTICULO 2o. Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.*
>
> *Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.*
>
> *(…)*
>
> *ARTICULO 217. La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea.*
>
> *Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional.*
>
> *La Ley determinará el sistema de reemplazos en las Fuerzas Militares, así como los ascensos, derechos y obligaciones de sus miembros y el régimen especial de carrera, prestacional y disciplinario, que les es propio."* (subrayas fuera del texto original)

En este sentido, el Gerente del Proyecto mediante oficio con radicado N° 0125004101902 del 15 de abril de 2025 manifiesta las razones técnicas por las cuales el objeto del presente proceso es considerado como bienes y servicios para la defensa y seguridad nacional, lo cual guarda estricta relación con la justificación y antecedentes de la necesidad, y avalado para cumplir los fines institucionales.

Por lo tanto, queda plenamente justificada la modalidad de selección bajo el entendido de que los servicios o licencias o suscripciones (plataformas) que se pretenden adquirir, se encuentran considerados para la defensa y seguridad nacional, como quiera que su utilización para los diferentes componentes permitirá optimizar y coadyuvar a impactar objetivos estratégicos, proteger la soberanía y la integridad de territorio colombiano.

CONVOCATORIA LIMITADA A MIPYME:

1. PROCEDIMIENTO PARA LIMITAR A MIPYMES.

De conformidad con lo establecido en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, se limitará el presente proceso de selección a las MIPYME colombianas siempre y cuando concurran los siguientes requisitos:

- "1. *El valor del Proceso de Contratación sea menor a ciento veinticinco mil dólares de los Estados Unidos de América (US$125.000), liquidados con la tasa de cambio que para el efecto determina cada dos años el Ministerio de Comercio, Industria y Turismo."*

Umbral PYMES US$	$ 125.000
Umbral PYMES COL$	$ 533.287.768 (vigente hasta dic 31 de 2025)

El valor del presupuesto asignado para el presente proceso asciende a la suma de $2.952.734.688,00 por lo que el presente proceso **NO podrá ser limitado a Mipymes**.

- *"2. Se hayan recibido solicitudes de por lo menos dos (2) Mipyme colombianas para limitar la convocatoria a Mipyme colombianas. Las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, deben recibir estas solicitudes por lo menos un (1) día hábil antes de la expedición del acto administrativo de apertura, o el que haga sus veces de acuerdo con la normativa aplicable a cada Proceso de Contratación.*
  Tratándose de personas jurídicas, las solicitudes solo las podrán realizar Mipyme, cuyo objeto social les permita ejecutar el contrato relacionado con el proceso contractual."

NOTA 1: Las cooperativas y demás entidades de economía solidaria, siempre que tengan la calidad de Mipymes, podrán solicitar y participar en las convocatorias limitadas en las mismas condiciones dispuestas en el presente numeral.

Para efectos de dar oportunidad a que el presente proceso se limite a Mipyme, los interesados deberán solicitarlo durante el término establecido en el cronograma del proceso, a través de la plataforma del SECOP II, por "MENSAJE", para lo cual deberán cumplir con los requisitos que se señalan a continuación, de conformidad con el artículo 2.2.1.2.4.2.4. del Decreto 1082 de 2015:

> *"(…)* ***Artículo 2.2.1.2.4.2.4. Acreditación de requisitos para participar en convocatorias limitadas.*** *La Mipyme colombianas deben acreditar que tiene el tamaño empresarial establecido por la ley de la siguiente manera:*
>
> *1. Las personas naturales mediante certificación expedida por ellos y un contador público, adjuntando copia del registro mercantil.*
>
> *2. Las personas jurídicas mediante certificación expedida por el representante legal y el contador o revisor fiscal, si están obligados a tenerlo, adjuntando copia del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la autoridad competente para expedir dicha certificación.*
>
> *Para la acreditación deberán observarse los rangos de clasificación empresarial establecidos de conformidad con la Ley 590 de 2000 y el Decreto 1074 de 2015, o las normas que lo modifiquen, sustituyan o complementen.*
>
> *PARÁGRAFO 1. En todo caso, las Mipyme también podrán acreditar esta condición con la copia del certificado del Registro Único de Proponentes, el cual deberá encontrarse vigente y en firme al momento de su presentación.*
>
> *PARÁGRAFO 2. Para efectos de la limitación a Mipyme, los proponentes aportarán la copia del registro mercantil, del certificado de existencia y representación legal o del Registro Único de Proponentes, según corresponda conforme a las reglas precedentes, con una fecha de máximo sesenta (60) días calendario anteriores a la prevista en el cronograma del Proceso de Contratación para el inicio del plazo para solicitar la convocatoria limitada.*
>
> *PARÁGRAFO 3. En las convocatorias limitadas, las Entidades Estatales independientemente de su régimen de contratación, los patrimonios autónomos constituidos por Entidades Estatales y los particulares que ejecuten recursos públicos, solo deberán aceptar las ofertas de Mipyme o de proponentes plurales integrados únicamente por Mipyme. (…)"*

NOTA 1: En caso de no obtener el número mínimo de dos (02) manifestaciones de interés para llevar a cabo la convocatoria limitada a MIPYME, el proceso de selección se adelantará de manera abierta.

NOTA 2: En el presente proceso de selección y de encontrar cumplidos los Requisitos para limitar la convocatoria a Mipyme colombianas, solo se aceptarán las ofertas de Mipyme colombianas o de proponentes plurales integrados únicamente por Mipyme colombianas.

NORMAS APLICABLES.

Las normas vigentes de la legislación Colombiana se presumen conocidas por todos los proponentes.

- Constitución Política de la República de Colombia.
- Ley 57 de 1887 "Código Civil".
- Ley 1564 de 2012 "Código de Procedimiento Civil.
- Decreto 410 de 1971 "Código de Comercio".
- Ley 1437 de 2011 "Código de Procedimiento administrativo y de lo Contencioso Administrativo".
- Ley 100 de 1993 "Por la cual se crea el Sistema de Seguridad Social Integral y se dictan otras disposiciones"
- Ley 80 de 1993 "Por la cual se expide el Estatuto de la Contratación de la Administración Pública".
- Ley 1150 de 2007 "Por la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos".
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".
- Ley 1480 de 2011 "Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones." y sus decretos reglamentarios.

- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales y sus decretos reglamentarios.*"*
- Decreto Ley 019 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".
- Decreto 1082 de 2015. "Por medio del cual se expide el decreto único reglamentario del sector administrativo de planeación nacional" y sus Decretos reglamentarios.
- Decreto 680 de 2021 "*Por el cual se modifica parcialmente el artículo 2.2.1.1.1.3.1. y se adiciona el artículo 2.2.1.2.4.2.9. al Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, en relación con la regla de origen de servicios en el Sistema de Compra Pública"*
- Decreto 1860 de diciembre de 2021 "*Por el cual se modifica y adiciona el Decreto 1082 de 2015, Único reglamentario del Sector Administrativo de Planeación nacional, con el fin de reglamentar los artículos 30,31,32,34 y 35 de la Ley 2069 de 2020 en lo relativo al sistema de compras pública y se dictan otras disposiciones*".
- *Decreto 310 de 2021 " Por el cual se reglamenta el artículo 41 de la Ley 1955 de 2019, sobre las condiciones para implementar la obligatoriedad y aplicación de los Acuerdos Marco de Precios y se modifican los artículos 2.2.1.2.1.2.7. y 2.2.1.2.1.2.12. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional*
- Ley 1882 del 15 de enero 2018 "Por la cual se adicionan, modifican y dictan disposiciones orientadas a fortalecer la contratación pública en Colombia, la ley de infraestructura y se dictan otras disposiciones".
- 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.".*
- *Decreto 358 del 5 de marzo de 2020 "Por el cual se reglamentan los artículos 511,615,616-1,616-2,616-4,617,618, 618-2 Y 771-2 del Estatuto Tributario, 26 de la Ley 962 de 2005 y 183 de la Ley 1607 de 2012 y se sustituye el Capítulo 4 del Título 1 de la Parte 6 del Libro 1 del Decreto 1625 de 2016 Único Reglamentario en Materia Tributaria*." y circulares expedidas por la DIAN.
- Ley 2069 de 2020 *Emprendimiento en Colombia*
- Ley 2195 de 2022 "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones".
- Resolución 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. 4130 del 2022 "Por la cual se expide el Manual de Contratación y de Convenios".
- Resolución No. 4213 del 13 de octubre de 2023 "Por la cual se modifica la Resolución No. 4130 de 2022, que "expide el Manual de Contratación y de Convenios."
- Manuales y Guías emitidos por Colombia Compra Eficiente.
- Demás normas que deroguen, modifiquen, adicionen, aclaren o reglamenten las anteriores.

XII. ANÁLISIS TÉCNICO Y ECONÓMICO QUE SOPORTA EL VALOR ESTIMADO DEL CONTRATO.

A. Precios Históricos: N/A

B. Actualización de precios históricos: N/A

Con el fin de analizar los valores contratados en vigencias anteriores, fueron verificados los contratos de la vigencia 2024 sin embargo, estos valores no se incluyen dentro del análisis económico toda vez que para el presente proceso fueron modificadas las especificaciones técnicas de manera especial la ampliación de la garantía para la renovación de los licenciamientos.

C. Consulta SECOP:

De acuerdo con la consulta que se hizo en el SECOP, se encontraron las siguientes contrataciones, con especificaciones técnicas similares más no idénticas a las establecidas en el ANEXO del presente proceso.

NO. PROCESO	AÑO	OBJETO	MODALIDAD	ENTIDAD CONTRATANTE	CONTRATISTA	VALOR CONTRATO
262-GINREDCE-2025	2025	ADQUISICIÓN DE LICENCIAS SOFTWARE PARA LA SEGURIDAD WAF PARA 20 SITIOS DE LA DIRECCIÓN GENERAL MARÍTIMA (WEB APLICATION FIREWALL) /ANTI-DDOS, RENDIMIENTO WAF/ANTI-DDOS, GESTIÓN DE LA SEGURIDAD WAF/ANTI-DDOS, CONFORME CON LAS ESPECIFICACIONES ESTABLECIDAS EN EL ANEXO TÉCNICO	Selección abreviada menor cuantía	DIRECCIÓN GENERAL MARÍTIMA - SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA - SUBAFIN	CCD COMPAÑÍA DE CIBERSEGURIDAD Y DEFENSA SAS	320.397.000

NO. PROCESO	AÑO	OBJETO	MODALIDAD	ENTIDAD CONTRATANTE	CONTRATISTA	VALOR CONTRATO
PN DIPOL SA 015-2024	2024	ADQUISICIÓN FIREWALL PARA EL NIVEL DESCONCENTRADO DEL SERVICIO DE INTELIGENCIA Y ADQUISICIÓN PLATAFORMA ANTISPAM PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	Selección abreviada menor cuantía	DIRECCIÓN DE INTELIGENCIA POLICIAL	Open Group S.A.S	1.101.799.996
TT-71-2024	2024	LICENCIAMIENTO DEL FIREWALL-ANTIVIRUS Y ACCESO REMOTO PARA LOS EQUIPOS DE CÓMPUTO Y SERVIDORES DE LA TERMINAL DE TRANSPORTE	CONTRATACIÓN RÉGIMEN ESPECIAL	TERMINAL DE TRANSPORTE S.A	CLUSTER DE SERVICIOS SAS	89.528.750,00
UPIT-INV-002-2024	2024	ADQUISICIÓN DEL SERVICIO DE INTERNET Y FIREWALL PARA LA UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE UPIT	CONTRATACIÓN RÉGIMEN ESPECIAL	UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE	CITCOMM	75.985.900
SAMC-001-2024	2024	RENOVACIÓN DE LA GARANTÍA, SOPORTE Y MANTENIMIENTO PARA LOS SIGUIENTES EQUIPOS: DOS (2) FIREWALL FORTIGATE 601E, UN (1) FORTIANALYZER 400E, CINCO (5) ACCESS POINT FORTIAP 231F UBICADOS EN LA CIUDAD DE BOGOTÁ, UN (1) FIREWALL FORTIGATE 100F UBICADO EN LA CIUDAD DE MEDELLÍN DE LA CONTADURÍA GENERAL DE LA NACIÓN	SELECCIÓN ABREVIADA MENOR CUANTÍA	CONTADURÍA GENERAL DE LA NACIÓN	HEIMCORE SAS	263.647.475
UAESP-SASI-01-2024	2024	TIC-007 RENOVAR EL LICENCIAMIENTO FIREWALL Y ANTIMALWARE (ANTIVIRUS), PARA CONTROL DE LA SEGURIDAD INFORMÁTICA PERIMETRAL Y ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA EN LOS DISPOSITIVOS DE USUARIO FINAL DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS -UAESP	SELECCIÓN ABREVIADA SUBASTA INVERSA	UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS..	BLACK HAT ARCHETYPE S.A.S	316.314.000
FA-MC-F-S-002-2024	2024	RENOVACIÓN DEL LICENCIAMIENTO DE ANTIVIRUS ESET-ENDPOINT PROTECTION STANDARD	MÍNIMA CUANTÍA	FONDO ADAPTACIÓN	KAVANTIC SAS	15.436.000
SAMC-001-2024	2024	ADQUIRIR SOFTWARE CORRESPONDIENTE LICENCIAS DE "KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED" REQUERIDOS POR EL INSTITUTO DEPARTAMENTAL DE BELLAS ARTES PARA EL PERIODO 2024 - 2027.	SELECCIÓN ABREVIADA MENOR CUANTÍA	BELLAS ARTES	GRUPO MICROSISTEMAS COLOMBIA SAS	68.960.976
SIE NO. 21 RENOVACIÓN SOFTWARE PROXY 2021	2021	CONTRATAR LA RENOVACIÓN SOFTWARE DE CONTROL DE NAVEGACIÓN (PROXY), PARA EL MINISTERIO DE JUSTICIA Y DEL DERECHO.	SELECCIÓN ABREVIADA SUBASTA INVERSA	SIE NO. 21 RENOVACIÓN SOFTWARE PROXY 2021	GLOBALTEK SECURITY S.A.S.	109.789.400

Sondeo de mercado:

El comité técnico estructurador realizó el sondeo de mercado, y para ello solicitó cotizaciones a través de los siguientes canales:

SECOP II.

Con el fin de elaborar el estudio de mercado que permita establecer las condiciones económicas que se presentan en el sector y definir los precios de referencia para el presente proceso, el Comando General de la Fuerzas Militares – COGFM, solicitó cotizaciones mediante la plataforma del SECOP II bajo el número CO 152 COGFM DIADF 2025, para contratar el mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 del COGFM, de acuerdo con las especificaciones técnicas del ANEXO a las empresas que se encuentran registrados como proveedores de estos bienes y servicios en el Sistema Electrónico para la Contratación Pública de Colombia Compra Eficiente, donde se evidencian 1854 empresas inscritas, 11 interesada en el proceso y se recibieron 5 cotizaciones.

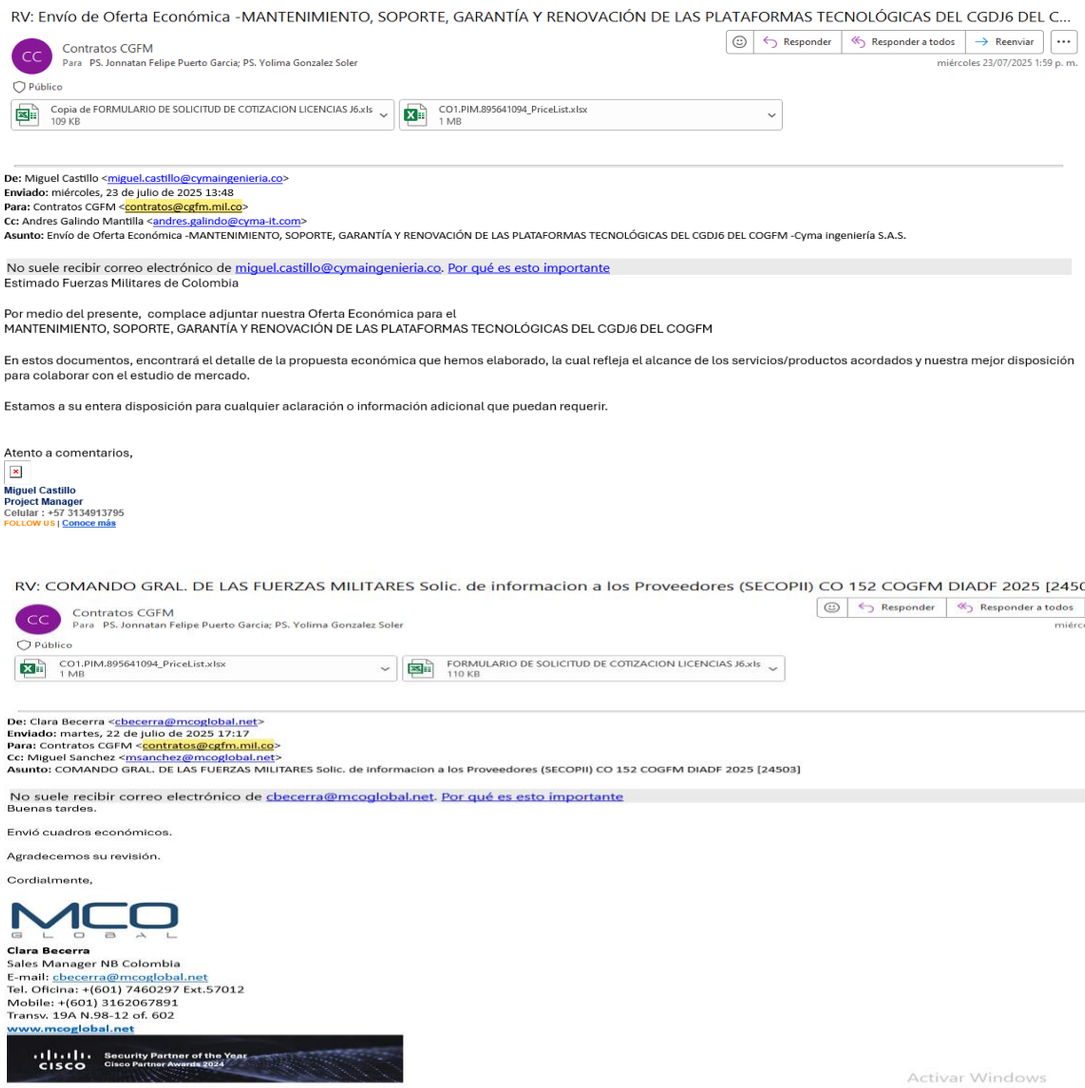


LISTA DE OFERTAS — Opciones

Referencia de oferta	Entidad	Presentada	Oferta
Estudio de Mercado Renovación - D&S	DATA Y SERVICE SAS	23/07/2025 1:49 PM	2.934.370.000
EM MANTENIMIENTO, SOPORTE Y GRANATIA PLATAFORMA TECNOLOGICA,	MCO GLOBAL SAS	23/07/2025 9:29 AM	75.803.897
EM_COGFM_Lotes_Ciber	Heimcore SAS	23/07/2025 9:03 AM	2.693.113.860
CO 152 COGFM DIADF 2025	NETWORK & ACCESORIES SAS	22/07/2025 9:39 AM	2.829.800.000
SPECTRUMCOTIZACION-CO-152-COGFM-DIADF-2025	SPECTRUMTECHNOLOGYSAS	21/07/2025 4:14 PM	2.901.200.000

Correo electrónico

Teniendo en cuenta que, durante la etapa del evento de cotización, la plataforma SECOP II, presentó indisponibilidad manifestando fallas para el recibido de información, las cotizaciones fueron allegadas al correo institucional **contratos@cgfm.mil.co,** como se muestra a continuación, donde se recibió información de 9 empresas para un total de 14 cotizaciones.



RV: Envío de Oferta Económica -MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL C...

Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler
Responder | Responder a todos | Reenviar
miércoles 23/07/2025 1:59 p. m.
Público
Copia de FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6.xls 109 KB
CO1.PIM.895641094_PriceList.xlsx 1 MB

De: Miguel Castillo <miguel.castillo@cymaingenieria.co>
Enviado: miércoles, 23 de julio de 2025 13:48
Para: Contratos CGFM <contratos@cgfm.mil.co>
Cc: Andres Galindo Mantilla <andres.galindo@cyma-it.com>
Asunto: Envío de Oferta Económica -MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM -Cyma ingeniería S.A.S.

No suele recibir correo electrónico de miguel.castillo@cymaingenieria.co. Por qué es esto importante
Estimado Fuerzas Militares de Colombia

Por medio del presente, complace adjuntar nuestra Oferta Económica para el
MANTENIMIENTO, SOPORTE, GARANTÍA Y RENOVACIÓN DE LAS PLATAFORMAS TECNOLÓGICAS DEL CGDJ6 DEL COGFM

En estos documentos, encontrará el detalle de la propuesta económica que hemos elaborado, la cual refleja el alcance de los servicios/productos acordados y nuestra mejor disposición para colaborar con el estudio de mercado.

Estamos a su entera disposición para cualquier aclaración o información adicional que puedan requerir.

Atento a comentarios,

Miguel Castillo
Project Manager
Celular : +57 3134913795
FOLLOW US | Conoce más

RV: COMANDO GRAL. DE LAS FUERZAS MILITARES Solic. de informacion a los Proveedores (SECOPII) CO 152 COGFM DIADF 2025 [24503]

Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler
Responder | Responder a todos | Reenviar
miércoles 23/07/2025 7:57 a. m.
Público
CO1.PIM.895641094_PriceList.xlsx 1 MB
FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6.xls 110 KB

De: Clara Becerra <cbecerra@mcoglobal.net>
Enviado: martes, 22 de julio de 2025 17:17
Para: Contratos CGFM <contratos@cgfm.mil.co>
Cc: Miguel Sanchez <msanchez@mcoglobal.net>
Asunto: COMANDO GRAL. DE LAS FUERZAS MILITARES Solic. de informacion a los Proveedores (SECOPII) CO 152 COGFM DIADF 2025 [24503]

No suele recibir correo electrónico de cbecerra@mcoglobal.net. Por qué es esto importante
Buenas tardes.

Envió cuadros económicos.

Agradecemos su revisión.

Cordialmente,

MCO GLOBAL

Clara Becerra
Sales Manager NB Colombia
E-mail: cbecerra@mcoglobal.net
Tel. Oficina: +(601) 7460297 Ext.57012
Mobile: +(601) 3162067891
Transv. 19A N.98-12 of. 602
www.mcoglobal.net

Activar Windows

RV: Cotización Estudio de Mercado -COGFM-J6

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler

Responder | Responder a todos | Reenviar

martes 22/07/2025 4:14 p. m.

Público

ANEXO ESPECIFICACIONES TECNICAS LICENCIAS - J6_ ITSTK.pdf 804 KB

Copia de FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6-ITSTK.pdf 218 KB

De: John Edwar Hennessey Calderon <John.hennessey@itstk.com>
Enviado: martes, 22 de julio de 2025 16:12
Para: PS. Yolima Gonzalez Soler <yolimagon@cgfm.mil.co>; Contratos CGFM <contratos@cgfm.mil.co>
Asunto: RV: Cotización Estudio de Mercado -COGFM-J6

Algunos contactos que recibieron este mensaje no suelen recibir correos electrónicos de john.hennessey@itstk.com. Por qué es esto importante

Cordialmente,

John E Hennessey C
Gerente Comercial Colombia

itstk comprometidos con tus retos



aws PARTNER Advanced Tier Services
- Public Sector
- Amazon EC2 for Windows Server Delivery

Cra 13 #93-35 piso 5
Cel: (57) 3114807311
Email:john.hennessey@itstk.com

Bogotá – Medellín – Lima - Mexico

www.itstk.com
IT's The Key to digital transformation

RV: Cotización Estudio de mercado CO 152 COGFM DIADF 2025

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler

Responder | Responder a todos | Reenviar

martes 22/07/2025 4:12 p. m.

Público

ANEXO ESPECIFICACIONES TECNICAS.pdf 836 KB

FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS.pdf 216 KB

De: Licitaciones Softsecurity <licitaciones@softsecuritycorp.com>
Enviado: martes, 22 de julio de 2025 16:10
Para: Contratos CGFM <contratos@cgfm.mil.co>
Cc: PS. Yolima Gonzalez Soler <yolimagon@cgfm.mil.co>
Asunto: RV: Cotización Estudio de mercado CO 152 COGFM DIADF 2025

No suele recibir correo electrónico de licitaciones@softsecuritycorp.com. Por qué es esto importante
Cordial Saludo,

Debido a la indisponibilidad de la plataforma de Secop II para responder al proceso CO 152 COGFM DIADF 2025 nos permitimos por este medio enviar oferta formal

Cordialmente,

20 AÑOS SoftSecurity



CATHERINE VELASCO CASTAÑEDA
Asistente Comercial y Licitaciones
licitaciones@softsecuritycorp.com
(601) 269 8731 Ext. 113 • Celular: 312 470 5231
Carrera 32A Bis No. 30 - 53 Bogotá
www.softsecuritycorp.com

RV: Oferta para Estudio de Mercado

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler

Responder | Responder a todos | Reenviar

martes 22/07/2025 3:35 p. m.

Público

ANEXO ESPECIFICACIONES TECNICAS LICENCIAS - J6 (1).pdf 827 KB

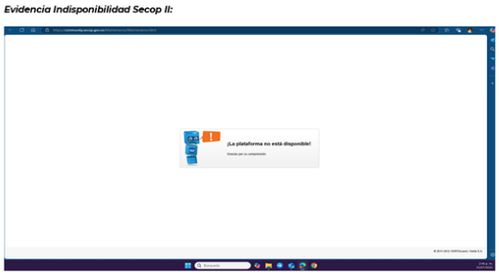
FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6.pdf 547 KB

Para: Contratos CGFM <contratos@cgfm.mil.co>
Asunto: Oferta para Estudio de Mercado

No suele recibir correo electrónico de valentina.mesa@dataysevice.com. Por qué es esto importante
Buenas tardes.

Debido a la indisponibilidad en la plataforma del Secop II, de la cual se adjunta evidencia, nos permitimos allegarles por este medio el formato de Oferta Económica y el Anexo Técnico para la renovación de las plataformas tecnológicas del CGDJ6 del COGFM.

Evidencia Indisponibilidad Secop II:



Agradecemos su atención.

Cordialmente,



Activar Windows
Ve a Configuración para activar Windows.

RV: OFERTA ESTUDIO CO 152 COGFM DIADF 2025

Responder | Responder a todos | Reenviar

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler
martes 22/07/2025 2:50 p. m.

Público

2 Observaciones ANEXO TÉCNICO LOTE 3.pdf 123 KB
FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6.pdf 444 KB

De: Gerencia Comercial <gerencia.comercial@htscorp.com.co>
Enviado: martes, 22 de julio de 2025 14:36
Para: Contratos CGFM <contratos@cgfm.mil.co>
Asunto: OFERTA ESTUDIO CO 152 COGFM DIADF 2025

No suele recibir correo electrónico de gerencia.comercial@htscorp.com.co. Por qué es esto importante
Buena tarde señores Comando General de las fuerzas Millitares,
Debido a que el SECOP se encuentra con indisponibilidad, se adjunta oferta para LOTE No. 3 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

Quedamos atentos a sus indicaciones.

Cordialmente,

High Tech Services

Juliana Sanabria Perez
HTS CORP | KAM
+57 3043423718
juliana.sanabria@htscorp.com.co

RV: Cotización estudio de mercado

Responder | Responder a todos | Reenviar

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler
martes 22/07/2025 2:50 p. m.

Público

Cotización COGFM.pdf 503 KB

De: licitacioneshsi@helpsoluciones.com.co <licitacioneshsi@helpsoluciones.com.co>
Enviado: martes, 22 de julio de 2025 14:35
Para: Contratos CGFM <contratos@cgfm.mil.co>
Asunto: Cotización estudio de mercado

No suele recibir correo electrónico de licitacioneshsi@helpsoluciones.com.co. Por qué es esto importante
Buenas tardes,

De acuerdo a lo solicitado adjunto la respectiva cotización.

Cordialmente,



FABIAN GONZALEZ
Analista Comercial
LICITACIONESHSI@HELPSOLUCIONES.COM.CO
310 767 0568
Help Soluciones Informaticas EXPERTOS EN TECNOLOGÍA
Diagonal 2B #82-30 Conjunto Naguara Américas Interior 5 Apartamento 118 Bogota- Colombia

HELP SOLUCIONES EXPERTOS EN TECNOLOGÍA

RV: COTIZACIÓN: CO 152 COGFM DIADF 2025

Responder | Responder a todos | Reenviar

CC Contratos CGFM
Para PS. Jonnatan Felipe Puerto Garcia; PS. Yolima Gonzalez Soler
martes 22/07/2025 2:49 p. m.

Público

FORMULARIO DE SOLICITUD DE COTIZACION LICENCIAS J6.xlsx 36 KB

De: Alejandra Betancourt Barrera <abetancourt@yeapdata.com>
Enviado: martes, 22 de julio de 2025 14:35
Para: Contratos CGFM <contratos@cgfm.mil.co>
Asunto: COTIZACIÓN: CO 152 COGFM DIADF 2025

No suele recibir correo electrónico de abetancourt@yeapdata.com. Por qué es esto importante
Buen día, espero se encuentren muy bien.

Teniendo en cuenta la indisponibilidad de la plataforma SECOP II, remito por este correo electrónico cotización del estudio de mercado para el proceso cuyo objeto consiste en: "contratar el mantenimiento, soporte, garantía y renovación de las plataformas tecnológicas del CGDJ6 del COGFM, de acuerdo con las especificaciones técnicas del ANEXO"

Quedamos atentos a cualquier inquietud, feliz día.

Cordialmente.

Yeapdata

Alejandra Betancourt Barrera.
Desarrollador de Negocios.
Carrera 19B # 84-17, Ofc 404
Bogotá, Colombia
(+57) 601 743 0077
(+57) 318 5896882
abetancourt@yeapdata.com

Activar Windows

Con los resultados que se muestran a continuación:

					COTIZACIÓN No. 1				COTIZACIÓN No. 2				COTIZACIÓN No. 3				COTIZACIÓN No. 5			
					SPECTRUM TECHNOLOGY SAS				NETWORK & ACCESORIES SAS				HEIMCORE SAS				DATA & SERVICE SAS			
	LOTE No. 1 LICENCIAS FIREWALL + VPN																			
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	MARCA OFERTADA	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1	Renovación y actualización del licenciamiento de la solución de seguridad perimetral del COGFM y garantía técnica por un (01) año. (De acuerdo a las especificaciones técnicas del Anexo)	5		UND	139.900.000,00	EXENTO	139.900.000,00	699.500.000,00	139.250.000,00	Exento	139.250.000,00	696250000	139.510.730,00	Exento	139.510.730,00	697.553.650,00	143.700.000,00	EXENTO	143.700.000,00	718.500.000,00
	VALOR TOTAL LOTE No. 1							699.500.000,00				696.250.000,00				697.553.650,00				718.500.000,00

				COTIZACIÓN No. 1				COTIZACIÓN No. 2				COTIZACIÓN No. 3				COTIZACIÓN No. 5				COTIZACIÓN No. 6			
				SPECTRUM TECHNOLOGY SAS				NETWORK & ACCESORIES SAS				HEIMCORE SAS				DATA & SERVICE SAS				YEAPDATA S.A.S.			
	LOTE No. 2 LICENCIAS PROXY																						
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM). (De acuerdo a las especificaciones técnicas del Anexo)	2	UND	161.350.000,00	EXENTO	161.350.000,00	322.700.000,00	147.310.000,00	Exento	147.310.000,00	294.620.000,00	141.730.000,00	Exento	141.730.000,00	283.460.000,00	158.930.000,00	EXENTO	158.930.000,00	317.860.000,00	142.510.000,00	Exento	142.510.000,00	285.020.000,00
VALOR TOTAL LOTE No. 2							322.700.000,00				294.620.000,00				283.460.000,00				317.860.000,00				285.020.000,00

					COTIZACIÓN No. 1				COTIZACIÓN No. 2	COTIZACIÓN No. 3	COTIZACIÓN No. 5				COTIZACIÓN No. 6			
					SPECTRUM TECHNOLOGY SAS				NETWORK & ACCESORIES SAS	HEIMCORE SAS	DATA & SERVICE SAS				YEAPDATA S.A.S.			
	LOTE No. 3 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS																	
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	MARCA OFERTADA	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR UNITARIO	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1,00	**SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS**																	
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	327.500.000,00	EXENTO	327.500.000,00	327.500.000,00	401.650.000,00	433.150.000,00	424.500.000,00	EXENTO	424.500.000,00	424.500.000,00	395.300.000,00	Exento	395.300.000,00	395.300.000,00
1.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	167.900.000,00	EXENTO	167.900.000,00	167.900.000,00	130.500.000,00	132.100.000,00	98.560.000,00	EXENTO	98.560.000,00	98.560.000,00	141.500.000,00	Exento	141.500.000,00	141.500.000,00
1.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	141.700.000,00	EXENTO	141.700.000,00	141.700.000,00	130.500.000,00	155.000.000,00	95.210.000,00	EXENTO	95.210.000,00	95.210.000,00	162.100.000,00	Exento	162.100.000,00	162.100.000,00
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	325.700.000,00	EXENTO	325.700.000,00	325.700.000,00	310.000.000,00	288.710.000,00	233.000.000,00	EXENTO	233.000.000,00	233.000.000,00	321.400.000,00	Exento	321.400.000,00	321.400.000,00
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	167.800.000,00	EXENTO	167.800.000,00	167.800.000,00	173.210.000,00	132.900.000,00	151.000.000,00	EXENTO	151.000.000,00	151.000.000,00	155.000.000,00	Exento	155.000.000,00	155.000.000,00
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	150.500.000,00	EXENTO	150.500.000,00	150.500.000,00	135.760.000,00	87.310.000,00	210.700.000,00	EXENTO	210.700.000,00	210.700.000,00	155.000.000,00	Exento	155.000.000,00	155.000.000,00
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	1,00		UND	185.600.000,00	EXENTO	185.600.000,00	185.600.000,00	172.100.000,00	95.200.000,00	265.000.000,00	EXENTO	265.000.000,00	265.000.000,00	113.600.000,00	Exento	113.600.000,00	113.600.000,00
	VALOR TOTAL LOTE No. 3							**1.466.700.000,00**						**1.477.970.000,00**				**1.443.900.000,00**

				COTIZACIÓN No. 7				COTIZACIÓN No. 8				COTIZACIÓN No. 10		
				HELP SOLUCIONES INFORMATICAS HSI SAS				HIGH TECH SERVICES CORP (HTS CORP) S.A.S.				RedNeet SAS		
	LOTE No. 3 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS													
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA
1,00	SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS													
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	223.268.000,00	-	223.268.000,00	223.268.000,00	250.505.600,00	-	250.505.600,00	250.505.600,00	237.789.104,00	-	237.789.104,00
1.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	180.333.300,00	-	180.333.300,00	180.333.300,00	191.083.500,00	-	191.083.500,00	191.083.500,00	189.820.365,00	-	189.820.365,00
1.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	143.808.800,00	-	143.808.800,00	143.808.800,00	151.664.800,00	-	151.664.800,00	151.664.800,00	152.492.374,00	-	152.492.374,00
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	66.956.900,00	-	66.956.900,00	66.956.900,00	71.631.400,00	-	71.631.400,00	71.631.400,00	67.541.902,00	-	67.541.902,00
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	47.069.300,00	-	47.069.300,00	47.069.300,00	49.210.100,00	-	49.210.100,00	49.210.100,00	46.367.056,00	-	46.367.056,00
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	12.657.700,00	-	12.657.700,00	12.657.700,00	13.877.200,00	-	13.877.200,00	13.877.200,00	13.642.293,00	-	13.642.293,00
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	390.253.900,00	-	390.253.900,00	390.253.900,00	400.931.300,00	-	400.931.300,00	400.931.300,00	388.372.514,00	-	388.372.514,00
	VALOR TOTAL LOTE No. 3						1.064.347.900,00				1.128.903.900,00			1.096.025.608,00

					COTIZACIÓN No. 9				COTIZACIÓN No. 11				COTIZACIÓN No. 12			
					IT SERVICIOS DE COLOMBIA SAS				ITSTK LTDA				SOFTSECURITY SAS			
LOTE No. 4 SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).																
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	MARCA OFERTADA	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1	SUSCRIPCIÓN FILTRADO Y PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM). (De acuerdo a las especificaciones técnicas del Anexo)	1.600		UND	124.944,04	0	124.944,04	199.910.464,00	136.633,13	-	136.633,13	218.613.008,00	128.415,00	0	128.415,00	205.464.000,00
	VALOR TOTAL LOTE No. 4							199.910.464,00				218.613.008,00				205.464.000,00

				COTIZACIÓN No. 1				COTIZACIÓN No. 2				COTIZACIÓN No. 3				COTIZACIÓN No. 5				COTIZACIÓN No. 6			
				SPECTRUM TECHNOLOGY SAS				NETWORK & ACCESORIES SAS				HEIMCORE SAS				DATA & SERVICE SAS				YEAPDATA S.A.S.			
LOTE No. 5 SUSCRIPCIÓN WAF.																							
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)	1,00	UND	412.300.000,00	EXENTO	412.300.000,00	412.300.000,00	385.210.000,00	Exento	385.210.000,00	385.210.000,00	387.730.210,00	Exento	387.730.210,00	387.730.210,00	377.900.000,00	EXENTO	377.900.000,00	377.900.000,00	433.100.000,00	Exento	433.100.000,00	433.100.000,00

					COTIZACIÓN No. 5				COTIZACIÓN No. 9				COTIZACIÓN No. 11				COTIZACIÓN No. 12			
					DATA & SERVICE SAS				IT SERVICIOS DE COLOMBIA SAS				ITSTK LTDA				SOFTSECURITY SAS			
LOTE No. 6 SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.																				
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD	MARCA OFERTADA	UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1	Suscripción de licenciamiento SASE, incluyendo (acceso de red de zero confianza (ZTNA), protección de amenazas sobre dispositivos móviles (MTD), acceso seguro para dispositivos no gestionados (Enterprise Browser) por un periodo de tiempo de 2 años. (De acuerdo a las especificaciones técnicas del Anexo	100		UND	421.400,00	EXENTO	421.400,00	42.140.000,00	1.997.386,97	0	1.997.386,97	199.738.697,00	2.184.000,00	-	2.184.000,00	218.400.000,00	2.000.540,00	0	2.000.540,00	200.054.000,00
	VALOR TOTAL LOTE No. 6							**42.140.000,00**				**199.738.697,00**				**218.400.000,00**				**200.054.000,00**

					COTIZACIÓN No. 4				COTIZACIÓN No. 13				COTIZACIÓN No. 14			
					MCO GLOBAL SAS				Cyma Ingeniería S.A.S				GLOBAL OPEN TECHNOLOGIES SAS			
LOTE No. 7 SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.																
No.	DESCRIPCIÓN DEL ELEMENTO O SERVICIO	CANTIDAD		UNIDAD DE MEDIDA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA	VALOR UNITARIO	VALOR IVA (*)	VALOR UNITARIO CON IVA	VALOR TOTAL INCLUIDO IVA
1,00	Suscripción del Licenciamiento de videoconferencia cisco Webex para equipos con aplicación en dispositivos móviles.	13,00		UND	5.831.069,00	EXENTO	5.831.069,00	75.803.897,00	5.820.000,00	-	5.820.000,00	75.660.000,00	5.800.000,00	-	5.800.000,00	75.400.000,00
	VALOR TOTAL LOTE No. 7							**75.803.897,00**				**75.660.000,00**				**75.400.000,00**

D. Términos de negociación (cuando se trate de importaciones). N/A.

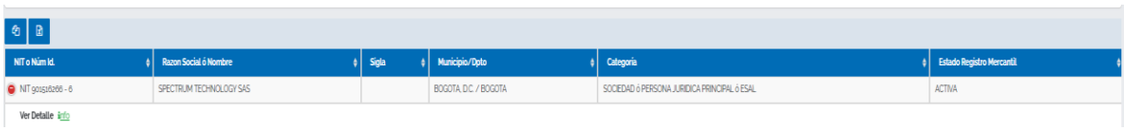
E. Consulta de la Tasa Representativa del Mercado: N/A.

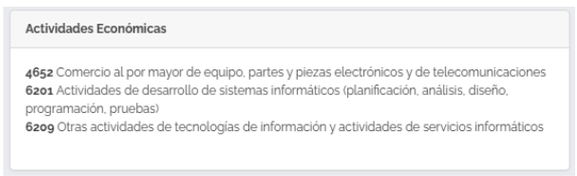
F. Información en el PORTAL DE INFORMACIÓN EMPRESARIAL DE LA SUPERSOCIEDADES/RUES:

El comité económico estructurador procedió a efectuar la verificación de las identificaciones tributarias en el Registro Único Empresarial y Social en el link www.rues.org.co, evidenciando que las firmas que presentaron información para el estudio de mercado, se encuentran activas en la consulta del RUES y que su actividad económica, guarda relación con el objeto del presente proceso de contratación, como se evidencia a continuación:

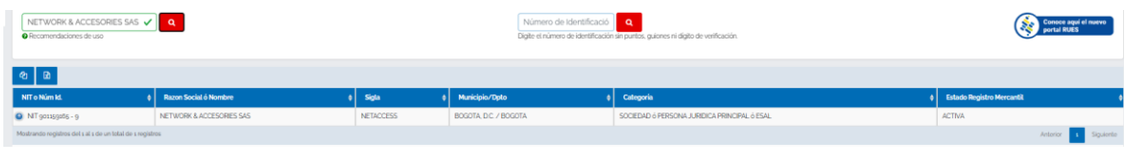
.

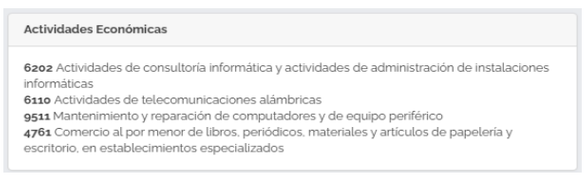
NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 901516266 - 6 SPECTRUM TECHNOLOGY SAS ACTIVA





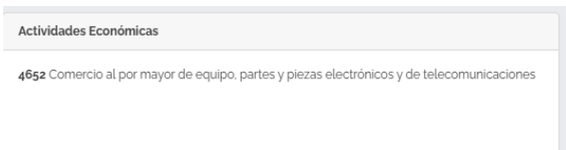
NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 901159165 - 9 NETWORK & ACCESORIES SAS ACTIVA



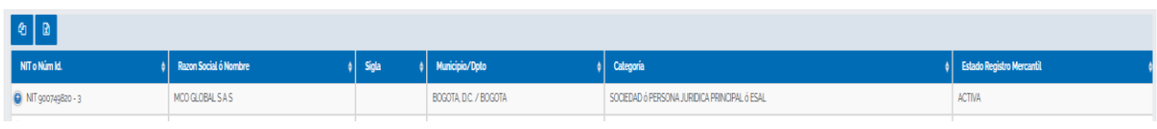


NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
HEIMCORE SAS ACTIVA





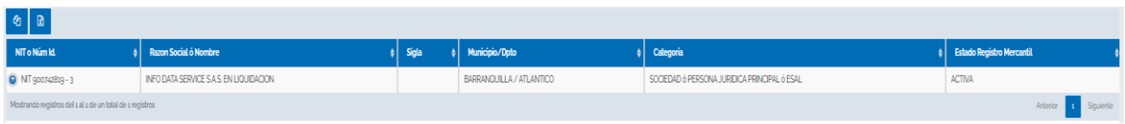
NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900749820 - 3 MCO GLOBAL S A S ACTIVA



Actividades Económicas

4652 Comercio al por mayor de equipo, partes y piezas electrónicos y de telecomunicaciones
6190 Otras actividades de telecomunicaciones
6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas

NIT o Núm. Id.	Razón Social o Nombre	Estado Registro Mercantil
NIT 900742819 - 3	INFO DATA SERVICE S.A.S. EN LIQUIDACIÓN	ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900742819 - 3	INFO DATA SERVICE S.A.S. EN LIQUIDACION		BARRANQUILLA / ATLANTICO	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

Mostrando registros del 1 al 1 de un total de 1 registros — Anterior 1 Siguiente

Actividades Económicas

8220 Actividades de centros de llamadas (call center)
7320 Estudios de mercado y realización de encuestas de opinión pública

NIT o Núm. Id.	Razón Social o Nombre	Estado Registro Mercantil
NIT 900311748 - 1	YEAPDATA S.A.S	ACTIVA



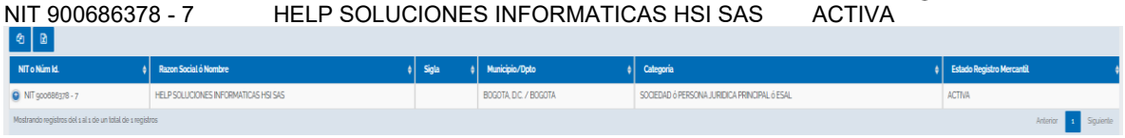
NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900311748 - 1	YEAPDATA S.A.S		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

Mostrando registros del 1 al 1 de un total de 1 registros — Anterior 1 Siguiente

Actividades Económicas

6190 Otras actividades de telecomunicaciones
4652 Comercio al por mayor de equipo, partes y piezas electrónicos y de telecomunicaciones
6810 Actividades inmobiliarias realizadas con bienes propios o arrendados

NIT o Núm. Id.	Razón Social o Nombre	Estado Registro Mercantil
NIT 900686378 - 7	HELP SOLUCIONES INFORMATICAS HSI SAS	ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900686378 - 7	HELP SOLUCIONES INFORMATICAS HSI SAS		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

Mostrando registros del 1 al 1 de un total de 1 registros — Anterior 1 Siguiente

Actividades Económicas

9511 Mantenimiento y reparación de computadores y de equipo periférico
9512 Mantenimiento y reparación de equipos de comunicación
4651 Comercio al por mayor de computadores, equipo periférico y programas de informática
4741 Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados

NIT o Núm. Id.	Razón Social o Nombre	Estado Registro Mercantil
NIT 901121717 - 1	HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	ACTIVA



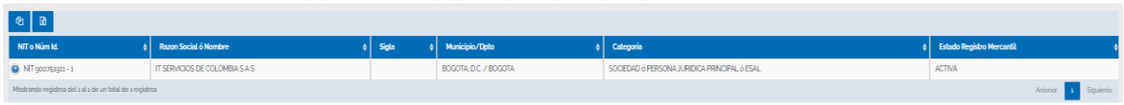
NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 901121717 - 1	HIGH TECH SERVICES CORP (HTS CORP) S.A.S.		BUCARAMANGA / SANTANDER	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	MATRÍCULA CANCELADA POR TRASLADO DE DOMICILIO
NIT 901121717 - 1	HIGH TECH SERVICES CORP (HTS CORP) S.A.S.		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

Mostrando registros del 1 al 2 de un total de 2 registros — Anterior 1 Siguiente

Actividades Económicas

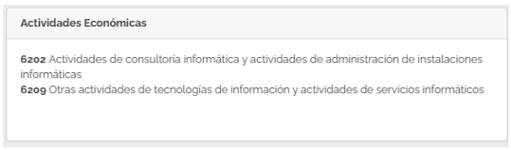
6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas
4651 Comercio al por mayor de computadores, equipo periférico y programas de informática
4741 Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados

NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900751911 - 1 IT SERVICIOS DE COLOMBIA S A S ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900751911 - 1	IT SERVICIOS DE COLOMBIA S A S		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

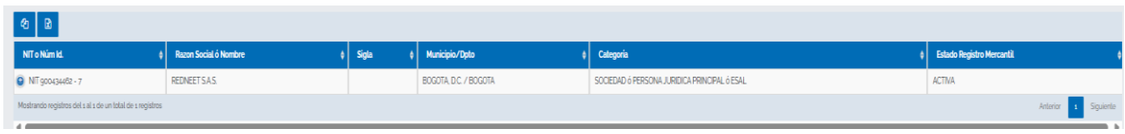
Mostrando registros del 1 al 1 de un total de 1 registros Anterior 1 Siguiente



Actividades Económicas

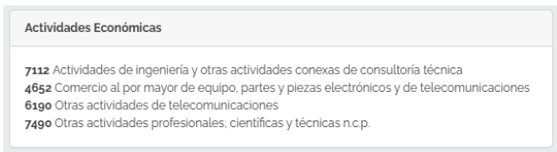
6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas
6209 Otras actividades de tecnologías de información y actividades de servicios informáticos

NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900434462 - 7 REDNEET S.A.S. ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900434462 - 7	REDNEET S.A.S.		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

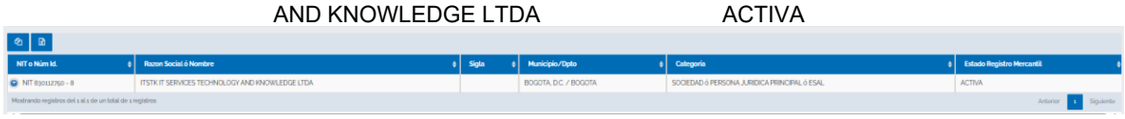
Mostrando registros del 1 al 1 de un total de 1 registros Anterior 1 Siguiente



Actividades Económicas

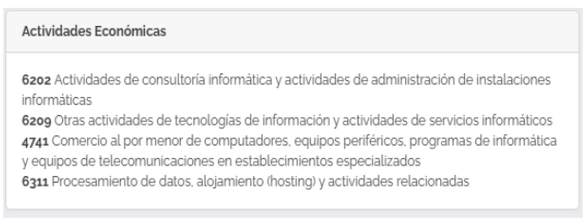
7112 Actividades de ingeniería y otras actividades conexas de consultoría técnica
4652 Comercio al por mayor de equipo, partes y piezas electrónicos y de telecomunicaciones
6190 Otras actividades de telecomunicaciones
7490 Otras actividades profesionales, científicas y técnicas n.c.p.

NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 830112750 - 8 ITSTK IT SERVICES TECHNOLOGY AND KNOWLEDGE LTDA ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 830112750 - 8	ITSTK IT SERVICES TECHNOLOGY AND KNOWLEDGE LTDA		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

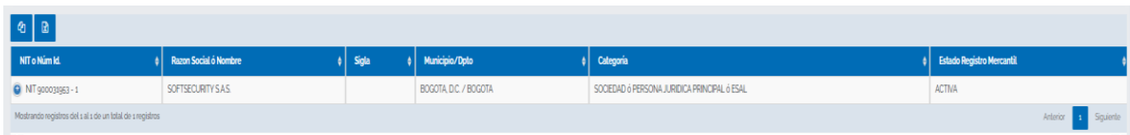
Mostrando registros del 1 al 1 de un total de 1 registros Anterior 1 Siguiente



Actividades Económicas

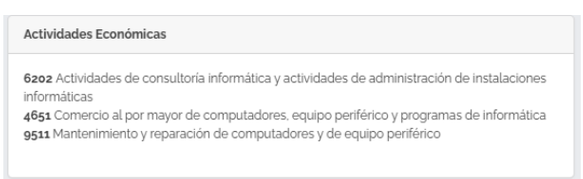
6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas
6209 Otras actividades de tecnologías de información y actividades de servicios informáticos
4741 Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados
6311 Procesamiento de datos, alojamiento (hosting) y actividades relacionadas

NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900031953 - 1 SOFTSECURITY S.A.S. ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900031953 - 1	SOFTSECURITY S.A.S.		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

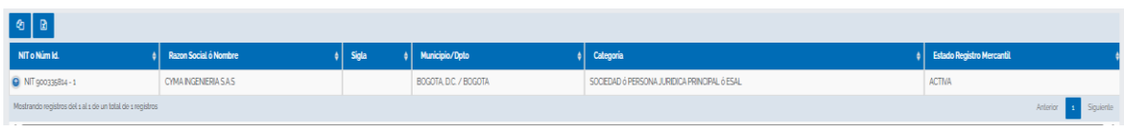
Mostrando registros del 1 al 1 de un total de 1 registros Anterior 1 Siguiente



Actividades Económicas

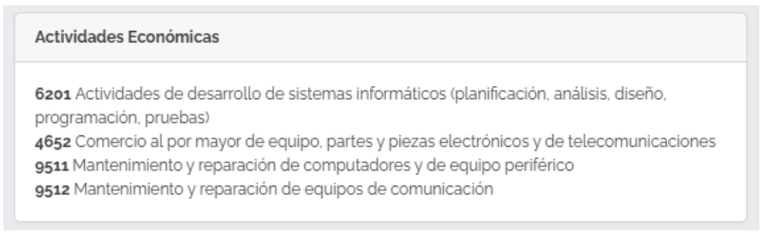
6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas
4651 Comercio al por mayor de computadores, equipo periférico y programas de informática
9511 Mantenimiento y reparación de computadores y de equipo periférico

NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900335814 - 1 CYMA INGENIERÍA S.A.SACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoría	Estado Registro Mercantil
NIT 900335814 - 1	CYMA INGENIERIA S.A.S		BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA

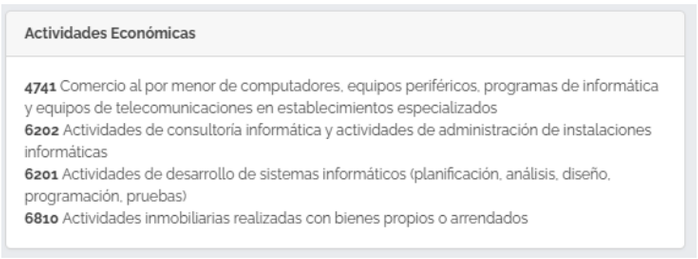
Mostrando registros del 1 al 1 de un total de 1 registros Anterior 1 Siguiente



NIT o Núm. Id. Razón Social o Nombre Estado Registro Mercantil
NIT 900461960 - 8 GLOBAL OPEN TECHNOLOGIES S A S ACTIVA



NIT o Núm Id.	Razon Social ó Nombre	Sigla	Municipio/Dpto	Categoria	Estado Registro Mercantil	Ver Detalle
NIT 900461960 - 8	GLOBAL OPEN TECHNOLOGIES S A S	GOTEC S A S	BOGOTA, D.C. / BOGOTA	SOCIEDAD ó PERSONA JURIDICA PRINCIPAL ó ESAL	ACTIVA	info



G. Análisis de impuestos a cancelar por parte del contratista:

Estarán a cargo del oferente todos los impuestos, derechos, tasas y similares que se deriven del contrato y por lo tanto su omisión en el pago será de su absoluta responsabilidad.

Los servicios por adquirir se encuentran excluidos de IVA:

Art. 476. Servicios excluidos del impuesto sobre las ventas

(…)

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

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

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

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

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

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

(…)

IMPUESTO AL TIMBRE

Conforme a lo establecido en el Estatuto Tributario, Art. 519. Base gravable en el impuesto de timbre nacional. (Modificado por el Art. 8 del Decreto 175 de 2025), aplica el pago por concepto de Impuesto del timbre, para los contratos en los que el valor estimado a celebrar supere los 6.000 UVT ($298.749.000).

Estarán a cargo del oferente todos los impuestos, derechos, tasas y similares que se deriven del contrato y por lo tanto su omisión en el pago será de su absoluta responsabilidad.

H. Cuadro cubrimiento de la necesidad:

LOTE No.	DESCRIPCIÓN DEL BIEN / SERVICIO	UNIDAD DE MEDIDA	NECESIDAD	PROYECTADO A ADQUIRIR	DÉFICIT
1	Renovación y actualización del licenciamiento de la solución de seguridad perimetral del COGFM y garantía técnica por un (01) año. (De acuerdo a las especificaciones técnicas del Anexo)	UN	5	5	0
2	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM). (De acuerdo a las especificaciones técnicas del Anexo)	UN	2	2	0
3	Suscripción de protección de datos				
3.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
3.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
4	SUSCRIPCIÓN FILTRADO Y PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM). (De acuerdo a las especificaciones técnicas del Anexo)	UN	1.600	1.600	0
5	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)	UN	1	1	0
6	Suscripción de licenciamiento SASE, incluyendo (acceso de red de zero confianza (ZTNA), protección de amenazas sobre dispositivos	UN	200	100	100

LOTE No.	DESCRIPCIÓN DEL BIEN / SERVICIO	UNIDAD DE MEDIDA	NECESIDAD	PROYECTADO A ADQUIRIR	DÉFICIT
	móviles (MTD), acceso seguro para dispositivos no gestionados (Enterprise Browser) por un periodo de tiempo de 2 años. (De acuerdo a las especificaciones técnicas del Anexo				
7	Suscripción del Licenciamiento de videoconferencia cisco Webex para equipos con aplicación en dispositivos móviles.	UN	13	13	0

Nota: El presente cuadro refleja las necesidades de la administración.

I. Conclusiones del análisis que soporta el valor estimado del contrato:

Una vez realizado el análisis comparativo de las cotizaciones allegadas y avaladas por el comité técnico estructurador, se realiza el análisis del precio del mercado conforme a las siguientes variables:

DESCRIPCIÓN		PROMEDIO	MEDIANA	MEDIA GEOMÉTRICA	MENOR VALOR	DESVIACIÓN ESTÁNDAR	MÉTODO ESCOGIDO
LOTE No. 1 LICENCIAS FIREWALL + VPN							
1	Renovación y actualización del licenciamiento de la solución de seguridad perimetral del COGFM y garantía técnica por un (01) año. (De acuerdo a las especificaciones técnicas del Anexo)	140.590.183,00	139.510.730,00	140.578.636,00	139.250.000,00	939.487,53	MENOR VALOR
LOTE No. 2 LICENCIAS PROXY WEB.							
1	Renovación garantía y soporte técnico, licencias de la plataforma de seguridad de filtrado y análisis web/proxy del fabricante (FORTINET Herramienta perteneciente al COGFM). (De acuerdo a las especificaciones técnicas del Anexo)	150.366.000,00	147.310.000,00	152.113.310,00	141.730.000,00	7.342.108,91	MEDIANA
LOTE No. 3 SUSCRIPCIÓN DE PROTECCIÓN DE DATOS							
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) (De acuerdo a las especificaciones técnicas del Anexo)	237.187.568,00	237.789.104,00	236.925.583,00	223.268.000,00	9.657.369,55	MEDIANA
1.2	SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA (De acuerdo a las especificaciones técnicas del Anexo)	187.079.055,00	189.820.365,00	187.016.808,00	180.333.300,00	4.725.953,83	MEDIANA
1.3	SUSCRIPCIÓN PARA LA DETECCIÓN Y PREVENCIÓN DE AMENAZAS SOBRE LA IDENTIDAD (De acuerdo a las especificaciones técnicas del Anexo)	149.321.991,00	151.664.800,00	149.270.090,00	143.808.800,00	3.861.715,19	MEDIANA
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES (De acuerdo a las especificaciones técnicas del Anexo)	68.710.067,00	67.541.902,00	68.679.009,00	66.956.900,00	1.217.714,95	MEDIANA
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS (De acuerdo a las especificaciones técnicas del Anexo)	47.548.819,00	47.069.300,00	47.533.578,00	46.367.056,00	824.855,62	MEDIANA
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS (De acuerdo a las especificaciones técnicas del Anexo)	13.392.398,00	13.642.293,00	13.381.804,00	12.657.700,00	512.018,85	MEDIANA
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA (De acuerdo a las especificaciones técnicas del Anexo)	393.185.905,00	390.253.900,00	393.147.242,00	388.372.514,00	3.376.242,55	MEDIANA
LOTE No. 4 SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).							
1	SUSCRIPCIÓN FILTRADO Y PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM). (De acuerdo a las especificaciones técnicas del Anexo)	129.997,00	128.415,00	129.906,00	124.944,00	3.508,66	MENOR VALOR
LOTE No. 5 SUSCRIPCIÓN WAF							
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF). (De acuerdo a las especificaciones técnicas del Anexo)	399.248.042,00	387.730.210,00	398.732.027,00	377.900.000,00	14.730.467,56	MEDIANA
LOTE No. 6 SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.							

	DESCRIPCIÓN	PROMEDIO	MEDIANA	MEDIA GEOMÉTRICA	MENOR VALOR	DESVIACIÓN ESTÁNDAR	MÉTODO ESCOGIDO
1	Suscripción de licenciamiento SASE, incluyendo (acceso de red de zero confianza (ZTNA), protección de amenazas sobre dispositivos móviles (MTD), acceso seguro para dispositivos no gestionados (Enterprise Browser) por un periodo de tiempo de 2 años. (De acuerdo a las especificaciones técnicas del Anexo	2.060.642,00	2.000.540,00	2.058.831,00	1.997.387,00	43.447,47	MENOR VALOR
LOTE No. 7 SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.							
1	Suscripción del Licenciamiento de videoconferencia cisco Webex para equipos con aplicación en dispositivos móviles.	5.817.023,00	5.820.000,00	5.817.009,00	5.800.000,00	12.027,18	MENOR VALOR

De acuerdo a lo anterior se tomó el método establecido conforme a las cotizaciones recibidas por cada lote, sin embargo, para el lote No. 1 teniendo en cuenta la dispersión tan alta entre las 8 cotizaciones recibidas, se tomó para el análisis las 3 cotizaciones de menor valor teniendo en cuenta que cumplen con las especificaciones técnicas requeridas y se ajusta al presupuesto de la entidad.

De igual manera para el lote No. 6, no se incluye dentro del análisis económico la cotización No. 5, toda vez que conforme a la información allegada el valor es muy disperso comparado con las demás cotizaciones recibidas, lo cual no garantiza el cumplimiento de las especificaciones técnicas requeridas, por lo cual se tomó el menor valor cotizado de las tres cotizaciones restantes.

El comité técnico verificó que el precio estimado incluye:

(i) Los costos de los bienes y/o servicios requeridos por la entidad IVA exento o excluido según aplique.
(ii) Personal profesional que prestará los servicios asociados con la instalación, configuración, pruebas, puesta en funcionamiento, etc.
(iii) Las demás erogaciones necesarias para el óptimo suministro de los bienes requeridos y prestación de los servicios asociados, tal como es requerido por la entidad contratante

XIII. REQUISITOS AMBIENTALES PROPIOS DEL PROCESO

El Comité técnico estructurador en coordinación con la Dirección de Protección de Recursos Estratégicos del COGFM, analizaron los aspectos e impactos ambientales asociados a la ejecución del contrato y determinan las obligaciones contractuales necesarias para el ejercer el control y/o disminución de impactos así:

ASPECTOS AMBIENTALES	IMPACTOS AMBIENTALES	OBLIGACIONES PARA EL CONTROL DE LOS ASPECTOS E IMPACTOS AMBIENTALES IDENTIFICADOS.
Para la ejecución del contrato no se identificaron aspectos ambientales	Para la ejecución del contrato no se identificaron impactos ambientales	Teniendo en cuenta que no se identificaron aspectos ni impactos ambientales, no se incluyen controles operacionales. Sin embargo, el contratista deberá garantizar las mejores prácticas durante la ejecución de su contrato y deberá cumplir con la normativa ambiental vigente.

XIV. REQUISITOS RELACIONADOS CON EL SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO. (Artículo 25 de la Resolución 0312 de 2019).

CUMPLIMIENTO SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO

Decreto 1072 de 2015 REGLAMENTO INTERNO DE TRABAJO, Artículo 2.2.4.6.4. Sistema de gestión de la seguridad y salud en el trabajo (SG-SST), señala: PARÁGRAFO 2. Dentro de los parámetros de selección y evaluación de proveedores y contratistas, el contratante podrá incluir criterios que le permitan conocer que la empresa a contratar cuente con el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SGSST). (Decreto 171 de 2016, Resolución 0312 de 2019 y demás normas que aplique al Sistema de Gestión de la Seguridad y Salud en el Trabajo.

En caso de tratarse de persona Natural o Jurídica o Consorcio o Unión Temporal, cada uno de sus miembros debe dar cumplimiento al presente requisito. Para lo anterior deberá diligenciar y presentar con la oferta ANEXO MANIFESTACIÓN DEL OFERENTE SOBRE EL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST)".

XV. JUSTIFICACIÓN DE LOS FACTORES DE SELECCIÓN QUE PERMITAN IDENTIFICAR LA OFERTA MAS FAVORABLE.

La modalidad para aplicar es la contemplada en el Título I, Artículo 2, Numeral 2, literal b de la Ley 1150 de 2007, y el Título I, Capitulo II, artículo 2.2.1.1.2.1.1 Estudios Previos y Artículo 2.2.1.2.1.2.20 del Decreto 1082 de 2015, que establece: "Procedimiento para la selección abreviada de menor cuantía". Adicionalmente de las demás normas establecidas en materia de contratación Estatal. Lo que nos permite que, por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual.

De acuerdo con el artículo 2.2.1.1.2.2.2 del Decreto 1082 de 2015 en las selecciones abreviadas se tendrá como criterio de evaluación la ponderación de los elementos de calidad y precios soportados en puntajes o formulas, para lo cual el pliego de condiciones establecerá las condiciones adicionales que representen ventajas cuantificables.

Tratándose de una selección objetiva se puede establecer que la modalidad a aplicar contemplada en el Título I, Capitulo II, Artículo 2.2.1.2.1.2.20 del Decreto 1082 de 2015 es SELECCIÓN ABREVIADA DE MENOR CUANTÍA, que rezan así:

Art 2.2.1.2.20: Procedimiento para la selección abreviada de menor cuantía. Además de las normas generales establecidas en el presente decreto, las siguientes reglas son aplicables a la selección abreviada de menor cuantía:

1. *En un término no mayor a tres (3) días hábiles contados a partir de la fecha de apertura del Proceso de Contratación los interesados deben manifestar su intención de participar a través del mecanismo establecido para el efecto en los pliegos de condiciones.*
2. *Si la Entidad Estatal recibe más de diez (10) manifestaciones de interés puede continuar el proceso o hacer un sorteo para seleccionar máximo diez (10) interesados con quienes continuará el Proceso de Contratación. La Entidad Estatal debe establecer en los pliegos de condiciones si hay lugar a sorteo y la forma en la cual lo hará.*
3. *Si hay lugar a sorteo, el plazo para la presentación de las ofertas empezará a correr el día hábil siguiente a la fecha en la cual la Entidad Estatal informe a los interesados el resultado del sorteo.*
4. *La Entidad Estatal debe publicar el informe de evaluación de ofertas durante tres (3) días hábiles".*

A. Requisitos habilitantes.

En cumplimiento de la exigencia de las condiciones técnicas, de experiencia, capacidad jurídica, financiera, de organización, la entidad exigirá el cumplimiento de los siguientes requisitos habilitantes, los cuales serán detallados en el proceso de selección y serán objeto de verificación por parte de los comités técnico, jurídico y económico evaluadores.

B. Criterios de verificación jurídica.

Se verificará la capacidad jurídica de acuerdo con la documentación presentada por el proponente con respecto a los requisitos de Ley para la contratación administrativa, según lo estipulado en el respectivo numeral de la invitación pública. Los aspectos jurídicos no darán lugar a puntaje, pero deshabilitarán o habilitarán las personas para su evaluación.

La oferta que cumpla con los documentos solicitados será considerada como elegible habilitado.

C. Criterios de verificación Económica

Para efectos de la evaluación económica se consideran propuestas hábiles aquellas que cumplan la totalidad de los requisitos habilitantes de orden jurídico, técnico y financiero.

D. Criterios de verificación Financiera:

Para efectos de la evaluación económica se consideran propuestas hábiles aquellas que cumplan la totalidad de los requisitos habilitantes de orden jurídico, técnico y financiero.

El Ministerio de Defensa Nacional - Comando General de las Fuerzas Militares – Dirección Administrativa y Financiera, efectuará el análisis a los estados Financieros teniendo en cuenta lo señalado en el artículo 6º de la Ley 1150 de 2007, en concordancia con el artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015, para lo cual realizará la verificación de los requisitos habilitantes de Capacidad Financiera y Capacidad Organizacional del Registro Único de Proponentes vigente y en firme al cierre del proceso ***(CIRCULAR EXTERNA ÚNICA,***

Código CCE-EICP-MA-06, Versión 03 de 27 de diciembre de 2023). La información financiera contenida en el RUP deberá corresponder al corte treinta y uno (31) de diciembre de 2024.

a. Para el caso de los proponentes nacionales, trátese de personas naturales, jurídicas, consorcios o uniones temporales, el cálculo de los indicadores financieros y capacidad organizacional serán tomadas de las cifras a 31 de diciembre de 2024, reportadas en el certificado del Registro Único de Proponentes, vigente y en firme.

b. Cuando se trate de personas natural o jurídicas extranjeras con domicilio o sucursal en Colombia, el cálculo de los indicadores financieros y capacidad organizacional de las cifras contenidas en el Certificado del Registro Único de Proponentes vigente y en firme, será de acuerdo con la información de la Capacidad Organizacional y los Estados Financieros de acuerdo al cierre fiscal en cada país de origen.

c. Para el caso de las personas natural o jurídicas nuevas o persona natural que no tenga antigüedad suficiente para tener estados financieros a 31 de diciembre de 2024, debe contener los estados financieros de corte trimestral, suscritos por el representante legal y el auditor o contador o estados financieros de apertura.

d. Para el análisis de la información e indicadores financieros se efectúo la respectiva consulta en la información disponible en el Sistema Integrado de información Societaria de la Súper Sociedades - SIIS con corte a diciembre 31 de 2024, la consulta se realiza en las actividades relacionadas con el código CIIU: G4774 - Comercio al por menor de otros productos nuevos en establecimientos especializados, El comercio al por menor de armas, municiones y chalecos blindados y El comercio al por menor de elementos de seguridad industrial y señalización industrial, donde se tomó una muestra de 359 empresas con este código de las cuales 271 son mipymes, como se muestra a continuación:

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
1	Plenas-Individuales	800143407	AVAL VALOR COMPARTIDO S.A	J6201	BOGOTÁ D.C.	8,19	12,21%	1,33	0,39%	0,32%
2	Plenas-Individuales	800198591	BRANCH OF MICROSOFT COLOMBIA INC	J6201	BOGOTÁ D.C.	1,42	70,53%	0,00	5,17%	1,55%
3	Plenas-Individuales	802015290	ANPALA S.A.S	J6201	ATLÁNTICO	1,51	66,36%	0,00	79,54%	27,33%
4	Plenas-Individuales	805012299	CODESA	J6201	VALLE	1,74	57,51%	1,30	3,63%	2,14%
5	Plenas-Individuales	811023886	INGENEO S.A.S.	J6201	ANTIOQUIA	2,14	46,63%	0,00	29,28%	11,60%
6	Plenas-Individuales	830013774	INDRA COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,34	74,49%	2,47	22,45%	7,43%
7	Plenas-Individuales	830096374	INDRA SISTEMAS S,A SUC COLOMBIA	J6201	BOGOTÁ D.C.	1,50	66,80%	0,00	87,36%	32,44%
8	Plenas-Individuales	830102565	MANTIZ ONLINE SAS	J6201	BOGOTÁ D.C.	5,66	17,67%	20,11	7,03%	6,17%
9	Plenas-Individuales	830111965	CONSULTORA NIVEL 7 SAS	J6201	BOGOTÁ D.C.	4,56	21,95%	20,16	30,84%	24,20%
10	Plenas-Individuales	830115764	BYTTE SAS	J6201	BOGOTÁ D.C.	1,03	97,33%	1,50	16,34%	7,11%
11	Plenas-Individuales	830118355	EASY SOLUTIONS SAS	J6201	BOGOTÁ D.C.	2,68	37,34%	0,18	2,09%	1,29%
12	Plenas-Individuales	900060799	IDEMIA IDENTITY & SECURITY SUCURSAL COLOMBIA	J6201	BOGOTÁ D.C.	1,08	92,94%	4,47	86,91%	7,91%
13	Plenas-Individuales	900129872	ZEMOGA S.A.S	J6201	BOGOTÁ D.C.	2,13	47,03%	4,91	49,99%	32,12%
14	Plenas-Individuales	900195138	EPAM SYSTEMS COLOMBIA S.A.S	J6201	BOGOTÁ D.C.	2,88	34,75%	3,56	52,53%	32,82%
15	Plenas-Individuales	900218578	SISTEMAS COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,50	66,52%	6,97	29,14%	13,18%
16	Plenas-Individuales	900237820	QUANTUM DATA PROCESSING DE COLOMBIA S.A.S.	J6201	BOGOTÁ D.C.	1,21	82,34%	18,66	107,49 %	78,47%
17	Plenas-Individuales	900294476	SYSTEMICO SOFTWARESAS	J6201	SANTANDER	0,35	284,81%	5,52	7,75%	1,63%
18	Plenas-Individuales	900376503	VASS CONSULTORIA DE SISTEMAS COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,99	50,24%	18,69	61,61%	32,43%
19	Plenas-Individuales	900420814	HITSS COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,59	62,81%	11,39	99,31%	40,21%
20	Plenas-Individuales	900512356	CAPGEMINI COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,82	55,09%	334,25	46,25%	21,71%
21	Plenas-Individuales	900569535	HELICE R&D GROUP SAS	J6201	BOGOTÁ D.C.	1,41	70,77%	4,88	1,38%	1,16%
22	Plenas-Individuales	900584902	LIBERA SUPPLY CHAIN FINANCE S.A.S. La	J6201	ANTIOQUIA	0,89	112,51%	0,00	17,74%	12,96%
23	Plenas-Individuales	900594521	Endava Colombia S.A.S	J6201	ANTIOQUIA	3,70	27,03%	4,83	32,53%	22,43%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 (CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
24	Plenas-Individuales	900620832	SOFKA TECHNOLOGIES S.A.S.	J6201	ANTIOQUIA	1,66	60,15%	0,00	63,14%	26,05%
25	Plenas-Individuales	900797285	HUGE SAS	J6201	BOGOTÁ D.C.	4,07	24,55%	2,91	28,59%	22,12%
26	Plenas-Individuales	900834939	TWILIO COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,41	71,06%	3,02	51,87%	18,66%
27	Plenas-Individuales	900843898	Rappi SAS	J6201	BOGOTÁ D.C.	1,38	72,30%	0,85	68,62%	16,60%
28	Plenas-Individuales	900955679	Endava S.A.S.	J6201	BOGOTÁ D.C.	4,26	23,46%	4,32	32,56%	22,36%
29	Plenas-Individuales	901245825	SOLINFTEC AMERICA LATINA SAS	J6201	VALLE	2,66	37,59%	21,00	31,08%	20,13%
30	Plenas-Individuales	901284844	PERFILES Y SOLUCIONES TECNOLÓGICAS SAS	J6201	ATLÁNTICO	2,34	42,80%	1,48	10,57%	4,61%
31	Plenas-Individuales	901323081	COPILOTO COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,25	79,70%	1,19	17,24%	9,56%
32	Plenas-Individuales	901361537	Loggro SAS	J6201	ANTIOQUIA	0,64	155,46%	1,95	4,45%	3,24%
33	Plenas-Individuales	901376233	VANTRAN SAS	J6201	VALLE	28,82	3,47%	317,71	37,86%	36,73%
34	Plenas-Individuales	901376797	SOFTLITICS SAS	J6201	VALLE	50,26	1,99%	117,17	25,16%	24,73%
35	Plenas-Individuales	901530710	VALTECH COLOMBIA SAS	J6201	BOGOTÁ D.C.	2,33	42,89%	3,46	44,70%	27,38%
36	Plenas-Separados	800090963	SOFTLAND COLOMBIA SAS	J6201	BOGOTÁ D.C.	0,64	155,81%	0,00	16,83%	9,39%
37	Plenas-Separados	805025355	NEXURA INTERNACIONAL SAS	J6201	BOGOTÁ D.C.	2,18	45,86%	51,73	31,53%	18,00%
38	Plenas-Separados	811003486	QUIPUX S.A.S.	J6201	ANTIOQUIA	1,96	50,93%	3,66	24,92%	13,06%
39	Plenas-Separados	811004057	PRAGMA S.A.	J6201	ANTIOQUIA	1,43	69,90%	1,98	38,20%	12,87%
40	Plenas-Separados	811020576	CHOUCAIR CARDENAS TESTING SA	J6201	ANTIOQUIA	1,41	70,74%	0,00	16,73%	9,63%
41	Plenas-Separados	830105621	OSP INTERNATIONAL CALA SAS	J6201	BOGOTÁ D.C.	1,87	53,54%	5,18	34,34%	17,74%
42	Plenas-Separados	890319193	SISTEMAS DE INFORMACIÓN EMPRESARIAL SAS	J6201	VALLE	1,63	61,52%	35,05	156,14 %	64,10%
43	Plenas-Separados	900224316	TECH AND SOLVE SAS	J6201	ANTIOQUIA	1,83	54,61%	2,90	37,73%	18,21%
44	Plenas-Separados	900353530	ACI WORLDWIDE COLOMBIA SAS	J6201	BOGOTÁ D.C.	3,48	28,72%	11,26	6,97%	4,31%
45	Plenas-Separados	900711074	SKG TECNOLOGÍA S.A.S.	J6201	BOGOTÁ D.C.	1,42	70,32%	1,87	43,21%	15,40%
46	Plenas-Separados	900718336	HIGH TECH SOFTWARE SAS	J6201	BOGOTÁ D.C.	1,44	69,28%	10,52	38,33%	19,01%
47	Plenas-Separados	901034523	MASIVIAN SAS	J6201	BOGOTÁ D.C.	2,86	34,96%	7,55	23,93%	18,58%
48	Plenas-Separados	901328325	ADL DIGITAL LABSAS	J6201	BOGOTÁ D.C.	1,78	56,08%	0,00	42,18%	24,67%
49	Pymes-Individuales	800028326	NOVASOFT SAS	J6201	BOGOTÁ D.C.	2,05	48,74%	81,83	54,11%	29,43%
50	Pymes-Individuales	800101428	PARADIGMA SAS	J6201	BOGOTÁ D.C.	6,04	16,57%	10,06	20,81%	18,45%
51	Pymes-Individuales	800111946	TRILLIANT NETWORKS COLOMBIA SAS	J6201	BOGOTÁ D.C.	2,21	45,23%	115,69	94,27%	50,57%
52	Pymes-Individuales	800132302	OFIMA SAS	J6201	ANTIOQUIA	1,94	51,49%	0,80	2,77%	1,64%
53	Pymes-Individuales	800146041	DMS SA	J6201	ANTIOQUIA	5,29	18,91%	0,00	19,75%	16,24%
54	Pymes-Individuales	800153961	OMNICON SAS	J6201	VALLE	2,79	35,80%	5,25	27,75%	18,28%
55	Pymes-Individuales	800182856	TNS SAS	J6201	NORTE DE SANTANDER	3,16	31,61%	31,56	44,43%	34,87%
56	Pymes-Individuales	800201664	ACIES SAS	J6201	BOGOTÁ D.C.	1,97	50,86%	0,00	9,18%	5,19%
57	Pymes-Individuales	800225066	T4I S.A.S. BIC	J6201	SANTANDER	2,42	41,38%	14,92	26,69%	17,72%
58	Pymes-Individuales	800233280	BANKVISION SOFTWARE SAS	J6201	BOGOTÁ D.C.	3,40	29,44%	6,30	21,66%	12,54%
59	Pymes-Individuales	800240660	SERVISOFT S.A.	J6201	ANTIOQUIA	5,09	19,66%	0,00	8,42%	3,93%
60	Pymes-Individuales	804002893	PENSEMOS S.A	J6201	SANTANDER	3,46	28,88%	2065,64	11,72%	9,24%
61	Pymes-Individuales	804010488	SCIENCE & TECHNOLOGY SAS	J6201	SANTANDER	2,25	44,48%	0,00	19,55%	7,57%
62	Pymes-Individuales	805020546	GRUPO BIT S.A.S	J6201	VALLE	2,77	36,14%	8,67	11,20%	7,33%
63	Pymes-Individuales	805027890	SMART TMT SAS	J6201	VALLE	1,92	51,95%	4,65	27,24%	18,84%
64	Pymes-Individuales	806009721	CONDOR LABS SAS	J6201	BOLÍVAR	8,58	11,66%	2,78	32,23%	25,41%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
65	Pymes-Individuales	811009452	XENCO S.A.	J6201	ANTIOQUIA	4,18	23,93%	19,36	47,17%	34,78%
66	Pymes-Individuales	811022382	PERSONAL SOFT S.A.S	J6201	ANTIOQUIA	1,64	60,90%	11,52	77,97%	25,82%
67	Pymes-Individuales	811022765	PERCEPTIO SAS	J6201	ANTIOQUIA	1,47	68,02%	2,51	34,46%	9,51%
68	Pymes-Individuales	830015727	AXESNET SAS	J6201	BOGOTÁ D.C.	0,91	110,05%	1,39	19,26%	3,82%
69	Pymes-Individuales	830016840	CROMASOFT S.A.S.	J6201	BOGOTÁ D.C.	14,50	6,90%	81,42	31,72%	29,53%
70	Pymes-Individuales	830016890	PCT LTDA	J6201	BOGOTÁ D.C.	4,18	23,94%	30,14	11,48%	10,16%
71	Pymes-Individuales	830028243	OPENCARD SAS	J6201	BOGOTÁ D.C.	3,45	28,95%	0,00	12,58%	9,23%
72	Pymes-Individuales	830042385	KRYPTO CONSULTORIA SAS BIC	J6201	BOGOTÁ D.C.	1,23	81,22%	1,27	39,30%	14,18%
73	Pymes-Individuales	830045792	Call Processing Technologies SA	J6201	BOGOTÁ D.C.	3,66	27,33%	0,00	19,41%	12,93%
74	Pymes-Individuales	830062674	INFORMACIÓN LOCALIZADA SAS	J6201	BOGOTÁ D.C.	4,91	20,37%	1,99	79,75%	24,08%
75	Pymes-Individuales	830065485	ALLIANCE ENTERPRISE SAS	J6201	BOGOTÁ D.C.	1,19	83,73%	5,54	8,76%	1,92%
76	Pymes-Individuales	830102216	PROCESOS Y SERVICIOS SAS	J6201	BOGOTÁ D.C.	5,28	18,92%	0,00	10,55%	7,96%
77	Pymes-Individuales	830116173	EVENTOS Y SISTEMAS SAS	J6201	BOGOTÁ D.C.	1,85	53,98%	0,00	79,36%	40,25%
78	Pymes-Individuales	830120348	TODOSISTEMAS OLUCIONES DE TECNOLOGÍA DE INFORMACIÓN SAS EN REORGANIZACION	J6201	BOGOTÁ D.C.	0,88	113,53%	6,23	7,43%	3,99%
79	Pymes-Individuales	830132832	IDENTICA SAS	J6201	BOGOTÁ D.C.	2,75	36,32%	0,00	11,85%	7,77%
80	Pymes-Individuales	830135010	OPENTECNOLOGIA S.A	J6201	BOGOTÁ D.C.	3,35	29,89%	63,28	71,14%	52,11%
81	Pymes-Individuales	830135451	SKIT CONSULTING SAS	J6201	BOGOTÁ D.C.	1,75	57,07%	2,57	55,48%	23,42%
82	Pymes-Individuales	830137539	ITAC, IT APPLICATIONS CONSULTING S.A.S.	J6201	BOGOTÁ D.C.	1,98	50,58%	1,12	61,58%	12,33%
83	Pymes-Individuales	830140028	PRAXIS I.T COLOMBIA LTDA	J6201	BOGOTÁ D.C.	3,31	30,22%	0,00	39,17%	21,78%
84	Pymes-Individuales	830141127	GRUPO DOT	J6201	BOGOTÁ D.C.	10,52	9,50%	0,00	0,69%	0,63%
85	Pymes-Individuales	830507528	TURRISYSTEM SAS	J6201	TOLIMA	0,58	173,52%	20,73	43,25%	22,12%
86	Pymes-Individuales	830511044	GROWING NETWORK SAS	J6201	SANTANDER	7,31	13,68%	0,00	22,83%	16,32%
87	Pymes-Individuales	860517277	SISTEMAS G&G SA	J6201	BOGOTÁ D.C.	3,09	32,33%	8,27	13,28%	9,17%
88	Pymes-Individuales	890914063	COMPONENTES ELECTRONICAS LTDA	J6201	ANTIOQUIA	3,71	26,96%	16,43	10,83%	8,81%
89	Pymes-Individuales	900037743	LINKTIC SAS	J6201	BOGOTÁ D.C.	7,17	13,95%	0,00	34,94%	21,60%
90	Pymes-Individuales	900046561	INFORMATICA CREATIVA SAS	J6201	VALLE	2,15	46,42%	9,81	31,50%	25,33%
91	Pymes-Individuales	900074458	GREEN SQA SAS	J6201	VALLE	5,76	17,37%	18,79	16,30%	13,49%
92	Pymes-Individuales	900093735	CYMETRIA GROUP SAS	J6201	BOGOTÁ D.C.	2,06	48,49%	395,59	85,95%	46,92%
93	Pymes-Individuales	900108082	Soluciones Profesionales Inteligentes SAS	J6201	CAUCA	2,51	39,80%	4,11	19,57%	12,56%
94	Pymes-Individuales	900122930	METROFFLEX SAS	J6201	VALLE	13,45	7,44%	1,02	16,84%	4,45%
95	Pymes-Individuales	900174004	ASESORIA Y CONSULTORIA PROFESIONAL EN INGENIERÍA DE AVANZADA LTDA	J6201	BOGOTÁ D.C.	2,24	44,60%	114,70	31,58%	21,49%
96	Pymes-Individuales	900182503	KOOMBEA SAS	J6201	ATLÁNTICO	0,87	115,23%	0,10	5,88%	0,85%
97	Pymes-Individuales	900184755	TIQAL SAS	J6201	VALLE	3,27	30,58%	0,00	17,86%	7,73%
98	Pymes-Individuales	900193641	MAYASOFT SAS	J6201	SANTANDER	12,43	8,05%	0,00	32,02%	29,48%
99	Pymes-Individuales	900193723	NETWCONSULTING S.A.S	J6201	ANTIOQUIA	1,22	81,78%	2,47	6,38%	4,66%
100	Pymes-Individuales	900219834	F2X SAS	J6201	ANTIOQUIA	1,69	59,31%	9,82	46,59%	24,14%
101	Pymes-Individuales	900242188	NEBULA ENGINEERING SAS	J6201	ANTIOQUIA	1,79	55,87%	6,19	46,60%	20,76%
102	Pymes-Individuales	900250454	ALTO COLOMBIA SAS	J6201	BOGOTÁ D.C.	2,16	46,34%	1,76	28,48%	15,47%
103	Pymes-Individuales	900272469	WG CONSULTORES SST SAS	J6201	ANTIOQUIA	1,15	86,77%	3,09	32,69%	12,75%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
104	Pymes-Individuales	900277173	INFORMATICA COLECTIVA S.A.	J6201	BOGOTÁ D.C.	1,17	85,50%	0,00	139,50 %	40,23%
105	Pymes-Individuales	900293512	SOLUCIONES DE INFORMACIÓN S.A.S	J6201	RISARALDA	1,69	59,14%	10,99	144,45 %	54,26%
106	Pymes-Individuales	900302739	R&C BUSINESS CONSULTING LTDA	J6201	BOGOTÁ D.C.	4,04	24,77%	12,52	14,93%	8,85%
107	Pymes-Individuales	900318963	INFORMATICA Y TRIBUTOS SAS	J6201	ATLÁNTICO	2,25	44,41%	0,00	27,20%	17,02%
108	Pymes-Individuales	900320258	PROSOF SAS	J6201	RISARALDA	0,45	221,30%	1,70	20,04%	10,10%
109	Pymes-Individuales	900331794	NETUX S.A.S.	J6201	ANTIOQUIA	1,96	51,04%	0,00	16,99%	8,21%
110	Pymes-Individuales	900332892	ENTERDEV SAS	J6201	ANTIOQUIA	5,43	18,43%	2,33	15,08%	12,28%
111	Pymes-Individuales	900335350	CREASISTEMAS S.A.S	J6201	BOGOTÁ D.C.	2,16	46,23%	293,78	85,52%	47,94%
112	Pymes-Individuales	900337757	INFODEC SAS	J6201	VALLE	2,58	38,72%	26,79	95,40%	59,43%
113	Pymes-Individuales	900358726	ENGHOUSE INTERACTIVE SAS	J6201	BOGOTÁ D.C.	11,78	8,49%	8,81	34,53%	31,51%
114	Pymes-Individuales	900369142	IWIN S.A.S	J6201	CUNDINAMARCA	1,52	65,84%	3,71	8,56%	6,90%
115	Pymes-Individuales	900379495	GRUPO CLICKIDEA SAS	J6201	BOGOTÁ D.C.	3,19	31,39%	18,63	37,78%	28,75%
116	Pymes-Individuales	900379770	SIGMATECNOL S.A.S.	J6201	BOLÍVAR	1,44	69,65%	365,86	22,94%	12,11%
117	Pymes-Individuales	900420501	OLSOFTWARE SAS	J6201	VALLE	1,63	61,51%	0,00	23,75%	12,45%
118	Pymes-Individuales	900530093	SIX TECHNOLOGY CONSULTORIA Y SERVICIOS SAS	J6201	VALLE	1,25	80,17%	0,00	3,14%	2,62%
119	Pymes-Individuales	900534356	WORLD OFFICE COLOMBIA SAS	J6201	BOGOTÁ D.C.	9,16	10,92%	118,31	23,57%	21,17%
120	Pymes-Individuales	900547305	ARCARIS LABS SAS	J6201	CALDAS	4,60	21,75%	12,05	12,52%	9,83%
121	Pymes-Individuales	900556261	INDIGO TECHNOLOGIES SAS	J6201	BOGOTÁ D.C.	1,51	66,07%	2,67	3,84%	1,97%
122	Pymes-Individuales	900590282	TEKUS SAS	J6201	ANTIOQUIA	4,50	22,22%	19,88	32,69%	25,66%
123	Pymes-Individuales	900601388	LABWARE COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,88	53,08%	10,24	45,23%	21,72%
124	Pymes-Individuales	900609904	INTICO COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,29	77,63%	4,03	35,02%	9,86%
125	Pymes-Individuales	900633204	TI724 SAS	J6201	ANTIOQUIA	1,41	71,04%	8,67	33,52%	9,38%
126	Pymes-Individuales	900642989	ASSERT SOLUTIONS SAS ASSERT SOLUTIONS SAS	J6201	BOGOTÁ D.C.	2,11	47,32%	0,00	24,14%	13,51%
127	Pymes-Individuales	900646721	EPI-USE COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,40	71,58%	2,99	77,16%	23,16%
128	Pymes-Individuales	900662410	CELUWEB.COM SAS	J6201	QUINDIO	4,29	23,32%	11,35	45,74%	32,19%
129	Pymes-Individuales	900664217	INTERFACES Y SOLUCIONES SAS	J6201	ANTIOQUIA	1,77	56,63%	24,08	122,36 %	75,07%
130	Pymes-Individuales	900664661	FERDIZ INVERSIONES SAS	J6201	BOGOTÁ D.C.	1,43	69,92%	0,00	5,28%	3,78%
131	Pymes-Individuales	900666654	LIVEVOX COLOMBIA SAS	J6201	ANTIOQUIA	3,37	29,66%	0,00	23,85%	17,09%
132	Pymes-Individuales	900675532	COLINKTEK SAS	J6201	BOGOTÁ D.C.	1,16	86,30%	3,14	29,53%	5,73%
133	Pymes-Individuales	900723696	Welii Colombia SAS	J6201	BOGOTÁ D.C.	2,49	40,16%	20,84	73,74%	41,78%
134	Pymes-Individuales	900753546	SENSORICA E INGENIERÍA SAS	J6201	BOGOTÁ D.C.	2,61	38,33%	3,04	10,43%	6,20%
135	Pymes-Individuales	900764863	SMART FINANCIAL SAS	J6201	VALLE	1,31	76,55%	0,00	40,55%	20,12%
136	Pymes-Individuales	900767427	GINKO FINANCIAL SOLUTIONS SAS BIC	J6201	BOGOTÁ D.C.	3,74	26,76%	11,96	15,53%	13,06%
137	Pymes-Individuales	900781407	TCM PARTNERS COLOMBIA S.A.S	J6201	BOGOTÁ D.C.	10,14	9,86%	0,00	13,64%	12,37%
138	Pymes-Individuales	900785730	Omg Worldwide group	J6201	ANTIOQUIA	1,03	96,66%	0,00	54,43%	10,14%
139	Pymes-Individuales	900787359	INTERNATIONAL SYSTEMS AND DESIGNS SAS	J6201	BOGOTÁ D.C.	1,21	82,55%	0,00	5,72%	4,14%
140	Pymes-Individuales	900793747	KEEP AGENCIA SAS	J6201	BOGOTÁ D.C.	3,57	28,04%	3,39	30,80%	21,95%
141	Pymes-Individuales	900809106	CSG INTERNATIONAL COLOMBIA SAS	J6201	BOGOTÁ D.C.	3,91	25,59%	0,00	43,37%	19,36%
142	Pymes-Individuales	900848435	GEOPROYECCIONES SAS	J6201	BOGOTÁ D.C.	2,79	35,82%	2,39	19,22%	11,50%
143	Pymes-Individuales	900882774	INFOTRANS COLOMBIA SAS	J6201	BOGOTÁ D.C.	1,86	53,64%	4,74	4,34%	2,27%
144	Pymes-Individuales	900901878	FORTINET COLOMBIA S.A.S.	J6201	BOGOTÁ D.C.	1,45	68,75%	0,00	50,36%	17,89%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
145	Pymes-Individuales	900924405	MAS GLOBAL SAS	J6201	ANTIOQUIA	2,86	34,99%	0,00	9,17%	6,00%
146	Pymes-Individuales	900924809	PYXIS S.A.S.	J6201	ANTIOQUIA	5,00	19,99%	3,42	4,99%	4,03%
147	Pymes-Individuales	900935262	General Business Machines de Colombia S.A.S.	J6201	ATLÁNTICO	4,14	24,16%	19,43	10,53%	8,17%
148	Pymes-Individuales	901047009	MINKA COLOMBIA SAS	J6201	BOGOTÁ D.C.	2,88	34,70%	0,00	24,36%	17,38%
149	Pymes-Individuales	901069380	FULL STACK LABS COLOMBIA SAS	J6201	ATLÁNTICO	2,48	40,27%	4,90	77,56%	26,35%
150	Pymes-Individuales	901087392	CECROPIA COLOMBIA SAS	J6201	SANTANDER	4,43	22,55%	5,73	8,23%	7,49%
151	Pymes-Individuales	901183491	HUBSPOT LATIN AMERICA SAS	J6201	BOGOTÁ D.C.	2,20	45,54%	14,77	64,96%	10,56%
152	Pymes-Individuales	901249158	GLOBALLOGIC COLOMBIA S.A.S	J6201	BOGOTÁ D.C.	1,73	57,76%	284,11	82,45%	40,77%
153	Pymes-Individuales	901252874	10PEARLS COLOMBIA S.A.S.	J6201	ANTIOQUIA	3,52	28,38%	16,15	50,51%	36,75%
154	Pymes-Individuales	901266582	HYLAND COLOMBIA S.A.S	J6201	BOGOTÁ D.C.	1,13	88,55%	0,00	15,91%	2,05%
155	Pymes-Individuales	901307208	VIRTUALSOFT SERVICIOS & SOFTWARE SAS	J6201	ANTIOQUIA	2,27	44,15%	74,89	111,89 %	65,85%
156	Pymes-Individuales	901310054	DATOLABS S.A.S	J6201	ANTIOQUIA	0,56	179,86%	3,86	34,78%	17,98%
157	Pymes-Individuales	901310911	XOLIT SAS	J6201	BOGOTÁ D.C.	1,83	54,75%	0,00	24,41%	13,08%
158	Pymes-Individuales	901312879	AUTOTRAFFIC SA DE CV SUCURSAL COLOMBIA	J6201	BOGOTÁ D.C.	6,93	14,44%	5,02	5,76%	4,93%
159	Pymes-Individuales	901317478	FACTORED SAS	J6201	ANTIOQUIA	2,39	41,90%	0,00	63,09%	38,88%
160	Pymes-Individuales	901323703	AVANTICA TECHNOLOGIES S.A.S.	J6201	VALLE	4,98	20,08%	35,92	22,89%	18,35%
161	Pymes-Individuales	901398109	WHALE CLOUD TECHNOLOGY (COLOMBIA) S.A.S	J6201	BOGOTÁ D.C.	1,22	82,03%	1,51	108,57 %	21,16%
162	Pymes-Individuales	901432751	SM TECH PARTNERS SAS	J6201	ANTIOQUIA	1,08	92,88%	5,57	76,97%	13,58%
163	Pymes-Individuales	901507911	NOVARTEC SAS	J6201	BOGOTÁ D.C.	1,06	94,33%	0,00	59,31%	1,60%
164	Pymes-Separados	805028460	LUCASIAN LABS SAS	J6201	VALLE	2,26	44,28%	4,14	6,57%	4,31%
165	Pymes-Separados	811003890	GLOBAL MVM SAS	J6201	ANTIOQUIA	1,45	69,08%	4,03	56,55%	19,46%
166	Pymes-Separados	811046318	Q-VISION - QUALITY VISION TECHNOLOGIES S.A.S.	J6201	ANTIOQUIA	1,65	60,78%	3,26	27,58%	13,21%
167	Pymes-Separados	830026014	SOFTMANAGEMENT S.A.	J6201	BOGOTÁ D.C.	2,54	39,42%	18,62	18,89%	11,54%
168	Pymes-Separados	830032586	GREEN TECH LTDA	J6201	BOGOTÁ D.C.	4,29	23,30%	0,00	23,07%	21,72%
169	Pymes-Separados	830070873	GCA TECHOLOGIES SAS	J6201	BOGOTÁ D.C.	1,34	74,55%	8262,93	27,49%	14,08%
170	Pymes-Separados	830074526	ELECTRONIC TRAFIC SUCURSAL COLOMBIA	J6201	BOGOTÁ D.C.	2,43	41,17%	0,00	38,34%	9,60%
171	Pymes-Separados	830512451	MICROSHIF S.A.S	J6201	SANTANDER	2,30	43,45%	2,64	46,56%	24,76%
172	Pymes-Separados	860503631	IDSYSTEMS SA	J6201	BOGOTÁ D.C.	25,90	3,86%	0,00	9,65%	9,11%
173	Pymes-Separados	900022972	CEIBA SOFTWARE HOUSE S.A.S.	J6201	ANTIOQUIA	2,17	46,00%	0,00	55,83%	32,49%
174	Pymes-Separados	900046462	ON BUSINESS CONSULTING S.A.S.	J6201	ANTIOQUIA	2,98	33,53%	1,77	23,46%	11,96%
175	Pymes-Separados	900395252	SOFTGIC S.A.S.	J6201	ANTIOQUIA	1,63	61,41%	5,19	15,85%	9,76%
176	Pymes-Separados	900440779	SOLUCIONES INTEGRADAS DE TECNOLOGÍA SAS	J6201	BOGOTÁ D.C.	2,55	39,19%	5,57	30,07%	16,12%
177	Pymes-Separados	900704304	INDEPRO INGENIERIAINDEPRO INGENIERÍA DE PROCESOS SAS	J6201	BOGOTÁ D.C.	3,52	28,43%	8,97	7,33%	4,69%
178	Pymes-Separados	901011198	I BUSINESS MASTER S.A.S	J6201	ATLÁNTICO	7,80	12,82%	0,00	27,95%	25,36%
179	Plenas-Individuales	800057965	VISION SOFTWARE SAS	J6202	BOGOTÁ D.C.	1,28	77,98%	13,66	62,45%	14,83%
180	Plenas-Individuales	800066453	SKANDIA PLANEACIÓN FINANCIERA S.A.	J6202	BOGOTÁ D.C.	15,27	6,55%	1120,41	19,61%	19,49%
181	Plenas-Individuales	800110980	ACCENTURE LTDA	J6202	BOGOTÁ D.C.	1,50	66,49%	1,20	61,35%	11,67%
182	Plenas-Individuales	800114672	STEFANINI COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,77	56,49%	5,89	15,14%	8,64%
183	Plenas-Individuales	800159527	AMADEUS IT GROUP COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,11	89,94%	11,51	61,65%	17,30%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
184	Plenas-Individuales	800226094	FINANCIAL SYSTEMS COMPANY SAS	J6202	CUNDINAMARCA	2,23	44,86%	5,31	18,90%	12,94%
185	Plenas-Individuales	805025216	FN TECNOLOGÍA SAS	J6202	BOGOTÁ D.C.	1,69	59,12%	220,26	44,96%	18,61%
186	Plenas-Individuales	830013988	Alfapeople Andino SAS	J6202	BOGOTÁ D.C.	1,76	56,68%	36,25	40,64%	26,65%
187	Plenas-Individuales	830047444	SERVICIOS ESPECIALIZADOS DE TECNOLOGÍA E INFORMATICA SETI SAS	J6202	ANTIOQUIA	1,10	91,02%	5,45	101,09 %	24,80%
188	Plenas-Individuales	830055791	AXITY COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,11	89,99%	1,77	29,51%	8,07%
189	Plenas-Individuales	830089336	tTD SYNNEX COLOMBIA LTDA	J6202	CUNDINAMARCA	1,42	70,49%	1,19	26,13%	7,46%
190	Plenas-Individuales	830094425	FISERV COLOMBIA LIMITADA	J6202	BOGOTÁ D.C.	5,78	17,29%	5,23	39,56%	32,02%
191	Plenas-Individuales	830110433	MQA BUSINESS CONSULTANTS S.A.	J6202	BOGOTÁ D.C.	1,39	71,96%	32,29	97,92%	32,34%
192	Plenas-Individuales	830114969	TOPAZ COLOMBIA SA	J6202	BOGOTÁ D.C.	1,85	53,99%	0,00	23,61%	12,55%
193	Plenas-Individuales	830142945	SYNERGY WORK SAS	J6202	BOGOTÁ D.C.	1,64	61,12%	1,75	77,51%	39,00%
194	Plenas-Individuales	890923937	PERICIENT COLOMBIA SAS	J6202	ANTIOQUIA	4,41	22,66%	0,00	25,39%	21,21%
195	Plenas-Individuales	900091709	LICENCIAS ON LINE SAS	J6202	BOGOTÁ D.C.	1,25	79,84%	0,00	15,33%	3,22%
196	Plenas-Individuales	900103457	TCS SOLUTION CENTER SUCURSAL COLOMBIA	J6202	BOGOTÁ D.C.	2,86	34,98%	17,69	21,90%	14,80%
197	Plenas-Individuales	900157788	TDC COLOMBIA LTDA	J6202	BOGOTÁ D.C.	2,65	37,78%	3,00	4,53%	2,42%
198	Plenas-Individuales	900173404	HEINSOHN HUMAN GLOBAL SOLUTIONS S.A.S. BIC	J6202	BOGOTÁ D.C.	2,56	39,02%	102,74	76,80%	48,27%
199	Plenas-Individuales	900266641	CIENA INTERNATIONAL INC	J6202	BOGOTÁ D.C.	7,72	12,96%	19,77	17,01%	14,75%
200	Plenas-Individuales	900478030	INDRA SOLUCIONES TECNOLOGIAS DE LA INFORMACIÓN SLU SUCURSAL	J6202	BOGOTÁ D.C.	4,32	23,15%	13,14	62,96%	49,02%
201	Plenas-Individuales	900555829	solex colombia sas	J6202	ANTIOQUIA	4,36	22,95%	1,59	9,76%	7,61%
202	Plenas-Individuales	900583745	HOLCREST S.A.S	J6202	ANTIOQUIA	1,10	91,22%	5,63	94,51%	15,39%
203	Plenas-Individuales	900601546	HITACHI VANTARA COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,55	39,23%	10,49	44,71%	21,31%
204	Plenas-Individuales	900912034	BIZAGI LATAM SAS	J6202	BOGOTÁ D.C.	1,40	71,18%	0,00	38,75%	13,21%
205	Plenas-Individuales	900987866	ENTERPRISE SERVICES COLOMBIA SAS	J6202	BOGOTÁ D.C.	3,87	25,81%	0,00	29,66%	20,95%
206	Plenas-Individuales	901429484	TASKUS COLOMBIA S.A.S.	J6202	VALLE	0,81	123,33%	3,45	127,31 %	15,03%
207	Plenas-Individuales	901445912	WIZELINE S.A.S.	J6202	BOGOTÁ D.C.	1,19	83,97%	1,35	141,51 %	45,72%
208	Plenas-Separados	800046226	HEINSOHN BUSINESS TECHNOLOGY S.A BIC	J6202	BOGOTÁ D.C.	3,13	31,95%	21,99	19,91%	14,30%
209	Plenas-Separados	800185008	THOMAS INSTRUMENTS S A	J6202	BOGOTÁ D.C.	3,21	31,16%	27,82	8,19%	6,35%
210	Plenas-Separados	830001637	SONDA DE COLOMBIA S.A.	J6202	BOGOTÁ D.C.	1,90	52,73%	2,71	8,21%	4,97%
211	Plenas-Separados	830027574	TIVIT COLOMBIA TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGÍA S.A.S.	J6202	BOGOTÁ D.C.	1,58	63,41%	6,01	13,78%	7,41%
212	Plenas-Separados	830042244	DIGITAL WARE SAS	J6202	BOGOTÁ D.C.	0,30	335,50%	0,45	2,91%	1,76%
213	Plenas-Separados	830048145	SIIGO SAS	J6202	BOGOTÁ D.C.	0,60	165,65%	0,67	12,71%	4,33%
214	Plenas-Separados	830077380	XERTICA COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,24	80,84%	0,45	16,66%	3,17%
215	Plenas-Separados	860002120	IBM DE COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,31	76,17%	86,83	70,92%	27,33%
216	Plenas-Separados	900032774	OLIMPIA IT SAS	J6202	BOGOTÁ D.C.	2,24	44,66%	13,46	27,55%	16,89%
217	Plenas-Separados	900074316	GFT TECHNOLOGIES COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,48	67,45%	9,28	63,59%	27,36%
218	Plenas-Separados	900128566	NTT DATA COLOMBIA S. A. S.	J6202	BOGOTÁ D.C.	1,71	58,38%	2,25	29,65%	12,38%
219	Pymes-Individuales	800134634	INTERLAN SAS	J6202	ANTIOQUIA	2,11	47,42%	13,32	13,98%	8,11%
220	Pymes-Individuales	800142557	ELECTRO SOFTWARE SAS BIC	J6202	SANTANDER	10,80	9,26%	0,00	15,07%	10,75%
221	Pymes-Individuales	800149562	SISTEMAS Y ASESORIAS DE COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,92	34,29%	0,00	69,76%	44,62%
222	Pymes-Individuales	800158125	INNOSOFT LTDA	J6202	VALLE	5,31	18,84%	9,25	9,35%	8,61%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
223	Pymes-Individuales	800198975	CLAI PAYMENTS COLOMBIA S.A.S.	J6202	BOGOTÁ D.C.	2,14	46,70%	12,73	26,65%	15,39%
224	Pymes-Individuales	800222753	SISTEMAS GESTIÓN Y CONSULTORIA ALFA GL SAS	J6202	BOGOTÁ D.C.	1,79	55,87%	9,72	51,07%	18,17%
225	Pymes-Individuales	800233464	UN&ON SOLUCIONES SISTEMAS DE INFORMACIÓN S.A.S.	J6202	BOGOTÁ D.C.	2,81	35,54%	0,00	57,05%	31,35%
226	Pymes-Individuales	800237835	APICE INGENIERÍA Y SOLUCIONES DE AVANZADA S.A. EN REORGANIZACION	J6202	BOGOTÁ D.C.	1,24	80,44%	1,41	32,60%	2,45%
227	Pymes-Individuales	800243347	PROCEDATA INTERNACIONAL S.A.S	J6202	BOGOTÁ D.C.	1,28	77,85%	0,00	28,33%	12,16%
228	Pymes-Individuales	805018674	ECOM SAS	J6202	VALLE	2,66	37,63%	10,98	27,80%	21,78%
229	Pymes-Individuales	810005747	SIGMA INGENIERÍA SA	J6202	CALDAS	0,58	173,18%	2,41	50,78%	27,09%
230	Pymes-Individuales	811025080	A-MAQ	J6202	ANTIOQUIA	1,67	59,77%	2,79	34,63%	21,59%
231	Pymes-Individuales	830005677	BIT CONSULTING SAS	J6202	BOGOTÁ D.C.	1,08	92,49%	8,49	128,49 %	32,17%
232	Pymes-Individuales	830007379	COMSISTELCO SAS	J6202	BOGOTÁ D.C.	3,04	32,86%	0,00	35,20%	16,48%
233	Pymes-Individuales	830018817	TAYLOR Y JOHNSON LTDA	J6202	BOGOTÁ D.C.	3,29	30,44%	52,06	57,34%	34,23%
234	Pymes-Individuales	830029560	QUIMBAYA AERIAL SERVICES SAS EN REORGANIZACION	J6202	BOGOTÁ D.C.	2,73	36,67%	2,17	7,30%	3,26%
235	Pymes-Individuales	830030281	GEOSPATIAL SAS EN REORGANIZACION	J6202	BOGOTÁ D.C.	1,11	89,80%	7,87	90,00%	19,63%
236	Pymes-Individuales	830037850	Siscomputo Ltda Servicios y Sistemas de computo	J6202	BOGOTÁ D.C.	7,77	12,87%	0,00	8,29%	7,23%
237	Pymes-Individuales	830039811	DB SYSTEM SAS	J6202	BOGOTÁ D.C.	2,18	45,94%	7,53	50,29%	27,31%
238	Pymes-Individuales	830047891	SISTRAN COLOMBIA S.A.	J6202	BOGOTÁ D.C.	3,97	25,22%	13,37	16,45%	11,68%
239	Pymes-Individuales	830053693	INETUM COLOMBIA SAS	J6202	BOGOTÁ D.C.	3,15	31,75%	0,47	27,57%	12,56%
240	Pymes-Individuales	830061576	ETEK INTERNATIONAL CORPORATION SUCURSAL COLOMBIA	J6202	BOGOTÁ D.C.	2,00	49,94%	0,13	0,95%	0,42%
241	Pymes-Individuales	830064639	SOLUCIONES LATINAS ADMINISTRATIVAS INTEGRALES SOLATI SAS	J6202	BOGOTÁ D.C.	3,05	32,80%	14,69	34,06%	25,24%
242	Pymes-Individuales	830074045	COGNOSONLINE SOLUTIONS COLOMBIA SA	J6202	BOGOTÁ D.C.	2,95	33,95%	76,96	67,11%	34,84%
243	Pymes-Individuales	830075303	ARIA PSW SAS	J6202	BOGOTÁ D.C.	2,00	49,92%	1,91	37,35%	15,35%
244	Pymes-Individuales	830078090	SINERGY & LOWELLS SAS	J6202	BOGOTÁ D.C.	4,62	21,66%	2,73	29,01%	15,78%
245	Pymes-Individuales	830080928	ITIS SUPPORT SAS	J6202	BOGOTÁ D.C.	1,74	57,39%	8,96	55,24%	23,54%
246	Pymes-Individuales	830081918	UNIVERSITAS XXI COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,85	54,09%	15,47	32,04%	18,36%
247	Pymes-Individuales	830086348	VC@SOFT S.A.S	J6202	BOGOTÁ D.C.	6,11	16,38%	1354,05	31,04%	26,03%
248	Pymes-Individuales	830087915	CERCA TECHNOLOGY SAS	J6202	BOGOTÁ D.C.	1,65	60,74%	14,64	23,77%	9,39%
249	Pymes-Individuales	830090100	ASSIST CONSULTORES DE SISTEMAS S.A	J6202	BOGOTÁ D.C.	1,17	85,59%	0,00	127,14 %	8,20%
250	Pymes-Individuales	830096620	PROFESIONALES EN TRANSACCIONES ELECTRONICAS S.A - PTESA	J6202	BOGOTÁ D.C.	1,33	75,00%	0,00	18,18%	3,66%
251	Pymes-Individuales	830096685	ILISIM INTERNATIONAL SAS	J6202	BOGOTÁ D.C.	3,84	26,06%	0,00	10,64%	8,37%
252	Pymes-Individuales	830096744	QUALITY DATA SAS	J6202	BOGOTÁ D.C.	4,71	21,25%	1,43	4,17%	3,73%
253	Pymes-Individuales	830099766	ARANDA SOFTWARE ANDINA SAS	J6202	BOGOTÁ D.C.	1,14	88,00%	17650,68	38,53%	24,10%
254	Pymes-Individuales	830130510	INALAMBRIA INTERNACIONAL SAS	J6202	BOGOTÁ D.C.	3,39	29,48%	8,10	18,12%	14,43%
255	Pymes-Individuales	830147777	Simplexity sas	J6202	BOGOTÁ D.C.	8,47	11,81%	42,34	11,16%	10,30%
256	Pymes-Individuales	830147784	EVOLUTION TECHNOLOGIES GROUP SAS	J6202	BOGOTÁ D.C.	1,71	58,56%	8,24	21,40%	6,44%
257	Pymes-Individuales	830502242	INFORMACIÓN DE NEGOCIOS Y PROCESOS INP LTDA	J6202	BOGOTÁ D.C.	1,51	66,01%	0,00	106,37 %	37,62%
258	Pymes-Individuales	830504013	PLAY TECHNOLOGIES SAS	J6202	VALLE	5,18	19,29%	3,53	24,82%	14,46%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
259	Pymes-Individuales	830511493	DIIT CONSULTORES SAS	J6202	BOGOTÁ D.C.	3,15	31,72%	17,99	30,80%	20,99%
260	Pymes-Individuales	860353611	Compucom SAS	J6202	BOGOTÁ D.C.	2,26	44,27%	1,76	18,62%	10,45%
261	Pymes-Individuales	890329946	SISTEMAS INTEGRALES DE INFORMATICA S A SISA S A	J6202	BOGOTÁ D.C.	3,08	32,44%	0,00	31,54%	25,28%
262	Pymes-Individuales	900034395	BLACK HAT ARCHETYPE SAS	J6202	BOGOTÁ D.C.	1,51	66,34%	0,00	38,38%	13,79%
263	Pymes-Individuales	900047660	APLYCA TECNOLOGÍA SAS	J6202	BOGOTÁ D.C.	2,61	38,25%	12,47	60,25%	42,60%
264	Pymes-Individuales	900047668	E SOLUTIONS LTDA	J6202	BOGOTÁ D.C.	1,59	62,95%	349,39	63,00%	33,91%
265	Pymes-Individuales	900050767	PROCESIX COLOMBIA SAS	J6202	ANTIOQUIA	2,88	34,69%	0,00	24,42%	16,03%
266	Pymes-Individuales	900052363	NET GROUP SA	J6202	VALLE	0,91	110,39%	3,75	60,98%	24,98%
267	Pymes-Individuales	900057661	DELTA IT SOLUTIONS SA	J6202	BOGOTÁ D.C.	4,37	22,90%	1,18	23,15%	11,55%
268	Pymes-Individuales	900087315	CONTACT & BUSINESS IT SAS	J6202	BOGOTÁ D.C.	2,67	37,44%	2,85	70,09%	35,55%
269	Pymes-Individuales	900145046	INFORMATION SYSTEMS SUDAMERICANA S.A.S.	J6202	ANTIOQUIA	5,57	17,95%	1,54	24,42%	20,20%
270	Pymes-Individuales	900148177	PEAR SOLUTIONS SAS	J6202	BOGOTÁ D.C.	2,03	49,28%	2,15	19,45%	9,78%
271	Pymes-Individuales	900169608	NEORIS COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,06	48,53%	0,00	48,02%	26,22%
272	Pymes-Individuales	900171749	Innatel -Innovacion Aplicada a las Telecomunicaciones SAS - BIC	J6202	BOGOTÁ D.C.	5,77	17,33%	11,07	19,91%	14,69%
273	Pymes-Individuales	900172604	STRUCTUM INGENIERÍA SA	J6202	VALLE	2,26	44,32%	0,00	4,47%	2,67%
274	Pymes-Individuales	900175316	PASSWORD CONSULTING SERVICES SAS	J6202	BOGOTÁ D.C.	2,26	44,25%	61,59	34,31%	19,23%
275	Pymes-Individuales	900177919	COLEGIUM REGION ANDINA LIMITADA	J6202	BOGOTÁ D.C.	1,01	99,14%	0,00	14,47%	2,60%
276	Pymes-Individuales	900180126	Quantum Data Systems SAS	J6202	BOGOTÁ D.C.	1,93	51,87%	2,00	12,65%	6,09%
277	Pymes-Individuales	900193806	OESIA NETWORKS SL SUCURSAL COLOMBIA	J6202	BOGOTÁ D.C.	1,29	77,81%	44,47	28,03%	6,22%
278	Pymes-Individuales	900200356	CLOUXTER SAS	J6202	BOGOTÁ D.C.	1,16	86,04%	0,54	78,67%	12,60%
279	Pymes-Individuales	900204272	GESTIÓN DE SEGURIDAD ELECTRONICA SA	J6202	BOGOTÁ D.C.	4,50	22,21%	0,00	35,43%	29,29%
280	Pymes-Individuales	900230023	OOH REDES DIGITALES LTDA	J6202	BOGOTÁ D.C.	1,95	51,40%	1,60	30,55%	10,74%
281	Pymes-Individuales	900237844	THE BEST EXPERIENCE IN TECHNOLOGY SAS	J6202	BOGOTÁ D.C.	1,32	75,79%	1,89	58,79%	16,24%
282	Pymes-Individuales	900238438	Grow Data SAS	J6202	BOGOTÁ D.C.	1,73	57,85%	63,52	49,08%	23,16%
283	Pymes-Individuales	900246638	TALENTO SOLIDO	J6202	BOGOTÁ D.C.	3,53	28,32%	3,72	26,32%	11,74%
284	Pymes-Individuales	900262503	IN MOTION COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,75	36,34%	10,89	33,09%	22,19%
285	Pymes-Individuales	900265026	E DEA NETWORKS S A S	J6202	BOGOTÁ D.C.	7,20	13,88%	3,40	28,26%	15,54%
286	Pymes-Individuales	900266612	BIONEXO COLOMBIA SAS	J6202	BOGOTÁ D.C.	5,28	18,93%	2374,89	75,26%	61,48%
287	Pymes-Individuales	900268071	INNOVATIVE EDUCATION: SERVICES AND SOLUTIONS S.A.S.	J6202	RISARALDA	7,44	13,44%	0,00	7,81%	6,94%
288	Pymes-Individuales	900297772	INVERSIONES TECNOLOGIAS DE AMERICA	J6202	BOGOTÁ D.C.	1,89	52,88%	0,00	5,41%	2,73%
289	Pymes-Individuales	900303759	GATTACA OUTSOURCING S.A.S.	J6202	BOGOTÁ D.C.	3,57	28,05%	2,60	38,88%	16,97%
290	Pymes-Individuales	900320011	PERIFERIA IT CORP SAS	J6202	BOGOTÁ D.C.	2,60	38,53%	0,00	52,58%	26,56%
291	Pymes-Individuales	900321702	DUNNHUMBY COLOMBIA S. A. S	J6202	ANTIOQUIA	1,55	64,71%	2,22	64,47%	11,07%
292	Pymes-Individuales	900321888	VERANO INGENIERÍA LTDA	J6202	BOGOTÁ D.C.	1,46	68,39%	2,35	35,28%	11,65%
293	Pymes-Individuales	900324056	ADVANCED TECHNOLOGIES & SOLUTIONS GROUP SAS	J6202	SANTANDER	6,92	14,45%	3,30	11,67%	7,05%
294	Pymes-Individuales	900333123	MARCO COLOMBIA S.A.S.	J6202	BOGOTÁ D.C.	1,90	52,58%	0,00	17,38%	8,47%
295	Pymes-Individuales	900340993	ADMISNISTRACION DE REDES Y PROYECTOS SAS	J6202	BOGOTÁ D.C.	1,37	72,81%	7,35	25,40%	10,36%
296	Pymes-Individuales	900346202	POSICION DIGITAL SAS	J6202	ANTIOQUIA	5,09	19,66%	6,09	25,20%	17,23%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
297	Pymes-Individuales	900360482	ENTELGY COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,95	51,22%	2,56	26,72%	13,06%
298	Pymes-Individuales	900373414	CORUS SYSTEMS & CONSULTING GROUP COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,15	46,51%	6,22	61,40%	31,12%
299	Pymes-Individuales	900379787	SOCIEDAD DE EXPLOTACIÓN DE REDES ELECTRONICAS Y SERVICIOS DE COLOMBIA S.A.S.	J6202	BOGOTÁ D.C.	3,04	32,94%	2,10	17,25%	9,10%
300	Pymes-Individuales	900392041	SCN SAS	J6202	BOGOTÁ D.C.	1,57	63,68%	0,00	13,00%	5,91%
301	Pymes-Individuales	900396176	MNEMO COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,45	40,89%	18,97	39,78%	17,03%
302	Pymes-Individuales	900413751	ZERONINE LATAM SAS	J6202	BOGOTÁ D.C.	1,58	63,10%	3,31	65,54%	24,43%
303	Pymes-Individuales	900415354	DATACENTER COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,41	71,17%	4,80	27,98%	11,09%
304	Pymes-Individuales	900428564	ESOFT COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,43	69,95%	2,15	34,15%	10,16%
305	Pymes-Individuales	900435185	OIS TELECOMUNICACIONES S.A.S.	J6202	BOGOTÁ D.C.	2,16	46,22%	0,00	50,47%	20,26%
306	Pymes-Individuales	900436226	ADOBE COLOMBIA SAS	J6202	BOGOTÁ D.C.	4,94	20,25%	114,77	25,45%	20,30%
307	Pymes-Individuales	900438438	CLM COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,87	53,61%	1,44	37,07%	17,27%
308	Pymes-Individuales	900440441	SEIDOR COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,52	65,73%	10,67	69,16%	26,77%
309	Pymes-Individuales	900441263	YUXI GLOBAL SAS	J6202	ANTIOQUIA	3,04	32,93%	13,02	25,54%	17,14%
310	Pymes-Individuales	900443044	SAFETY IN DEEP SAS	J6202	BOGOTÁ D.C.	3,20	31,29%	0,00	40,08%	28,84%
311	Pymes-Individuales	900444717	CONEXIA SAS	J6202	BOGOTÁ D.C.	1,87	53,58%	4,07	74,35%	34,17%
312	Pymes-Individuales	900448500	ASPECT SOFTWARE COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,14	87,81%	7,45	20,99%	2,62%
313	Pymes-Individuales	900483420	VIVO CONSULTING COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,46	68,52%	1,51	44,89%	16,67%
314	Pymes-Individuales	900483707	NTICS SAS SERVICIOS Y SOLUCIONES	J6202	SANTANDER	2,80	35,72%	0,00	19,33%	1,69%
315	Pymes-Individuales	900505780	LAN SECURITY NETWORKS SAS	J6202	ATLÁNTICO	1,54	64,90%	0,00	30,49%	9,89%
316	Pymes-Individuales	900507611	CINTE COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,37	72,93%	2,45	139,58 %	31,75%
317	Pymes-Individuales	900513709	TYG CONSULTING SAS	J6202	BOGOTÁ D.C.	1,69	59,21%	2,51	20,07%	8,35%
318	Pymes-Individuales	900554898	GIGA COLOMBIA S.A.S	J6202	BOGOTÁ D.C.	1,59	62,70%	90,87	142,09 %	53,44%
319	Pymes-Individuales	900557218	DAVINCI TECNOLOGIES SAS	J6202	BOGOTÁ D.C.	0,91	110,44%	1,19	153,22 %	11,50%
320	Pymes-Individuales	900564561	quiter colombia sas	J6202	BOGOTÁ D.C.	7,55	13,24%	8,93	29,84%	25,90%
321	Pymes-Individuales	900575877	SUNTRUST TECH SAS	J6202	BOGOTÁ D.C.	13,85	7,22%	91,44	27,01%	25,62%
322	Pymes-Individuales	900599694	ANALYTICS DATA SAS - EN REORGANIZACIÓN	J6202	BOGOTÁ D.C.	13,03	7,67%	2,71	7,37%	3,74%
323	Pymes-Individuales	900610491	IMAGINE CONSULTING SAS	J6202	BOGOTÁ D.C.	2,24	44,58%	27,73	57,64%	36,84%
324	Pymes-Individuales	900631710	Veritran Colombia S.A.S.	J6202	RISARALDA	3,07	32,59%	40,13	62,76%	43,81%
325	Pymes-Individuales	900641938	SRF CONSULTORES SAS	J6202	BOGOTÁ D.C.	4,42	22,61%	46,89	58,97%	42,78%
326	Pymes-Individuales	900644920	TRES HTP COLOMBIA SAS	J6202	BOGOTÁ D.C.	2,84	35,19%	0,00	10,39%	7,42%
327	Pymes-Individuales	900651473	QINTESS COLOMBIA S.A.S	J6202	BOGOTÁ D.C.	2,36	42,29%	1,59	8,25%	4,95%
328	Pymes-Individuales	900663379	WOLKVOX S.A.S	J6202	ANTIOQUIA	2,45	40,80%	134,93	43,75%	35,25%
329	Pymes-Individuales	900672953	NIMBUTECH SAS	J6202	BOGOTÁ D.C.	1,21	82,40%	0,52	4,87%	0,96%
330	Pymes-Individuales	900678367	IT SECURITY SERVICE SAS	J6202	BOGOTÁ D.C.	37,82	2,64%	0,64	7,70%	7,50%
331	Pymes-Individuales	900796115	CORE CONSULTORES S.A.S.	J6202	BOGOTÁ D.C.	3,42	29,25%	3,47	7,03%	5,81%
332	Pymes-Individuales	900803867	SOFTWARE PROFESSIONAL SERVICES SAS	J6202	ANTIOQUIA	2,65	37,75%	0,00	46,54%	29,08%
333	Pymes-Individuales	900810588	ESC COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,67	59,71%	6,38	43,50%	19,09%
334	Pymes-Individuales	900856181	THARSIS SAS	J6202	BOGOTÁ D.C.	19,50	5,13%	36,20	19,57%	18,59%
335	Pymes-Individuales	900881750	VENETIC INC SUCURSAL COLOMBIA	J6202	BOGOTÁ D.C.	2,43	41,19%	10,82	56,31%	33,85%

No.	Punto de Entrada	NIT	Razón social de la sociedad	Clasificación Industrial Internacional Uniforme Versión 4.0 (CIIU	Departamento de la dirección del domicilio	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO
336	Pymes-Individuales	900935602	AIS APLICACIONES DE INTELIGENCIA ARTIFICIAL COLOMBIA SAS	J6202	BOGOTÁ D.C.	1,40	71,20%	7,14	43,42%	11,12%
337	Pymes-Individuales	900962841	ESTUDIO Y TECNOLOGÍA PROGRESIVA SAS	J6202	BOGOTÁ D.C.	1,74	57,57%	0,00	7,22%	3,13%
338	Pymes-Individuales	900987447	PDC-SOLUTIONS COLOMBIA S A S	J6202	BOGOTÁ D.C.	3,06	32,63%	1,01	1,38%	0,41%
339	Pymes-Individuales	901040602	CARGAYA SAS BIC	J6202	VALLE	1,54	64,90%	0,73	117,90 %	11,17%
340	Pymes-Individuales	901043004	PAYNET SAS	J6202	BOGOTÁ D.C.	2,49	40,22%	29,39	24,06%	15,81%
341	Pymes-Individuales	901148432	IGT SERVICES AND TECHNOLOGIES COLOMBIA SAS	J6202	BOGOTÁ D.C.	5,12	19,52%	13,41	45,36%	38,82%
342	Pymes-Individuales	901184760	TECNOFACTORY S.A.S - BIC	J6202	BOGOTÁ D.C.	2,96	33,79%	647,86	54,27%	35,95%
343	Pymes-Individuales	901199246	S2 GRUPO SUCURSAL COLOMBIA	J6202	BOGOTÁ D.C.	1,16	86,35%	2,57	15,86%	2,51%
344	Pymes-Individuales	901207449	TENGO SOLUTIONS COLOMBIA SAS	J6202	ANTIOQUIA	1,57	63,69%	0,00	81,21%	36,62%
345	Pymes-Individuales	901237267	PROQUEST COLOMBIA S.A.S.	J6202	BOGOTÁ D.C.	4,00	25,03%	3,88	25,34%	8,07%
346	Pymes-Individuales	901264616	GORILLA LOGIC SAS	J6202	ANTIOQUIA	0,65	153,41%	0,89	128,41 %	17,28%
347	Pymes-Separados	800042928	PROASISTEMAS S.A.	J6202	BOGOTÁ D.C.	0,78	128,98%	19,75	26,54%	12,91%
348	Pymes-Separados	800089002	CONSENSUS SAS	J6202	BOGOTÁ D.C.	1,32	75,81%	7,32	41,51%	16,95%
349	Pymes-Separados	800135532	ASESORES DE SISTEMAS ESPECIALIZADOS EN SOFTWARE SAS ASESOFTWARE SAS	J6202	BOGOTÁ D.C.	1,85	54,17%	1,35	40,99%	13,14%
350	Pymes-Separados	805023132	ITERIA SAS	J6202	VALLE	1,81	55,29%	6,76	16,32%	8,78%
351	Pymes-Separados	816004765	SOLUCIONES GLOBALES SAS	J6202	BOGOTÁ D.C.	2,66	37,65%	56,45	40,04%	22,94%
352	Pymes-Separados	830117028	HEON HEALTH ON LINE S.A.	J6202	BOGOTÁ D.C.	6,84	14,62%	0,05	1,58%	1,39%
353	Pymes-Separados	830131674	HR SOLUTIONS SAS	J6202	BOGOTÁ D.C.	2,07	48,36%	5,99	23,77%	14,94%
354	Pymes-Separados	860514047	SISTEMAS ENLINEA SAS	J6202	BOGOTÁ D.C.	2,27	44,04%	28,08	52,39%	38,69%
355	Pymes-Separados	900426578	SAVIOS SAS	J6202	ANTIOQUIA	1,79	55,82%	6,94	39,65%	25,23%
356	Pymes-Separados	900665829	DIGITAL TRAINING COLOMBIA SAS	J6202	BOYACÁ	9,37	10,68%	585,74	34,85%	31,18%
357	Pymes-Separados	900701314	SAMTEL CONSULTORES COLOMBI SAS	J6202	BOGOTÁ D.C.	2,44	40,92%	5,63	26,50%	14,34%
358	Pymes-Separados	900923636	SOLUCIONES Y SERVICIOS DE PROCESAMIENTO Y OPERACIÓN DE TECNOLOGÍA S A S	J6202	BOGOTÁ D.C.	2,74	36,47%	1,33	5,93%	2,52%
359	Pymes-Separados	901103080	INVERSIONES TECNOLÓGICAS CALANDA SAS	J6202	BOGOTÁ D.C.	0,87	114,78%	0,00	0,30%	0,18%
					VALOR PROMEDIO	3,29	52%	112,44	37%	18%
					MENOR VALOR	0,30	2%	0,00	0%	0%
					VALOR MÁXIMO	50,26	336%	17650, 68	156%	78%

INFORMACIÓN DE LAS EMPRESAS INTERESADAS DURANTE EL ESTUDIO DE MERCADO con información de RUP que se encuentra en plataforma a fin de determinar indicadores del sector específico, se establecen los indicadores financieros para el presente proceso de contratación que permitan que exista pluralidad de oferentes y al mismo tiempo que las empresas que participen cuenten con la solidez económica suficiente para ejecutar de manera óptima el objeto contractual, minimizando los riesgos financieros que puedan afectar al futuro contratista conforme a la modalidad y naturaleza del contrato.

TAMAÑO EMPRESA	EMPRESA	LIQUIDEZ	ENDEUDAMIENTO	RAZÓN COBERTURA INTERÉS	RENTABILIDAD PATRIMONIO	RENTABILIDAD ACTIVO	INFORMACIÓN
MICROEMPRESA	SPECTRUM TECHNOLOGYSAS	2,72	31%	27,29	0,07	0,05	2024
MEDIANA EMPRESA	NETWORK & ACCESORIES SAS	2,62	48%	20,33	0,38	0,19	2024
GRAN EMPRESA	HEIMCORE SAS	1.89	55%	20.60	0.36	0.16	2024

PEQUEÑA EMPRESA	MCO GLOBAL SAS	2,5	38%	521,73	0,16	0,10	2024
PEQUEÑA EMPRESA	HELP SOLUCIONES INFORMATICAS HSI SAS	1,17	63%	8,77	0,29	0,10	2024
MEDIANA EMPRESA	RedNeet SAS	3,03	59%	69,86	0,6	0,24	2024

INDICADORES FINANCIEROS DEL PROPONENTE – INDICADORES GENERALES (para todos los oferentes)

CAPACIDAD FINANCIERA

a. Índice de Liquidez: L

L= ACTIVO CORRIENTE / PASIVO CORRIENTE. Debe ser mayor o igual (≥) a 1.10

b. Índice de Endeudamiento: NET

NET= (PASIVO TOTAL / ACTIVO TOTAL) 100%. Debe ser menor o igual (≤) al 70%

c. Razón de cobertura de intereses: RCI

RCI = UTILIDAD OPERACIONAL / GASTOS DE INTERESES. Debe ser mayor o igual a 2.00

Nota: Si el proponente no tiene obligaciones financieras, la propuesta será considerada hábil. En el caso de tener indicador indeterminado la propuesta también será hábil.

CAPACIDAD ORGANIZACIONAL

a. Rentabilidad del Patrimonio

Rentabilidad del Patrimonio = Utilidad Operacional / Patrimonio mayor o Igual a 0.04

b. Rentabilidad del Activo

Rentabilidad del Activo = Utilidad Operacional / activo Total mayor o Igual a 0.02

NOTA: Cuando el proponente sea un consorcio, unión temporal o promesas de sociedad futura cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador en la figura del oferente plural y se aplicará la siguiente formula:

Suma de los componentes de los indicadores

En esta opción cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador.

$$(ii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i\right)}$$

Donde n es el número de integrantes del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

En esta opción el indicador es el mismo independientemente de la participación de los integrantes del oferente plural.

CRITERIOS DIFERENCIALES PARA MYPIMES, EMPRENDIMIENTOS Y EMPRESAS DE MUJERES - FINANCIEROS

Según lo establecido en la Ley 2069 del 31 de diciembre de 2020 ARTÍCULO 31. CRITERIOS DIFERENCIALES PARA MIPYMES EN EL SISTEMA DE COMPRA PÚBLICA. Las Entidades Estatales de acuerdo con el análisis de Sector podrán incluir, en los Documentos del Proceso, requisitos diferenciales y puntajes adicionales, en función del tamaño empresarial para la promoción del acceso de las MIPYMES al mercado de Compras Públicas.

Por lo anterior y conforme al Decreto 1860 de 2021, mediante el cual se reglamenta los artículos 30, 31, 32, 34 Y 35 de en lo relativo al sistema de compras públicas, Artículos 2.2.1.2.4.2.15 y 2.2.1.2.4.2.18 Criterios diferenciales para emprendimientos y empresas de mujeres en el sistema de compras públicas y Criterios

diferenciales para Mipyme en el sistema de compras públicas. En los procesos de licitación pública, selección abreviada de menor cuantía y concurso de méritos, así como en los procesos competitivos que adelanten las Entidades Estatales no sometidas al Estatuto General de Contratación de la Administración Pública, las Entidades incluirán condiciones habilitantes para incentivar los emprendimientos y empresas de mujeres con domicilio en el territorio nacional. Para el efecto, los Documentos del Proceso deberán incorporar requisitos habilitantes diferenciales relacionados con alguno o algunos de los siguientes aspectos:

1. Tiempo de experiencia.
2. Número de contratos para la acreditación de la experiencia.
3. Índices de capacidad financiera.
4. **Índices de capacidad organizacional.**
5. Valor de la garantía de seriedad de la oferta

INDICADORES DE CAPACIDAD ORGANIZACIONAL - DIFERENCIALES PARA MIPYMES, EMPRENDIMIENTOS Y EMPRESAS DE MUJERES

a. Rentabilidad del Patrimonio

Rentabilidad del Patrimonio = Utilidad Operacional / Patrimonio mayor o Igual a 0.00

b. Rentabilidad del Activo

Rentabilidad del Activo = Utilidad Operacional / activo Total mayor o Igual a 0.00

NOTA: Cuando el proponente sea un consorcio, unión temporal o promesas de sociedad futura cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador en la figura del oferente plural y se aplicará la siguiente formula:

Suma de los componentes de los indicadores

En esta opción cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador.

$$(ii)\ Indicador = \frac{\left(\sum_{i=1}^{n} Componente\ 1\ del\ indicador_i\right)}{\left(\sum_{i=1}^{n} Componente\ 2\ del\ indicador_i\right)}$$

Donde n es el número de integrantes del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

En esta opción el indicador es el mismo independientemente de la participación de los integrantes del oferente plural.

NOTA: El proponente que pretenda acogerse al criterio diferencial, deberá aportar con la oferta documento suscrito por el representante legal o quien haga sus veces o la persona natural según corresponda, manifestando su intención de ser beneficiado de tal circunstancia, para lo cual deberá aportar la documentación soporte de acuerdo con el ARTÍCULO 2.2.1.2.4.2.4 del Decreto 1082 de 2015.

E. Capacidad residual: N/A.

F. Criterios de verificación técnica:

APLICA PARA CADA UNO DE LOS LOTES.

1. CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS:

Los aspectos técnicos son todos aquellos que por su especial característica requieren de una exigencia particular de cumplimiento que no puede obviarse y por lo tanto son de carácter obligatorio.

El proponente acreditará que los bienes y/o servicios a prestar cumplen con las especificaciones técnicas mínimas objeto del proceso, según sea el caso, exigidas en la descripción contenida en el anexo de especificaciones técnicas.

2. EXPERIENCIA HABILITANTE:

El proponente deberá acreditar experiencia, la cual deberá estar inscrita en el registro único de proponentes, de conformidad con los requerimientos establecidos por el comité técnico estructurador.

De conformidad con el artículo 6° de la Ley 1150 de 2007 modificado por el artículo 221 del Decreto Ley 019 de 2012 y reglamentado por el artículo 2.2.1.1.1.5.6 del Decreto 1082 de 2015, el oferente debe acreditar su experiencia habilitante con corte a 31 de diciembre de 2024 siempre y cuando se encuentre vigente a la fecha de cierre del proceso, de acuerdo con los siguientes parámetros:

a) Información vigente y en firme contenida en el Registro Único de Proponentes “RUP”, en las condiciones señaladas en el presente proceso contractual.

b) Experiencia establecida en el Registro Único de Proponentes, identificada con el clasificador de bienes y servicios en el tercer nivel, es decir hasta clase, en los siguientes códigos UNSPSC.

CÓDIGO ONU *(Segmento/Familia/Clase/Producto)*	**DESCRIPCIÓN**
43222500	Equipo de seguridad de red
43232600	Software específico para la industria
43233200	Software de seguridad y protección
81111800	Servicios de sistemas y administración de componentes de sistemas.
81112200	Mantenimiento y soporte de software
81112500	Servicios de alquiler o arrendamiento de licencias de software de computador.
81161500	Servicios de administración de acceso

c) El proponente deberá acreditar experiencia en los anteriores códigos UNSPSC; la cual será verificada en el registro único de proponentes, cuya sumatoria sea igual o superior al 100% del valor del presupuesto oficial expresado en SMMLV.

Cada ítem de la documentación se evaluará como CUMPLE O NO CUMPLE.

Para efectos de verificar la experiencia de los proponentes se realizará solo si el Registro Único de Proponentes expedido en la respectiva Cámara de Comercio, siempre y cuando se encuentre vigente a la fecha de cierre del proceso.

ACREDITACIÓN DE LA EXPERIENCIA ESPECÍFICA EN LA MODALIDAD DE CONSORCIO O UNIÓN TEMPORAL O PROMESA DE SOCIEDAD FUTURA

Cuando se trate de consorcios o uniones temporales o promesa de sociedad futura se requiere acreditar el 100% de la experiencia exigida para el oferente singular; cada uno de sus integrantes debe acreditar experiencia en cualquiera de los códigos exigidos, mínima del 25% sin importar el porcentaje individual de participación; en todo caso la sumatoria debe corresponder mínimo al 100% del presupuesto oficial de la presente selección, expresada en Salarios Mínimos Mensuales Legales Vigentes. Esta información será verificada en el RUP de cada uno de los integrantes del proponente plural. En consecuencia, junto con la propuesta debe ser aportado el RUP de los integrantes del proponente a través de la plataforma del SECOP II.

Cuando las actividades correspondientes hayan sido ejecutadas por el proponente o por uno de sus miembros bajo la modalidad de consorcio o unión temporal, sólo se tendrá en cuenta como experiencia del proponente o de uno de sus miembros, aquella referida al porcentaje de participación que el proponente hubiera tenido en el grupo o asociación que ejecutó la actividad.

Para efectos de verificar la experiencia de los proponentes se realizará solo si el Registro Único de Proponentes expedido por la respectiva Cámara de Comercio, se encuentre vigente a la fecha de cierre y en firme al momento de la adjudicación del proceso de selección.

NOTA: Todos los integrantes del Consorcio o Unión Temporal deberán demostrar experiencia certificada en el RUP.

EXPERIENCIA ESPECÍFICA HABILITANTE DE PERSONA JURÍDICA O NATURAL EXTRANJERA (SIN DOMICILIO EN COLOMBIA O JURÍDICA SIN SUCURSAL EN COLOMBIA)

Para el cumplimiento de la experiencia habilitante requerida, diligenciará el ANEXO EXPERIENCIA HABILITANTE DE PERSONA NATURAL EXTRANJERA (SIN DOMICILIO EN COLOMBIA O JURÍDICA SIN SUCURSAL EN COLOMBIA" del pliego de condiciones de acuerdo con los siguientes parámetros:

1. La información suministrada, se entiende bajo la gravedad del juramento y debe ser correlativa a la documentación aportada.
2. El formulario debe ir firmado por el representante legal del proponente o suplente.
3. Anexo de los soportes que demuestren la acreditación de la experiencia requerida

Requisitos que debe cumplir el oferente:

a. Que el proponente tenga experiencia relacionada con el objeto del proceso
b. La experiencia acreditada deberá ser del 100% del presupuesto oficial del proceso.
c. La experiencia podrá acreditarse aportando contratos o facturas ejecutados, acompañadas del documento donde se certifique de manera fehaciente el cumplimiento de cada uno de estos y siguiendo los lineamientos establecidos en el pliego de condiciones.

EL MINISTERIO DE DEFENSA. COMANDO GENERAL- DIRECCIÓN ADMINISTRATIVA Y FINANCIERA se reserva el derecho de verificar la información aportada, y no será tenida en cuenta aquella que se pueda establecer que no es cierta.

NOTA: La experiencia deberá acreditarse a través de:

a. Fotocopia legible de los contratos que se presentan para acreditar la experiencia.
b. Certificación de los contratos ejecutados:
c. Cada certificación deberá contener como mínimo la siguiente información:

- Nombre o razón social de la empresa o persona contratante.
- Nombre de la persona natural o jurídica contratada, con identificación.
- En caso de tratarse de un consorcio o Unión Temporal debe adjuntarse copia del respectivo documento de constitución del ejecutante del contrato que se está certificando.
- Objeto del contrato.
- Valor del contrato.
- Fecha de iniciación y de terminación del contrato (día, mes, año)
- Firma del funcionario competente.
- Indicación de la dirección comercial y teléfono del contratante o la del dueño del proyecto.
- Indicación sobre el cumplimiento del contratista

Nota 1: No se aceptan certificaciones con enmendaduras y que no contengan como mínimo la información solicitada o que presenten inconsistencias.
Nota 2: EL MINISTERIO DE DEFENSA. COMANDO GENERAL- DIRECCIÓN ADMINISTRATIVA Y FINANCIERA se reserva el derecho de verificar la veracidad de la información.
Nota 3: No se acepta ningún otro documento para acreditar la experiencia. NO SE ACEPTAN AUTO CERTIFICACIONES.
Nota 4: Las copias de los documentos presentadas deben ser completamente legibles.
Nota 5: Si los contratos fueron ejecutados bajo la modalidad de consorcio o unión temporal el valor registrado que debe informar el proponente será el correspondiente al porcentaje de participación que hubiere tenido en los mismos.
Nota 6: Para el proponente extranjero todos los documentos que aporte deberán venir apostillados en idioma castellano y con traducción oficial castellano.
Nota 7: Cuando se relacionen contratos en moneda extranjera, el proponente deberá realizar las conversiones respectivas a pesos colombianos e indicar en el Anexo "ANEXO EXPERIENCIA HABILITANTE DE PERSONA NATURAL EXTRANJERA (SIN DOMICILIO EN COLOMBIA O JURÍDICA SIN SUCURSAL EN COLOMBIA el valor obtenido y su equivalente a SMMLV a la fecha de terminación del contrato, de acuerdo con los siguientes parámetros:

Cuando el valor este dado en dólares de los Estados Unidos de América (USD$) se convertirá a pesos colombianos utilizando para esta conversión la tabla Serie de datos promedio anual de la Serie empalmada de la tasa de cambio del peso colombiano frente al dólar (TRM y Certificado de Cambio) correspondiente al año de terminación para lo cual el proponente debe tomar la publicada por el Banco de la Republica para el año correspondiente en el siguiente link

http://www.banrep.gov.co/series-estadisticas/see ts trm.htm#cotizacion

En todo caso, la Entidad revisará las conversiones realizadas por el proponente y en caso de encontrarse diferencias, errores aritméticos o inconsistencias con respecto a lo indicado en el Anexo se realizarán las correcciones respectivas de acuerdo con lo indicado en el presente numeral y el valor que se obtenga primará para todos los efectos.

Para experiencia en el área privada se acepta certificación de recibo a satisfacción

3. Perfil del personal requerido en la ejecución del contrato.

APLICA PARA CADA UNO DE LOS LOTES.

El Ministerio de Defensa Nacional – Comando General FFMM, requiere que el futuro contratista cuente mínimo con el personal que cumpla con los siguientes perfiles, para lo cual deberá aportar con la oferta la documentación respectiva:

- LOTE 1: LICENCIAS FIREWALL + VPN.

CARGO	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO SOPORTE	Profesional en: Ingeniería de Sistemas o electrónico o Telecomunicaciones o áreas afines de acuerdo con el SNIES. - Debe aportar Certificaciones en: . Certificación (CCME) . Certificación de Experto en seguridad (CCSE).	UNO (1)	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional de mínimo tres (03) años en instalación, soporte o mantenimiento en productos Checkpoint	Se requiere de manera remota; sin embargo; según incidencias o requerimientos del supervisor del contrato, de acuerdo con necesidad de la Entidad, podrá ser presencial. de acuerdo al anexo de especificaciones técnicas.

- LOTE 2: LICENCIAS PROXY WEB.

CARGO	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO DE SOPORTE	- Profesional en: Ingeniería de Sistemas o electrónico o Telecomunicaciones o áreas afines de acuerdo con el SNIES. - Certificación vigente Fortinet Certified Solution Specialist Network Security Certified Solution Professional Network Security.	UNO (1)	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional de mínimo cinco (05) años como Ingeniero soporte de soluciones de seguridad de filtrado web/proxy	100% durante la ejecución del contrato y deberá estar presente en las reuniones y/o comités, en la toma de decisiones y cuando sea requerido por el supervisor.

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

ROL	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
GERENTE DE PROYECTO	- Profesional en: Ingeniero de sistemas o telecomunicaciones o electrónico o carreras	Uno (1).	. Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta	La supervisión y coordinación de todas las actividades relacionadas con la

	afines de acuerdo con la SNIES . Debe contar con posgrado en Gerencia de proyectos de telecomunicaciones Con certificados en: ✓ Certificación PMP vigente ✓ Certificación Itil Expert		profesional de Mínimo de cinco (05) años en cargos o contratos relacionados con funciones u obligaciones como Gerente de proyectos en proyectos de TI. . Debe acreditar por medio de tres (03) certificaciones experiencia relacionada con la implementación o soporte u operación o administración de soluciones EDR, XDR y DLP.	implementación y administración de la solución de seguridad. Su trabajo se enfoca en garantizar el cumplimiento de los objetivos del proyecto, la eficiencia en la gestión y la mejora continua de la seguridad de la entidad. 50% del tiempo durante el plazo de ejecución o cuando sea requerido por el supervisor del contrato.
INGENIERO IMPLEMENTADOR	- Profesional en: Ingeniería en sistemas o electrónico o telecomunicaciones o carreras afines acuerdo con la SNIES. . Debe contar con posgrado en Seguridad Informática o ciberseguridad o Seguridad de la información. Con certificados en: . Certificación o constancia de entrenamiento en la solución ofertada emitido por el fabricante de la solución ofertada. . Certificación CISM (Certified Information Security Manager) . CISP (Certified Information Security Professional) o Certificado CCFA (Certified Cyber Forensics Analyst).	Uno (1).	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional de Mínimo de cuatro (04) años en cargos o contratos relacionados con funciones u obligaciones con la implementación o soporte u operación o administración de proyectos de ciberseguridad focalizados en EDR/XDR/SIEM. . Debe demostrar por medio de una (01) certificación la participación en un (01) proyecto de implementación o soporte de la solución adquirir.	Implementación y despliegue de soluciones de seguridad del agente, el ingeniero será responsable de instalar, configurar y desplegar las soluciones de seguridad del agente en los dispositivos finales de la organización. Afinamiento y configuración de la solución. 100% del tiempo durante el plazo de ejecución o cuando sea requerido por el supervisor del contrato.

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

CARGO	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO IMPLEMENTADOR Y SOPORTE	- Profesional titulado en: Ingeniería de sistemas o Electrónico o telecomunicaciones o áreas a fines, de	Uno (1).	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional de mínimo tres (03)	Quien realizará las actividades de configuración, puesta en funcionamiento y soporte de la herramienta ofrecida descritas en el anexo técnico.

	acuerdo con el SNIES. - Debe contar con certificaciones técnicas del fabricante relacionadas con la implementación, operación o soporte de la solución de seguridad ofertada en: . Solución de filtrado y seguridad de Correo Electrónico . Troubleshooting de Solución de filtrado y seguridad de Correo Electrónico		años en instalación, configuración, soporte o mantenimiento en productos de filtrado y seguridad de Correo Electrónico.	Con dedicación total durante el proceso de implementación, será el encargado de realizar el despliegue de la solución de seguridad de filtrado de Correo Electrónico a adquirir, generación de reglas, políticas y estándares para la clasificación sensible de activos de información y buenas prácticas de seguridad de acuerdo a las especificaciones técnicas. De manera presencial en las instalaciones del COGFM, para las actividades de implementación de la solución de filtrado y seguridad de Correo Electrónico.

- LOTE 5: SUSCRIPCIÓN WAF.

CARGO	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO DE SOPORTE E IMPLEMENTADOR DE LA SOLUCIÓN DE SEGURIDAD	- Profesional titulado en: Ingeniería de sistemas o Electrónico o telecomunicaciones o áreas a fines, de acuerdo con el SNIES. - Debe aportar Certificaciones del fabricante de la solución de seguridad ofertada como administrador y técnico especialista.	Uno (1).	Debe demostrar experiencia especifica contada a partir de la expedición de la tarjeta profesional de mínimo tres (03) años de experiencia en diseño, implementación, configuración y soporte de la plataforma WAF.	Con dedicación de tiempo parcial de forma presencial o remota, Quien realizará las actividades de configuración, mantenimiento y soporte del presente proceso descritas en el anexo técnico. Para la implementación de la solución de seguridad deberá ser se manera presencial en las instalaciones del COGFM.

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

CARGO	FORMACIÓN ACADÉMICA	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO IMPLEMENTADOR	- Profesional titulado en: ingeniería de sistemas, o electrónica o telecomunicaciones, o áreas afines de	Uno (1).	Debe demostrar experiencia específica contada a partir de la expedición de la tarjeta profesional de mínimo tres (03)	Con dedicación total de manera presencial durante el proceso de implementación de la solución de SASE de acuerdo al anexo de especificaciones técnicas.

	acuerdo con el SNIES Debe contar con certificaciones en: . Experto en Troubleshooting (CCTE) vigente . Security Master Elite (CCSM Elite)		años relacionada con la implementación o soporte u operación de la solución a adquirir.	

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

ROL	FORMACIÓN	CANTIDAD	EXPERIENCIA ESPECIFICA	DEDICACIÓN / ACTIVIDADES
INGENIERO DE IMPLEMENTACIÓN	Profesional titulado en: ingeniería de sistemas o electrónica o informática o telecomunicaciones o áreas afines de acuerdo con el SNIES. Deberá contar con la siguiente certificación vigente: Cisco Certified Network Professional (CCNP) Collaboration.	Uno (01)	Debe demostrar experiencia específica contada a partir de la expedición de la tarjeta profesional de mínimo tres (03) años de experiencia en la solución ofertada objeto del presente LOTE.	Con dedicación del 100% de manera presencial durante las fases del proyecto incluyendo la implementación, instalación, configuración y puesta en funcionamiento, y conforme a lo establecido en el anexo de especificaciones técnicas.

Los profesionales deberán acreditar y aportar lo siguiente:

1. Para acreditar la “Formación Académica” se debe adjuntar copia del(os) título(s) académico(s) o acta(s) de grado(s) y de la(s) certificación(es) o constancia(s) o cursos requerido(s).

2. Para acreditar “Experiencia Específica”, debe anexar con la oferta copia de certificaciones laborales o contractuales, que indiquen por lo menos: (i) fecha de inicio, (ii) fecha de terminación, (iii) firma, nombre, dirección y teléfono de quien la expide, (iv) objeto.

En el evento de aportar auto certificaciones, anexar copia de los contratos laborales y/o contractuales, que las soporten.

NOTA: Entendiéndose como auto certificaciones aquellas emitidas por el mismo proponente o por uno de sus integrantes en los casos de Consorcios o Uniones Temporales, o aquellas emitidas por empresas que formen parte del mismo grupo empresarial al cual pertenece el proponente, ya sea proponente individual o plural.

No se aceptan certificaciones expedidas o suscritas por supervisores, estas deberán ser expedidas por el competente contractual.

3. Se debe adjuntar con la oferta Hoja de vida, de la cédula de ciudadanía y de la matricula y/o tarjeta profesional vigente según aplique, expedida por el Consejo Profesional correspondiente para los profesionales.

4. Certificado vigente de antecedentes y vigencia expedido por el consejo profesional respectivo para los profesionales.

5. Anexar “carta de compromiso”, mediante la cual se compromete a prestar sus servicios en caso de que el oferente resulte adjudicatario del presente proceso de selección, en las condiciones y dedicaciones establecidas por la Entidad.

Nota 1: Para el cálculo de la experiencia del personal en años, se tomará como base años de 360 días y meses de 30 días.

Nota 2: El oferente que no cumpla con el perfil mínimo del profesional y con las condiciones mínimas requeridas, no será HABILITADO.

El comité técnico evaluador realizará las consultas de CERTIFICADO DE RESPONSABILIDAD FISCAL, CERTIFICACIÓN ANTECEDENTES DISCIPLINARIOS, CERTIFICACIÓN DE ANTECEDENTES JUDICIALES y REGISTRO NACIONAL DE MEDIDAS CORRECTIVAS, y emitirá el concepto de acuerdo con las inhabilidades e incompatibilidades establecidas en la Ley y la Constitución.

Nota 3:

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

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

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

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

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

NOTA 4: Para el cumplimiento del futuro contrato el proponente debe vincular personal que sean empleados colombianos o contratistas por prestación de servicios colombianos. El porcentaje mínimo de empleados colombianos o contratistas por prestación de servicios colombianos asociados al cumplimiento del futuro contrato se establece en el 100%.

NOTA 5: Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. En todo caso el proponente deberá efectuar el respectivo análisis del pliego de condiciones del presente proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos del contrato derivado del presente proceso. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

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

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

4. Certificación del cumplimiento del SEGURIDAD Y SALUD EN EL TRABAJO. (SG-SST)

Para el efecto debe diligenciar el Anexo CERTIFICADO DE CUMPLIMIENTO SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO.

5. Documentación

APLICA PARA CADA UNO DE LOS LOTES.

El proponente deberá aportar con la oferta los siguientes documentos:

- LOTE 1: LICENCIAS FIREWALL + VPN.

- ✓ Certificación vigente emitida directamente por el fabricante Check Point Software Technologies que lo acredite como partner o distribuidor o comercializador autorizado, con fecha de expedición no mayor a treinta (30) días calendario con respecto a la fecha fijada para la presentación de ofertas del presente proceso dirigida al COGFM.

- LOTE 2: LICENCIAS PROXY WEB.

- ✓ Certificación emitida directamente por el fabricante FORTINET que lo acredite como partner o distribuidor o comercializador, con fecha de expedición no mayor a treinta (30) días calendario con respecto a la fecha fijada para la presentación de ofertas del presente proceso dirigida al COGFM.
- ✓ El oferente deberá contar con una mesa de servicios, encargada de gestionar todos los incidentes y requerimientos reportados, con el fin de realizar un seguimiento del cumplimiento de los acuerdos de nivel de servicio garantizando calidad del servicio. Por lo tanto, se debe adjuntar una certificación donde conste que es partner y que dicha herramienta cumple con mínimo 12 procesos de ITIL certificados (verificados por PinkVerify).

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

- ✓ Deberá aportar la ficha técnica, data sheet o link de referencia emitido por el fabricante de la solución ofertada, donde se describa su marca y/o referencia, con el fin de que el comité técnico evaluador pueda verificar el cumplimiento de las especificaciones técnicas requeridas en el Anexo.
- ✓ Certificación vigente emitida directamente por el fabricante de la solución ofertada que lo acredite como partner o distribuidor o comercializador autorizado, con fecha de expedición no mayor a treinta (30) días calendario con respecto a la fecha fijada para la presentación de ofertas del presente proceso dirigida al COGFM.
- ✓ El oferente deberá contar con una mesa de servicios, encargada de gestionar todos los incidentes y requerimientos reportados, con el fin de realizar un seguimiento del cumplimiento de los acuerdos de nivel de servicio garantizando calidad del servicio. Por lo tanto, se debe adjuntar una certificación donde conste que es partner y que dicha herramienta cumple con mínimo 12 procesos de ITIL certificados (verificados por PinkVerify).

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

- ✓ Certificación vigente emitida directamente por el fabricante que lo acredite como partner o distribuidor o comercializador autorizado para comercializar los productos de la marca ofertada, con fecha de expedición no mayor a treinta (30) días calendario con respecto a la fecha fijada para la presentación de ofertas del presente proceso dirigida al COGFM.
- ✓ Deberá aportar la ficha técnica, data sheet o link de referencia emitido por el fabricante de la solución ofertada, donde se describa su marca y/o referencia, con el fin de que el comité técnico evaluador pueda verificar el cumplimiento de las especificaciones técnicas requeridas en el Anexo.

- LOTE 5: SUSCRIPCIÓN WAF.

- ✓ Deberá aportar la ficha técnica, data sheet o link de referencia emitido por el fabricante de la solución ofertada, donde se describa su marca y/o referencia, con el fin de que el comité técnico evaluador pueda verificar el cumplimiento de las especificaciones técnicas requeridas en el Anexo.
- ✓ Certificación vigente emitida por el fabricante de la solución de seguridad ofertada, que lo acredite como partner o distribuidor o comercializador autorizado. Esta certificación deberá estar dirigida al Comando General de las Fuerzas Militares, con fecha de expedición no mayor a 2 meses calendario anteriores a la fecha de recepción de ofertas (cierre) del presente proceso.
- ✓ El oferente deberá contar con una mesa de servicios, encargada de gestionar todos los incidentes y requerimientos reportados, con el fin de realizar un seguimiento del cumplimiento de los acuerdos de nivel de servicio garantizando calidad del servicio. Por lo tanto, se debe adjuntar una certificación donde conste que es partner y que dicha herramienta cumple con mínimo 12 procesos de ITIL certificados (verificados por PinkVerify).

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

- ✓ Deberá aportar la ficha técnica, data sheet o link de referencia emitido por el fabricante de la solución ofertada, donde se describa su marca y/o referencia, con el fin de que el comité técnico evaluador pueda verificar el cumplimiento de las especificaciones técnicas requeridas en el Anexo.
- ✓ Certificación vigente emitida directamente por el fabricante del equipo ofertado, que lo acredite como partner o distribuidor o comercializador autorizado. Esta certificación deberá estar dirigida al Comando General de las Fuerzas Militares para el presente proceso, con fecha de expedición no mayor a 2 meses calendario anteriores a la fecha de recepción de ofertas (cierre) del presente proceso.

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

✓ Certificación emitida directamente por el fabricante CISCO que lo acredite como partner o distribuidor o comercializador, con fecha de expedición no mayor a treinta (30) días calendario con respecto a la fecha fijada para la presentación de ofertas del presente proceso dirigida al COGFM.

G. CRITERIOS DE PONDERACIÓN.

Una vez culminada la verificación jurídica, financiera y técnica de las ofertas y habiéndose efectuado los requerimientos previos a que hubiere lugar y obtenidas las correspondientes respuestas, se determinarán las ofertas que se consideran hábiles, según lo establecido en el pliego de condiciones "Orden de Elegibilidad", para efectos de asignar el puntaje económico y técnico, según corresponda. (Artículo 2.2.1.1.2.2.2 del DECRETO 1082 de 2015) así:

FACTORES DE PONDERACIÓN TÉCNICA

- LOTE 1: LICENCIAS FIREWALL + VPN.

	DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN	PUNTAJE MÁXIMO
01	El oferente que ofrezca sin costo adicional: una bolsa de 20 horas de soporte técnico especializado para nuevas implementaciones, las cuales podrán utilizarse de manera remota o, según la criticidad del caso, de forma presencial en las instalaciones del Complejo Militar CAN, en la ciudad de Bogotá, sin que este ofrecimiento genere costo adicional para el COGFM.	100
PUNTAJE TOTAL (Máximo)		**100**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 100 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 2: LICENCIAS PROXY WEB.

	DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN	PUNTAJE MÁXIMO
01	El oferente que ofrezca sin costo adicional: la actualización del fortiAnalyzer a la versión VM y que cuente con una capacidad mínima de procesamiento de +100gb por día de logs, sin que este ofrecimiento genere costo adicional para el COGFM.	100
02	El oferente que ofrezca sin costo adicional: 25 horas de transferencia de conocimiento en administración y configuración del Proxy para (02) dos funcionarios del CGDJ6 con Voucher incluido, sin que este ofrecimiento genere costo adicional para el COGFM.	100
PUNTAJE TOTAL (Máximo)		**200**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 200 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN		PUNTAJE MÁXIMO
01	El oferente que ofrezca sin costo adicional: transferencia de conocimiento de la solución de protección de datos ofertada con certificación de Voucher para cuatro (04) funcionarios del Comando General de las Fuerzas Militares – CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.	200
PUNTAJE TOTAL (Máximo)		**200**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 200 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN		PUNTAJE MÁXIMO
01	El oferente que ofrezca sin costo adicional: transferencia de conocimiento de la solución de protección de correo electrónico con Voucher para tres (03) funcionarios del CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.	100
02	El oferente que ofrezca sin costo adicional: transferencia de conocimiento de la solución de protección de correo electrónico con Voucher para cinco (05) funcionarios del CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM.	200
PUNTAJE TOTAL (Máximo)		**200**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 200 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 5: SUSCRIPCIÓN WAF.

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN		PUNTAJE MÁXIMO
01	El oferente que ofrezca sin costo adicional: Terminal para administración y gestión de la solución de seguridad que debe incluir como mínimo Intel® Core™ Ultra 7 265KF, Windows 11 Pro, NVIDIA® GeForce RTX™ 5080, 32 GB DDR5, SSD de 2 TB, Con periféricos incluidos y 02 dispositivos de visualización de 25" que permitan visualización y monitoreo de datos críticos, sin que este ofrecimiento genere costo adicional para la entidad.	200
PUNTAJE TOTAL (Máximo)		**200**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 200 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN		PUNTAJE MÁXIMO
1	El oferente que ofrezca sin costo adicional: **CURSO CERTIFICADO Y ENTRENAMIENTO INCLUYE (VOUCHER) POR EL FABRICANTE SOBRE LA ADMINISTRACIÓN Y TROUBLESHOOTING DE LA SOLUCIÓN SASE PARA DOS (2) FUNCIONARIOS DEL COGFM**; sin que este ofrecimiento genere costo adicional para el COGFM.	100
2	El oferente que ofrezca sin costo adicional: diez (10) licencias de acceso seguro con las mismas características de las especificaciones técnicas; sin que este ofrecimiento genere costo adicional para el COGFM.	100
PUNTAJE TOTAL (Máximo)		**200**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 200 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

DESCRIPCIÓN DEL ELEMENTO / FACTOR DE PONDERACIÓN		PUNTAJE MÁXIMO
1	El oferente que ofrezca sin costo adicional: dos (02) Voucher del curso CCNA con entrenamiento y certificación; sin que este ofrecimiento genere costo adicional para el COGFM.	100
PUNTAJE TOTAL (Máximo)		**100**

Serán ponderados única y exclusivamente los proponentes que hayan superado la habilitación o verificación técnica, financiera, económica y jurídica.

La puntuación técnica será de un mínimo de 0 puntos y un máximo de 100 puntos.

NOTA 1: El Ministerio de Defensa Nacional – COGFM - Dirección Administrativa y Financiera sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, NO REALIZARA ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.

NOTA 2: En caso de no ofrecer criterios técnicos de evaluación adicionales, a la oferta se le asignará cero (0) puntos y no es factor excluyente.

NOTA 3: Los factores de ponderación son opcionales, no son obligatorios y su ofrecimiento no genera costo económico adicional para el Comando General.

NOTA 4: El puntaje total de la ponderación técnica se dará única y exclusivamente si cumplen con las especificaciones técnicas, jurídica, financiera y la valoración de la propuesta económica.

FACTORES DE PONDERACIÓN ECONÓMICA (Máximo 300 puntos por Lote).

APLICA PARA CADA UNO DE LOS LOTES.

EL M.D.N.-COMANDO GENERAL DE LAS FUERZAS MILITARES – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA a partir del valor total IVA exento o excluido según aplique de las ofertas asignará máximo 300 puntos por lote de acuerdo con el método escogido en forma aleatoria para la ponderación de la oferta económica:

MÉTODO DE EVALUACIÓN DE LA OFERTA ECONÓMICA
Mediana con valor absoluto
Media geométrica
Media aritmética baja
Menor valor

Para determinar el método de ponderación, la entidad tomará los centavos de la **Tasa de Cambio Representativa del Mercado (TRM),** certificada por la Superintendencia Financiera de Colombia (en su sitio web oficial).

La **TRM** que la entidad utilizará para determinar el método de ponderación será la que rija el **segundo día hábil después del cierre del proceso**. Esto es, la que la Superintendencia publique en horas de la tarde del día hábil siguiente a la fecha efectiva de cierre del proceso.

El método debe ser escogido de acuerdo con los rangos establecidos en la tabla que se presenta a continuación.

ASIGNACIÓN DE MÉTODO DE EVALUACIÓN SEGÚN TRM		
Rango (Inclusive)	**Número**	**Método**

De ,00 a ,24	1	Mediana con valor absoluto
De ,25 a ,49	2	Media geométrica
De ,50 a ,74	3	Media aritmética baja
De ,75 a ,99	4	Menor valor

Las propuestas que al aplicar las fórmulas obtengan puntajes negativos obtienen cero (0) puntos en la oferta económica.

A. Mediana con valor absoluto

La Entidad calculará el valor de la mediana con los valores de las propuestas hábiles. En esta alternativa se entenderá por mediana de un grupo de valores el resultado del cálculo que se obtiene a través de la aplicación del siguiente proceso: la Entidad ordenará los valores de las propuestas hábiles de manera descendente. Si el número de valores es impar, la mediana corresponde al valor central, si el número de valores es par, la mediana será el promedio de los dos valores centrales.

$$Me = Mediana(V_1; V_2..; ... V_m)$$

Donde:

- Vi : Es el valor total corregido de cada una de las propuestas "i".
- m: Es el número total de propuestas económicas válidas recibidas por la Entidad.
- Me: Es la mediana calculada con los valores de las propuestas económicas válidas.

Bajo este método la Entidad asignará el puntaje así:

- Si el número de valores de las propuestas hábiles es impar, el máximo puntaje será asignado a la propuesta que se encuentre en el valor de la mediana. Para las otras propuestas, se utilizará la siguiente fórmula:

$$Puntaje = \left[\left\{1 - \left|\frac{Me - V_i}{Me}\right|\right\} * Puntaje\ máximo\right]$$

Donde:

- Me: Es la mediana calculada con los valores de las propuestas económicas válidas.
- Vi : Es el valor total corregido de cada una de las propuestas "i".

- Si el número de valores de las propuestas hábiles es par, se asignará el máximo puntaje a la propuesta que se encuentre inmediatamente por debajo de la mediana. Para las otras propuestas, se utilizará la siguiente fórmula:

$$Puntaje = \left[\left\{1 - \left|\frac{V_{Me} - V_i}{V_{Me}}\right|\right\} * Puntaje\ máximo\right]$$

Donde:

- VMe: Es el valor de la propuesta económica válida inmediatamente por debajo de la mediana.
- Vi: Es el valor total corregido de cada una de las propuestas "i"

B. Media Geométrica

Para calcular la Media Geométrica se tomará el valor de las propuestas hábiles para el respectivo factor de calificación para asignar el puntaje de conformidad con el siguiente procedimiento:

$$MG = \sqrt[n]{V_1 * V_2 * V_3 * ... * V_n}$$

Donde:

- MG: Es la media geométrica de todas las ofertas habilitadas.
- V_1: Es el valor de una propuesta habilitada.
- Vn: Es el valor de la propuesta n habilitada.
- n: La cantidad total de propuestas habilitadas.

Para efectos de la asignación de puntaje se tendrá en cuenta lo siguiente: se otorgará el máximo puntaje al valor de la propuesta que se encuentre más cerca (por exceso o por defecto) al valor de la media geométrica calculada para el factor correspondiente.
Las demás propuestas recibirán puntaje de acuerdo con la siguiente ecuación:

$$Puntaje = Puntaje\ máximo * \left(1 - \left(\frac{|MG - V_i|}{MG}\right)\right)$$

C. Media Aritmética Baja

Consiste en determinar el promedio aritmético entre la propuesta válida más baja y el promedio simple de las ofertas hábiles para calificación económica.

$$\overline{X_B} = \frac{(V_{min} + \overline{X})}{2}$$

Donde:

- Vmin: Es el valor total corregido de la propuesta válida más baja.
- $\overline{X}$: Es el promedio aritmético simple de las propuestas económicas válidas.
- XB: Es la media aritmética baja.

La Entidad procederá a ponderar las propuestas de acuerdo con la siguiente formula:

$$Puntaje = \begin{cases} Puntaje\ máximo * \left(1 - \left(\frac{\overline{X_B} - V_i}{\overline{X_B}}\right)\right) \ Para\ valores\ menores\ o\ iguales\ a\ \overline{X_B} \\ \\ Puntaje\ máximo * \left(1 - \left(\frac{|\overline{X_B} - V_i|}{\overline{X_B}}\right)\right) \ Para\ valores\ mayores\ a\ \overline{X_B} \end{cases}$$

Donde:

- XB : Es la media aritmética baja.
- Vi : Es el valor total corregido de cada una de las propuestas “i”.

D. Menor Valor

La Entidad otorgará el máximo puntaje a la oferta económica hábil para calificación económica de menor valor.

$$V_{min} = Mínimo\ (V_1; V_2..; ...V_m)$$

Donde:

- Vi : Es el valor total corregido de cada una de las propuestas “i”.
- m: Es el número total de propuestas económicas válidas recibidas por la Entidad.
- Vmin: Es el valor total corregido de la propuesta válida más baja.

La Entidad procederá a ponderar las propuestas de acuerdo con la siguiente fórmula:

$$Puntaje = \frac{Puntaje\ máximo * V_{min}}{V_i}$$

Donde:

- Vmin: Es el valor total corregido de la propuesta válida más baja.
- Vi : Es el valor total corregido de cada una de las propuestas “i”.

En este caso se tomará el valor absoluto de la diferencia entre el menor valor y el valor de la Oferta, como se observa en la fórmula de ponderación.

Para todos los métodos descritos se tendrá en cuenta hasta el séptimo (7°) decimal del valor obtenido como puntaje.

El puntaje máximo que es posible obtener, en la calificación de ponderación de precios es hasta de 300 puntos, sin requerirse de un puntaje mínimo para la elegibilidad de la propuesta.

Las ofertas serán analizadas para determinar si en los cálculos se han cometido errores en las operaciones aritméticas, en cuyo caso y para efectos de evaluación y selección el comité económico evaluador realizará las correcciones necesarias teniendo en cuenta dos (2) decimales.

Artículo 2.2.1.1.2.2.4 DECRETO 1082 de 2015 - OFERTA CON VALOR ARTIFICIALMENTE BAJO. SI DE ACUERDO CON LA INFORMACIÓN OBTENIDA POR LA ENTIDAD ESTATAL EN SU DEBER DE ANÁLISIS DE QUE TRATA EL ARTICULO 2.2.1.1.1.6.1 DEL PRESENTE DECRETO, EL VALOR DE UNA OFERTA PARECE ARTIFICIALMENTE BAJO, LA ENTIDAD ESTATAL DEBE REQUERIR AL PROPONENTE PARA QUE EXPLIQUE LAS RAZONES QUE SUSTENTEN EL VALOR OFRECIDO.

ANALIZADAS LAS EXPLICACIONES, EL COMITÉ EVALUADOR O QUIEN HAGA LA EVALUACIÓN DE LAS OFERTAS DEBE RECOMENDAR RECHAZAR LA OFERTA O CONTINUAR CON EL ANÁLISIS DE LA MISMA EN LA EVALUACIÓN DE LAS OFERTAS.

CALIFICACIÓN DE ORIGEN DE LOS BIENES Y SERVICIOS.

APLICA PARA CADA UNO DE LOS LOTES.

De conformidad con lo dispuesto en la Ley No. 816 de 2003, ARTICULO 51 del Decreto 019 de 2012, los artículos 2.2.1.2.4.1.3 “Existencia de trato nacional” y 2.2.1.2.4.2.1 “Incentivos en la contratación pública” del Decreto 1082 de 2015; el artículo 1 del decreto 680 de 2021 que modifica parcialmente el artículo 2.2.1.1.1.3.1. del decreto 1082 de 2015, y el artículo 2 del decreto 680 de 2021 que adicionó el artículo 2.2.1.2.4.2.9. del decreto 1082 de 2015 el puntaje que se aplicará como consecuencia de la protección a la industria nacional será el siguiente:

Una vez efectuada la ponderación económica y ponderación técnica a las ofertas habilitadas técnica, jurídica y económicamente; al puntaje obtenido por cada proponente, se adicionará así:

- LOTE 1: LICENCIAS FIREWALL + VPN.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	80
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	40
Bienes y/o servicios extranjeros	0

- LOTE 2: LICENCIAS PROXY WEB.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	100
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	50
Bienes y/o servicios extranjeros	0

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	100
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	50
Bienes y/o servicios extranjeros	0

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	100
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	50
Bienes y/o servicios extranjeros	0

- LOTE 5: SUSCRIPCIÓN WAF.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	100

Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	50
Bienes y/o servicios extranjeros	0

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	100
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	50
Bienes y/o servicios extranjeros	0

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

PROTECCIÓN A LA INDUSTRIA NACIONAL	PUNTOS
Bienes y/o Servicios Nacionales y/o con trato nacional	80
Bienes y/o Servicios extranjeros que incorporen componente colombiano de bienes y/o servicios profesionales, técnicos y operativos	40
Bienes y/o servicios extranjeros	0

El puntaje señalado en el párrafo anterior se aplicará cuando se cumpla con alguna de estas condiciones:

a) Oferentes de bienes y/o servicios provenientes de Estados con los cuales Colombia tenga acuerdos, en los términos establecidos en tales Acuerdos Comerciales.

b) A los bienes y servicios provenientes de Estados con los cuales no exista un acuerdo comercial, pero respecto de los cuales el gobierno nacional haya certificado que los oferentes de bienes y servicios nacionales gozan de trato nacional, con base en la revisión y comparación de la normativa en materia de compras y contratación pública de dicho Estado.

c) A los servicios prestados por oferentes miembros de la Comunidad Andina de Naciones teniendo en cuenta la regulación andina aplicable a la materia.

Se entenderá como bienes la definición contenida en el Decreto 2680 de 2009.

Entiéndase por bienes o servicios acreditados, aquellos bienes importados que cuentan con componente nacional en bienes o servicios profesionales, técnicos y operativos. El proponente indicará en su oferta si incluirá componente nacional. En el evento en que exista dicho ofrecimiento por parte del proponente, éste tendrá la obligación de cumplir con el mismo en la ejecución del contrato, so pena de hacerse acreedor a las sanciones de ley contempladas en el contrato.

Para efectos de la evaluación del origen de los bienes y/o servicios, el proponente diligenciará el Anexo “ORIGEN DE LOS BIENES Y/O SERVICIOS”, y el comité técnico verificará que la información en él consignada sea acorde con los documentos que se presenten como soporte de la acreditación respectiva. La asignación del puntaje en este aspecto corresponde al comité técnico evaluador.

Documentos para acreditar el origen nacional de los bienes.

Son bienes nacionales los bienes inscritos en el Registro de Productores de Bienes Nacionales -RPBN-. Se debe aportar el RPBN.

Se entenderá como servicios nacionales la definición contenida en el artículo 1 del Decreto 680 de 2021.

Para el caso de servicios nacionales, el proponente deberá manifestarlo en su oferta bajo la gravedad del juramento y para ello diligenciará el Anexo “ORIGEN DE LOS BIENES Y/O SERVICIOS”.

Ahora bien, teniendo en cuenta el objeto y naturaleza del presente proceso, se establece que, no se tienen bienes que sean relevantes y aplicables para la prestación del servicio a contratar y a lo establecido en la nota 4 del numeral 3 del literal F del numeral XV del presente estudio previo; la entidad determina que para el cumplimiento del futuro contrato, el proponente debe vincular personal que sean empleados colombianos o contratistas por prestación de servicios colombianos.

El porcentaje mínimo de empleados colombianos o contratistas por prestación de servicios colombianos asociados al cumplimiento del futuro contrato se establece en el 100%. Por lo tanto, al proponente que cumpla con el porcentaje establecido por la entidad y que lo certifique así en el Anexo "ORIGEN DE LOS BIENES Y/O SERVICIOS" se le otorgará el respectivo puntaje. Lo cual será corroborado de acuerdo con la documentación requerida en el numeral 4.3. PERFIL PROFESIONAL REQUERIDO EN LA EJECUCIÓN DEL CONTRATO del Pliego de Condiciones; en caso de no certificar y acreditar el porcentaje mínimo establecido por la entidad, no se le otorgará puntaje alguno.

Para efectos de la evaluación del origen de los bienes y/o servicios, el oferente diligenciará el Formulario "ORIGEN DE LOS BIENES Y/O SERVICIOS", y el comité técnico y jurídico evaluador verificarán que la información en él consignada sea acorde con los documentos que se presenten como soporte de la acreditación respectiva. La asignación del puntaje en este aspecto corresponde al comité técnico evaluador.

Para el caso de servicios de origen nacional deberá manifestarlo en su oferta bajo la gravedad del juramento. Dicha manifestación debe presentarse con la oferta, so pena de no otorgarse el respectivo puntaje por este aspecto.

NOTA: Considerando que el porcentaje asignado por la acreditación de los bienes o servicios tiene el carácter de comparación de propuestas y asignación de puntaje, el Anexo correspondiente, se presentará con la oferta y no será susceptible de requerimiento por parte del Ministerio de Defensa Nacional.

El oferente seleccionado con productos de origen nacional o acreditado no podrá cambiar el origen de los bienes al momento de la ejecución del contrato, salvo circunstancias de fuerza mayor o caso fortuito, éstos últimos debidamente acreditados.

En el caso de Consorcios o Uniones Temporales conformados por integrantes nacionales y extranjeros, el puntaje se asignará en proporción al porcentaje de participación de cada integrante, según sea su condición de nacional o extranjero.

Para la verificación de este aspecto, el oferente deberá presentar carta de certificación de componente nacional.

En ningún caso podrán acumularse puntajes en dos condiciones de este factor, salvo el establecido en el siguiente párrafo.

En caso de consorcios o uniones temporales conformadas por integrantes nacionales y extranjeros ubicados en distinta condición, el puntaje de cada condición se asignará al integrante correspondiente en proporción al porcentaje de participación y la calificación en el factor será la sumatoria de ambos puntajes.

INCENTIVOS PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES EN EL SISTEMA DE COMPRAS PÚBLICAS

APLICA PARA CADA UNO DE LOS LOTES.

Se otorgará el cero punto uno por ciento (0.1%) del valor total de los puntos establecidos en el Pliego de Condiciones, a los proponentes que acrediten alguno de los supuestos consagrados en el artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015.

NOTA 1: El proponente que pretenda acogerse al criterio diferencial, deberá aportar con la oferta documento suscrito por el representante legal o quien haga sus veces o la persona natural según corresponda, manifestando su intención de ser beneficiado de tal circunstancia, para lo cual deberá aportar la documentación soporte de acuerdo con el Artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015. La omisión de la presentación de la documentación requerida no será subsanable y por lo tanto no se dará aplicación al criterio diferencial.

NOTA 2: Teniendo en cuenta que es un factor de asignación de puntaje, la documentación que acredite tal condición, debe ser presentada con la oferta y no será susceptible de requerimiento alguno por parte del Ministerio de Defensa Nacional-COGFM-DIADF.

INCENTIVOS PARA MIPYME EN EL SISTEMA DE COMPRAS PÚBLICAS

APLICA PARA CADA UNO DE LOS LOTES.

Se otorgará el cero punto uno por ciento (0.1%) del valor total de los puntos establecidos en el Pliego de Condiciones, a la oferta presentada por una Mipyme, lo cual se verificará en los términos del artículo 2.2.1.2.4.2.4 del Decreto 1082 de 2015, en concordancia con el artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.

NOTA: Teniendo en cuenta que es un factor de asignación de puntaje, la documentación que acredite tal condición, debe ser presentada con la oferta y no será susceptible de requerimiento alguno por parte del Ministerio de Defensa Nacional-COGFM-DIADF.

FOMENTO A LA EJECUCIÓN DE CONTRATOS ESTATALES POR PARTE DE POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN Y SUJETOS DE ESPECIAL PROTECCIÓN CONSTITUCIONAL.

APLICA PARA CADA UNO DE LOS LOTES.

Esta provisión se establecerá en un porcentaje que no será superior al diez por ciento (10%) ni inferior al cinco por ciento (5%) de los bienes o servicios requeridos para la ejecución del contrato, de manera que no se ponga en riesgo su cumplimiento adecuado. Previo análisis de oportunidad y conveniencia, la Entidad Estatal incorporará esta obligación en la minuta del contrato del pliego de condiciones o documento equivalente, precisando las sanciones pecuniarias producto del incumplimiento injustificado de esta a través de las causales de multa que estime pertinentes.

NOTA: El proponente deberá manifestar con la oferta, si para ejecución del contrato destinaran para el cumplimiento del objeto contractual la provisión de bienes o servicios por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional.

PUNTAJE FINAL DE LAS PROPUESTAS.

APLICA PARA CADA UNO DE LOS LOTES.

El puntaje final de la(s) propuesta(s) será la sumatoria del puntaje técnico, más el puntaje económico, más el puntaje por ley 816 de 2003, más el puntaje por el Decreto 392 de 2018 y más, en caso de que aplique, el puntaje asignado correspondiente al artículo 3 del decreto 1860 de 2021, descritos anteriormente asignado por el comité evaluador, constituyéndose en el determinante para el orden de elegibilidad.

- LOTE 1: LICENCIAS FIREWALL + VPN.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 100 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 80 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 2: LICENCIAS PROXY WEB.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO

3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 200 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 100 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 200 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 100 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 200 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 100 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 5: SUSCRIPCIÓN WAF.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO

2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 200 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 100 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 100 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 80 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

1	DOCUMENTOS DE CONTENIDO JURÍDICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
2	DOCUMENTOS DE CONTENIDO FINANCIERO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
3	DOCUMENTOS DE CONTENIDO TÉCNICO OBJETO DE VERIFICACIÓN	HABILITADO O NO HABILITADO
4	PONDERACIÓN TÉCNICA	MÁXIMO 200 PUNTOS
5	PONDERACIÓN ECONÓMICA	MÁXIMO 300 PUNTOS
6	APLICACIÓN LEY 816/ 03	MÁXIMO 100 PUNTOS
7	SUBTOTAL PUNTAJE	Total de (4 + 5 + 6)
8	CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES (1).	0.10% DEL NUMERAL 7
9	CRITERIOS DIFERENCIALES PARA MIPYME (2).	0.10% DEL NUMERAL 7
10	SUBTOTAL PUNTAJE CRITERIOS DIFERENCIALES	Total de 8 + 9
11	REDUCCIÓN DE PUNTAJE POR INCUMPLIMIENTO DE CONTRATOS (3).	2% * (7 + 10)
TOTAL PUNTAJE		7 + 10 - 11

APLICA PARA CADA UNO DE LOS LOTES.

Nota (1): En cumplimiento de lo establecido en el artículo 3 del Decreto 1860 de 2021, el cual adicionó el artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015, el comité jurídico evaluador realizará la respectiva verificación de la información aportada por el proponente.
Nota (2): En cumplimiento de lo establecido en el artículo 3 del Decreto 1860 de 2021, el cual adicionó el artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, el comité jurídico evaluador realizará la respectiva verificación de la información aportada por el proponente.
Nota (3): En cumplimiento de lo establecido en el artículo 58 de la Ley 2195 de 2022, que impone la reducción de puntaje por incumplimiento de contratos, se reducirá durante la evaluación de las ofertas el dos por ciento (2%) del total de los puntos establecidos en el proceso a los proponentes que se les haya impuesto una o más multas o cláusulas penales durante el último año, contado a partir de la fecha prevista para la presentación de las ofertas; sin importar la cuantía y sin perjuicio de las demás consecuencias derivadas del incumplimiento, por lo que el comité jurídico evaluador realizará la respectiva verificación.

ORDEN DE ELEGIBILIDAD

APLICA PARA CADA UNO DE LOS LOTES.

Se establecerá el orden de elegibilidad de los proponentes, ordenando las propuestas según el puntaje total obtenido por las mismas, de mayor a menor y se asignará el primer puesto en el orden de elegibilidad al mayor puntaje, el segundo al siguiente, y así sucesivamente.

La valoración de las propuestas surtida conforme con lo previsto en los numerales anteriores será objeto del informe de evaluación, del cual se dará traslado a los diferentes proponentes.

FACTORES DE DESEMPATE

APLICA PARA CADA UNO DE LOS LOTES.

En caso de empate en el puntaje total de dos o más ofertas, la Entidad Estatal aplicará las reglas contenidas en el Artículo 2.2.1.2.4.2.17. Factores de desempate y acreditación, del Decreto 1082 de 2015 o las normas que las modifiquen, adicionen, sustituyan o deroguen, así:

LA OMISIÓN DE LA INFORMACIÓN REQUERIDA PARA APLICAR LOS CRITERIOS DE DESEMPATE, NO SERÁ SUBSANABLE POR SER CRITERIO DE DESEMPATE, EN TODO CASO, LA NO PRESENTACIÓN DE LA INFORMACIÓN REQUERIDA NO RESTRINGE LA PARTICIPACIÓN DEL PROPONENTE, NI ES CAUSAL DE RECHAZO DE LA PROPUESTA.

“ARTÍCULO 2.2.1.2.4.2.17. Factores de desempate y acreditación. En caso de empate en el puntaje total de dos o más ofertas en los Procesos de Contratación realizados con cargo a recursos públicos, en los Procesos de Contratación realizados por las Entidades Estatales indistintamente de su régimen de contratación, así como los celebrados por los Procesos de Contratación de los patrimonios autónomos constituidos por Entidades Estatales, el contratante deberá utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar al oferente favorecido, respetando en todo caso las obligaciones contenidas en los Acuerdos Comerciales vigentes, especialmente en materia de trato nacional.

1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros. Para acreditar este factor de desempate se tendrán en cuenta las definiciones de que trata el artículo 2.2.1.1.1.3.1., en concordancia con el artículo 2.2.1.2.4.2.9. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, que trata del puntaje para la promoción de la industria nacional en los Procesos de Contratación de servicios. Para estos efectos, incluso se aplicará el inciso tercero de la definición de Servicios Nacionales establecida en el artículo 2.2.1.1.1.3.1., citado anteriormente.

En este sentido, en los procesos en los que aplique el puntaje previsto en el inciso 1 del artículo 2 de la Ley 816 de 2003, el requisito se cumplirá en los mismos términos establecidos en los artículos indicados en el inciso anterior. Por tanto, este criterio de desempate se acreditará con los mismos documentos que se presenten para obtener dicho puntaje.

En similares términos, en los procesos en que no aplique el referido puntaje, la Entidad Estatal deberá definir en el pliego de condiciones, invitación o documento equivalente, las condiciones y los documentos con los que se acreditará el origen nacional del bien o servicio a efectos aplicar este factor, los cuales, en todo caso, deberán cumplir con los elementos de la noción de Servicio Nacional establecida en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional y observando los mismos lineamientos prescritos en el artículo 2.2.1.2.4.2.9, solo que el efecto de acreditar dichas circunstancias consistirá en beneficiarse de este criterio de desempate en lugar de obtener puntaje.

2. Preferir la propuesta de la mujer cabeza de familia. Su acreditación se realizará en los términos del parágrafo del artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008, o la norma que lo modifique, aclare, adicione o sustituya. Es decir, la condición de mujer cabeza de familia y la cesación de esta se otorgará desde el momento en que ocurra el respectivo evento y se declare ante un notario. En la declaración que se presente para acreditar la calidad de mujer cabeza de familia deberá verificarse que la misma dé cuenta del cumplimiento de los requisitos establecidos en el artículo 2 de la Ley 82 de 1993, modificado por el artículo 1 de la Ley 1232 de 2008.

Igualmente, se preferirá la propuesta de la mujer víctima de violencia intrafamiliar, la cual acreditará dicha condición de conformidad con el artículo 21 de la Ley 1257 de 2008, esto es, cuando se profiera una medida de protección expedida por la autoridad competente. En virtud del artículo 16 de la Ley 1257 de 2008, la medida de protección la debe impartir el comisario de familia del lugar donde ocurrieron los hechos y, a falta de este, del juez civil municipal o promiscuo municipal, o la autoridad indígena en los casos de violencia intrafamiliar en las comunidades de esta naturaleza.

En el caso de las personas jurídicas se preferirá a aquellas en las que participen mayoritariamente mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar, para lo cual el representante legal o el revisor fiscal, según corresponda, presentará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por mujeres cabeza de familia y/o mujeres víctimas de violencia intrafamiliar. Además, deberá acreditar la condición indicada de cada una de las mujeres que participen en la sociedad, aportando los documentos de cada una de ellas, de acuerdo con los dos incisos anteriores.

Finalmente, en el caso de los proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral.

De acuerdo con el artículo 5 de la Ley 1581 de 2012, el titular de la información de estos datos sensibles, como es el caso de las mujeres víctimas de violencia intrafamiliar, deberá autorizar de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la precitada Ley, como requisito para el otorgamiento del criterio de desempate.

3. Preferir la propuesta presentada por el proponente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad, de acuerdo con el artículo 24 de la Ley 361 de 1997, debidamente certificadas por la oficina del Ministerio del Trabajo de la respectiva zona, que hayan sido contratados con por lo menos un (1) año de anterioridad a la fecha de cierre del Proceso de Contratación o desde el momento de la constitución de la persona jurídica cuando esta es inferior a un (1) año y que manifieste adicionalmente que mantendrá dicho personal por un lapso igual al término de ejecución del contrato.

Si la oferta es presentada por un proponente plural, el integrante que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad, en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en la estructura plural y aportar como mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

El tiempo de vinculación en la planta referida de que trata este numeral se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarias de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la ley, para ello, la persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda, entregará un certificado, en el que se acredite, bajo la gravedad de juramento, las personas vinculadas en su nómina y el número de trabajadores que no son beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que cumplieron el requisito de edad de pensión. Solo se tendrá en cuenta la vinculación de aquellas personas que se encuentren en las condiciones descritas y que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del proceso. Para los casos de constitución inferior a un (1) año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de la constitución de la persona jurídica.

El tiempo de vinculación en la planta referida, de que trata el inciso anterior, se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de constitución de la persona jurídica, cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

En el caso de los proponentes plurales, su representante legal acreditará el número de trabajadores vinculados que son personas mayores no beneficiarias de la pensión de vejez, familiar o de sobrevivencia, y

que cumplieron el requisito de edad de pensión establecido en la ley, de todos los integrantes del proponente. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes.

En cualquiera de los dos supuestos anteriores, para el otorgamiento del criterio de desempate, cada uno de los trabajadores que cumpla las condiciones previstas por la ley, allegará un certificado, mediante el cual acredita, bajo la gravedad de juramento, que no es beneficiario de pensión de vejez, familiar o sobrevivencia, y cumple la edad de pensión; además, se deberá allegar el documento de identificación del trabajador que lo firma.

La mayor proporción se definirá en relación con el número total de trabajadores vinculados en la planta de personal, por lo que se preferirá al oferente que acredite un porcentaje mayor. En el caso de proponentes plurales, la mayor proporción se definirá con la sumatoria de trabajadores vinculados en la planta de personal de cada uno de sus integrantes.

5. Preferir la propuesta presentada por el oferente que acredite que por lo menos el diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana, para lo cual, la persona natural, el representante legal o el revisor fiscal, según corresponda, bajo la gravedad de juramento señalará las personas vinculadas a su nómina, y el número de identificación y nombre de las personas que pertenecen a la población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Solo se tendrá en cuenta la vinculación de aquellas personas que hayan estado vinculadas con una anterioridad igual o mayor a un (1) año contado a partir de la fecha del cierre del proceso. Para los casos de constitución inferior a un (1) año, se tendrá en cuenta a aquellos que hayan estado vinculados desde el momento de constitución de la persona jurídica.

El tiempo de vinculación en la planta referida, de que trata el inciso anterior, se acreditará con el certificado de aportes a seguridad social del último año o del tiempo de su constitución cuando su conformación es inferior a un (1) año, en el que se demuestren los pagos realizados por el empleador.

Además, deberá aportar la copia de la certificación expedida por el Ministerio del Interior, en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

En el caso de los proponentes plurales, su representante legal presentará un certificado, mediante el cual acredita que por lo menos diez por ciento (10%) del total de la nómina de sus integrantes pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitana. Este porcentaje se definirá de acuerdo con la sumatoria de la nómina de cada uno de los integrantes del proponente plural. Las personas enunciadas anteriormente podrán estar vinculadas a cualquiera de sus integrantes. En todo caso, deberá aportar la copia de la certificación expedida por el Ministerio del Interior, en la cual acredite que el trabajador pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana en los términos del Decreto Ley 2893 de 2011, o la norma que lo modifique, sustituya o complemente.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como es el caso de las personas que pertenece a la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana autoricen de manera previa y expresa el tratamiento de la información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, como requisito para el otorgamiento del criterio de desempate.

6. Preferir la propuesta de personas naturales en proceso de reintegración o reincorporación, para lo cual presentará copia de alguno de los siguientes documentos: i) la certificación en las desmovilizaciones colectivas que expida la Oficina de Alto Comisionado para la Paz, ii) el certificado que emita el Comité Operativo para la Dejación de las Armas respecto de las personas desmovilizadas en forma individual, iii) el certificado que emita la Agencia para la Reincorporación y la Normalización que acredite que la persona se encuentra en proceso de reincorporación o reintegración o iv) cualquier otro certificado que para el efecto determine la Ley. Además, se entregará copia del documento de identificación de la persona en proceso de reintegración o reincorporación.

En el caso de las personas jurídicas, el representante legal o el revisor fiscal, si están obligados a tenerlo, entregará un certificado, mediante el cual acredite bajo la gravedad de juramento que más del cincuenta por ciento (50 %) de la composición accionaria o cuotas partes de la persona jurídica está constituida por personas en proceso de reintegración o reincorporación. Además, deberá aportar alguno de los certificados del inciso anterior, junto con los documentos de identificación de cada una de las personas que está en proceso de reincorporación o reintegración.

Tratándose de proponentes plurales, se preferirá la oferta cuando todos los integrantes sean personas en proceso de reincorporación, para lo cual se entregará alguno de los certificados del inciso primero de este

numeral, y/o personas jurídicas donde más del cincuenta por ciento (50 %) de la composición accionaria o cuotas parte esté constituida por personas en proceso de reincorporación, para lo cual el representante legal, o el revisor fiscal, si está obligado a tenerlo, acreditará tal situación aportando los documentos de identificación de cada una de las personas en proceso de reincorporación.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo con el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como son las personas en proceso de reincorporación o reintegración, autoricen a la entidad de manera previa y expresa el manejo de esta información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012 como requisito para el otorgamiento de este criterio de desempate.

7. Preferir la oferta presentada por un proponente plural siempre que se cumplan las condiciones de los siguientes numerales:

7.1. Esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, para lo cual se acreditarán estas condiciones de acuerdo con lo previsto en el inciso 1 del numeral 2 y/o el inciso 1 del numeral 6 del presente artículo; o por una persona jurídica en la cual participe o participen mayoritariamente madres cabeza de familia y/o personas en proceso de reincorporación o reintegración, para lo cual el representante legal o el revisor fiscal, si están obligados a tenerlo, presentarán un certificado, mediante el cual acrediten, bajo la gravedad de juramento, que más del cincuenta por ciento (50 %) de la composición accionaria o cuota parte de la persona jurídica está constituida por madres cabeza de familia y/o personas en proceso de reincorporación o reintegración. Además, deberá acreditar la condición indicada de cada una de las personas que participen en la sociedad que sean mujeres cabeza de familia y/o personas en proceso de reincorporación o reintegración, aportando los documentos de cada uno de ellos, de acuerdo con lo previsto en este numeral. Este integrante debe tener una participación de por lo menos el veinticinco por ciento (25 %) en el proponente plural.

7.2. El integrante del proponente plural de que trata el anterior numeral debe aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

7.3. En relación con el integrante del numeral 7.1. ni la madre cabeza de familia o la persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales podrán ser empleados, socios o accionistas de otro de los integrantes del proponente plural, para lo cual el integrante del que trata el numeral 7.1. lo manifestará en un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

Debido a que para el otorgamiento de este criterio de desempate se entregan certificados que contienen datos sensibles, de acuerdo el artículo 5 de la Ley 1581 de 2012, se requiere que el titular de la información de estos, como es el caso de las personas en proceso de reincorporación y/o reintegración autoricen de manera previa y expresa el tratamiento de esta información, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, como requisito para el otorgamiento del criterio de desempate.

8. Preferir la oferta presentada por una Mipyme, lo cual se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.

Asimismo, se preferirá la oferta presentada por una cooperativa o asociaciones mutuales, para lo cual se aportará el certificado de existencia y representación legal expedido por la Cámara de Comercio o la autoridad respectiva. En el caso específico en que el empate se presente entre cooperativas o asociaciones mutuales que tengan el tamaño empresarial de grandes empresas junto con micro, pequeñas o medianas, se preferirá la oferta las cooperativas o asociaciones mutuales que cumplan con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

Tratándose de proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite alguna de las condiciones señaladas en los incisos anteriores de este numeral. En el evento en que el empate se presente entre proponentes plurales cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

9. Preferir la oferta presentada por el proponente plural constituido en su totalidad por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.

La condición de micro o pequeña empresa se verificará en los términos del artículo 2.2.1.2.4.2.4 del presente Decreto, en concordancia con el parágrafo del artículo 2.2.1.13.2.4 del Decreto 1074 de 2015.

La condición de cooperativa o asociación mutual se acreditará con el certificado de existencia y representación legal expedido por la Cámara de Comercio o la autoridad respectiva. En el evento en que el empate se presente entre proponentes plurales cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuáles al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

10. Preferir al oferente persona natural o jurídica que acredite, de acuerdo con sus estados financieros o información contable con corte al 31 de diciembre del año anterior, que por lo menos el veinticinco por ciento (25 %) del total de sus pagos fueron realizados a Mipyme, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, efectuados durante el año anterior, para lo cual el proponente persona natural y contador público; o el representante legal de la persona jurídica y revisor fiscal para las personas obligadas por ley; o del representante legal de la persona jurídica y contador público, según corresponda, entregará un certificado expedido bajo la gravedad de juramento, en el que conste que por lo menos el veinticinco por ciento (25%) del total de pagos fueron realizados a Mipyme, cooperativas o asociaciones mutuales.

Igualmente, cuando la oferta es presentada por un proponente plural se preferirá a este siempre que:

10.1. Esté conformado por al menos una Mipyme, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural, para lo cual se presentará el documento de conformación del proponente plural y, además, ese integrante acredite la condición de Mipyme, cooperativa o asociación mutual en los términos del numeral 8 del presente artículo;

10.2. La Mipyme, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25 %) de la experiencia acreditada en la oferta; y

10.3. Ni la Mipyme, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los otros integrantes del proponente plural, para lo cual el integrante respectivo lo manifestará mediante un certificado suscrito por la persona natural o el representante legal de la persona jurídica.

En el evento en que el empate se presente entre proponentes plurales, que cumplan con los requisitos de los incisos anteriores, cuyos integrantes estén conformados únicamente por cooperativas y asociaciones mutuales que tengan la calidad de grandes empresas junto con otras en las que los integrantes tengan la calidad de micro, pequeñas o medianas, se preferirá la oferta de aquellos proponentes plurales en los cuales al menos uno de sus integrantes sea una cooperativa o asociación mutual que cumpla con los criterios de clasificación empresarial definidos por el Decreto 1074 de 2015, que sean micro, pequeñas o medianas.

11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento Mipymes, para lo cual se presentará el certificado de existencia y representación legal en el que conste el cumplimiento a los requisitos del artículo 2 de la Ley 1901 de 2018, o la norma que la modifique o la sustituya. Asimismo, acreditará la condición de Mipyme en los términos del numeral 8 del presente artículo.

Tratándose de proponentes plurales, se preferirá la oferta cuando cada uno de los integrantes acredite las condiciones señaladas en el inciso anterior de este numeral.

12. Utilizar un método aleatorio para seleccionar al oferente, el cual deberá estar establecido previamente en el pliego de condiciones, invitación o documento que haga sus veces.

NOTA: EL MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL FFMM – DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, establece el siguiente factor de desempate y de selección en aplicación del criterio de desempate No. 12, en el evento en que dos o más proponentes se encuentren empatados en puntos:

- ✓ El proponente adjudicatario del proceso de selección será aquel que haya presentado la oferta primero en el tiempo entre los proponentes empatados, para lo cual se realizará la verificación en el SECOP II.

PARÁGRAFO 1. Los factores de desempate deberán aplicarse en armonía con los Acuerdos Comerciales vigentes suscritos por Colombia. De esta manera, en el evento en que el empate se presente entre ofertas cubiertas por un Acuerdo Comercial, se aplicarán los factores de desempate que sean compatibles con los mencionados Acuerdos.

Sin perjuicio de la obligación anterior, el Ministerio de Comercio, Industria y Turismo y la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente señalarán en un Manual o Guía no vinculante los lineamientos para la aplicación de los factores de desempate en cumplimiento de un Acuerdo Comercial en la etapa de selección del Proceso de Contratación.

PARÁGRAFO 2. Si el empate entre las propuestas se presenta con un proponente, bien o servicio extranjero cuyo país de origen no tiene Acuerdo Comercial con Colombia, ni trato nacional por reciprocidad o con ocasión de la normativa comunitaria, se dará aplicación a todos los criterios de desempate previstos en el presente numeral.

PARÁGRAFO 3. Conforme con el artículo 18 de la Ley 1712 de 2014 y los artículos 5 y 6 de la Ley 1581 de 2012, la Entidad Estatal garantizará el derecho a la reserva legal de toda aquella información que acredita el cumplimiento de los factores de desempate de: i) las mujeres víctimas de violencia intrafamiliar, ii) las personas en proceso de reincorporación y/o reintegración y iii) la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana.

En armonía con lo anterior, en la plataforma del SECOP no se publicará para conocimiento de terceros la información relacionada con los factores de desempate de personas en procesos de reincorporación o reintegración o mujeres víctimas de violencia intrafamiliar o la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, puesto que su público conocimiento puede afectar el derecho a la intimidad de los oferentes o de sus trabajadores o socios o accionistas.”

H. Causales de rechazo.

APLICA PARA CADA UNO DE LOS LOTES.

Sin perjuicio de lo establecido por la ley aplicable, serán rechazadas las propuestas en general cuando por su contenido, impidan la selección objetiva, especialmente en los siguientes casos:

1. Cuando la actividad de la persona natural o el objeto de la persona jurídica del oferente no esté relacionada con el objeto del presente proceso.
2. La no entrega de la garantía de seriedad junto con la propuesta. (Ley 1882/2018)
3. Cuando se compruebe que un proponente ha interferido, influenciado, u obtenida correspondencia interna, proyectos de concepto de evaluación o de respuesta a observaciones, no enviados oficialmente a los proponentes.
4. Cuando se compruebe confabulación entre los proponentes que altere la aplicación del principio de selección objetiva.
5. Cuando el proponente se encuentre incurso en las causales de inhabilidades o incompatibilidades fijadas por la constitución y la ley.
6. Cuando el proponente una vez requerido por la entidad no allegue las aclaraciones y/o explicaciones solicitadas o cuando no cumpla con lo solicitado en dicho requerimiento; o cuando allegue la respuesta a los requerimientos fuera del término establecido en la ley, impidiendo evaluar con precisión los términos de la oferta.
7. Cuando en la propuesta se encuentre información o documentos que contengan datos tergiversados, alterados o tendientes a inducir a error al Ministerio de Defensa Nacional – Comando General – Dirección Administrativa y Financiera.
8. Cuando las ofertas estén incompletas en cuanto omitan la inclusión de información o de alguno de los documentos necesarios para la comparación objetiva de las propuestas, o solicitada su aclaración, éstos no cumplan los requisitos establecidos en el pliego de condiciones, salvo cuando el evaluador pueda inferir o deducir la información necesaria para la comparación de los demás documentos que conforman la propuesta.
9. Cuando la propuesta se presente en forma subordinada al cumplimiento de cualquier condición o modalidad.
10. Cuando no presente o presente en forma incompleta, extemporánea o insuficiente las aclaraciones solicitadas dentro del término establecido por el Ministerio de Defensa Nacional – Comando General – Dirección Administrativa y Financiera.
11. Cuando el proponente no cumpla con todos y cada uno de los indicadores financieros establecidos en el presente pliego de condiciones.
12. Cuando la capacidad organizacional que se acredite para el proceso de contratación sea menor a la requerida.
13. Cuando la propuesta económica supere el presupuesto oficial de precio unitario IVA exento o excluido según aplique de cualquiera de los ítems según los precios de mercado del LOTE(s), estimados para este proceso y/o efectuada la corrección aritmética por el comité económico evaluador lo supere.

14. Cuando el proponente no cumpla con el compromiso de cumplimiento de las especificaciones técnicas exigidas en el presente proceso de selección.
15. Cuando se ofrezcan menores cantidades a las requeridas.
16. Cuando el proponente deje de ofertar al menos uno de los ítems requeridos.
17. Cuando el precio ofertado en alguno de los ítems sea igual a cero pesos ($0,00), vacío o espacio en blanco.
18. Cuando no se haya efectuado la renovación del RUP en el término establecido en el Decreto 1082 de 2015.
19. Cuando el oferente no acredite la experiencia en los códigos UNSPSC en el porcentaje de SMMLV y la cantidad de códigos requeridos.
20. Cuando una misma persona natural o jurídica, o integrante de un Proponente Plural presente o haga parte en más de una propuesta para el presente Proceso de Contratación.
21. Cuando el oferente se encuentre incurso en alguna de las causales de inhabilidad por incumplimiento reiterado establecidas en el artículo 90 de la Ley 1474 de 2011.
22. Cuando la oferta sea enviada en físico, por correo electrónico, fax o medios magnéticos. Se exceptúa lo previsto en la Guía para actuar ante una indisponibilidad del SECOP II.
23. Cuando el oferente no conteste o conteste parcialmente o no allegue las aclaraciones y/o solicitudes y/o requerimientos respecto de los precios artificialmente bajos; y/o cuando el comité económico al momento de realizar el análisis de precios evidencie precios artificialmente bajos.
24. Toda otra causa contemplada en las normas legales vigentes.

G. CRITERIOS DE ADJUDICACIÓN.

Criterio de adjudicación por LOTE.

El proceso se adjudicará de forma parcial, es decir por LOTE, al proponente que, habiendo presentado una propuesta hábil, obtenga el primer orden de elegibilidad, de acuerdo con lo establecido en el presente pliego de condiciones para el respectivo LOTE.

La adjudicación se hará de forma parcial, es decir por LOTE, de acuerdo con los precios presentados en la propuesta teniendo en cuenta el MAYOR PUNTAJE OBTENIDO, PRIMER ORDEN DE ELEGIBILIDAD, registrado entre las ofertas del respectivo LOTE. La Administración se reserva el derecho de adjudicar mayores cantidades, hasta completar el 100% del valor del CDP y de acuerdo con las necesidades establecidas por la administración, evidenciadas en el Estudio Previo, y sin sobrepasar el presupuesto disponible para cada uno de los LOTES.

XVI. SOPORTE QUE PERMITA EL ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGACIÓN.

APLICA PARA CADA UNO DE LOS LOTES.

De acuerdo con lo estipulado en el numeral 6 del Artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, se deberán prever todos los riegos involucrados en la contratación, es decir todas aquellas circunstancias que, de presentarse durante el desarrollo del proceso de contratación y ejecución del contrato, que puedan generar efectos adversos y de distinta magnitud en el logro de los objetivos del proceso.

No.	CLASE	FUENTE	ETAPA	TIPO	Descripción (Qué puede pasar y, si es posible, cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración del riesgo	Categoría	A quien se le asigna?	Tratamiento/Controles a ser implementados	Impacto después del Tratamiento				Afecta la ejecución del	Persona responsable por implementar el tratamiento / control	Fecha estimada en que se inicia el	Fecha en que se	Monitoreo y revisión	
													Probabilid	Impacto	Valoración	Categoría					Cómo	Cuando
1	ESPECIFICO	EXTERNO	SELECCIÓN	ECONÓMICO	La proyección inadecuada de los diferentes costos que se tuvieron en cuenta al momento de la presentación de su oferta, sin haber efectuado un detallado estudio de mercado, buscando afectar de manera	Desequilibrio económico del contrato	1	2	3	BAJO	Contratista	la entidad deberá realizar un estudio minucioso acerca del objeto del Contrato	1	1	2	BAJO	No	Comité económico Estructurador y Evaluador	En la etapa de selección	N/A	Verificar el estudio del mercado en cuanto a la proyección de costos se refiere.	En el momento de la selección y evaluación de las propuestas.

					intencional el equilibrio económico del contrato celebrado, correrán por cuenta y riesgo del oferente adjudicatario																	
2	ESPECIFICO	EXTERNO	SELECCIÓN	ECONÓMICO	Oferta artificialmente baja con el propósito de obtener la adjudicación del contrato.	Desequilibrio económico del contrato	2	2	4	BAJO	Contratista	La entidad requerirá al oferente para que explique las razones que sustenten el valor por él ofertado. Oídas las explicaciones, el comité evaluador recomendará al jefe de la entidad o su delegado, el rechazo o la continuidad de la oferta en el proceso, de acuerdo al artículo 28 del decreto 1510 de 2013.	1	1	2	BAJO	No	Comité Evaluador	En la etapa de selección	N/A	Comparando precios ofertados con los precios del mercado y verificando si los productos ofrecidos cumplen con las especificaciones técnicas requeridas.	En el momento de la presentación de ofertas.
3	ESPECIFICO	INTERNO	EJECUCIÓN	OPERACIONAL	Ampliación del plazo inicialmente programado por circunstancias imputables al contratista	No se cumple el objeto contractual.	3	2	5	MEDIO	Contratista	El contratista debe contar con el personal, equipo producción, planta, mano de obra calificada, y cronograma a fin de evitar retardos en la prestación del servicio	1	1	2	BAJO	SI	Gerente y Supervisor	En la ocurrencia del evento	N/A	Supervisión de la ejecución del contrato, acta de recepción del contrato a celebrar y documentación soporte, control sobre el contratista, verificación del cronograma..	Durante la ejecución del contrato.
4	ESPECIFICO	INTERNO	PLANEACIÓN - SELECCIÓN	FINANCIERO	Variación de precios por no tener en cuenta todos los impuestos, tasas y contribuciones que rigen la contratación	Desequilibrio económico del contrato	4	4	8	EXTREMO	Contratista	EL Contratista y la Entidad deberán Verificar los Estatutos, leyes y normas tributarias que rijan las condiciones existentes al momento de la presentación de la oferta	1	1	2	BAJO	SI	Comité Evaluador - Oferente	PLANEACIÓN Y SELECCIÓN	N/A	Verificación de información como lo son: Estatuto Tributario, Ley 1607 del 26 de diciembre de 2012, decreto 1794 del 21 de agosto de 2013, entre otros, que regulan las normas tributarias.	Evaluación de ofertas.
5	ESPECIFICO	EXTERNO	EJECUCIÓN	FINANCIERO	VARIACIÓN EN LA TASA DE CAMBIO POR DÓLAR (TRM) AL ALZA	Desequilibrio económico	4	4	8	EXTREMO	CONTRATISTA	Supervisión constante en la ejecución del contrato y búsqueda de cobertura cambiaria por parte del contratista	1	1	2	BAJO	SI	SUPERVISOR Y CONTRATISTA	Durante el plazo de ejecución	Durante el plazo de ejecución	Verificación permanente del comportamiento de la tasa de cambio por dólar (trm)	Permanente mente
6	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	No cumplir con los tiempos para prestar los servicios objeto del presente proceso de contratación	No se cumplen los tiempos programados en el cronograma del contrato	2	3	5	MEDIO	Contratista	Reuniones de seguimiento permanentes, para verificar el estricto cumplimiento del cronograma del contrato.	1	2	3	BAJO	SI	CONTRATISTA	Ejecución	N/A	actas de reunión, cronograma del contrato	EJECUCIÓN
7	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	Ausencia de un profesional en el evento de ser requerido.	Traumas operativos o en el desarrollo de tareas actividades ordenadas por el COGFM	2	3	5	MEDIO	Contratista y supervisor	Establecer horarios de apoyos y asesorías.	1	2	3	BAJO	SI	Contratista	En la ocurrencia del evento	N/A	Elaboración cronograma al inicio del contrato	En la etapa de ejecución
8	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	Falta de idoneidad por parte de los Profesionales.	Verificación de certificaciones y hojas de vida los profesionales en temas específicos para el desarrollo del contrato	2	4	6	ALTO	Evaluador y contratista	Incluir en el Estudio Previo, la inclusión de la documentación necesaria que evidencie la idoneidad del personal.	1	2	3	BAJO	SI	Contratista	En la ocurrencia del evento	N/A	Establecer dentro del Estudio Previo se anexe Certificados vigentes de los centros de capacitación	En la etapa de planeación
9	ESPECIFICO	INTERNO-EXTERNO	EJECUCIÓN	OPERACIONAL	La ejecución del contrato se realice en tiempos distintos a los	Generación de prorrogas y entorpecimiento de la	3	2	5	MEDIO	CONTRATIST	Supervisión constante en la ejecución del contrato	1	2	3	BAJO	SI	SUPERVISOR Y CONTRATIS	Una vez se conoce el	Desde el inicio	A través de los informes de supervisión rendidos por el	EJECUCIÓN

					programados por razones no imputables a las partes	producción de las áreas que presentan la necesidad															supervisor del contrato	
10	ESPECIFICO	INTERNO	PLANEACIÓN	OPERACIONAL	Falta de la debida representación legal	No firma del contrato	1	2	3	BAJO	OFERENTE	Los proponentes deben presentar con la oferta la debida representación jurídica	1	1	2	BAJO	SI	COMITÉ JURÍDICO EVALUADOR	Durante el termino de evaluación	Dentro del plazo de	Verificación por parte del Comité Jurídico Evaluador	EN LA ETAPA DE EVALUACIÓN
11	GENERAL	EXTERNO	EJECUCIÓN	REGLAMENTARIO	Reformas legales o reglamentarias durante la ejecución del contrato	Atención de la ejecución económica del contrato y/o retraso en el cronograma de ejecución	1	4	5	MEDIO	ENTIDAD Y CONTRATISTA	Establecer junto con el contratista el mecanismo de ajuste frente a la ocurrencia del riesgo.	1	1	2	BAJO	SI	ENTIDAD - OFERENTE	ETAPA CONTRACTUAL	N/A	Seguimiento al cambio de regulación	En la ocurrencia del hecho
12	ESPECIFICO	INTERNO	EJECUCIÓN	OPERACIONAL	Que los o servicios prestados no cumplan con las especificaciones técnicas requeridas.	No se cumple el objeto contractual	3	4	7	ALTO	Contratista	El CONTRATISTA deberá realizar el cambio de los bienes, que presenten la falla cuantas veces sea necesario hasta alcanzar su cumplimiento técnico.	1	2	3	BAJO	**SI**	Contratista	**En la ocurrencia del evento**	N/A	Supervisión de la ejecución del contrato, acta de recepción del contrato a celebrar y documentación soporte, cumplimiento de las garantías exigidas.	Durante la ejecución del contrato. Tiempo adicional para dar cumplimiento al objeto contratado
13	**ESPECIFICO**	**INTERNO**	**EJECUCIÓN**	**OPERACIONAL**	no cumplir con las garantías exigidas en el contrato	retardo en los tiempos estimados para el reemplazo o reparación de los bienes	2	3	**5**	**MEDIO**	Contratista	Seguimiento permanente a las garantías por medio de informes post contractuales, hasta la elaboración del acta de cierre.	1	2	3	**BAJO**	**SI**	CONTRATISTA	Ejecución	N/A	informes post-contractuales y acta de cierre	después de la liquidación del contrato
14	**ESPECIFICO**	**INTERNO**	**EJECUCIÓN**	**OPERACIONAL**	Riesgo humano, todo aquello que pueda provocar perjuicio a la integridad física del personal que participe en la ejecución del contrato	Accidentes durante la ejecución del contrato y/o por situaciones de fuerza mayor o caso fortuito.	3	4	7	**ALTO**	CONTRATISTA	Será responsabilidad y competencia total y absoluta del CONTRATISTA asegurar a su personal por accidentes laborales en la ejecución del contrato.	2	2	4	MEDIO	**NO**	Contratista	EJECUCIÓN	N/A	Verificación del contratista que el personal cumpla con todas las condiciones se seguridad industrial	Durante la ejecución del contrato
15	**ESPECIFICO**	**INTERNO**	**EJECUCIÓN**	**OPERACIONAL**	Riesgo por incumplimiento de las obligaciones del contrato	Cuando el contratista incumpla las obligaciones suscritas en el Contrato	2	4	**6**	**ALTO**	CONTRATISTA	Será responsabilidad total del contratista cumplir con las obligaciones a su cargo suscritas en el Contrato, con excepción de situaciones de fuerza mayor y/o caso fortuito o en todas aquellas donde el contratista demuestre que no tuvo responsabilidad.	2	2	**4**	**MEDIO**	**SI**	CONTRATISTA	Ejecución	N/A	El Contratista suscribirá la garantía amparando el cumplimiento del Contrato por cuantía del 20% del valor del Contrato, por un lapso de tiempo igual al plazo de duración del l Contrato.	En la suscripción del contrato

XVII. ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS.

Se deberá realizar un análisis de los riesgos previsibles que deben cubrir las garantías en la contratación, con el fin de determinar el Amparo y Valor a asegurar lo cual debe estar en concordancia con lo establecido en el Decreto No. 1082 de 2015; con el fin de garantizar el cumplimiento de las obligaciones surgidas con ocasión al desarrollo de los procesos contractuales en sus diferentes etapas, amparando de esta manera los perjuicios de naturaleza contractual o extracontractual, derivados del incumplimiento del ofrecimiento o del contrato según el caso, así como la pertinencia de la división de aquellas, de acuerdo con la reglamentación sobre el particular.

a. Garantía en la etapa precontractual

El proponente deberá constituir a su costa, a favor del MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL -DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, NIT: 800.230.729-9. Y presentar con su propuesta, una garantía de seriedad utilizando cualquiera de las garantías establecidas en el DECRETO 1082 de 2015 legalmente establecida en Colombia o por una Entidad Bancaria, autorizada para expedir la póliza de cumplimiento y seriedad de la oferta, **por un valor equivalente al diez por ciento (10%) del valor de la propuesta presentada EN EL RESPECTIVO LOTE**, con una vigencia de noventa (90) días calendario contados a partir de la fecha y hora de cierre del proceso de selección.

El pago de la garantía, cuando ésta se haga exigible, tiene el carácter de indemnizatoria por la no firma del contrato o por incumplimiento de la propuesta presentada por el adjudicatario y se entiende sin perjuicio del derecho que le asiste al MINISTERIO de exigir, por los medios reconocidos en Colombia, la indemnización de los perjuicios que con dicho incumplimiento se le hayan causado o se le llegaren.

CONTENIDO MÍNIMO DE LA PÓLIZA

La garantía de seriedad de la oferta deberá incluir en su texto el contenido que a continuación se requiere, en los términos y con los alcances que se indican, mediante constancias o cláusulas adicionales o complementarias a las de la póliza de seguro, de manera expresa y escrita, y cuyos alcances no podrán ser limitados por otras cláusulas, constancias o documentos privados:

La identificación del amparo de la póliza debe estar expresado en los siguientes términos:

La garantía de seriedad de la oferta cubrirá la sanción derivada del incumplimiento del ofrecimiento, en los siguientes eventos (Artículo 2.2.1.2.3.1.6. Decreto 1082 de 2015):

1. La no ampliación de la vigencia de la garantía de seriedad de la oferta cuando el plazo para la adjudicación o para suscribir el contrato es prorrogado, siempre que tal prórroga sea inferior a tres (3) meses.
2. El retiro de la oferta después de vencido el plazo fijado para la presentación de las ofertas.
3. La no suscripción del contrato sin justa causa por parte del adjudicatario.
4. La falta de otorgamiento por parte del proponente seleccionado de la garantía de cumplimiento del contrato.

En el evento en que, para el presente proceso contractual, se llegare a presentar oferta por parte de alguna Entidad Estatal, de las citadas en el artículo 2 de la Ley 80/93, ésta no estará obligada a constituir garantía de seriedad de la oferta. No obstante, en el caso en que la entidad estatal se presente en unión temporal o consorcio con una entidad de naturaleza jurídica privada, ésta deberá prestar la garantía a que se refiere el presente numeral.

Para las Uniones Temporales o consorcios, la póliza deberá ser expedida a nombre de los integrantes de la unión temporal o de los consorciados y el porcentaje de participación de cada uno.

a. Garantía en la etapa contractual:

Para la ejecución del contrato EL MINISTERIO DE DEFENSA NACIONAL – COMANDO GENERAL– DIRECCIÓN ADMINISTRATIVA Y FINANCIERA, exigirá al contratista la constitución de una póliza de garantía, de conformidad con el Decreto No. 1082 de 2015, que ampare:

APLICA PARA EL LOTE 1 Y 7.

1. CUMPLIMIENTO

Tipo de Riesgo	Garantía Exigibles
CUMPLIMIENTO DEL CONTRATO	Por el VEINTE POR CIENTO (20%) del valor total del contrato, cuya vigencia será igual al plazo de duración del contrato y de las prórrogas si las hubiere.
CALIDAD DEL SERVICIO:	Por el TREINTA POR CIENTO (30%) del valor total del contrato, la cual permanecerá vigente durante el plazo de ejecución del contrato y un (01) año más y de las prórrogas si las hubiere.
PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES.	Por el CINCO POR CIENTO (5%) del valor del contrato, con una vigencia igual a la ejecución del contrato y tres (3) años más y de las prórrogas si las hubiere.

APLICA PARA EL LOTE 2, 3, 4, 5 Y 6.

1. CUMPLIMIENTO

Tipo de Riesgo	Garantía Exigibles
CUMPLIMIENTO DEL CONTRATO	Por el VEINTE POR CIENTO (20%) del valor total del contrato, cuya vigencia será igual al plazo de duración del contrato y de las prórrogas si las hubiere.
CALIDAD DEL SERVICIO:	Por el TREINTA POR CIENTO (30%) del valor total del contrato, la cual permanecerá vigente durante el plazo de ejecución del contrato y dos (02) años más y de las prórrogas si las hubiere.
PAGO DE SALARIOS, PRESTACIONES SOCIALES LEGALES E INDEMNIZACIONES LABORALES.	Por el CINCO POR CIENTO (5%) del valor del contrato, con una vigencia igual a la ejecución del contrato y tres (3) años más y de las prórrogas si las hubiere.

NOTA: Todos los costos en que deba incurrir el oferente en el cumplimiento de su deber de garantía estarán a su cargo.

Teniendo en cuenta que la nueva versión del Sistema Electrónico de Contratación Pública (SECOP), que le permite a la administración y proveedores hacer todo el Proceso de Contratación en línea. El SECOP II funciona como una plataforma transaccional, por medio de la cual el proceso ocurre en línea y en tiempo real, para mayor información y apoyo de las herramientas ingrese al siguiente link:

https://www.colombiacompra.gov.co/secop/que-es-el-secop-ii/87anuals-y-guias-de-uso-del- SECOP-II

XVIII. INDICACIÓN DE SÍ LA CONTRATACIÓN ESTA COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE.

De conformidad con el inciso final del Decreto 1082 de 2015, en su artículo 2.2.1.1.2.1.1, indica lo siguiente:

Al revisar los parámetros contenidos en el manual explicativo emitido por Colombia Compra Eficiente *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, se evidencia lo siguiente:

PLAZOS PREVISTOS PARA ACUERDOS COMERCIALES

ACUERDO COMERCIAL	**PLAZO GENERAL**	**PLAZO CUANDO HAY PUBLICIDAD EN EL PLAN ANUAL DE ADQUISICIONES**
ALIANZA PACIFICO	30 DÍAS	10 DÍAS
CANADÁ	30 DÍAS	10 DÍAS
CHILE	10 DÍAS	10 DÍAS
COREA	30 DÍAS	10 DÍAS
COSTA RICA	30 DÍAS	10 DÍAS
ESTADOS AELC	10 DÍAS	10 DÍAS
ESTADOS UNIDOS	30 DÍAS	10 DÍAS
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE	30 DÍAS	10 DÍAS
ISRAEL	40 DÍAS	10 DÍAS
MÉXICO	40 DÍAS	25 DÍAS
TRIANGULO NORTE	NO HAY PLAZO MÍNIMO	NO HAY PLAZO MÍNIMO
CAN	NO HAY PLAZO MÍNIMO	NO HAY PLAZO MÍNIMO

- LOTE 1: LICENCIAS FIREWALL + VPN.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	SI	NO	SI
	MÉXICO	SI	SI	SI	NO	SI
	PERÚ	SI	SI	SI	NO	SI
CANADÁ		SI	SI	SI	NO	SI
CHILE		SI	SI	SI	SI. Excepción No. 18.	NO
COREA		SI	SI	SI	NO	SI
COSTA RICA		SI	SI	SI	NO	SI
ESTADOS UNIDOS		SI	SI	SI	NO	SI
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	SI	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, México, Triángulo Norte y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Corea, Costa Rica, Estados Unidos, Triángulo Norte (*con excepción de Honduras*) y CAN; y por lo tanto reciben trato nacional.

- LOTE 2: LICENCIAS PROXY WEB.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	SI	NO	SI
	MÉXICO	SI	SI	SI	NO	SI
	PERÚ	SI	SI	NO	NO	NO
CANADÁ		SI	SI	NO	NO	NO
CHILE		SI	SI	SI	SI. Excepción No. 18.	NO
COREA		SI	SI	NO	NO	NO
COSTA RICA		SI	SI	SI	NO	SI
ESTADOS UNIDOS		SI	SI	NO	NO	NO
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	NO	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Alianza Pacífico (*con excepción de Perú*), Chile, Costa Rica, Triángulo Norte y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Alianza Pacífico (*con excepción de Perú*), Costa Rica, Triángulo Norte (*con excepción de Honduras*) y CAN; y por lo tanto reciben trato nacional.

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	SI	NO	SI
	MÉXICO	SI	SI	SI	NO	SI
	PERÚ	SI	SI	SI	NO	SI
CANADÁ		SI	SI	SI	NO	SI
CHILE		SI	SI	SI	SI. Excepción No. 18.	NO
COREA		SI	SI	SI	NO	SI
COSTA RICA		SI	SI	SI	NO	SI
ESTADOS UNIDOS		SI	SI	SI	NO	SI
ESTADOS AELC *		SI	SI	SI	NO	SI
MÉXICO		SI	SI	SI	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	SI	NO	SI
ISRAEL		SI	SI	SI	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC *, México, Triángulo Norte, Unión Europea, Reino Unido e Irlanda del Norte, Israel y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Corea, Costa Rica, Estados Unidos, Estados AELC *, Triángulo Norte, Unión Europea, Reino Unido e Irlanda del Norte y CAN; y por lo tanto reciben trato nacional.

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	NO	NO	NO
	MÉXICO	SI	SI	NO	NO	NO
	PERÚ	SI	SI	NO	NO	NO
CANADÁ		SI	SI	NO	NO	NO
CHILE		SI	SI	NO	SI. Excepción No. 18.	NO
COREA		SI	SI	NO	NO	NO
COSTA RICA		SI	SI	NO	NO	NO
ESTADOS UNIDOS		SI	SI	NO	NO	NO
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	NO	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Triángulo Norte y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Triángulo Norte (*con excepción de Honduras*) y CAN; y por lo tanto reciben trato nacional.

- LOTE 5: SUSCRIPCIÓN WAF.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	SI	NO	SI
	MÉXICO	SI	SI	SI	NO	SI
	PERÚ	SI	SI	NO	NO	NO
CANADÁ		SI	SI	NO	NO	NO
CHILE		SI	SI	SI	SI. Excepción No. 18.	NO
COREA		SI	SI	NO	NO	NO
COSTA RICA		SI	SI	NO	NO	NO
ESTADOS UNIDOS		SI	SI	NO	NO	NO
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	SI	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Alianza Pacífico (*con excepción de Perú*), Chile, Triángulo Norte y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Alianza Pacífico (*con excepción de Perú*), Triángulo Norte (*con excepción de Honduras*) y CAN; y por lo tanto reciben trato nacional.

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	NO	NO	NO
	MÉXICO	SI	SI	NO	NO	NO
	PERÚ	SI	SI	NO	NO	NO
CANADÁ		SI	SI	NO	NO	NO
CHILE		SI	SI	NO	SI. Excepción No. 18.	NO
COREA		SI	SI	NO	NO	NO
COSTA RICA		SI	SI	NO	NO	NO
ESTADOS UNIDOS		SI	SI	NO	NO	NO
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	NO	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	SI, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	SI
	GUATEMALA	SI	SI		NO	SI
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: Triángulo Norte y CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: Triángulo Norte (*con excepción de Honduras*) y CAN; y por lo tanto reciben trato nacional.

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

ACUERDO COMERCIAL	PAÍS	VIGENTE	ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
ALIANZA PACIFICO	CHILE	SI	SI	NO	NO	NO
	MÉXICO	SI	SI	NO	NO	NO
	PERÚ	SI	SI	NO	NO	NO
CANADÁ		SI	SI	NO	NO	NO
CHILE		SI	SI	NO	SI. Excepción No. 18.	NO
COREA		SI	SI	NO	NO	NO
COSTA RICA		SI	SI	NO	NO	NO
ESTADOS UNIDOS		SI	SI	NO	NO	NO
ESTADOS AELC *		SI	SI	NO	NO	NO
MÉXICO		SI	SI	NO	SI. Excepción No. 18.	NO
TRIANGULO NORTE	EL SALVADOR	SI	SI	NO, Valor de la menor cuantía de la entidad estatal *(desde $142.350.000,01)*	NO	NO
	GUATEMALA	SI	SI		NO	NO
	HONDURAS	SI	NO		NO	NO
UNIÓN EUROPEA, REINO UNIDO E IRLANDA DEL NORTE		SI	SI	NO	NO	NO
ISRAEL		SI	SI	NO	SI. Excepción No. 18.	NO
CAN (Comunidad Andina)		SI	SI	SI	NO	SI

**Estados AELC incluye Islandia, Liechtenstein, Noruega y Suiza*

MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN

CONCLUSIONES:

De conformidad con lo señalado en el "*MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN*", se concluye lo siguiente:

a. Los acuerdos comerciales con los países de: Alianza Pacífico, Canadá, Chile, Corea, Costa Rica, Estados Unidos, Estados AELC, México, países de Triángulo Norte, Unión Europea, Reino Unido, Irlanda del Norte, Israel y CAN se encuentran vigentes.

b. El Comando General de las Fuerzas Militares se encuentra incluido en los listados de entidades cubiertas de los acuerdos comerciales, con excepción de Honduras en el acuerdo con el Triángulo Norte.

c. La cuantía del proceso excede los umbrales establecidos en los acuerdos comerciales publicados con los países de: CAN.

d. Aplican las siguientes excepciones:

   - Excepción No. 18 *"… Las contrataciones relacionadas con la defensa y seguridad nacional…"* con los países de: Chile, México e Israel.

e. De conformidad con lo señalado en el *"MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN"*, el presente proceso aplica para los acuerdos comerciales con los países de: CAN; y por lo tanto reciben trato nacional.

Teniendo en cuenta que la información del presente proceso se encuentra incluida en el Plan Anual de Adquisiciones y el cual se encuentra publicado desde el 31 de enero de 2025, de conformidad con lo señalado en el manual para el manejo de los acuerdos comerciales, se toma el plazo de 10 días contados a partir de la Publicación del Aviso de Convocatoria.

XIX. COMITÉS.

a. Comité técnico estructurador:

CT. JORGE ANTONIO GONZÁLEZ

Cargo: Jefe Sistemas de información
C.C.1101682890
Teléfono: 3026619050
Email: jorgegon@cgfm.mil.co

b. Comité técnico evaluador:

CT. STEVEN ALEXANDER ERIRA FIERRO
Cargo: Jefe de Área de Seguridad Informática
C.C. 1085262429
Teléfono: 3108526168
Email: steveri@cgfm.mil.co

c. Comité jurídico estructurador:

PS. JONNATAN F. PUERTO.

d. Comité económico estructurador:

PS. YOLIMA GONZALEZ SOLER.

e. Supervisor del contrato:

LOTES 1 AL 6

MY. JOSE FRANCISCO LOMBANA CARDONA
Cargo: Director Tecnologías de la Información TI
C.C. 14.395.966
Teléfono: 3165775377
Email: joselom@cgfm.mil.co

LOTE 7

TE. ALEX EDUARDO MORALES PRASCA
Cargo: Jefe de Capacidades Operacionales
C.C. 1018473469
Teléfono: 3137901773
Email: alexmo@cgfm.mil.co

f. Gerente del proyecto:

TC. RAMIRO ESTEBAN SILVA GUTIERREZ
Cargo: Director de Tecnologías de la Información
C.C. 16286812
Teléfono: 3045470642
Email: ramiro.silva@cgfm.mil.co

Firmas

TC. RAMIRO ESTEBAN SILVA GUTIERREZ
Gerente de Proyecto

CT. JORGE ANTONIO GONZÁLEZ
Comité técnico estructurador

PS. JONNATAN F. PUERTO.
Comité jurídico estructurador

PS. YOLIMA GONZALEZ SOLER.
Comité Económico Estructurador

ANEXO
ESPECIFICACIONES TÉCNICAS MÍNIMAS

- LOTE 1: LICENCIAS FIREWALL + VPN.

ÍTEM No.	DESCRIPCIÓN DEL BIEN / SERVICIO *(1)*	UNIDAD DE MEDIDA	CANTIDAD
1	Renovación y actualización del licenciamiento de la solución de seguridad perimetral del COGFM y garantía técnica por un (01) año.	UNIDAD	5
ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO			
1	RENOVACIÓN Y ACTUALIZACIÓN DEL LICENCIAMIENTO DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL DEL COGFM Y GARANTÍA TÉCNICA POR UN (01) AÑO.		

El contratista deberá proporcionar la renovación de la suscripción, el servicio de soporte, así como los servicios de upgrade, update o parches (Software Suscripción), y el servicio de garantía extendida (acompañamiento correctivo) directamente con el fabricante o casa matriz Checkpoint. Además, se incluirá la garantía técnica para todos los productos y/o herramientas que forman parte de la solución de seguridad perimetral detallada en el presente anexo, con cobertura desde la fecha de vencimiento de cada uno de los equipos hasta el 25 de diciembre de 2026.

- RENOVACIÓN DEL SERVICIO DE GARANTÍA EXTENDIDA Y SOPORTE FABRICANTE
- PROGRAMA DE SOPORTE: Direct Standard 5x9
- ACCOUNT ID: 0005692578 - 0008571570
- CPES-SS-STANDARD Direct Standard 5x9
- CPES-SS-STANDARD-ADD Direct Standard 5x9

La renovación de las licencias y la garantía de toda la solución de seguridad perimetral del Comando General de las Fuerzas Militares (COGFM) deberá tener una vigencia desde el inicio del contrato hasta el 25 de diciembre de 2026.

Product Type	Key	Product
6000 Appliances	00:1C:7F:C2:27:CB	CPAP-SG6200-PLUS-SNBT
6000 Appliances	00:1C:7F:C2:28:6B	CPAP-SG6200-PLUS-SNBT
6000 Appliances	00:1C:7F:C2:28:9D	CPAP-SG6200-PLUS-SNBT
6000 Appliances	00:1C:7F:C2:A4:99	CPAP-SG6200-PLUS-SNBT
Smart-1 Appliances	B4:96:91:F3:3B:88	CPAP-NGSM600M-BASE
Services Additional Support	0096DCF9DF00	CP-HAR-BROWSE-ADVANCED-LICENSE-EVAL
Services Additional Support	117BA3680757	CP-MTP-1Y-LICENSE
Services Additional Support	7DC27B952467	CP-SASE-PA-COMP
Attached Software Blades	DF0FD28D1372	CPSB-MOB-200
Attached Software Blades	F8EE551EF550	CPSB-MOB-200-HA
Software Products	6A6A29300AB4	CPSM-NGSM10-EVNT Y COMPLIANCE

GARANTÍA TÉCNICA Y SERVICIO

- El proveedor deberá garantizar soporte técnico con disponibilidad 7x24 para toda la solución de firewall del COGFM, desde la fecha de vencimiento de cada uno de los equipos hasta el 25 de diciembre de 2026. Este servicio deberá prestarse cada vez que el supervisor del contrato o el administrador lo requieran, durante toda la vigencia de la garantía.
- El soporte técnico para la solución de firewall del COGFM deberá ser brindado de manera inmediata, ya sea por medio telefónico o remoto, tan pronto como se presente cualquier novedad. En caso de que el incidente no se resuelva de manera definitiva dentro de las cuatro (04) horas posteriores a la notificación del mismo, se deberá enviar personal técnico especializado al sitio en un plazo máximo de dos (02) horas para garantizar la pronta solución del problema.
- El servicio de soporte técnico se podrá ofrecer a través de herramientas de servicio remoto. En caso de ser necesario, el soporte presencial se realizará en la ciudad de Bogotá las instalaciones del Complejo Militar CAN.

- El servicio de soporte brindado deberá incluir un procedimiento de escalamiento claramente definido, en caso de que sea necesario, para asegurar una pronta resolución de los incidentes.
- Se deberá ofrecer atención ilimitada a los casos reportados por el COGFM, relacionados con cualquier evento que afecte el funcionamiento, administración, incidentes o eventos de seguridad de la solución de seguridad descrita en el presente anexo, hasta garantizar que el sistema o herramienta de ciberseguridad se encuentre en pleno funcionamiento y operando con normalidad.

ALCANCE GARANTÍA TÉCNICA

GARANTÍA: El término de la garantía técnica o garantía legal, de conformidad con los artículos 7, 8, 9 y 11 de la Ley 1480 de 2011, deberá tener una vigencia desde la fecha de vencimiento de cada uno de los equipos hasta el 25 de diciembre de 2026.

- Se deberá realizar dos (02) mantenimientos preventivos a los equipos y plataforma de toda la solución de seguridad perimetral descrita en el presente anexo, durante el período de la garantía, con el objetivo de asegurar su óptimo rendimiento y prevenir posibles fallos en su funcionamiento.

Estos mantenimientos deben incluir como mínimo las siguientes actividades:

- Actualizaciones *(Upgrade, Update, criticas de Seguridad)*.
- Revisión y solución de errores.
- Realización y programación de copias de seguridad.
- Revisión logs.
- Revisión y Mejoramiento de espacio de disco, Utilización de CPU – RAM.
- Desinstalación de funcionalidades inoperativas.
- Procedimientos de hardening.
- Nuevas implementaciones.

Las ventanas de mantenimiento deberán ser programadas en horarios no hábiles, previa coordinación con el Supervisor del contrato y en función de las necesidades del COGFM, para minimizar el impacto en las operaciones y garantizar la continuidad del servicio.

- En caso de presentarse fallas en la solución de seguridad perimetral o en los equipos descritos en el presente anexo, el proveedor deberá garantizar la prestación de soporte técnico cuando sea requerido. Este servicio deberá incluir, como mínimo, las siguientes actividades:
  - Cambio de partes y/o repuestos y/o equipos nuevos, asegurando la compatibilidad con la solución existente.
  - Reemplazo de equipos por otros de iguales o superiores características, garantizando la continuidad operativa.
  - Instalación y/o reparación de software, incluyendo actualizaciones, parches de seguridad y configuraciones necesarias.
  - Configuración, puesta en producción y funcionamiento, asegurando la operatividad óptima del sistema.

- El servicio será brindado en sitio en la ciudad de Bogotá de acuerdo con los tiempos de respuesta establecidos.
- El tiempo máximo permitido para cambio de partes, repuestos o reparaciones de los equipos es de 20 días calendario a partir del reporte del incidente, en caso que la falla genere afectación de servicio el contratista deberá suministrar, instalar, configurar y poner en funcionamiento temporalmente, un equipo, repuestos o partes de iguales o superiores características técnicas, hasta tanto se dé solución definitiva a la novedad o incidente reportado, sin costo adicional para COGFM, con el fin de garantizar la continuidad en la prestación de los servicios.
- El contratista deberá suministrar, instalar, configurar y poner en perfecto funcionamiento los equipos, partes o repuestos, después de realizar el mantenimiento (cuando aplique), garantizando la continuidad de los servicios.
- En caso de que el reemplazo de partes o repuestos requiera la reinstalación o reconfiguración de software, sistema operativo o firmware, estas actividades deberán ser realizadas por el contratista sin costo adicional para el Comando General de las Fuerzas Militares (COGFM). Asimismo, el contratista deberá garantizar que, una vez realizado el cambio de repuesto, el equipo quede completamente operativo y en condiciones óptimas de funcionamiento, asegurando la compatibilidad con los sistemas existentes.
- Todos los gastos asociados al transporte de equipos, partes y cualquier otro costo necesario para la ejecución de los mantenimientos serán asumidos en su totalidad por el contratista, sin generar cargos adicionales para el Comando General de las Fuerzas Militares (COGFM).
- El contratista deberá garantizar que los materiales suministrados estarán libres de defectos de fabricación y calidad. En caso de que, durante el período de garantía, se compruebe la existencia de algún defecto, el contratista deberá realizar el reemplazo correspondiente, asumiendo todos los costos asociados, hasta la completa satisfacción del Comando General de las Fuerzas Militares (COGFM).
- Todos los repuestos y/o equipos remplazados deben tener garantía durante la ejecución del contrato

- Los equipos que sean reemplazados deben contar con todas sus conexiones físicas marcadas de acuerdo con la normativa establecida por TIA/EIA-606-B, con el propósito de simplificar su identificación.
- El contratista deberá garantizar la calidad de todos los acompañamientos prestados, asegurando que estos cumplan con los estándares técnicos y operativos requeridos para la correcta ejecución del contrato.

FUNCIONAMIENTO Y CONTINUIDAD

- El contratista deberá garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios de toda la solución de seguridad perimetral del Comando General de las Fuerzas Militares (COGFM) descrita en este anexo, a partir de la fecha de activación del producto, asegurando su operatividad sin interrupciones.
- Se deberá garantizar el funcionamiento óptimo de cada uno de los elementos de software y hardware del Sistema de Seguridad durante, como mínimo, el período de garantía técnica. En caso de fallas o mal funcionamiento, el contratista deberá reemplazar los elementos afectados sin costo adicional, asegurando la continuidad operativa del sistema.

ACTUALIZACIONES

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

REPORTES E INFORMES TÉCNICOS

- Una vez realizados los acompañamientos (remotos o en sitio), se deberá hacer entrega o enviar dentro de los cinco (05) días siguientes, un reporte técnico donde se indique las actividades realizadas, observaciones y pendientes, el informe técnico como mínimo debe indicar:
  - Actividades realizadas.
  - Actualizaciones aplicadas.
  - Procedimientos preventivos y/o correctivos aplicados.
  - Recomendaciones.
  - Pendientes.

SEGURIDAD

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

OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO

- El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.
- El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
- Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
- El contratista deberá disponer de una bolsa de 50 horas de soporte técnico especializado para nuevas implementaciones para toda la solución de seguridad perimetral del COGFM, las cuales podrán utilizarse de manera remota o, según la criticidad del caso, de forma presencial en las instalaciones del Complejo Militar CAN, en la ciudad de Bogotá, previa coordinación con el supervisor del contrato.

CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma de actividades para la ejecución del objeto del futuro contrato, previa aprobación del supervisor del contrato.

- LOTE 2: LICENCIAS PROXY WEB.

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

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

- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado son el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.

ALCANCE GARANTÍA TÉCNICA

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

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

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

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

FUNCIONAMIENTO Y CONTINUIDAD

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

SEGURIDAD

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

OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO

- El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.
- El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
- Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.

CRONOGRAMA

Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma de actividades para la ejecución del objeto del futuro contrato, previa aprobación del supervisor del contrato.

- LOTE 3: SUSCRIPCIÓN DE PROTECCIÓN DE DATOS.

ÍTEM Nro.	DESCRIPCIÓN DEL BIEN O SERVICIO	UNIDAD DE MEDIDA	CANTIDAD
1	SUSCRIPCIÓN PLATAFORMA PROTECCIÓN DE DATOS		
1.1	SUSCRIPCIÓN DE ENDPOINT DETECTION & RESPONSE EDR	UNIDAD	1
1.2	SUSCRIPCIÓN DE CACERÍA DE AMENAZAS ADMINISTRADA	UNIDAD	1
1.3	SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES	UNIDAD	1
1.4	SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES	UNIDAD	1
1.5	SUSCRIPCIÓN DE PROTECCIÓN DE DATOS	UNIDAD	1
1.6	SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS	UNIDAD	1
1.7	SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA	UNIDAD	1
ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO			
1.2	**LICENCIAMIENTO**		
1.2.1	El proveedor debe brindar la suscripción de toda la solución, este deberá ser un modelo por suscripción por un periodo de 24 meses a partir del 02 de noviembre del 2025 para todos los módulos; debe ser entregado al Comando General de las Fuerzas Militares-COGFM de acuerdo con los siguientes productos: ítem / Descripción 1 – SUSCRIPCIÓN DE ENDPOINT DETECTION AND RESPONSE (EDR) 2 – SUSCRIPCIÓN CACERÍA DE AMENAZAS ADMINISTRADA 3 – SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES 4 – SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES 5 – SUSCRIPCIÓN DE PROTECCIÓN DE DATOS 6 – SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS 7 – SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA		
1.2.2	Se requiere que la solución sea cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, contenedores de nube, dispositivos OT inclusive si estos se encuentran distribuidos de forma remota. No se aceptan soluciones que involucren hardware o virtualización. La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía. En caso de que se requieran módulos o funcionalidades adicionales deberían activarse sobre la misma plataforma con el mismo sensor.		
1.2.3	El proveedor deberá rendir un informe en donde certifique la funcionabilidad de la plataforma, la activación de las suscripciones licencias con sus respectivos soportes; así mismo entregará los certificados de las licencias al Departamento Conjunto de Comunicaciones del COGFM.		
1.3	**GENERALIDADES DE LA PLATAFORMA:**		
1.3.1	La solución integral debe ser soportada sobre una plataforma en la cual se garanticen las siguientes generalidades:		
1.3.2	La solución debe contar con las siguientes condiciones generales para su operación y correcto desempeño: - Consola única central 100% nube (cloud) para administración y operación de todos los módulos ofrecidos y futuros. - Sensores/software que serán instalados en estaciones de trabajo, servidores, máquinas virtuales, contenedores o dispositivos OT. - La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola por grupos de direcciones IP.		
1.3.3	En caso de requerir activación de funcionalidades adicionales no debe requerir nuevos despliegues de producto, ni de sensores o agentes en la infraestructura.		

1.3.4	Se requiere que se despliegue un sensor/agente único para realizar todas las funcionalidades solicitadas con las siguientes condiciones como mínimo: - Sensor que NO requiera ser reiniciado en su instalación como desinstalación. - El proceso de despliegue del sensor debe ser compatible y tener documentado el uso de plataformas de terceros como (SystemCenter / AWS automatic Deployment / GPO / PowerShell / PDQ) entre otros. - El consumo de recursos del agente debe ser en promedio 1% de CPU, teniendo activas todas las capacidades de detección, prevención y riesgo. No debe tener requerimientos de hardware específicos para su funcionamiento. - El sensor a desplegar en ambientes de OT de ser necesario deber ser el mismo que se utiliza en el ámbito OT. - El sensor a desplegar debe convivir con cualquier otra solución de EPP existente en el ambiente sin causar ninguna incompatibilidad ni lentitud en el dispositivo. - El despliegue del sensor no debe requerir desinstalar las soluciones de EPP existentes en el ambiente y no debe crearse ninguna exclusión para su operación de detección de amenazas.
1.3.5	- Los sensores a desplegar NO deben requerir actualizaciones de patrones/firmas/comportamientos de forma completa o parcial. - La solución debe estar basada en AI/ML (Inteligencia Artificial / Machine Learning), No se aceptan combinaciones de modelo de firmas/herística u otros mecanismos no especificados.
1.3.6	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional. - La plataforma debe contar con un "Market Place" para poder realizar las integraciones con terceros mediante API y ver el estado de la integración. También disponer de la posibilidad de realizar la prueba o test de nuevos módulos sin necesidad de nuevos despliegues o autorizaciones de terceros.
1.3.7	- La plataforma debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API.
1.3.8	- La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días consulta en segundos.
1.3.9	- La consola de gestión debe incluir capacidades de analítica mediante motores de AI, incluir para todos los módulos capacidades de SOAR que no implique un licenciamiento independiente y que no se limite su uso en la creación de playbooks de automatización.
1.3.10	- La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, auto triage notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros.
1.3.11	- La plataforma debe permitir la definición de roles personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que deben ingresar a la consola como permitir el acceso mediante MFA e integración con SSO.
1.3.12	- La plataforma debe estar administrada por una única consola en un ambiente jerárquico basado en padres e hijos. En caso de que la entidad requiera, puede dividirse o ser parte de un sistema de CSIRT/SOC para poder ser gestionada de forma colaborativa delegada. Sin que esto impacte la operación y administración de la plataforma.
1.3.13	- La plataforma debe contar con un portal de ayuda, webinar y base de conocimiento integrado a la consola para poder ampliar los conocimientos sobre los módulos o webinar para poder aplicar buenas prácticas en el desarrollo de la solución. Como también hacer el escalamiento de casos en caso de requerirse con el fabricante en modalidad 7x24. NO se aceptan plataformas o soluciones que tengan múltiples interfaces o múltiples consolas.
1.3.14	- La consola debe incorporar un mecanismo de autodepuración para eliminar los dispositivos que no se gestionan en un periodo mayor a 45 días calendario o definir una política de retención para poder hacer procesos de autodepuración más acelerados.
1.3.15	- El licenciamiento de la plataforma se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados.
1.3.16	- Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes. Estos tokens deben ser de un único uso y deben ser generados de forma aleatoria para que solo los usuarios con el perfil asociado puedan hacer uso de este token de desinstalación.
1.3.17	- La plataforma debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un arbol de procesos de forma: Gráfica, listado de actividades y líneas de tiempo.

1.3.18	- La plataforma debe poder establecer control o comunicación directa por medio de línea de comandos con los sensores (win/linx/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros, estos accesos directos a los dispositivos se deben validar mediante un acceso de Multi factor conocido como MFA.		
2	**REQUISITOS ESPECÍFICOS DE LOS MÓDULOS**		
2.1	**SUSCRIPCIÓN DE ENDPOINT DETECTION & RESPONSE EDR, QUE INCLUYE:** - **Antivirus de nueva generación y EDR** - **Antimalware** - **Firewall Management** - **Control de dispositivos**	**(Número de endpoints)**	**1400**
2.1.1	- Uso de la inteligencia de amenazas basado en la identificación de como los adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques, como también sus asociaciones, IOCs y vulnerabilidades objetivo, detecciones asociadas en los EDR.		
2.1.2	Capacidades de detección y prevención de: - Detección y prevención de virus/malware conocido y desconocido o día cero. - Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades. - Detección y prevención por indicadores de ataque (File-less attacks). - Capacidad de independizar la detección de la prevención por políticas. - Identificación y prevención de actividades sospechosas (procesos, registro, script, comandos, drivers). - Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usado por los ataques de Ransomware basado en comportamiento. - Identificación y prevención de movimientos laterales y Accesos a credenciales. - Identificación y prevención de ataques y explotación de vulnerabilidades día cero.		
2.1.3	Capacidades de detección de TTPs en post ejecución como: - Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP). - Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos.		
2.1.4	La plataforma debe tener capacidad de desarrollar actividades forenses como: - Contar con un acceso remoto (vía línea de comandos) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual. - Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos. Contar con comandos de colección de datos que permitan dar paso a investigaciones. Los comandos requeridos son: - Explorar el sistema de archivos y extraer archivos. - Lista de procesos en ejecución. - Extraer el registro de eventos de Windows. - Consultar registro de Windows. - Enumere las conexiones de red actuales y la configuración de la red. - Extraer la memoria de un proceso (memory dump). Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son: - Eliminar un archivo. - Terminar un proceso (Kill process). - Eliminar o modificar la clave o el valor del registro de Windows. - Enviar scripts programados. - Enviar y recibir archivos por demanda.		
2.1.5	- La solución deberá contar con la capacidad de aislar una activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación externa a la computadora con excepción a la comunicación con la propia consola de gestión de la solución.		
2.1.6	- La solución debe hacer un mapeo de alertas basado en el modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).		

2.1.7	- La solución deber tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, estado de la conexión a la consola, tags predefinidos, roles de los dispositivos, esto basado en la meta data de los dispositivos registrados como mínimo. - La organización en grupos de forma automática o manual basado en reglas o filtros de acuerdo a los atributos de los dispositivos.
2.1.8	- La plataforma debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como Virus total vía API.
2.1.9	La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales. La solución debe contar como mínimo los siguientes elementos de análisis y características: - Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control. - Capacidad de protección aun cuando los equipos no cuenten con conectividad a la nube. - Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente. - Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS. - Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos. - Detección y prevención de explotaciones de tipo Force DEP (Data Execution Prevention), Heap Spray preallocation, Force ASLR (Address space layout randomization), SEH (Structured Exception Handling Ovewrite protection), NULL Page Allocation, Remote library Loading, Untrusted font. Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente: - Cadenas ejecutadas dinámicamente vía el cmdlet “invoke-expression”. - Comandos vía –EncodedCommand. - Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware. - Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware. - Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware. - Detección y prevención de movimientos laterales. - Detección y prevención de intentos de robo de credenciales. - Detección y prevención de intentos de elevación de privilegios. - Detección y prevención de intentos de uso de “sticky keys”. - Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés). - Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe
2.1.10	- El módulo de EDR debe tener una cuarentena de archivos el cual debe integrar un análisis de sandboxing automático sin límite de uso. Esto es cuando un archivo llegue a cuarentena se tenga un reporte de sanboxing con el análisis comportamental.
2.1.11	- Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura, como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas Windows y MAC.
2.1.12	- Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento.
2.1.13	- Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.
2.1.14	- Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.
2.1.15	- Debe tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.
2.1.16	- Se deben contar con dashboards para poder ver la actividad de dispositivos externos como: Audio/video, Imaging, Mass Storge, Mobiles (MTP/PTP), impresoras, Wireless (Bluetooth), Any Class.

2.1.17	- Debe permitir configurar de forma personalizada la notificación que le aparece a los usuarios cuando se realizar alguna restricción en el acceso.		
2.1.18	- Capacidad de tomar el control del Firewall nativo de estaciones para sistemas Windows y MAC para la restricción o permisos de puertos, IPs y procesos.		
2.1.19	- Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de red, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.		
2.1.20	- Deberá utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall.		
2.1.21	- Debe tener la capacidad de poder identificar el tipo de conexión para poder hacer bloqueos de tráfico hacia redes wifi, por ejemplo, y con ello poder restringir de forma granular el acceso dependiendo de la política de la entidad.		
2.1.22	Las reglas de Firewall deben poder definir la localización del dispositivo con ello aplicar políticas de forma contextual, para identificar la ubicación se debe hacer con la definición de: - Tipo de conexión & SSID, IP Gateway, Servidor DHCP, Prueba de resolución DNS, Prueba de certificado Https, Prueba de ping, dirección IP.		
2.2	**SUSCRIPCIÓN DE CACERÍA DE AMENAZAS ADMINISTRADA que debe incluir:** - **Analítica de telemetría de comportamiento con IA - Inteligencia Artificial** - **Servicio de cacería de amenazas administrada por parte del fabricante 7x24**	**(Numero de endpoints)**	**1400**
2.2.1	- Sistema de detección y respuesta de puntos finales, identidad y nube con monitoreo continuo para poder tener visibilidad de actividad anómala, respuesta y desarrollo de actividad forense para evitar potenciales brechas o compromiso en las operaciones. Se deben integrar un sistema de analítica y correlación para realizar análisis retrospectivos.		
2.2.2	- Que permita acceso instantáneo al "quién, qué, cuándo, dónde y cómo" de un ataque.		
2.2.3	- Que la solución EDR permita detectar incidentes automáticamente sin requerir ningún ajuste o configuración antes de estar en pleno funcionamiento.		
2.2.4	- Que tenga la posibilidad de realizar búsquedas personalizadas sobre las detecciones que se remontan a 90 días para buscar amenazas de manera proactiva y que los resultados de las consultas se devuelvan en cinco segundos o menos.		
2.2.5	- Que brinde protección contra fallas silenciosas (que se producen cuando un ataque se desliza a través de las soluciones de seguridad sin que se active ninguna alarma) y que registre todas las actividades de interés de un equipo tanto en tiempo real como después del hecho.		
2.2.6	La plataforma debe permitir realizar investigaciones forenses en tiempo real y retrospectivos basado en (Para estos casos con menús dedicados para): - Host (actividad de procesos, actividad sospechosa, actividad de red, entre otros). - Usuarios (terminar donde ha registrado un usuario, que servicios accede, como y de que tipo fue el registro). - Hash (Búsquedas de ejecuciones de Hash, creaciones, modificaciones). - Direcciones IP. - Grupos de dominios. - Búsquedas por el identificador de sensor. - Búsquedas por contexto de procesos. - Contar con un buscador de consultas para identificar (dispositivos con riesgo, con detecciones críticas, con vulnerabilidades materializables entre otros). - Realizar cacería de amenazas en sensores windows, mac, linux, directorio activo y contenedores. - Realizar una evaluación de Mitre mediante mapas de calor, tácticas en el tiempo. - Líneas de comando y actividad ASEP(Aggregate System Entry Point). - Ejecutables que se ejecutan desde la papelera o carpetas temporales. - Actividad de logon, actividad de powershell, actividad de tareas registradas.		
2.2.7	- Debe realizar un diagnóstico de "Zero Trust Assessment (ZTA)" para determinar el estado del equipo en la organización. Es decir que evalué el nivel de seguridad en cuanto parámetros de seguridad del sistema operativo y políticas de seguridad de prevención.		
2.2.8	- Que permita desarrollar reglas o indicadores que identifican y previenen ataques sin archivos que aprovechan los malos comportamientos y que con el tiempo ajuste y amplíe los indicadores integrados.		

2.2.9	- Debe permitir la creación de Indicadores de Ataque por sus siglas IOA, incluso permita crear reglas de IOA personalizadas en la plataforma, Como bloqueos de procesos, archivos, dominios o IPs dependiendo ejecuciones de comandos archivos o procesos antecesores.
2.2.10	- Para la creación de las reglas personalizadas deberá especificar el "tipo de regla" y seleccionar acciones como: operaciones de creación de procesos, creación de archivos, conexión de red y nombre de dominio.
2.2.11	- Para las detecciones de dichas reglas de IOA, tenga la capacidad de buscar las detecciones provocadas por una regla específica.
2.2.12	Tener la capacidad de realizar búsquedas proactivas (hunting) para eventos de cambios registrados por la telemetría de la plataforma, en un rango o periodo de tiempo específico ejemplos: - Realizar búsquedas de nuevos servicios o tareas programados a alrededor de un proceso de investigación. - Realizar búsquedas de cambios en llaves de registros, accesos remotos, logins alrededor de un proceso, equipo, IP o dominio específico.
2.2.13	- Visualización de incidentes calificados por la plataforma que correlacione las detecciones y actividades asociadas a los incidentes, asignando el indicador de riesgo del impacto del incidente.
2.2.14	- La plataforma debe mostrar en forma gráfica el incidente relacionando los dispositivos impactados, procesos y línea de tiempo en la que ocurren los eventos relacionados tanto bloqueados como observados que tiene relación con el incidente.
2.2.15	- La solución debe permitir consultar información de telemetría relacionados con un proceso, tarea o comportamiento para ampliar el proceso de investigación y consulta con un alcance de 7 días historicos.
2.2.16	- La plataforma debe incluir servicios de fábrica para actividades de threat hunting y MDR para tener búsquedas/investigaciones proactivas sobre detecciones y anomalías en el entorno del cliente.
2.2.17	- La solución debe realizar el envío de la telemetría en tiempo real y consultada inclusive aun si los dispositivos están fuera de línea esto por un periodo de al menos 7 días.
2.2.18	La información de telemetría debe ser colectada 7x24 y esta no debe ser mayor a 40MB por día por dispositivo, la información a tomar debe incluir como mínimo +1100 tipos de eventos entre ellos: - Process - Token info events, Creations, Injections, Grandparent, Parent, Child relationships. - Network - Close, Connect, Listen, Receive/Accept for IP4/IP6. - File - Writes, deleted, rename, open and info. - Registry - ASEP. Updates, Dumps, Impersonation. - User - Logon, Logoff, Failed attempts. - DLL - Injection and reflection attempts. - Detalle de los dispositivos incluido, pero no limitado a: - OS - OU Attributes, Hostname, Device type, OS Version, Manufacturer, Model. - Network - MAC, Local and External IP, Neighbors.
2.2.19	- La solución debe permite la configuración de consultas personalizadas utilizando un lenguaje de consulta estándar y documentado, estas consultas pueden ser personalizadas y programadas para poder ser utilizadas como reportes vía correo electrónico.
2.2.20	- Deberá ofrecer un servicio administrado de cacería de amenazas capaz de detectar intrusiones, actividades maliciosas y adversarios, realizado directamente por el fabricante por medio de un equipo capacitado y certificado sin necesidad de realizar ningún tipo de VPN o instalación de plataforma de terceros para obtener la información. Este servicio se debe prestar en modalidad 7x24x365.
2.2.21	Como parte del servicio deberá buscar de manera proactiva campañas de malware sigilosas y en caso de existir alguna se notificar según corresponda. El proceso de notificación debe ser vía correo electrónico por medio de la misma consola de gestión y administración de los anteriores módulos presentar: - Reportes de cacería. - Librerías para cacería de amenazas. - Investigaciones documentadas. - Espacio para poder someter muestras para análisis.
2.2.22	- El servicio deberá ir más allá de la detección pasiva y automatizada, deberá investigar e incluso responder a indicadores que apunten a ataques. Alertar con recomendaciones de remediación, con un análisis detallado que permita determinar ¿qué sucedió? y ¿cómo? responder al incidente.

2.2.23	- Deberá contar con investigaciones retroactivas revisando datos históricos en busca de evidencia de una intrusión. Recopilar artefactos de investigación como direcciones IP, dominios, hashes y otros. Estos artefactos deberán ser cargados a una base de inteligencia propietaria del fabricante y generar alertas en la interfaz de usuario de la plataforma de seguridad ofertada.		
2.2.24	- El proceso de investigación debe contar con un playbook de investigación y análisis para poder clasificar las detecciones como mínimo: Falso positivo, verdadero positivo, indeterminado, sospechoso.		
2.2.25	- Se debe tener en la consola de gestión de EDR un dashboard que muestre el número de investigaciones realizadas por el equipo de cacería de amenazas.		
2.2.26	- Contar en el portal de gestión con una librería de cacería de amenazas, como: tips para hacer consultas, TTPs para ataques cloud, Exfiltración de datos, cacería de DLLs, credenciales no seguras, explotación Web, herramientas de acceso remoto, movimientos laterales en windows.		
2.3	**SUSCRIPCIÓN DE DETECCIÓN Y PREVENCIÓN DE AMENAZAS EN LAS IDENTIDADES, que debe incluir:** **- Diagnóstico continuo de riesgos del AD e Intra ID** **- Detección y prevención de ataques y anomalías de identidad con el uso de Inteligencia Artificial**	**(Número de usuarios endpoints)**	**1400**
2.3.1	- El sistema debe inspeccionar profundamente los protocolos de autenticación (NTLM, Kerberos, LDAP, etc.) para ayudar a controlar el uso inseguro de protocolos y reducir el riesgo de amenazas de seguridad, incluido el reenvío de credenciales y el análisis de hash de contraseñas con bases de datos de passowords expuestos, así como la detección de ataques como Kerberoasting, Pass-the-Hash y Golden Ticket.		
2.3.2	- El sistema debe unificar la visibilidad de las cuentas y las identidades en la nube (EntraID), remota (VPN) y local (Directorio activo local).		
2.3.3	- El sistema debe proporcionar una calificación del nivel de riesgo de detecciones, anomalías y auditoria del AD indicando niveles (alta, media, baja).		
2.3.4	- El sistema debe perfilar el comportamiento de cada usuario y dispositivo en la red, incluidos los usuarios privilegiados y las cuentas de servicio y desarrollar una puntuación de riesgo para cada uno de ellos.		
2.3.5	- El sistema debe descubrir todos los usuarios conectados al directorio activo, detectar y responder a las amenazas relacionadas con la identidad en tiempo real.		
2.3.6	- El sistema debe ser capaz de descubrir continuamente todas las categorías de usuarios, incluidos los privilegiados, las cuentas de servicio, los usuarios regulares y las cuentas obsoletas.		
2.3.7	- El sistema debe rastrear y hacer cumplir la política basada en la identidad del usuario para servidores y aplicaciones confidenciales. Debería descubrir, monitorear y administrar automáticamente las cuentas privilegiadas en la red.		
2.3.8	- La plataforma debe permitir la definición de segmentos como VPNs, Contratistas, redes de servidores, DMZ para que con este contexto se pueda aumentar la visibilidad del tráfico de red que se debe monitorear para hacer la detección de amenazas y determinar su acción para protección, contención o solicitud de verificación de identidad.		
2.3.9	- La plataforma debe mapear el proceso de "Kill Chain Attack & Defense" de Active Directory para proteger el entorno del AD.		
2.3.10	- El sistema debe reducir la superficie de ataque mediante la identificación de administradores sigilosos, cuentas de servicio mal utilizadas y comportamiento anómalo de los usuarios.		
2.3.11	- La plataforma debe incluir informes completos sobre riesgo y cumplimiento con ayudas gráficas.		
2.3.12	- La plataforma debe utilizar ciencia de datos "Data Science" para la investigación de seguridad interna y para cuantificar el riesgo. Como también debe utilizar información basada en hechos (es decir, niveles de privilegio, alertas de seguridad o inteligencia de amenazas para generar una puntuación de riesgo.		
2.3.13	- La plataforma sebe usar el mismo sensor de EDR para las capacidades de detección y análisis sobre la identidad del directorio activo (En los controladores de dominio).		
2.3.14	- La plataforma debe responder proactivamente a las amenazas en tiempo real según las políticas preestablecidas sin interrumpir a los usuarios válidos. Debe evitar u orquestar aprobaciones cuando terceros, como proveedores, contratistas o socios, acceden a servidores confidenciales con el entorno del cliente, mediante integraciones con sistemas MFA.		
2.3.15	- La plataforma debe tener la capacidad de forzar cambios de contraseña para sus usuarios, basado en el nivel de seguridad de las credenciales (como credenciales comprometidas, credenciales con bajos niveles de seguridad, credenciales sin rotación).		

2.3.16	- La plataforma debe integrarse a una plataforma de protección EDR y gestión de vulnerabilidades nativa de forma que se pueda correlacionar amenazas desde la perspectiva de Endpoint, vulnerabilidades y la protección de la identidad usando una consola única.		
2.3.17	- La plataforma debe tener la capacidad de tomar medidas de prevención en función de los umbrales de puntuación de riesgo.		
2.3.18	- La plataforma debe entregar capacidades para definir políticas granulares sobre estado de seguridad de las entidades, tráfico de red de autenticación, estado de seguridad de los dispositivos, roles de las cuentas, orígenes, destino de las conexiones, protocolos, ubicaciones geográficas, riesgos, dispositivos que no se usan normalmente, entre los mínimos.		
2.3.19	- El sistema debe informar sobre el estado de las contraseñas para todas las cuentas de usuario, identificará a los administradores ocultos, las cuentas obsoletas y otros problemas que tradicionalmente son difíciles de encontrar.		
2.3.20	- la plataforma debe permitir realizar un desglose o "drill down" bajo demanda desde una búsqueda personalizada que coincida con una o más características de la sesión.		
2.3.21	- La plataforma debe correlacionar y analizar automáticamente los eventos de seguridad, dentro del contexto de la sesión de un usuario.		
2.3.22	- La plataforma debe almacenar información de telemetría de usuario para ser consultada sobre detalles tanto para auditoría como para cacería de amenazas usando un lenguaje para consulta de metadata y telemetría.		
2.3.23	- La plataforma debe proporcionar capacidades de análisis privilegiado (calcular puntajes de riesgo para cuentas y usuarios privilegiados a través de análisis de comportamiento y correlación de actividad privilegiada con información de vulnerabilidad).		
2.3.24	- La plataforma debe tener la capacidad de utilizar el aprendizaje automático (Machine Learning) no supervisado para crear y mantener modelos de datos de usuarios, grupos de pares de la organización y comportamiento de los activos utilizando funciones en datos de eventos históricos recopilados durante un período definido por el usuario.		
2.3.24	El módulo de detección prevención de ataques de identidad debe: - Detectar contraseñas codificadas utilizadas por aplicaciones que estén en las GPO. - Detectar la creación y eliminación de cuentas de usuario en un período de tiempo. - Admitir esquemas del AD de varios bosques/dominios. - Permitir agregar empleados ejecutivos, de alto privilegio o en riesgo en listas de seguimiento, como también la posibilidad de agregar password conocidos. - Tener la capacidad de crear flujos de trabajo para automatizar respuestas. - Detectar un cambio de credencial anómalo para un usuario. - Detectar una cantidad anómala de activos a los que se accede dentro de una sesión. - Detectar actividades de inicio de sesión de cuentas revocadas. - Detectar el inicio de sesión del usuario desde múltiples ubicaciones geográficas. - Detectar inicios de sesión exitosos desde cuentas no correlacionadas. - Detectar el inicio de sesión desde una ubicación geográfica rara. - Detectar la actividad de administración de DC (creación/eliminación de cuentas) usando VPN. - Detectar la conexión VPN por parte de un no usuario (cuenta de servicio). - Detectar la conexión VPN por cuenta deshabilitada. - Realizar un seguimiento de las actividades de los usuarios en sesiones desde el inicio hasta el cierre de sesión. - Identificar a los usuarios que realizan cambios de credenciales. - Identificar automáticamente cuentas de servicio mediante aprendizaje automático ML. - Detectar la conexión VPN por cuenta de servicio. - Detectar cuentas humanas que se comportan como cuentas de servicio. - Detectar anomalías de acceso por cuentas de servicio. - Detectar el inicio de sesión interactivo por parte de cuentas que no son de usuario (no correlacionadas). - Detectar el inicio de sesión de un usuario no ejecutivo en un activo ejecutivo.		
2.4	**SUSCRIPCIÓN DE HIGIENE DE TI Y GESTIÓN DE VULNERABILIDADES que debe incluir:** - **Descubrimiento de activos en la red con y sin sensor** - **Inventario de aplicaciones instaladas y usadas** - **Listado de accesos exitosos y fallidos a los dispositivos** - **Gestión de vulnerabilidades**	**(Numero de endpoints)**	**1400**
2.4.1	- Módulo que deberá proporcionar la visibilidad el todo el entorno de tecnología de la organización, desde la consola central supervisar todo desde un panel de control para explorar aplicaciones, accesos y activos utilizando datos históricos y en tiempo real que tengan o no tengan el sensor instalado.		

2.4.2	- La herramienta deberá ofrecer inventario de aplicaciones instaladas y usadas, listados de extensiones usadas en los navegadores, las versiones que se están ejecutando para identificar aplicaciones sospechosas o no autorizadas. Adicionalmente deben brindar una clasificación y categorización de fábrica.
2.4.3	- Se deberán definir grupos de aplicaciones para poder clasificar las aplicaciones como también se podrán crear IOCs para autorizar o bloquear aplicaciones basadas en hash mediante workflows de manera automática.
2.4.4	- La herramienta deberá tener la capacidad de identificar todos los dispositivos en la red, incluso si están protegidos o no por la plataforma. Se deben tener 3 clasificaciones (Dispositivo gestionados, dispositivos no gestionados y candidatos a instalar el sensor, dispositivos no soportados entre ellos (impresoras, Routers, dispositivos OT)).
2.4.5	- Sobre los dispositivos administrados se debe obtener información de estado de salud como uso de CPU, Memoria, espacio libre de disco, entre otros.
2.4.6	- La herramienta deberá tener la capacidad de monitorear los logins de todos los usuarios activos en la red, con privilegios de administrador, locales o de dominio, historial de inicio de sesión e información de actualización de contraseña.
2.4.7	- Cómo parte de la plataforma unificada, la plataforma de higiene de TI deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint.
2.4.8	- La herramienta deberá proporcionar información contextual para todos los sistemas, utilizando cuadros de mando, gráficos y funciones de búsqueda para profundizar en los datos de apoyo. Los resultados deberán correlacionarse con los dispositivos que están en línea, fuera de línea o no conectados a la red corporativa.
2.4.9	- La herramienta de higiene de TI, deberá utilizar la información de la solución de detección y respuesta de endpoints (EDR) para alimentar los datos de búsqueda.
2.4.10	- La herramienta deberá tener la capacidad de minimizar el abuso de cuentas privilegiadas monitoreando el uso y creación de credenciales de administrador.
2.4.11	- Las búsquedas de inventario deberán realizarse en la nube para no tener ningún impacto en el rendimiento de los equipos o en la red.
2.4.12	- Solución de administración de vulnerabilidades automática sin escaneos y siempre activa con datos en tiempo real. Donde se pueda realizar análisis de impacto basado en la determinación de si se dispone de exploits o inclusive si se tienen exploits activos en la organización.
2.4.13	- La herramienta deberá ofrecer la gestión unificada de amenazas y vulnerabilidades, como parte de una plataforma integral para prevenir vulnerabilidades y la actividad posterior a la explotación de las mismas.
2.4.14	- La herramienta deberá permitir investigar vulnerabilidades y exposiciones comunes (CVE) para examinar los objetivos y perfiles de los actores de amenazas.
2.4.15	- La herramienta no deberá realizar escaneos para su funcionamiento, lo cual permita la administración de vulnerabilidades automatizada y siempre activa con datos en tiempo real.
2.4.16	- Cómo parte de la plataforma unificada, la plataforma de gestión de vulnerabilidades deberá utilizar el mismo agente ligero que el resto de la plataforma de seguridad de endpoint EDR.
2.4.17	- La herramienta deberá permitir supervisar continuamente el estado de vulnerabilidad de todos los equipos dondequiera que residan: en las instalaciones, fuera de las instalaciones o en la nube.
2.4.18	- No debe requerir dispositivos de hardware ni infraestructura adicionales para su funcionamiento.
2.4.19	- La herramienta deberá monitorear todos los equipos a través de un sensor ya sea dentro o fuera de la red, en la nube, en equipos físicos y virtuales.
2.4.20	- Debe permitir que los datos estén disponibles a través de un dashboard intuitivo y búsqueda en tiempo real.
2.4.21	- Deberá proporcionar el contexto de las amenazas para ver tanto la presencia de una vulnerabilidad como la evidencia de intentos de explotación.
2.4.22	- Deberá permitir operar instantáneamente tan pronto como sea instalado, monitoreando e identificando las vulnerabilidades sin necesidad de reiniciar o realizar una configuración compleja.
2.4.23	- Desarrollar por medio del SOC el programa de gestión de vulnerabilidades a lo largo de todo el ciclo de vida, desde el aspecto fundamental del descubrimiento de activos, pasando por la evaluación y priorización de vulnerabilidades y exposiciones, hasta la corrección eficaz.

2.5	**SUSCRIPCIÓN DE PROTECCIÓN DE DATOS que debe incluir:** - **Clasificación de información en tiempo real** - **Detección y prevención de salida de información sensible** - **Analítica y correlación de eventos con el uso de Inteligencia Artificial**	**(Numero de endpoints)**	**1400**
2.5.1	- Se debe proveer funciones de protección de datos para evitar su fuga utilizando el mismo sensor de EDR, con la misma consola de gestión y sin requerir hacer un nuevo despliegue para activar esta funcionalidad.		
2.5.2	- El módulo de protección de datos debe identificar información sensible por medio de patrones de contenido, expresiones regulares o etiquetas de Microsoft y Google.		
2.5.3	- El módulo debe poder identificar y mostrar los flujos de información por volumen de datos o por número de eventos que coinciden con políticas de protección de datos. Esto de forma gráfica para los vectores de salida tanto web como Dispositivos de almacenamiento USB y uso del copiar en el portapapeles.		
2.5.4	- Los eventos de salida de información deben indicar el archivo que se detecta en la salida, vector de salida, política, usuario donde se debe llevar al perfil de usuario mediante la protección de identidad, el dispositivo donde se debe llevar a la descripción y detalles del dispositivo.		
2.5.5	- Las políticas se deben asignar a los dispositivos, se debe hacer la asignación varios tipos de clasificaciones, debe tener la posibilidad de hacer identificación por porcentaje de similaridad, bloquear el uso de browsers en caso de tener coincidencia con datos sensibles salientes, personalizar las notificaciones de alertamiento a los usuarios.		
2.5.6	- Las políticas podrán ser configuradas en modo simulación para realizar entrenamiento de reglas antes de activar la prevención.		
2.5.7	- Se podrán crear patrones de contenido por medio de expresiones regulares, como también indicar la cantidad de veces que puede repetirse una coincidencia.		
2.5.8	- Se podrá crear grupos de aplicaciones web para poder ser granular en las políticas de protección de datos.		
2.5.9	- La solución debe tener la capacidad para inspeccionar nuevos formatos de archivos cifrados y detectar intentos de exfiltrar archivos cifrados.		
2.5.10	- Las reglas de protección de información deben tener la opción de creación de detecciones indicando el tipo de criticidad y este debe ser procesado y analizado por Inteligencia artificial para poder generar detecciones de anomalías por volumetría y estado de criticidad.		
2.5.11	- Las reglas de protección de datos deben tener la opción de almacenar la evidencia de los archivos que coinciden con los patrones de detección de salida de datos, definiendo la cantidad de espacio para evidencias en cada uno de los dispositivos y el porcentaje mínimo de ocupación del disco duro.		
2.5.12	- La solución de protección de datos debe tener un panel de control para poder ver los flujos de datos, esto es: origen de la información, medio de salida y canal de salida, indicando por colores las acciones tomadas en volumen de eventos o tamaño de datos.		
2.5.13	- Por medio de políticas se podrá definir que dispositivos se activa la protección de datos, con esto logrando ser selectivos en dispositivos que no lo requieran.		
2.6	**SUSCRIPCIÓN INTELIGENCIA DE AMENAZAS que debe incluir:** - **Indicadores de compromisos en tiempo real IOCs,** - **Análisis de Sandboxing automático** - **Perfiles de grupos o actores de ataques y campañas de ciberseguridad**	**(Numero de endpoints)**	**1400**
2.6.1	- Protección de dispositivos, protección de Identidad y protección de nube al siguiente nivel que combine sandboxing de malware, la búsqueda de malware y la inteligencia de amenazas en una solución integral. Además, que tenga la capacidad de producir un indicador de Compromiso (por sus siglas IOC) tanto para la amenaza que encontró como para todas sus variantes conocidas.		
2.6.2	- Inteligencia de amenazas tipo TIP (Threat inteligence Platform) que permita la consulta e inyección de IOCs (Indicadores de compromiso) vía API manual o automáticamente. Con actualización en tiempo real.		
2.6.3	- Debe tener Sandbox en nube, capacidad de enviar muestras para análisis por demanda o automáticamente desde los endpoints para complementar el análisis de muestras desconocidas, al menos 100 muestras mensuales por demanda.		
2.6.4	- Tener disponible una base de datos de archivos de malware al menos los últimos 5 años para poder hacer consulta y descarga de muestras de malware para estudio e ingeniería inversa por parte del equipo de la organización.		

2.6.5	- La plataforma debe entregar reportes de inteligencia al menos semanales programados sobre amenazas, campañas y ataques más reconocidos para preparación y conocimiento centralizado en la consola de administración.		
2.6.6	- Se debe contar con un panel que permita consultar inteligencia de Vulnerabilidades para brindar información sobre nuevas vulnerabilidades con una descripción de su impacto en la plataforma y vinculación a campañas de adversarios en ciberseguridad.		
2.6.7	- Se deben contar con una sección de servicios para poder tener: resúmenes, violaciones, eventos, fuentes de datos, temas y consultas, integraciones API e interfaces, despliegues, dependencias, librerías, Modelos o Frameworks, datos recolectados.		
2.6.8	- El módulo de inteligencia debe contar con el listado de actores o grupos para ser analizados de forma continua en la cual se pueda definir IOCs, vulnerabilidades, TTPs de mitre de forma gráfica.		
2.7	**SUSCRIPCIÓN DE SISTEMA DE DETECCIÓN Y PREVENCIÓN EXTENDIDA**	**UNIDAD**	**01**
2.7.1	El módulo debe incluir como mínimo las siguientes funcionalidades: - Analítica y correlación automática de EDR, ITDR, Data Protection, inteligencia de manera integrada XDR - Sistema de SOAR nativo integrado - Analítica de ciberseguridad BOT de Inteligencia Artificial Capacidad por día de 75GB de ingesta adicional a la que ya se cuenta por identidad y el EDR y tiempo de retención de 3 meses (90 dias). En la misma plataforma de administración de EDR/protección identidad/ gestión de riesgo, XDR se debe tener la capacidad de ingestión de cualquier tipo de dato/logs sin limitación en el uso de conectores OnPremise o conectores cloud para desarrollar las capacidades de SIEM de nueva generación desarrollando a profundidad las siguientes características en una sola plataforma y en una única consola: - Monitoreo y gestión de Incidentes basado en los diferentes vectores usando AI/ML sin configuración de reglas. - Configuración de reglas de correlación personalizadas clasificando los resultados en detecciones y tipificando de acuerdo al modelo de MITRE Attack (Enterprise o Mobile). - Gestión de eventos para hacer consultas avanzadas, dashbboards mediante operaciones condiciones para poder fortalecer los procesos de cacería de amenazas. - Ingesta de datos por medio de conectores que puedan personalizarse o tenerse configurados para poder parametrizar cualquier fuente de información. - Ingesta de datos con capacidad de respuesta orquestada para los vectores de: EDR / Cloud / Identidad / correo / Navegación Web /Red y/o Firewall con el objetivo de mitigar el impacto de incidentes de seguridad. - Se requiere que se puedan crear flujos de trabajo o "playbooks" de respuesta en un SOAR nativo para poder automatizar acciones. - Integrar una plataforma de inteligencia de amenazas "TIP" (Threat Intelligence Platform) Nativa para enriquecer y tener el contexto de amenazas cibernéticas en las investigaciones, detecciones y correlaciones.		
2.7.2	- La plataforma de SIEM debe tener la capacidad de activar capacidades nativas de detección y respuesta que no requieran configuración para su integración, pero se requiere que se tengan una o más de las siguientes funcionalidades nativas: EDR / ITDR - Identitity Detection & Response del mismo fabricante que ofrece el SIEM.		
2.7.3	La plataforma de SIEM debe tener la capacidad de poder integrar de manera nativa las siguientes capacidades, de acuerdo a la solicitud del presente proyecto: - Inteligencia de amenazas reconocida como lider en el mercado (TIP - Threat Intelligence Platform). - Administración de logs sin usar bases de datos estándares ni bases de datos indexadas, para retención de datos de 3 meses. - Investigación en profundidad basado en telemetría, comportamientos o funciones lógicas como funciones de inteligencia Artificial. - Módulo de reportería personalizada con detalles avanzados para tener filtros gráficos (Mapas de calor, ubicación geográfica, pipes, tendencias, barras, tablas,) que se actualicen en tiempo real en segundos y puedan exportarse en documentos pdf. - Incorporar parámetros para realizar una gestión de incidentes (Delegación de casos, seguimientos, escalamientos, documentación específica de cada situación, triage) - Correlación avanzada y personalizada. - Capacidad de desarrollar casos de uso de cumplimiento mediante personalización de correlación e ingesta de datos personalizados.		

	- Entregar capacidades para realizar cacería de amenazas para extrapolar procesos, tareas, dependencias a partir de artefactos o actividades de comportamiento sobre todo el ambiente. - Basado en lago de Datos flexible y de crecimiento adaptable. - Capacidades de UBEA - User Behavior & Entity Analytics por medio de la protección de identidad solicitado anteriormente. - Conectores y capacidades XDR - Extended Detection and response. - Capacidades de SOAR para orquestación y automatización.
2.7.4	- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bi-Direccional.
2.7.5	- La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL via puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.
2.7.6	- La plataforma de SIEM debe tener la capacidad de crear gráficos de tendencia o de observación de datos que pueda visualizarse en: Tablas, pipes, columnas, mapas de calor, mapas de ubicación geográfica, "sandkey", para poder tener el análisis gráfico los cuales se deben actualizar en tiempo real. También en los gráficos se debe tener opción de hacer consultas y filtros para poder hacer profundización en los eventos.
2.7.7	- Los gráficos deben exportarse en formato PDF, pueden exportarse para poder convertirse en un formulario o clonarse o eliminarse.
2.7.8	La plataforma debe permitir la creación de tableros de control que permita: - Realizar seguimiento a tendencias, búsquedas de IOCs. - Seguimiento a las operaciones de seguridad para determinar: Tiempos promedio de detección, tiempos promedio de diagnóstico, tiempos promedio de cierre de incidentes. - Tableros de control de mapas de calor con las TTPs de Mitre para determinar frecuencias, impactos sobre la organización.
2.7.9	- La plataforma debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, para la automatización de actividades de respuesta como: Aislamiento automático de dispositivos, enriquecimiento de inteligencia, "autotriage", notificaciones personalizadas, plugins con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks, lanzar scripts de forma remota, entre otros.
2.7.10	El módulo de SOAR debe ser parte de la plataforma en la misma consola de SIEM integrada de manera nativa, debe contar con un tablero de gestión para ver las ejecuciones de playbooks de los últimos 30 días que muestre: - Cantidad de ejecuciones de playbooks provenientes de alertas, detecciones o incidentes. - Cantidad de ejecuciones que provengan de aprobaciones de usuarios. - Tendencia de ejecuciones de playbooks completas y fallidas. - Top de ejecuciones por tipo de disparo o iniciación de los playbooks. - Listado de la ejecuciones más recientes y listado de ejecuciones que corren por demanda.
2.7.11	- El módulo de SOAR debe contar con una biblioteca de playbooks para poder incorporar sin necesidad de construirlos de cero estos, como también debe tener la opción de importar playbook de objetos .yaml provenientes de comunidades y colaboración del ecosistema.
2.7.12	El módulo de SOAR debe permitir la creación de playbooks como mínimo: - A partir de un evento, alerta, detección, incidente, estado de un dispositivo, detección de una instalación de aplicación, cambios de políticas o auditoria de sistema, estado de seguridad de los dispositivos o de la nube, un evento de identidad como mínimo. - A partir de una tarea programada la cual puede ejecutarse de forma recurrente definiendo una fecha, hora, día, mes. - Por demanda, donde un administrador puede iniciar para poder automatizar una tarea. En este caso se puede crear un esquema de variables para poder personalizar las consultas al sistema.
2.7.13	- El módulo de SOAR debe contar con información de la ejecución de cada playbook para entender que actividades desarrolló, comprender los procesos de decisión y poder determinar errores para mejorar en el diseño y respuesta de los mismos. Como también deben contar con un módulo de auditoria para determinar quién o cuando se cambió, modificó, Guardando las versiones de cambio y permitiendo volver a versiones anteriores de playbooks.
2.7.14	La plataforma debe contar con capacidades de establecer conversaciones en lenguaje natural mediante motor de Inteligencia artificial para: - Hacer consultas para buscar información en la plataforma (ej: listados de dispositivos con características específicas, búsquedas de aplicaciones de riesgo, vulnerabilidades, consultas de IOCs, que permiten reducir el tiempo de investigación de los analistas). - Consultar sobre ejecuciones de scripts y explicación en lenguaje natural sobre significados de códigos. - Consultas para poder solicitar las consultas a realizar para acelerar la cacería de amenazas. - Consultas para solicitar apoyo en la creación de flujos de automatización.

	Esta funcionalidad debe estar disponible para poder ser agregada como apoyo a los consultores de SOC, CSIRT o encargados de analizar o investigar incidentes de seguridad.
2.7.15	- El módulo de SOAR debe tener la capacidad de tomar medidas de corrección inmediatas desde el gráfico/ árbol de procesos de incidentes activando un flujo de trabajo SOAR por demanda esto puede ser: Aislamiento de dispositivos, bloqueo de autenticación de usuarios, deshabilitación de usuarios, envío de artefactos al sandboxing, captura de datos de análisis forense, entre otros los cuales pueden ser personalizados o creados de acuerdo a las necesidades.
2.7.16	- La plataforma debe contar con un BOT que tenga el rol de analista de ciberseguridad que apoye los equipos de investigación, cacería de amenazas y administradores de seguridad para poder acelerar las actividades de su día a día. - El BOT debe simplificar el proceso de determinar riesgos y actividad maliciosa en el entorno y reducir la necesidad de revisar y filtrar manualmente grandes cantidades de datos. Puede generar avisos o registros de avisos para determinar rápidamente qué adversarios se han detectado en la organización o han atacado a otras organizaciones del sector, encontrar endpoints afectados por vulnerabilidades de alto riesgo y mucho más.
2.7.17	- La interacción con el BOT debe ser por medio del establecimiento de conversaciones introduciendo una consulta en la barra de conversaciones o ejecutando un libro de indicaciones (conjunto de preguntas), la plataforma debe mantener el contexto de varias preguntas para llegar a la respuesta. la información consultada debe corresponder únicamente a los datos alojados por la plataforma y sus módulos activos únicamente.
2.7.18	- Las respuestas se deben generar en el orden en que las solicitudes se encuentran en la cola. El formato y la cantidad de información de una respuesta pueden variar según la solicitud. De acuerdo a las consultas deben incluir en su mayoría tablas de resultados y un resumen general que los describe, con un concepto de seguridad y análisis. Según los datos de la tabla, puede copiar los datos JSON generados o descargar un CSV, si está disponible. Siempre utilizando lenguaje natural.
2.7.19	El analista BOT debe tener integraciones con el sistema para tener un uso adicional para: - Crear y correr consultas (queries) sobre los datos y datos crudos recopilados sobre la plataforma. - Analizar líneas de comando ejecutados en las cargas de trabajo sin límite de uso: Esto es decodificar, desofuscar y explicar el propósito de una línea de comando o script que se capture en una detección de EDR (ej. Comandos vía powershell). - Crear diagnósticos de detecciones indicando un Score de evaluación de impacto vía AI, explicando porque puede ser potencialmente peligroso y teniendo un concepto para acelerar el proceso de diagnóstico de detecciones, esto por medio del uso de lenguaje natural.
2.7.20	La capacidad de que el analista BOT haga el diagnóstico de detecciones (triage) debe presentar un tablero de control que muestre en un rango de tiempo desde 1 hora, un día, una semana, 30 días, o 90 días: - Cantidad total de diagnósticos y diagnóstico en el tiempo. - Tiempo promedio que toma hacer los diagnósticos. - Tiempo ahorrado en esta actividad. - Detecciones más recientes. - Cantidad de veredictos realizados: Verdaderos positivos, Falsos positivos o sin veredicto.
2.7.21	- El consumo de este servicio de BOT debe basar en el número de consultas ejecutadas por mes con el objetivo de tener una consulta de su consumo, teniendo en cuenta que si se realiza una consulta que se ha realizado en los últimos 30 días la plataforma no debe considerarlo una nueva consulta ejecutada.
3	**SERVICIO DE SOPORTE Y GARANTÍA TÉCNICA**
3.1	**SOPORTE DE FÁBRICA**
3.1.1	**SOPORTE DEL FABRICANTE:** El fabricante debe brindar un soporte en horario de 24x7 (Las 24 horas del día, los 7 días a la semana) desde la firma del contrato, por una vigencia de 24 meses. - Acceso al portal de soporte (base de conocimiento, Escalamiento de Tickets). - 7x24x365 soporte telefónico. - Priorización de Caso. - Asignación de un TAM (especialista de producto) para revisión y evaluación periódica. - Healthcheck de la solución de forma trimestral. - Reportes trimestrales. - Gestión de casos proactivos. - Acompañamiento en nuevas funcionalidades y actualizaciones. - Acompañamiento en el Kick Off del proyecto.

3.1.2	**SOPORTE DEL PROVEEDOR:**
	- El proveedor debe brindar un soporte en horario de 24x7 (24 horas del día, los 7 días de la semana) remoto o presencial según lo solicite la entidad a partir de la firma del contrato, o cada vez que el supervisor lo requiera, por una vigencia de 24 meses.
	- El proveedor debe brindar un soporte presencial dos días a la semana en horario de 8x2 (8 horas del día, 2 días de la semana) presencial, a partir de la firma del contrato, por una vigencia de 24 meses, los días se programarán previa coordinación con el supervisor del contrato.
	- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario.
	- El proponente debe garantizar que las actividades propias de soporte no afecten la continuidad de la operación y funcionamiento de los equipos o herramientas que requieran intervención.
	- Las ventanas de mantenimiento, actualizaciones, deben ser programados en horarios no hábiles, previas coordinaciones con el Supervisor del contrato y de acuerdo con las necesidades del COGFM.
	- El proponente debe contar con una mesa de ayuda para atención de incidentes disponible para el COGFM 7x24 durante la vigencia del contrato, esta mesa debe contar con una herramienta de atención de incidentes que cumpla con mínimo 14 procesos de ITIL certificados; esta mesa será la encargada de gestionar todos los incidentes y requerimientos reportados durante la vigencia del contrato.
	- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket de servicio para los incidentes presentados).
	- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado son el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.
	
	- **Tiempos de respuesta**: El servicio de soporte debe ser atendido de manera inmediata de acuerdo a lo solicitado por el supervisor del contrato.
	  - Tiempo máximo de respuesta dos (02) horas después de haber reportado el incidente.
	  - De ser necesario el proveedor deberá enviar personal técnico especializado a sitio en un tiempo máximo de cuatro (04) horas.
	  - El tiempo máximo permitido para restablecer el servicio es de 4 horas.
	
	- **Tipo De Atención:**
	  - Soporte Nivel 1: De manera presencial dos días a la semana con duración de 8 horas laborales (2x8) en las instalaciones del Comando General de las Fuerzas Militares Centro Administrativo Nacional CAN edificio Fortaleza Carrera 54 # 26-25 en la ciudad de Bogotá, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato.
	
	  - Soporte Nivel 2: Cuando se requiera por medio telefónico o de manera remota a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de ejecución del contrato, y de acuerdo con los términos y tiempos de respuesta especificados.

4	**OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO**
4.1	**GARANTÍA DE SOPORTE**
4.1.1	- El Contratista deberá garantizar el normal funcionamiento después de la implementación y puesta en marcha de la solución, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. - Soporte disponible los 365 días del año en horario 7x24 (7 días a la semana las 24 horas del día). - El servicio de soporte debe ser atendido de manera inmediata a través de una línea telefónica gratuita, servicio de correo electrónico o en forma remota de acuerdo a los niveles de servicio. En un lapso de cuatro (04) horas después de haber reportado el incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas.
4.1.2	El proponente debe integrar a su propuesta los siguientes servicios: - Servicio por parte del fabricante para poder hacer al menos 02 workshops durante el despliegue de la plataforma (Taller de buenas prácticas de despliegue y análisis de detecciones para una correcta comprensión). - Servicio de asignación de un TAM - Tecnical account manager por parte del fabricante para que realice una evaluación continua de la configuración de la plataforma y apoyo en la gestión de casos de soporte cuando se hace el escalamiento con fábrica. - Se debe tener acceso a entrenamientos en línea por parte del fabricante sin límite para los funcionarios de la entidad durante la vigencia del contrato.

4.2	**TRASFERENCIA DE CONOCIMIENTO**
4.2.1	- El Contratista debe realizar transferencia de conocimiento para el personal que administra la solución, de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares, dictado directamente por el canal implementador en las instalaciones adecuadas por mínimo 40 horas. Se debe expedir certificado por parte de fábrica. - Debe incluir material técnico, en la ciudad de Bogotá en Idioma español; se debe ofrecer una metodología teórica y práctica con laboratorios de cómputo debidamente configurados, en instalaciones dispuestas por el contratista que incluya equipos de cómputo, material impreso, digital, de software y hardware. - El contratista debe disponer de aulas completamente dotadas que cubran todos los aspectos logísticos para la ejecución de los entrenamientos requeridos, igualmente proveer instructores idóneos, calificados y certificados, con experiencia en la ejecución de capacitación. - El Contratista deberá entregar el material de clases necesario para desarrollar el entrenamiento de acuerdo a cada uno de los módulos. Así mismo, se deberán entregar las presentaciones utilizadas por los instructores. - El Contratista deberá emitir un certificado a cada uno de los estudiantes que aprueben la transferencia tecnológica. **<u>LA CAPACITACIÓN DEBERÁ ESTAR ENFOCADA EN:</u>** - Configurar la solución la solución adquirir. - Crear políticas para la protección dentro de la organización. - Gestión de hosts. - Respuesta de incidentes. - Caza de Amenazas. - Despliegue del Agente. - Protección de datos. - Detención y respuesta EDR-XDR. - Antivirus y Antimalware. - El objetivo de esta transferencia de conocimiento es capacitar al personal de la Dirección de Tecnologías de la Información del Comando General de las Fuerzas Militares para que puedan gestionar, instalar, configurar y analizar los productos adquiridos de manera efectiva y adecuada. El certificado emitido por el fabricante y/o distribuidor autorizado servirá como evidencia de la participación y aprobación de la capacitación por parte de los funcionarios.
4.3	**CONFIDENCIALIDAD DE LA INFORMACIÓN**
4.3.1	- El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción **"acuerdo de confidencialidad".** - La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización. - A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento. - Por lo anterior es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así

	como la que genere, como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros. - El contratista y los recursos humanos que formarán parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, **el acuerdo de confidencialidad** donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.
4.4	**CRONOGRAMA**
4.4.1	Dentro de los primeros cinco (05) días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma para la ejecución del objeto del futuro contrato, para aprobación del supervisor del contrato, que incluya el proceso y actividades de: - Planeación (requerimientos y preparación) - Despliegue (Posibles esquemas de despliegue de sensores, como puede acelerar el proceso), proceso de implementación para minimizar la fricción o interrupciones con la plataforma actual. - Post-Implementación (se debe indicar como es el proceso de escalamiento de nuevos requerimientos, atención de solicitudes de soporte - portales/teléfono/equipo encargado, apoyo en la revisión del estado de la plataforma como informar las nuevas funcionalidades que son importantes incorporar, durante la ejecución del contrato).
5	**Servicio de ingeniera soporte e implementación y puesta en funcionamiento de la solución de acuerdo a documento de especificaciones técnicas.**
5.1	**<u>Implementación del Proyecto</u>** - El contratista junto con el supervisor del contrato debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar con la seguridad perimetral. - El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones. - Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Comando General de las Fuerzas Militares. - El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Comando General que sean necesarias para el óptimo funcionamiento de todas las tecnologías. - El contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de la solución a adquirir con sus correspondientes integraciones, con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Comando General de las Fuerzas Militares. - Las soluciones a implementar deben ser compatibles con las plataformas actuales del Comando General y cumplir con el protocolo IPv4 e IPV6. - Toda la actividad de implementación se debe realizar en producción sin afectar los servicios del centro de cómputo previa coordinación con el supervisor del contrato. De ser necesario un apagado programado, este debe ser coordinado con el supervisor del contrato. **<u>Caso de Fallas:</u>** - Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. - En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo: ✓ Implementación de software. ✓ Configuraciones, puesta en producción y funcionamiento.

Integración:

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

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

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

Herramienta o software de implementación y despliegue masivo de agentes:

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

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

- La herramienta de despliegue debe tener la capacidad de personalizar tareas y paquetes para poder lanzar tareas en paralelo sin afectar despliegues anteriores.
- La herramienta de despliegue debe permitir un seguimiento detallado del proceso de despliegue indicando errores en el proceso para poder remediar de forma adecuada.

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

. El Comando General de las Fuerzas Militares no asumirá ninguna responsabilidad contractual ni laboral con los funcionarios que la empresa oferente asigne para el cumplimiento del contrato.

- LOTE 4: SUSCRIPCIÓN FILTRADO DE CORREOS ELECTRÓNICOS (ANTISPAM).

ÍTEM No.	DESCRIPCIÓN DEL BIEN / SERVICIO	UNIDAD DE MEDIDA	CANTIDAD
1	SUSCRIPCIÓN FILTRADO Y PROTECCIÓN DE CORREO ELECTRÓNICO (ANTISPAM).	UNIDAD	1600
ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO			
REQUERIMIENTOS GENERALES Y ARQUITECTURA			
La vigencia de las licencias y de la garantía deberá ser de dos (2) años contado a partir del 31 de octubre de 2025 o fecha que indique la plataforma o documento de fabricante.			
La solución debe deberá proporcionar un servicio para 1600 usuarios o buzones.			
La solución suministrada debe ser a través un servicio SaaS.			
La disponibilidad del servicio SaaS debe ser de al menos 99.9% o superior.			
La solución debe usar protocolos de cifrados modernos para salvaguardar la organización.			
La solución debe ser escalable y nativa de nube para soportar crecimiento a cientos de miles de usuarios			
La solución debe proteger de Ciber Amenazas para de correo electrónico en la nube Office 365 y/ Google Workspace.			
La solución debe soportar proteger de Ciber Amenazas, en las siguientes aplicaciones SaaS de Colaboración y Almacenamiento de archivos: o Microsoft Teams o Microsoft OneDrive o Microsoft SharePoint o Google Drive o Dropbox			
La solución debe proveer protección contra los siguientes Ciber ataques: • Prevención ataques a Correo electrónico (Phishing, Spoofing, Spam) • Prevención de Malware (en correo, herramientas de colaboración y almacenamiento) • Prevención de Malware de día Cero con Sandboxing (en correo, herramientas de colaboración) y Limpieza de Documentos con tecnología CDR (content disarm and reconstruction) • Anomalías de usuarios e inicios de sesión anómalos (Indicios de robo de cuenta). • Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT. • Prevención de Fuga de Datos (DLP) en correo, herramientas de colaboración			
La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado.			
La solución deberá poder ser administrada vía HTTPS y debe ser compatible con los navegadores Chrome, Firefox y Edge.			
La solución debe ser fácil y rápida de usar, con configuraciones de políticas listas para usar.			
CARACTERÍSTICAS DEL PRODUCTO			
La solución debe bloquear sofisticados ataques de ingeniería social, como la suplantación de identidad, spam, phishing de día cero y Business Email Compromise (BEC) usando motores de machine learning (ML), Deep Learning y de Inteligencia Artificial (IA)			
La solución debe proteger los correos electrónicos de entrada, salientes y proteger la comunicación interna en tiempo real para ataques laterales y amenazas internas.			
La solución debe proveer prevención en línea (no solo detección y/o remediación), es decir intercepción de correo antes que lleguen al usuario final.			
La solución debe permitir el despliegue automático por integración nativa de API sin requerir cambios en los registros MX de DNS para prevenir ataques por correo.			
La integración por API debe ser automática y sencilla de gestionar, debe permitir reglas granulares por usuarios y/o grupos que pueden estar en prevención y/o remediación y no requerir de configuraciones manuales del lado del servicio de correos (Microsoft 365 o Google).			
La solución debe ser invisible para los atacantes y debe aplicar seguridad en profundidad siendo una capa de seguridad como última línea de defensa y no desactivar la seguridad nativa de las soluciones de Correo de Nube de office 365 y/o Google Workplace.			
La solución debe contar con un periodo de aprendizaje que realice un escaneo de metadatos de correo electrónico (remitente, destinatario, asunto, hora) en los buzones de correo de los usuarios para determinar los patrones de comunicación y ajustar los motores de IA.			

La solución debe tener soporte multilingüe para el análisis del contenido de los mensajes de correo electrónico utilizando Inteligencia Artificial, incluyendo al menos 100 idiomas que incluyan el español.
La solución debe inspeccionar los metadatos, archivos adjuntos, enlaces e idioma de la comunicación, dominios, OCR, QR codes, así como todas comunicaciones históricas, para determinar relaciones de confianza previas entre el emisor y el receptor del correo para de identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.
La solución debe etiquetar los correos electrónicos dependiendo del tipo de amenaza identificada, como mínimo: • Extorsión • Suplantación • Estafa Financiera • Ingeniería Social, • Facturas falsas • Robo de credenciales
La solución debe analizar cada correo electrónico como un todo y no de manera individual, permitiendo establecer al menos los siguientes puntos: 1. A nivel de contexto del correo analizado: • ¿Este remitente ha escrito antes a la organización? • ¿Algunos de los usuarios internos han estado en contacto previo con esta dirección o dominio? • ¿Relación entre la dirección externa o dominio externo y la organización? • ¿Qué tan común es para estos destinatarios de la organización recibir el mismo correo? • ¿Ha sido mencionado este remitente por los usuarios internos en algún correo previo? • La dirección del remitente se parece a alguna dirección interna o externa conocida (dirección/dominio)? 2. A nivel de Contenido del correo analizado: • ¿La estructura del link es sospechosa? • ¿Los enlaces contenidos en el correo son similares a los correos de Phishing? • ¿El enlace se encuentra ofuscado a través de algún método conocido? • ¿El enlace está diseñado para redirigir al destinatario a un dominio diferente del sugerido por enlace original? • ¿El adjunto contiene contenido potencialmente malicioso como enlaces o macros? • ¿Hay signos de intento de extorción en el cuerpo de este correo? • ¿El lenguaje del correo sugiere que es un correo típico de Phishing o Spam?
La solución debe ser capaz de analizar tanto el encabezado como el contenido del mensaje para detectar e identificar ataques de suplantación de dominio, suplantación de nombre.
La solución debe ser totalmente compatible con los siguientes mecanismos de autenticación de correo electrónico: • Sender Policy Framework (SPF), • Domain Keys Identified Mail (DKIM), • Domain-based Message Authentication, Reporting & Conformance (DMARC).
La solución debe contar con la opción de configuración de listas blancas y listas negras.
La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus funcionarios.
La solución debe utilizar la integración con el directorio para crear automáticamente listas de usuarios VIP para protegerlos Protección contra la suplantación de identidad
La solución debe inspeccionar enlaces cuando el usuario hace clic en la URL, Es decir re-escribir el(los) enlace(s) en el correo.
La solución debe emular (sandboxing) los enlaces URLs re-escritos para exponer indicadores de phishing ocultos.
La solución debe permitir a los administradores detectar a los usuarios que hicieron clic en los enlaces que resultaron maliciosos y que requieren mayor educación y capacitación para evitar hacer clic en enlaces maliciosos
La solución debe interactuar con Microsoft a través de la API, no debe generar interferencia cuando MS ATP o Defender inspeccionan la URL antes que se reescriba la URL. Por lo tanto, puede usarse con MS ATP o Defender, como una capa adicional de protección.
La solución debe re-escribir enlaces en el cuerpo del correo y también en links dentro de documentos adjuntos en el correo.
La solución debe permitir a los administradores configurar la lista de excepciones, de correos detectados mediante como maliciosos o sospechosos

La solución debe soportar la rescritura de URLs embebidas incluso si son códigos QR, reemplanzado la imagen del código QR en el cuerpo del correo con un nuevo código QR que apunta a un enlace reescrito.
La reescritura de enlaces de la solución debe tener la opción de permite ofuscar la ruta completa de la URL, dejando solo visible el dominio de la URL, de esta manera, los usuarios pueden comprender aproximadamente a dónde apunta el enlace, sin permitirles eludir la seguridad.
La solución debe ser capaz de poner en cuarentena los correos electrónicos, los archivos y los mensajes según las políticas de seguridad y la configuración de los motores de seguridad
La solución de acuerdo con la política debe permitir a los usuarios finales enviar solicitudes de restauración para correos electrónicos en cuarentena, seleccionar administradores autorizados puedan aprobar o no las solicitudes de restauración.
La solución debe permitir a los administradores configurar enviar notificaciones sobre solicitudes de restauración de correos en cuarentena a cualquier dirección de correo electrónico, así como parte del equipo de soporte o el SOC, este equipo recibe notificaciones de las solicitudes y las gestiona según su SLA.
La solución debe permitir a los administradores configurar un remitente personalizado para las notificaciones enviadas a los usuarios finales sobre la aprobación o rechazo de solicitudes de restauración de correos en cuarentena y los reportes sobre correos de phishing, siendo posible configurar al menos los siguientes parámetros: • Dirección del remitente • Nombre del remitente • Dirección de respuesta
Cuando la organización utilice soluciones de Simulación y Entrenamiento de Phishing, en las que envían campañas de phishing falsas para evaluar la respuesta de los usuarios y educarlos, la solución de seguridad de correo electrónico debe detectar automáticamente estos reportes y los distingue de otros correos, y cuando los usuarios reporten estos correos simulados, pueden enviar una respuesta automatizada para reconocer su conciencia.
La solución debe permitir a los administradores monitorear y gestionar la lista de remitentes confiables desde el portal de gestión de Excepciones de Anti-Spam.
Los administradores de la solución deben poder editar o agregar remitentes de confianza para destinatarios específicos a través del portal de la solución.
Los administradores pueden agregar remitentes de confianza no solo para un destinatario específico, sino para toda la organización. De esta manera, los correos electrónicos de ese remitente de confianza, si se encuentran como spam o Graymail, llegarán al buzón del destinatario, independientemente de quién sea el destinatario.
La solución debe crear y mantener la carpeta debajo de la bandeja de entrada de todos los usuarios finales, para que todos los funcionarios sepan exactamente dónde encontrar los correos electrónicos de Graymail.
La solución debe permitir correos electrónicos incluidos en la lista de permitidos de la solución también en sean permitidos por Microsoft/Google.
La solución debe contar con acciones automatizadas como marcar y alertar al usuario en el correo, mover a la carpeta Spam/Junk, cuarentena y/o añadir una cabecera en el correo.
La solución debe contar acciones automatizadas diferenciadas para phishing, malware, spam, correo de mercadeo (marketing).
La solución debe permitir al administrador que los usuarios finales confíen en los remitentes para que los correos electrónicos clasificados como spam se entreguen en su buzón, en cambio, si los correos electrónicos se clasifican como phishing o contienen malware, se pondrán en cuarentena.
La solución debe permitir que el administrador personalizar las plantillas que usaría para notificar a los usuarios finales sobre las amenazas.
La solución debe tener un periodo de retención de correos electrónicos originales **cuarentenados** por al menos 180 días.
La solución debe tener un periodo de retención de los **metadatos** de los correos electrónicos analizados maliciosos por al menos 180 días.
La solución debe permitir conservar los correos electrónicos puestos en cuarentena por Microsoft por un período de tiempo más largo que la retención de Microsoft y esta duración se puede configurar hasta 180 días.
La solución debe tener un periodo de retención de todos los correos electrónicos originales analizados por al menos 14 días, aun si son clasificados como limpios.
La solución debe permitir opcionalmente como **backup** almacenar localmente los correos electrónicos/archivos en cuarentena.
La solución debe tener la capacidad de remediación de las amenazas que llegan a las bandejas de entrada de los usuarios, desde la interfaz de gestión debe poder realizar la identificación, el análisis y la corrección. Si llega un correo electrónico o un archivo, se puedan tomar medidas inmediatas en miles de bandejas de entrada con unos pocos clics, sin PowerShell ni codificación de ningún tipo.
La solución debe permitir a los usuarios y administradores proporcionar comentarios sobre correos electrónicos sospechosos para ayudar en la clasificación de phishing.

La solución debe permitir que los usuarios puedan ayudar a detectar ataques perdidos y permitir que los administradores de seguridad bloqueen los ataques detectados y prevenir ataques similares en el futuro. La solución debe integrarse con el este mecanismo reporte de suplantación de identidad de MS Outlook.
La solución debe permitir la adición de Banners de correo electrónico educativos usando inteligencia artificial para los correos electrónicos entrantes, que permita a la organización concienciación sobre ciberseguridad y recordar a los usuarios que sigan la política, los banners deben ser totalmente personalizables para el color que represente la gravedad y el texto, e informar al destinatario sobre correos con contenido como: • Solicitud de pago a través del servicio de pago • Correos electrónicos con facturas / órdenes de compra • Correos electrónicos con enlaces a recursos restringidos • Nombre del remitente diferente a la dirección • Dominio de respuesta creado recientemente y su dirección es diferente a la del remitente • Error en el SPF del remitente • Dominio del remitente creado recientemente • Correos electrónicos entrantes de remitentes externos
La solución debe permitir al administrador realizar personalizaciones o configurar excepciones en las reglas de seguridad basándose en al menos las siguientes opciones: • Hosts, • direcciones IP, • Usuarios, • Dominios, • Cabeceras / Headers • Asunto • Links • Adjuntos
La solución debe ser permitir a los administradores desde la misma consola de gestión de seguridad de correo electrónico ver y restaurar todos los correos electrónicos en cuarentena, ya sea que hayan sido puestos en cuarentena por Microsoft o por la solución de seguridad ofertada basada en API.
La solución debe permitir a los administradores bloquear automáticamente las URL procedentes de las fuentes de indicadores de compromiso (IOC)
Revisión de correos electrónicos de phishing reportados por el usuario: Los usuarios pueden ayudar a detectar ataques perdidos, permitir que los administradores de seguridad corrijan los ataques detectados y ajustar las políticas para evitar ataques similares en el futuro. La solución debe ingerir automáticamente estos **informes**, alertar a los administradores sobre ellos y los presentar un panel dedicado que permita a los administradores investigar y tomar las medidas necesarias.
La solución se debe poder integrar con el complemento nativo Report Message para Microsoft 365, para marcar como phishing en Outlook. Cuando un usuario hace clic en esta opción
Responder automáticamente y corregir los informes de los usuarios finales sobre correos electrónicos de phishing: Cada vez que un usuario envíe un reporte de correo de phishing, la solución debe volver a evaluar el correo electrónico, utilizando la reputación actualizada, los motores de seguridad actualizados y con el informe como un indicador adicional para la IA. El resultado es un veredicto reevaluado: limpio, phishing o no concluyente. Para cada veredicto reevaluado, los administradores ahora pueden configurar un flujo de trabajo (poner en cuarentena el correo electrónico o mantener el correo electrónico en el buzón), así como definir notificaciones personalizables tanto para los administradores como para los usuarios finales.
La solución debe permitir a los administradores configurar un comentario automatizado para que se envíe a los usuarios finales cuando informen de correos electrónicos de entrenamiento de phishing
La solución debe permitir a los administradores configurar un remitente personalizado para las notificaciones enviadas a los usuarios finales sobre las solicitudes de restauración de cuarentena aprobadas o rechazadas y los informes sobre correos electrónicos de suplantación de identidad (phishing).
La solución debe permitir a los administradores pueden enviar notificaciones sobre los usuarios que envían solicitudes de restauración a cualquier destinatario de correo.
La solución debe permitir enviar un reporte diario por correo electrónico a los usuarios finales sobre los correos electrónicos en cuarentena y basura/spam en las últimas 24 horas.
La solución debe permitir a los administradores configurar la liberación automática de correos electrónicos de la cuarentena de Microsoft si son clasificados como limpios por el sistema de seguridad, es decir falsos positivos en las detecciones de Phishing de Alta Confianza evitando que los administradores dediquen mucho tiempo a liberar estos correos de la cuarentena, como una última línea de defensa y capa de seguridad la solución debe poder configurarse para liberar automáticamente los correos en cuarentena por Microsoft como Phishing de Alta Confianza si el sistema los clasifica como limpios.
Los correos electrónicos que Microsoft / Google entregan falsamente a la carpeta de correo no deseado pueden redirigirse a la bandeja de entrada del usuario.

La solución debe permitir corregir detecciones de falsos positivos, para que los equipos de SOC no dediquen tiempo a ayudar a los usuarios finales a localizar sus correos electrónicos legítimos perdidos.
Portal Dedicado para la Gestión de Correos en Cuarentena por los Usuarios Finales: En casos raros en los que un correo es puesto en cuarentena erróneamente por el sistema de seguridad o por Microsoft, y no es liberado automáticamente, es crucial que el usuario pueda recuperarlo rápidamente. El Portal de Seguridad de Correos Electrónicos para Usuarios Finales, debe permitir a los usuarios ver todos sus correos en cuarentena, filtrarlos, pre visualizarlos y restaurarlos o enviar solicitudes de restauración, todo conforme a las políticas organizacionales definidas.
Los usuarios pueden iniciar sesión en el portal de cuarentena de usuario final a través de Microsoft, aplicando los mismos controles de seguridad, incluido el inicio de sesión único, a través de su cuenta corporativa de Microsoft.
La solución debe permitir a los usuarios solicitar al administrador la liberación de los correos cuarentenados conforme a las políticas organizacionales definidas.
PREVENCIÓN DE MALWARE EN CORREO ELECTRÓNICO Y HERRAMIENTAS DE COLABORACIÓN Y ALMACENAMIENTO SaaS
La solución debe escanear malware a través de análisis estático.
La solución debe tener protección antivirus/malware basado en firmas.
La solución debe permitir a los administradores configurar la lista de bloqueo cualquier tipo de archivo y marcado como malware y para los tipos de archivos (PDF, EML, HTML) optar por bloquear estos archivos en función de si contienen enlaces o no.
La solución debe detectar archivos protegidos con contraseña al menos de las siguientes extensiones Documentos: Word, Excel, PowerPoint y PDF. Archivos: ZIP, 7Z, RAR, CAB, TAR, TAR.GZ, TGZ, GZ, BZ2, XZ, TXZ, TBZ2, TB2, TBZ, ISO, TAR.XZ, TAR.BZ2, CHM, IZH, RPM, WIM, ARJ, CPIO, CRAMFS, QCOW2, UDF, AR e IMG, ISO, AR.
Si un archivo está protegido con contraseña, la solución debe intentar extraer la contraseña mediante varias técnicas, como buscar la contraseña en el cuerpo del correo electrónico y si se encuentra la contraseña, debe usar la contraseña para descifrar el archivo e inspeccionarlo en busca de malware.
Si no se encuentra la contraseña, el administrador debe poder seleccionar alguna de las siguientes acciones: • Requerir que el usuario final ingrese una contraseña • El usuario recibe el correo electrónico con una advertencia. • Cuarentena. • Identificar el correo como sospechoso de malware
La solución debe permitir a los administradores excluir remitentes externos del flujo de trabajo predeterminado para el manejo de correos con archivos adjuntos protegidos por contraseña, para evitar solicitar contraseñas repetidamente de sistemas automatizados o dominios confiables que envían muchos correos con archivos adjuntos protegidos, las exclusiones deben permitir las direcciones de remitente o dominios específicos pueden ser excluidos del flujo de trabajo, permitiendo que sus correos sigan siendo inspeccionados para malware.
La solución debe escanear todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados.
La solución debe escanear y analizar cada archivo en busca de enlaces maliciosos que luego pueda bloquear en todas sus aplicaciones para compartir archivos.
La solución debe detectar directamente el comportamiento malicioso y poner en cuarentena los archivos antes de que la amenaza se propague.
La solución debe brindar protección contra enlaces de phishing, código o archivos maliciosos y fuga de datos en plataformas de chat institucional.
La solución debe permitir a los administradores bloquear direcciones, URL exactas y dominios completos en mensajes de Teams.
Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Foleder (Carpeta bóveda)
PREVENCIÓN DE MALWARE DE DÍA CERO (SANDBOXING) EN CORREO Y HERRAMIENTAS DE COLABORACIÓN Y ALMACENAMIENTO SaaS Y LIMPIEZA DE DOCUMENTOS
La solución debe incluir capacidades de “Sanboxing” resistente a la evasión para bloquear el malware de día cero, con un análisis dinámico en un entorno virtual aislado y escalable basado en la nube
La solución debe incluir el uso del análisis de sandboxing para revisar los archivos adjuntos y los recursos web asociados a los hipervínculos incluidos en los mensajes. Incluso debe tener la capacidad de ver un vídeo del resultante de la emulación.
El análisis de sandboxing debe obtener un veredicto respecto de un archivo adjunto o del recurso web asociado a un hipervínculo en un lapso no mayor a 5 minutos.
La solución debe contar con una página de bloqueo para impedir el acceso de los usuarios a los sitios web maliciosos asociados a los hipervínculos contenidos en los mensajes de correo analizados.

La solución debe ser capaz de realizar sandboxing al menos los siguientes tipos de archivos: EXE, DLL, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, SWF, JAVA (.jar, .js/.jse), VBS, scripts y archivos PowerShell (.ps1).
La solución debe permitir que los administradores puedan seleccionar los sistemas operativos que utilizará el sandbox del Anti-Malware para emular archivos. La Emulación debe soportar hacerlo en Win7, Win8.1, Win10 o inclusive Win11.
La solución debe admitir capacidades CDR (Content disarm and Reconstruction) es decir, podrá limpiar los documentos o imágenes adjuntos en los correos electrónicos de contenido malicioso.
La solución debe emular los archivos en los correos electrónicos detrás de enlaces de descarga directa para extender la protección contra archivos desconocidos que se ocultan detrás de enlaces, antes de ser entregados a los usuarios finales. Además, debe prevenir ataques en los que el archivo detrás del enlace se altera después de que se envía el correo aplicando la protección de reescritura del enlace, así la inspección debe realizarse cuando los usuarios hagan clic en estos enlaces después de ser reescritos, y si se detecta que el archivo es malicioso, el acceso al archivo deberá ser bloqueado.
ANOMALÍAS DE USUARIOS Y DETECCIÓN DE CUENTAS COMPROMETIDAS
La solución debe evitar ataques avanzados de apropiación de cuentas aumentando los procesos de autenticación, evitar usuarios no autorizados y los dispositivos comprometidos accedan a su correo electrónico en la nube o a las aplicaciones SaaS.
La solución debe contar con un motor que analice el comportamiento utilizando un algoritmo de aprendizaje automático que crea un perfil basado en eventos históricos que incluyen ubicaciones y horas de inicio de sesión, comportamiento de transferencia de datos y patrones de mensajes de correo electrónico.
La solución debe detectar comportamientos y acciones que parecen anormales cuando se observan en el contexto de una organización y la actividad histórica de un usuario.
Para identificar cuentas potencialmente comprometidas, debe incluir un motor de inteligencia artificial para inspeccionar todos los parámetros de los eventos de inicio de sesión para identificar los realizados por actores malintencionados: • Borrado de todos los correos electrónicos del buzón • Usuarios que envían correos electrónicos maliciosos • Mover todos los correos electrónicos a una subcarpeta • Detección basada en Inteligencia artificial de inicios de sesión anómalos • Iniciar la sesión desde una dirección IP maliciosa • Primera vez en un nuevo país • Reenvío automático a una dirección de correo electrónico externa • Acceso inusual desde un país • Acceso desde una geográfica sospechosa (viaje imposible) • Error de inicio de sesión sospechoso en MFA • El cliente es un navegador vulnerable.
La solución debe tener la capacidad de tomar las siguientes acciones de respuesta cuando detecte cuentas potencialmente comprometidas o cuentas secuestradas: • Bloquear la cuenta; • Restablecer la contraseña.
Las Anomalías Críticas y de inicio de sesión identificados de los usuarios comprometidos podrán ser bloqueadas automáticamente.
La solución debe permitir a los administradores configurar un buzón dedicado al que se enviarán alertas sobre cuentas comprometidas.
La solución debe realizar el bloqueo de cuentas que inicien se sesión desde direcciones IPs conocidas como maliciosas por una base de inteligencia de amenazas del fabricante (TIP) de la solución ofertada.
Entre los eventos que la solución debe analizar para identificar cuentas secuestradas (“account takeover”) deben incluirse: • El inicio de sesión; • La ubicación desde donde se hizo el inicio de sesión; • Anomalías recientes • Correos recientes • Acciones del usuario recientes
Los administradores pueden configurar y/o agregar automáticamente una lista de bloqueo para todo el tráfico saliente de las cuentas detectadas como comprometidas o sospechosas de estar comprometidas, como una capa agregada de seguridad en escenarios como: • Mensajes maliciosos programados: el atacante puede programar el envío de correos electrónicos en una etapa posterior que se adapte a su ataque, sabiendo que el usuario que comprometió puede ser bloqueado en cualquier momento.

• Entornos híbridos: en los casos en los que el Active Directory local invalida el Azure Active Directory, es posible que se desbloqueen los usuarios bloqueados. En este caso, todos los correos electrónicos salientes de este usuario comprometido seguirán bloqueados.
SHADOW IT & APPLICATION CONTROL
La solución basada en el análisis de correos electrónicos (Office 365 y/o Gmail), debe identificar los correos electrónicos de las aplicaciones en la nube para los usuarios que sugieren que han estado usando, para brindar visibilidad de las aplicaciones en la nube que se utilizan.
La solución debe detectar y proporcionar informes de aplicaciones de Shadow IT y top de usuarios.
La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.
La solución debe indicar el uso de las aplicaciones a lo largo del tiempo.
La solución debe presentar las aplicaciones usadas según su categoría.
La solución debe permitir aprobar una aplicación o crear lista blanca la aplicación
DATA LOST PREVENTION (DLP) PARA CORREO Y HERRAMIENTAS DE COLABORACIÓN Y ALMACENAMIENTO SaaS
La solución debe contar con un motor de prevención de pérdida de datos (DLP) debe proteger los datos de la organización de posibles violaciones de datos o transmisiones de filtración de datos.
El motor DLP debe analizar correos electrónicos, archivos adjuntos, archivos compartidos y mensajes de texto publicados en las plataformas de colaboración y detectar patrones de datos que no deben compartirse con personas o destinos no autorizados.
El motor DLP debe permitir crear políticas para controlar cómo se comparten los archivos entre usuarios internos y externos. El DLP debe identificar y marca archivos que contienen información confidencial, financiera y de identificación personal, incluidos números de tarjetas de crédito, números de ruta bancaria o datos protegidos por HIPAA, etc.
La solución de DLP deberá admitir Expresiones Regulares, Diccionarios personalizados definidos por el cliente.
La política DLP debe permitir filtrar los correos electrónicos salientes para garantizar que los datos confidenciales no lleguen a destinatarios no autorizados. La política DLP debe permitir filtrar los correos electrónicos entrantes para garantizar que los datos confidenciales no se almacenen en los buzones de correo de la entidad o que se compartan solo a través de métodos de entrega autorizados.
Para los Correos salientes la solución de DLP debe permitir al menos las siguientes acciones: ✓ Bloquear el correo electrónico y alertar al usuario. ✓ Bloquear el correo electrónico y solicitar se vuelva a enviar como encriptado ✓ Permitir el correo agregando una cabecera al correo.
Para los correos entrantes la solución de DLP debe permitir al menos las siguientes acciones, bloquear el correo electrónico y alertar al usuario, bloquear el correo electrónico y solicitar se vuelva a enviar como encriptado, permitir el correo agregando una cabecera al correo.
La solución debe permitir a los administradores poner en cuarentena los correos electrónicos entrantes que violen la política de Prevención de Pérdida de Datos (DLP) sin notificar a los usuarios finales.
La solución debe permitir configurar alertas por correo electrónico para los administradores y usuarios cuando los correos electrónicos entrantes o salientes detectados que contengan una infracción de DLP.
La solución debe permitir que los administradores puedan configurar su directiva DLP para que los correos electrónicos se envíen cifrados por Microsoft 365.
El sistema debe permitir a los administradores definir políticas de DLP no solo basadas en tipos de datos predeterminados o personalizados, sino también en las Etiquetas de Sensibilidad de Microsoft Purview asociadas a correos electrónicos, archivos adjuntos, archivos compartidos o mensajes. La sección de Criterios de DLP debe permitir elegir las etiquetas de sensibilidad de Microsoft, con opciones para seleccionar cualquier etiqueta, etiquetas específicas, todas excepto algunas, o sin etiquetas.
La solución debe permitir una correspondencia segura por correo electrónico donde las partes externas ven los correos electrónicos confidenciales a través de un portal autenticado, y la organización remitente controla la disponibilidad del mensaje para la parte externa.
La solución debe permitir que los administradores puedan personalizar el portal de correspondencia segura agregado imágenes o logotipos.
La solución debe permitir lista de remitentes / destinatarios individuales o dominios completos de la inspección de DLP para granularidad sobre la política.
Para Aplicaciones como OneDrive, SharePoint debe permitir por política dos tipos de acciones de remediación Cuarentena y Vault Folder (Carpeta bóveda)
La solución debe definir sensibilidades personalizadas para las reglas DLP, de modo que se active un flujo de trabajo diferente, dependiendo de la cantidad de datos confidenciales que se filtran.
La solución debe permitir a los administradores configurar alertas por correo electrónico para que los directores o jefes de dependencias reciban notificaciones en tiempo real cuando sus subalternos envíen o intenten enviar datos clasificados que coincidan con las reglas de la política DLP de Microsoft 365.

Estas notificaciones deben poder configurarse para cualquier regla de política DLP, ya sea que el correo sea bloqueado o no, e incluso para reglas que solo se monitorean.
GESTIÓN DE EVENTOS, TABLEROS, REPORTES Y AUDITORIA
La solución debe permitir gestionar los eventos de seguridad, ya sea que se detecten/prevengan automáticamente o que los administradores/usuarios finales encuentren después de no haber sido prevenidos de diversas amenazas, desde correos maliciosos y spam hasta cuentas comprometidas y socios riesgosos.
La solución debe contar con una vista detallada de todos los eventos de seguridad en tiempo real. Mediante la búsqueda y los filtros, puede ver eventos relacionados con cualquier período de tiempo, estado, nivel de gravedad y SaaS.
La solución debe contar con una vista centrada en las amenazas de correo electrónico con información como: - Categorías de phishing detectadas. - Acción sobre el correo electrónico malicioso, si está en cuarentena, en la bandeja de entrada, o en la carpeta de no deseado) usuarios involucrados en el evento (destinatarios, remitentes, propietarios de archivos compartidos) - Información de quien remedió la amenaza que puede ser el administrador, por la herramienta de seguridad o por el proveedor de correo en nube
La solución debe proporcionar tableros de análisis de eventos maliciosos detallados para cada aplicación SaaS. Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.
La solución deberá proveer reportes ejecutivos de eventos de seguridad de la última semana, dos semanas y últimos 30 días.
La solución debe permitir a los administradores programar informes de seguridad que se envíen con diferentes zonas horarias y a diferentes destinatarios.
Debe proveer capacidades de investigación que apoyen los procesos de cacería de amenazas de la organización, poder realizar consultas a toda la metadata (correos electrónicos, archivos, inicios de sesión de usuario, etc.) capturada y almacenados en el tenant
Las capacidades de investigación deben permitir los siguientes tipos de filtros: **Múltiples Valores en una Consulta:** listas extensas de hasta 200 valores en un solo campo de búsqueda que acepta texto libre, con condiciones disponibles (Contiene Cualquiera, Coincide con Cualquiera, Excluir Contiene, Excluir Coincide), **Múltiples Condiciones de Búsqueda para el Mismo Campo:** aplicar filtros a un campo, definir múltiples condiciones para ajustar la búsqueda de manera más precisa, gestionar el operador (Y/O) entre cada condición
La solución debe proveer un tablero de resumen que proporcione a los administradores una visibilidad instantánea de todas las tareas pendientes de revisión, incluyendo: • Usuarios comprometidos • Socios riesgosos • Solicitudes abiertas de restauración de cuarentena por parte de usuarios finales • Reportes abiertos de phishing por parte de usuarios finales • Ataques BEC incluye un indicador que muestra si las cuentas comprometidas se bloquean automáticamente o no
La solución debe tener la posibilidad de exportar eventos a archivos CSV, json, xlsx
La solución deberá proveer reportes de los eventos por hasta 180 días, en formato csv o xlsx.
La solución debe permitir filtrar los correos electrónicos en función de su dirección, entrante, saliente e interno.
La solución debe permitir que los administradores tengan la capacidad de filtrar correos por el campo de Message ID
Los administradores de la solución deben poder filtrar los correos electrónicos utilizando indicaciones en el idioma nativo, utilizando la IA generativa, el Asistente de IA, Con el Asistente de IA, puede buscar correos electrónicos utilizando indicaciones en el idioma nativo y obtener resultados instantáneos.
La solución debe contar con un tablero con el número de reportes phishing de los usuarios, solicitudes de restauración y socios de riesgo, así como una indicación de si las cuentas comprometidas se bloquean automáticamente o no.
La solución debe permitir a los administradores tener visibilidad del riesgo de los socios con los que comunican utilizando un motor de IA y recibir alertas sobre los socios que pueden estar comprometidos.
La solución debe permitir que los administradores puedan desencadenar una acción específica cuando el dominio del remitente se parece mucho al dominio de un socio, o evitar ataques de socios comprometidos.
La solución debe permitir a los administradores puedan ver la justificación de los usuarios finales antes de aprobar / rechazar las solicitudes antes de liberar un correo de cuarentena.
Los administradores de la solución deben tener visibilidad en tiempo real cómo Microsoft 365 clasificó cada correo electrónico y qué acción que tomó son sus soluciones de EOP o Defender, es decir la solución debe trabajar con seguridad en profundidad y en capas.

Los eventos y en cada correo electrónico, deben tener la clasificación de (SCL, BCL) y que acción de cumplimiento (cuarentena, mover a junk folder) que tomó sobre el correo electrónico de acuerdo con la clasificación.
La solución debe permitir filtrar correos electrónicos basado en las acciones tomadas por las herramientas o para las decisiones de cumplimiento de Microsoft.
La solución debe brindar el detalle del análisis de un archivo identificado como malicioso incluyendo los comportamientos riesgosos que fueron identificados y las técnicas identificadas.
El panel principal debe proporcionar una descripción general de como la solución clasificó los correos electrónicos que Microsoft decidió dejar pasar a los usuarios finales.
La solución debe incluir un informe diario de cuarentena, enviando un informe por correo electrónico diariamente a los usuarios finales sobre los correos electrónicos en cuarentena y no deseados/spam. Los usuarios finales obtienen un informe detallado que contiene información sobre los correos electrónicos que se les enviaron y se pusieron en cuarentena en las últimas 24 horas.
La solución debe permitir a los usuarios finales generar un nuevo informe de cuarentena (resumen) para las últimas 24 horas en cualquier momento.
La solución debe permitir que los administradores pueden personalizar: - Cuándo y cuántas veces al día sus usuarios finales reciben el informe de cuarentena. - La dirección de respuesta del informe de cuarentena diario enviado a los usuarios finales. - Los textos en el cuerpo y el asunto del informe diario de cuarentena del usuario final. - El texto del enlace en el que los usuarios hacen clic para generar un reporte.
La solución debe permitir que los administradores puedan configurar, para cada detección de Microsoft 365, si los usuarios finales pueden solicitar una restauración, restaurar por su cuenta o no pueden restaurar los correos electrónicos en absoluto.
Todas las solicitudes de restauración enviadas por los usuarios finales deberán estar disponibles para que los administradores en el panel de solicitudes de restauración.
La solución debe permitir a los administradores puedan cargar un logotipo personalizado para agregarlo a las notificaciones por correo electrónico, las páginas del navegador y los informes.
La solución debe permitir a los administradores que puedan buscar en la consola de seguridad de correo electrónico ofertado los correos electrónicos detectados debido a una regla de transporte de Microsoft, ya sea que se entreguen al usuario final, en la carpeta de correo no deseado o que la solución de seguridad o Microsoft los pongan en cuarentena.
La solución debe permitir que los administradores desde portal de gestión se mantengan actualizados sobre las actividades de mantenimiento y el estado del servicio.
La solución debe permitir que los administradores puedan definir buzones dedicados para recibir alertas sobre el estado del servicio
PORTAL DE GESTIÓN
Control de acceso granular basado en roles al portal web de gestión, al menos para Administrador y solo Lectura.
Los usuarios del Help Desk y los usuarios de solo lectura pueden recibir permisos de solo visualización para la sección de Políticas.
Los usuarios del Help Desk y los usuarios de solo lectura pueden recibir permisos para ver y editar la sección de Políticas. Por defecto, los usuarios del Help Desk y de solo lectura no tienen permiso para ver ni editar las reglas de políticas. Anteriormente, se había anunciado la capacidad de otorgar permisos de solo visualización para esta sección.
La solución debe permitir que los administradores puedan restringir el acceso al portal de la organización a una dirección IP o CIDR específica.
INTEGRACIONES A SIEMS Y API
La solución ofertada debe permitir integrarse con soluciones SIEM vía syslog, vía TCP, vía HTTP o json
La solución debe soportar API Rest para administrar y actuar sobre los eventos de seguridad detectados
GARANTÍA TÉCNICA DURANTE LA VIGENCIA DEL CONTRATO
Se deberá brindar el acompañamiento de soporte con un horario 7x24 por el proveedor, por el término de Veinticuatro (24 meses) contados a partir de la fecha de activación de la licencia y/o cada vez que el supervisor del contrato lo requiera durante el término de la garantía.
El servicio de soporte puede brindarse de manera remota; sin embargo, en caso de ser requerido por el supervisor de manera presencial deberá hacer presencia en sitio; según incidencias o requerimientos del supervisor del contrato, de acuerdo con la necesidad del COGFM.
Se deberá proveer una línea telefónica para que la Dirección de Tecnología de la Información del Departamento Conjunto de Comunicaciones y del Comando General de las Fuerzas Militares de Colombia, pueda reportar inconvenientes con los productos. Los Centros de acompañamiento deben estar disponibles en horario hábil, durante el tiempo de duración del contrato.
Se debe brindar soporte técnico por medio telefónico o remoto de forma inmediata en el momento de presentar alguna novedad con el servicio adquirido. Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al incidente, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).

El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá.
Durante el periodo de garantía técnica deberá comprometerse a enviar informes periódicos con frecuencia trimestral vía correo electrónico, que permitan estar al tanto de los nuevos virus que aparecen y los medios para combatirlos y evitar próximos ataques.
Durante el periodo de garantía técnica, se requiere dos (02) visitas semanales mínimo de ser necesario, con el fin que se realice verificación del correcto funcionamiento de la herramienta de solución antispam.
En el soporte de manera remota se debe verificar la correcta actualización del software de solución antispam, realizando verificación de parches y versiones del producto los cuales deben permanecer totalmente actualizados.
Una vez finalizado el soporte de manera remota, se debe recibir por parte del técnico contratista, un informe escrito de cada actividad realizada.
El tiempo promedio para restablecer los servicios de antispam o solución del problema vírico, no debe ser superior a ocho (8) horas, una vez realizada la solicitud de servicio.
El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se llevará a cabo por medio de un Ticket de servicio para los incidentes presentados).
Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.
GARANTÍA
Se deberá entregar certificado donde se evidencien las licencias adquiridas, con su respectiva clave y fechas de vigencia.
GARANTÍA: El término de la garantía técnica o garantía legal de conformidad con el art. 6, 7, 8, 9 y 11 de la Ley 1480 de 2011, será de (24) meses contado a partir del 31 de octubre de 2025 o fecha que indique la plataforma o documento de fabricante.
El término de la garantía técnica (o garantía legal de conformidad con el art. 7º de la Ley 1480 de 2011), deberá cumplir con los siguientes requisitos:
Es la obligación, en los términos de la ley 1480 de 2011 de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad y el buen estado y funcionamiento del software.
Se deberá garantizar las licencias que están respaldadas por la casa propietaria del software, de la última versión disponible en el mercado, de acuerdo con las especificaciones técnicas exigidas.
Se deberá contar con personal técnico capacitado para atender y solucionar los incidentes de soporte reportados.
SEGURIDAD
ACUERDO DE CONFIDENCIALIDAD: El oferente y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista seleccionada, lo cual será verificado por el supervisor del contrato.
Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares.
El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO
El contrato debe ejecutarse a todo costo, el contratista se compromete a realizar la instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad de la herramienta ofrecida.
Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el futuro contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma para la ejecución del objeto del futuro contrato, para aprobación del supervisor del contrato.

- LOTE 5: SUSCRIPCIÓN WAF.

ÍTEM No.	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANTIDAD
1	SUSCRIPCIÓN FIREWALL PARA APLICACIONES WEB (WAF).	UNIDAD	1

GENERALIDADES

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

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

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

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

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

CARACTERÍSTICAS TÉCNICAS

REQUERIMIENTOS ESPECÍFICOS

FUNCIONALIDAD	DESCRIPCIÓN
SaaS	La solución deberá soportar una arquitectura Software as a Servicie (SaaS), donde la manera de consumo de los servicios sea dentro de su propio cloud, incluyendo todos los puntos de presencia distribuidos de manera global.
	La solución deberá ofrecer disponibilidad de ancho de banda limpio en su solución WAF o protección de aplicaciones web, sin limitación en la cantidad de tráfico inspeccionado o mitigado, garantizando la protección para todo el tráfico que llegue a la Entidad.
	La solución deberá incluir al menos dos balanceadores de carga, cada uno con soporte para un mínimo de 32 aplicaciones web, y al menos dos direcciones IP ANYCAST distribuidas en todos los centros de datos de la solución para la publicación de los servicios web de la entidad. Estas aplicaciones podrán estar asociadas a un mínimo de 200 nombres de dominio raíz diferentes.
ADMINISTRACIÓN	
Gestor Centralizado / Consola Central	La solución deberá proporcionar una consola central SaaS para la administración centralizada de las configuraciones de red y seguridad, así como también acceso a herramientas de troubleshooting y dashboard donde se visualice la disponibilidad y el estado de los servicios. Además, debe permitir que la gestión se realice mediante clickops, API requests, Terraform o integrandose al pipeline CI/CD de la organización
API de la solución	La solución deberá ser full RESTful-API o API first: - permitiendo realizar todas las configuraciones a través de su API, así como también, la petición de información de los dashboards. .- debe estar bien documentada y proveer de las configuraciones en JSON y YAML de cualquiera de los objetos que se definan. .- debe permitir la creación de credenciales por usuario, el uso de API token, certificados, así como la creación de usuarios API con RBAC.
Usuarios Admin	La solución deberá soportar la creación de múltiples usuarios, así como roles de acceso como read only, SecOps, DevOps, NetOps, SuperUser, Billing User entre otros.

RBAC	La solución deberá permitir el uso de RBAC para el control de acceso de los usuarios al gestor centralizado, permitiendo la delimitación de las APIs/recursos que se pueden visualizar y/o administrar.
Self Service	La solución deberá proporcionar al usuario del gestor centralizado la posibilidad de administrar sus servicios dentro de una consola unificada y donde se permita la colaboración de distintos equipos (SecOps,DevOps,entre otros)
Servicio Administrado	La solución deberá proporcionar la opción de contratar un servicio administrado para WAAP con gente especializada y certificada del fabricante para llevar adelante dichas tareas.
Soporte	La solución deberá contar con soporte 24x7, ya sea por medio de Teléfono, Mail u otros medios de contacto. Asimismo, el servicio de soporte deberá permitir la interacción con el Centro de Soporte en idioma español en el uso horario de la región (Colombia) durante horario laboral.
Capacitación	La solución deberá contar con capacitación onDemand a través de videos y/o documentación que ejemplifiquen configuraciones básicas y que sean accesible desde la plataforma o página web del fabricante
VISIBILIDAD	
Integración con SIEM	La solución deberá proporcionar integración con herramientas de logging de terceros.
Dashboard de Performance	La solución SaaS deberá proporcionar visibilidad acerca de: .- Salud de la aplicación .- Alertas activas .- Origin Servers/Backends .- Latencia de fin a fin .- Visitantes unicos .- Tipo de dispositivo .- Peticiones (Request Rate, Total Request, Error rate, total errors, drop rate, drop count) .- Throughput .- ASN .- TLS Fingerprint .- TLS Ciphers y protocolos .- Códigos de error de HTTP .- Localización de clientes .- Top URLs
Dashboard de Seguridad	La plataforma SaaS deberá proporcionar visibilidad sobre: .- Eventos de seguridad por aplicación (WAF, APISec, DDoS, Anti-Bot entre otros) .- Top ten de las firmas con más hits .- Eventos localizados geográficamente .- Tipos de ataques .- Score de usuarios maliciosos .- Clasificación de bots (humano, malicioso, Sospechoso) Asimismo, la solución deberá proporcionar filtros para búsquedas utilizando el identificador asociado con el evento de seguridad.
Auditoria	La plataforma SaaS deberá proporcionar visibilidad sobre los cambios de configuración realizados por los usuarios del gestor centralizado durante un periodo de tiempo de 30 días
CERTIFICACIONES	
California Consumer Privacy Act (CCPA)	Deberá estar en cumplimiento con lo dispuesto por California Consumer Privacy Act (CCPA)
General Data Protection Regulation (GDPR)	Deberá estar en cumplimiento con lo dispuesto por General Data Protection Regulation (GDPR)
System and Organization Controls (SOC) Type 2	La solución deberá contar con la certificación System and Organization Controls (SOC) Type 2
SLAs	
Disponibilidad	La plataforma SaaS deberá proporcionar un 99.99% de disponibilidad
Tiempo de Respuesta	El servicio de Soporte técnico de la solución propuesta deberá tener un tiempo de respuesta de 30min para el primer contacto
Analisis deCausa Raiz	El servicio de Soporte técnico de la solución debe cumplir con el siguiente SLA relacionado con el análisis de causa raíz de un incidente: Incidente de severidad crítica: proporcionar un draft a las 24 hrs y el análisis final en 7 días

WEB SECURITY	
Funcionalidad	**Descripción**
Web Application & API Security	1.- La solución propuesta deberá emplear una combinación de técnicas algorítmicas, basadas en firmas, utilización de bases reputacionales y machine learning para identificar ataques a nivel de aplicación y API, proporcionando una solución holística de firewall aplicativo de próxima generación. 2.- La solución deberá contar con un motor de machine learning para determinar de manera automática todos los API endpoints que son accedidos a través de cualquiera de los servicios virtuales publicados. Además, deberá permitir que la información aprendida pueda ser utilizada para la definición de políticas por aplicación
Web Application Firewall	La solución deberá proporcionar una plataforma SaaS con motor de Machine Learning y firmas para la detección de ataques a nivel de capa de aplicación, que incluya la detección de ataques del OWASP TOP 10 así como los últimos ataques conocidos con actualización automática en valores de firmas, así como la utilización de una base de datos asistida de campanas de amenazas para detección de ataques específicos alrededor del mundo.
Detección de Usuarios Maliciosos	La solución deberá contar con la capacidad de detectar usuarios maliciosos mediante el análisis de su comportamiento utilizando técnicas y modelos avanzados, tal como Machine Learning.
Supresión de falsos positivos	La solución deberá utilizar un modelo de Machine Learning para el perfilamiento del tráfico dentro del WAF que permita la supresión de falsos positivos.
Tuning de la base de firmas	La solución deberá contar con un mecanismo automático que permita el tuning de las firmas de ataques
DDoS L3/L4	La solución deberá contar con la capacidad de detección y mitigación automática de ataques volumétricos de denegación de servicio, sin límite en la cantidad de este tipo de eventos y sin ancho de banda mínimo para la mitigación.
DDoS L7	La solución deberá permitir el bloqueo de clientes/usuarios de la aplicación basándose en su comportamiento. La solución deberá permitir la definición de políticas de retos de identificación de usuario de la aplicación utilizando JavaScript y CAPTCHA
Antibot	La solución deberá contar con la funcionalidad de Anti-Bot permitiendo la categorización de bots en buenos, sospechosos y malos y, por ende, su mitigación.
Servicio de reputación de IP	La solución deberá contar con la funcionalidad de bloqueo automático de conexiones desde IPs consideradas maliciosas, mediante la utilización de una base dinámica de reputación de IPs.
Bloqueo de peticiones no deseadas	La solución deberá permitir el bloqueo de clientes basándose en su comportamiento, el ASN, la red, la dirección IP y el país desde donde se generó la conexión
Cifrado	La solución deberá permitir la configuración de Cifrados de acuerdo a diferentes perfiles: alto, medio o bajo, así como la creación de políticas personalizadas para utilización de ciphers y protocolos específicos por aplicación. **High:** TLS 1.2 y 1.3 TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Generación Automática de Certificados Digitales	La solución deberá permitir la configuración de certificados públicos firmados de manera automática y controlados de manera automática a través de alguna delegación de dominio o validación de registros de DNS
Reescrituras HTTP	La solución deberá permitir la configuración de reescrituras HTTP.

	Asimismo, deberá permitir el tratamiento tanto de las peticiones HTTP hacia las aplicaciones, como de respuestas personalizadas según los diferentes códigos de HTTP.
Balanceo de cargas	La solución deberá permitir la configuración de origen servers/backend servers y sus correspondientes monitores de salud de manera ilimitada. Asimismo, la solución deberá permitir el uso de los siguientes métodos de balanceo: .- RoundRobin .- Least Active Request .- Random .- Persistencia por direccion IP .- Persistencia basada en cookie .- Ring Hash Así como crear pesos sobre los orígenes que se deseen y asignar esquemas activo-pasivo.
Analítica de Comportamiento de Usuario	La solución deberá contar con mecanismos que permitan el análisis de comportamiento utilizando métricas y logs. El análisis de comportamiento debe incluir: .-Detección de anomalías por petición, utilizando métricas como tamaño de la petición, tamaño de la respuesta, latencia. .-Lógica de Negocio, utilizando los logs de peticiones, por cliente por servidor y el host virtual para aprender: elementos dinámicos, probabilidad de función, tiempos y anomalías analiza esto utilizando redes neuronales.
Control sobre el número de peticiones (Rate Limit L7 DoS)	La solución deberá permitir controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre API endpoints específicos.
CSRF	La solución deberá controlar los subdominios permitidos en las peticiones cruzadas dentro de un Load Balancer/Proxy
Manejo de Información sensible	La solución deberá permitir controlar la información a visualizar de las respuestas del servidor, permitiendo enmascarar la información considerada como sensible, como, por ejemplo: datos de tarjeta de crédito
Client Side Defense	La solución debe proveer de un sistema de protección multifase a las aplicaciones Web, contra Formjacking, Magecart-style, y otros ataques de JavaScript. La protección multifase debe incluir detección, alertamiento y mitigación
Identificación del usuario	La solución deberá identificar usuarios teniendo en consideración los siguientes parámetros: ClientIP, TLSFingerprint, Cookie, HTTP Header, Client ASN, Client City, Client Region, Query Parameter Key.
Engine de WAF unificado	La solución deberá utilizar el mismo motor de WAF cualquiera sea la arquitectura implementada: SaaS, On-Premise, Hibrido, permitiendo la extensión de las políticas o servicios de seguridad a los diferentes ambientes que la constituyen.
Mutual TLS	La solución deberá permitir la utilización de MTLS para comunicación hacia los clientes y hacia los servidores.
Cookie Protection	La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticacion.
GraphQL Inspection	La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando instrospeccion, de los recursos, disponibles en el esquema actual.
Ruteo de requests HTTP	La solución deberá permitir la redirección de peticiones a distintos grupos de origen servers/backend servers dependiendo de: .- prefijo de URI .- HTTP header .- cookie .- metodo HTTP aplicando reglas de WAF por cada ruta, así como reglas de seguridad específicas.
Mitigación de Usuarios Maliciosos	La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos: low, medium, high. Dependiendo del puntaje por los eventos de seguridad de un usuario, la solución debe contar con la capacidad de mitigación

	automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.
Errores de Respuesta Personalizados	La solución deberá permitir crear un mensaje de respuesta personalizado por cada código de error HTTP
Tamaño de los headers	La solución deberá permitir limitar el tamaño de los headers HTTP de los requests/peticiones de los usuarios
Manipulación de Headers	La solución deberá permitir la eliminación o adición de nuevos headers HTTP en las respuestas o peticiones entre el cliente y servidor. Por ejemplo: la solución deberá ser capaz de insertar el header X-Forwarded-For HTTP Header para informar al origen server/backend server de la dirección IP original del request del cliente
CORS	La solución deberá tener la capacidad de proteger contra CORS
GeoIP protection	La solución deberá permitir el control de acceso de los usuarios a la aplicación según el país de origen, permitiendo reglas de allow o deny desde países en específico; por ejemplo: que se permita el acceso solo a un país, y se bloquee el resto.
Service Policies	La solución deberá permitir la creación de reglas de L3, L7 para permitir o negar el acceso a recursos, así como el manejo de los diferentes motores de seguridad para la creación de excepciones.
Protección contra ataques sofisticados o campañas activas	La solución deberá contar con la capacidad de proteger a las aplicaciones contra ataques sofisticados o ataques "In-the-wild" con gran precisión, de manera que la información contextual de esos ataques reales utilizados alrededor del mundo sea empleada para la creación de firmas de WAF en tiempo real.

API Security	
Funcionalidad	**Descripción**
Monitoreo y Protección de APIs	La solución deberá tener la capacidad de monitorear y proteger las APIs tan cerca del origen como sea posible. Además, la solución debe brindar esta capacidad utilizando el mismo motor de protección tanto en el propio cloud, como en clouds públicos/privados y en las premisas.
API Anomaly Detection	La solución deberá contar con un mecanismo de análisis de comportamiento de las peticiones/request hacia cualquier de los API endpoints definidos, permitiendo la detección de anomalías por petición/request.
API Discovery	La solución deberá contar con la capacidad de aprender/determinar todos los API endpoints que son accedidos, incluyendo petición y respuesta, y detectando información sensible. Además, debe proveer la vista de API endpoints en inventario, shadow y descubiertas y generar un Probability Distribution Function (PDF) para las métricas relacionadas a cada endpoint. Dicho análisis debe ser generado de forma periódica, y los PDFs ser actualizados de acuerdo a eso.
Sensitive Data	La solución deberá contar con la capacidad de identificar y localizar la información sensible en las peticiones desde los clients y en las respuestas de los API endpoints. Deberá identificar PII, tal como números de tarjeta de crédito y numero de seguridad social e indicar el parámetro/campo donde la información esta localizada.
API Endpoint Learning	La solución deberá contar con un mecanismo que permita el descubrimiento dinámico de las APIs, determinar cuáles endpoints deberían ser utilizados y permitir únicamente estos API endpoints, obtener información de la utilización, como tamaño de las peticiones y frecuencia. Asimismo, la solución deberá proporcionar las siguientes métricas: tamaño de la petición/respuesta, latencia con datos y latencia sin datos, frecuencia de peticiones, frecuencia de errores, troughput de las respuestas.
API Schema Learning	La solución deberá aprender la estructura del esquema de las APIs, analizando los requests/peticiones y respuestas para cada una de ellas. Asimismo, deberá permitir la descarga del swagger file aprendido.
Importación de especificación (Swagger file)	La solución deberá permitir la importación de las especificaciones del API contenidas en un archivo Swagger.
API Authentication Discovery	La solución debe contener sensores integrados para la detección de tipos de autenticación, y localización en las llamadas API. Una vez detectados, se deben asociar con un edpoint y mostrar un estado de autenticación.

JSON Web Token Discovery	La solución deberá ser capaz de descubrir el header, payload y firma de JWTs así como la identificación de campos utiles para el cliente, permitiendo la identificación de datos sensibles en los payloads de JWT así como la definición del score de riesgo.
Detección de Usuarios Maliciosos	La solución debe contar con un motor de WAF que permita realizar un perfilamiento de usuarios, utilizando: la cantidad de firmas identificadas, cantidad de accesos prohibidos, errores de login, tasa de errores.
Mitigación de Usuarios Maliciosos	La solución deberá realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos, low, medium, high y dependiendo del puntaje por los eventos de seguridad de un usuario, realizar una mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JavaScript o CAPTCHA.
Control sobre el número de peticiones Rate Limit L7	La solución deberá controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre endpoints específicos.
API Security	La solución deberá permitir la carga de archivos Swagger para cada versión de la API, controlando el modo de consumo de los endpoints por frecuencia o método HTTP. Donde todo lo que no se encuentra dentro de la definición de Open API (swagger file) (o explícitamente permitido) sea bloqueado. La solución deberá permitir la creación de políticas de seguridad, donde se contemplen excepciones que permitan el acceso a usuarios específicos dentro de API end points o grupos de API.
Manejo versionamiento de definición de APIs	La solución deberá permitir la carga de distintos archivos Swagger, dependiendo de la versión de la API a proteger, y añadir la definición en distintos segmentos dentro del balanceador.
Cookie Protección	La solución deberá realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTPOnly y Secure, en las respuestas de cookies. Además, deberá permitir habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticación.
GraphQL Inspection	La solución deberá permitir la definición del API endpoint, así como los métodos de HTTP que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando introspección, de los recursos, disponibles en el esquema actual.
API Discovery	La solución debe disponer de una función de descubrimiento de API que lea e identifique los API endpoints en el repositorio de código.
	La solución debe tener una función de descubrimiento de API que lea e identifique los puntos finales de API de dominios externos, rastreando los dominios externos.

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

	Vulnerable and Outdated Components Identification and Authentication Failures Software and Data Integrity Failures Security Logging and Monitoring Failures Server-Side Request Forgery (SSRF)
Tipos de servicios	La solución de seguridad debe realizar scans y servicios de recon.

GARANTÍA TÉCNICA Y SERVICIO

- Garantizar soporte del fabricante 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante.
  . El soporte del fabricante deberá incluir:
  - Soporte vía correo electrónico
  - Soporte vía telefónica
  - Recepción de alertas, mensajes o noticias sobre las actualizaciones del servicio durante el periodo contratado.
  - Ningún límite en la cantidad de apertura de casos, incidentes, solicitudes, requerimientos, consultas, soporte técnico, resolución de problemas.
- Soporte 7x24 durante (2) años a partir del 06 de octubre de 2025 o fecha que indique la plataforma o documento del fabricante.
  . El soporte debe incluir:
  - Apoyo en nuevas configuraciones.
  - Atención de incidentes (correo electrónico, teléfono, mesa de ayuda).
  - Instalación de nuevas actualizaciones (si aplica)
  - Un mantenimiento general en el año.
  - Atención de casos de carácter técnico en temas funcionales de las diferentes aplicaciones las cuales estén siendo protegidas en la presente solución.

  Si en el lapso de cuatro (04) horas después de haber reportado el incidente no se ha dado una solución definitiva al mismo, se deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. (tiempos de respuesta).
- El servicio de soporte se podrá brindar a través de herramientas de servicio remoto, o también en sitio en la ciudad de Bogotá.
- El servicio de soporte brindado deberá indicar procedimiento de escalamiento si es necesario (se *llevará a cabo por medio de un Ticket de servicio para los incidentes presentados)*.
- Se debe tener una atención ilimitada a casos reportados por el COGFM, referentes a cualquier evento relacionado con el funcionamiento, administración, incidentes o eventos de seguridad de los sistemas, equipos o plataformas descritas en el presente anexo, hasta dejar en normal y completo funcionamiento el sistema o herramienta de ciberseguridad.

ALCANCE GARANTÍA TÉCNICA

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

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

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

Estos mantenimientos deben incluir como mínimo las siguientes actividades:

- Actualizaciones y Parches de Seguridad
- Aplicación de actualizaciones y parches de seguridad críticos en el WAF.
- Revisión periódica de las nuevas versiones del WAF y su impacto en la configuración actual.
- Revisión y Solución de Errores
- Monitoreo y resolución de errores o fallos en las reglas de seguridad.
- Identificación y mitigación de falsos positivos y falsos negativos en la protección del WAF.
- Copias de Seguridad y Recuperación
- Programación y validación de copias de seguridad de configuraciones y reglas de seguridad.
- Plan de recuperación en caso de incidentes o errores de configuración.
- Monitoreo y Análisis de Logs
- Revisión periódica de logs de actividad y eventos de seguridad.
- Generación de reportes sobre ataques detectados y acciones de mitigación aplicadas.
- Optimización de Recursos
- Análisis del consumo de recursos en la nube y optimización de configuraciones.

- Ajustes en las reglas de caching y mitigación de ataques para mejorar la disponibilidad y rendimiento del servicio.
- Desactivación de Funcionalidades Inoperativas
- Identificación y eliminación de reglas o configuraciones obsoletas o ineficaces.
- Mantenimiento de una configuración optimizada basada en buenas prácticas.
- Procedimientos de Hardening
- Implementación de medidas de refuerzo de seguridad recomendadas por los principales proveedores de WAF en la nube.
- Configuración avanzada de mitigación de amenazas (Rate Limiting, Bot Management, Geo-blocking, etc.).
- Nuevas implementaciones.

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

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

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

FUNCIONAMIENTO Y CONTINUIDAD

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

ACTUALIZACIONES

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

REPORTES E INFORMES TÉCNICOS

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

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

SEGURIDAD

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

del desarrollo del proyecto por parte de la empresa contratista seleccionada, lo cual será verificado por el supervisor del contrato. Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares. El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO
El contrato debe ejecutarse a todo costo, el contratista se compromete a realizar la suscripción con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad. El contratista deberá realizar transferencia de conocimiento y entrenamiento como mínimo de 20 horas, en el manejo y administración de la plataforma de protección de aplicaciones web, Adicionalmente suministrar el respectivo voucher para presentar examen de certificación como técnico especialista ante el fabricante de la solución de seguridad, para tres (03) funcionarios del CGDJ6, sin que este ofrecimiento genere costo adicional para el COGFM. Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma de actividades para la ejecución del objeto del futuro contrato, para aprobación del supervisor del contrato.

- LOTE 6: SUSCRIPCIÓN PARA ACCESO SEGURO DE TI.

ÍTEM No.	DESCRIPCIÓN DEL BIEN / SERVICIO	UNIDAD DE MEDIDA	CANTIDAD
1	Suscripción de licenciamiento SASE, incluyendo (acceso de red de zero confianza (ZTNA), protección de amenazas sobre dispositivos móviles (MTD), acceso seguro para dispositivos no gestionados (Enterprise Browser) por un periodo de tiempo de 2 años.	UNIDAD	100

ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO
El presente ítem tiene como objetivo la contratación de la suscripción del licenciamiento SASE, incluyendo su instalación, configuración, soporte y garantía. Este proceso abarcará todos los elementos necesarios, así como los servicios relacionados, garantizando una implementación completa y efectiva. El propósito es asegurar su puesta en funcionamiento al 100%, garantizando alta disponibilidad y el correcto desempeño de la solución en las aplicaciones e infraestructura del COGFM.
REQUERIMIENTOS GENERALES DE LA SOLUCIÓN SASE
• La solución deberá estar licencianda para 100 usuarios por un periodo de tiempo de dos (2) años a partir de la activación, en un esquema 24x7x730 por parte del fabricante. • Plan de soporte 7x24, permitiendo la apertura de casos de soporte por medio de los canales de atención y el acceso a soporte por parte de ingenieros especializados de segundo nivel. • La solución ofertada deberá ser de licencia exclusiva del COGFM, no se aceptarán soluciones de uso compartido, licenciamiento open source y reúso de licenciamiento. • La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada. • La solución ofertada debe ser propiedad y operada como un servicio en la nube (SaaS) • La solución debe tener más de 80 puntos de presencia (PoPs)a nivel Global en 44 data centers • La solución debe manejar su infraestructura en la nube del fabricante • La solución propuesta debe proporcionar políticas de confianza cero basadas en la identidad del usuario y la postura del dispositivo • La herramienta debe posibilitar la invitación de usuarios vía correo electrónico • La solución debe incluir los siguientes tipos de autenticación para la administración: - SAML 2.0 - Azure AD/Entra ID - OKTA

- Google Workspace
- Directorio Activo en Premisa
- Usuario / Password locales

- La solución debe ofrecer mecanismos para garantizar doble factor de autenticación, al menos para:
  - Microsoft Authenticator
  - Google Authenticator
- La arquitectura del Servicio SASE debe ser Full Mesh es decir, garantizar la conectividad en la que todas las ubicaciones, usuarios y recursos pueden comunicarse directamente entre sí, sin necesidad de pasar por un nodo centralizado.
- La solución ofertada deberá poder integrarse con las plataformas de Ciberdefensa Avanzada y Analítica Avanzada, con fin de contribuir a la convergencia de información de brechas y apoyar tareas de identificación de riesgos y automatización de respuestas en caso de incidentes de seguridad.
- Debe contar con su propia solución de Threat Intelligente con Inteligencia Artificial.
- Debe contar con asistentes de Inteligencia Artificial generativa en la misma consola.
- Debe contar con su propia solución de gestión de IoC central con soporte de integrar IoC de Terceros.
- Debe contar con su propia solución para gestión de eventos unificados con todas las soluciones del fabricante y de terceros que sean integrados.

Zero Trust Network Access (ZTNA)

- La solución ofertada debe ser propiedad y operada como un servicio en la nube para garantizar una mejor experiencia del usuario final y proteger a los usuarios autorizados que acceden a los servicios que se ejecutan en nubes públicas o privadas.
- Garantizar el acceso a los aplicativos internos basado en el modelo de Zero Trust (Zero Confianza) tanto para usuarios de la entidad y/o terceros, aun si no hay control de seguridad sobre sus dispositivos.
- La solución ofertada debe ser propiedad y operada como un servicio en la nube para garantizar una mejor experiencia del usuario final y proteger a los usuarios autorizados que acceden a los servicios que se ejecutan en nubes públicas o privadas.
- Proporcionar controles críticos y consolidados para el uso seguro de los servicios en la nube, incluida la visibilidad, la aplicación del cumplimiento, la seguridad de los datos y la protección contra amenazas.
- Debe permitir el acceso remoto seguro, para dispositivos que no son administrados, sin la necesidad de la instalación de un cliente, pero midiendo su postura de Seguridad.
- Para el acceso contratistas, proveedores y demás terceros, el acceso debe ser a través una solución de proxy reverso, a través de URLs y con la opción de manejo de certificados.
- Para el acceso sin agente (vía portal) deben poderse realizar los siguientes accesos:
  - SSH
  - RDP
  - VNC
  - WEB
- La plataforma debe soportar RDP nativo o solo con RDP a través de HTTPS.
- La solución debe soportar tener múltiples métodos de conexión estándares entre el DataCenter y de las oficinas a la nube y PoP (Punto de Presencia):
  - IPSEC
  - Wireguard
  - OpenVPN
- Debe permitir la conexión a recursos privados vía TCP/UDP/ICMP,FQDNs.
- La conexión de dispositivo de usuario final puede ser con agente o sin agente.
- El acceso a las aplicaciones desde el borde/perímetro se hace a través de túneles.
- La solución debe permitir mantener el túnel siempre conectado y puede desconectarse si está dentro de la red de la oficina.
- Las aplicaciones sin agentes se pueden definir con alias de dominio privado para facilitar el acceso al usuario.
- La solución sin agente debe proporcionar la separación de las credenciales de acceso reales de las credenciales de acceso del usuario final.
- Gestión de certificados: La solución debe permitir administrar certificados de dominio para el acceso fácil de usuario asociado al dominio a aplicaciones sin agentes.
- La plataforma debe permitir el túnel dividido (Split Tunneling), incluidas las opciones de inclusión/exclusión y la compatibilidad con IP y FQDN.
- Soportar la función "Always On" para el acceso basado en agentes y su implementación.
- La solución debe proporcionar direcciones IP estáticas privadas para cada Tenant.
- La solución debe soportar conectividad de malla completa: cualquier sitio interno conectado puede comunicarse con cualquier otro sitio y usuario remoto. Cualquier usuario remoto puede conectarse a cualquier sitio interno conectado
- Debe permitir definir múltiples entornos de red en el mismo sistema de gestión con los GW de acceso y el enrutamiento separado para el acceso de los usuarios y data center al servicio en la nube.
- Debe permitir gestión de acceso del usuario basado en identidad de usuarios individuales y grupos de usuarios.

- Los administradores deben permitir el acceso a redes solo desde dispositivos que cumplan con una o más de las siguientes políticas:
  - La presencia de un antivirus específico
  - Si el dispositivo está cifrado.
  - Si un dispositivo posee el certificado definido por el administrador
  - Si un Proceso especifico está en ejecución:
  - verifica una clave de registro específica
  - Si está en dominio de inicio de sesión
  - Si está en una Versión del sistema operativo
- La solución debe evaluar las siguientes características de postura en los dispositivos Windows:
  - La presencia de un antivirus, trabajando y actualizado.
  - La solución debe verificar la presencia de algún firewall local o la habilitación del firewall de Microsoft.
  - Debe evaluar la presencia o ausencia de ciertos archivos presentes en la estación de trabajo, para permitir su acceso.
  - Debe evaluar la presencia o ausencia de ciertas llaves y/o valores dentro del registro del sistema operativo.
  - La presencia de un Certificado Digital.
  - Evaluar si el equipo pertenece al Directorio Activo de la entidad.
  - Debe evaluarse la postura del dispositivo antes de la conexión y cada 20 minutos después de autorizada la conexión.
- Al menos los siguientes Antivirus deben ser soportados:
  - Symantec
  - McAfee
  - Crowdstrike
  - Check Point
  - Kaspersky
  - SentinelOne
  - Falcon
  - Bitdefenser
  - Windows Defender
  - Eset
  - Clamav
- Restringir el acceso a través de la verificación de la identidad, el contexto y el cumplimiento de las políticas de los usuarios antes de permitir el acceso y durante la sesión misma, en intervalos de 20, 40 o 60 minutos
- La herramienta debe generar un inventario de los dispositivos usados en la conexión, aquí debe incluir la siguiente información:
  - Versión del Sistema Operativo
  - Nombre de la Maquina
  - Versión del Agente ZTNA ejecutándose
  - Estado de la conexión
  - Cumplimiento de la Postura
- La solución se debe poder conectar a dispositivos perimetrales existentes.

AGENTE

- La solución debe garantizar acceso vía agente para los siguientes sistemas operativos:
  - Windows
  - Linux
  - MacOS
  - IOS
  - Android
  - Chromebook
- El Agente la opción de actualizarse automáticamente en los dispositivos de los usuarios.
- El administrador debe controlar las actualizaciones de versiones de los agentes.
- Proporcionar detalles de dispositivos, incluida la visibilidad de los dispositivos conectados, el estado de estado, el número de serie, la ubicación y el estado en línea/fuera de línea.
- Cliente de punto final único (Agente)para acceso "remoto/privado", así como para acceso a Internet.
- capacidad de aplicar diferentes configuraciones en función de los grupos de usuarios, siguiendo una política de primera coincidencia.
- El agente de la solución debe ser capaz de instalarse en remoto en dispositivos que se administran a través de una herramienta de administración de escritorios centralizada (MDM).
- El agente en sistemas operativos Windows debe tener una protección Anti-tamper para no poder cerrar la sesión y no poder ser desinstalado sin código provisto por el administrador de la plataforma.

LOG Y MONITOREO Y REPORTES

- Logs sobre sesiones activas para obtener datos en tiempo real de las sesiones activas actualmente en todas las ubicaciones, agentes y aplicaciones.

- Logs sobre la actividad de miembros que permitan monitorizar los cambios identificando y clasificando todas las actividades de los miembros.
- Logs de la Actividad Web para supervisar las actividades web bloqueadas o advertidas de sus miembros
- Logs de Protección de malware supervisando todo el contenido malicioso bloqueado
- Logs de la Actividad administrativa monitorizando los cambios, identificando y clasificando todas las actividades del administrador.

CUMPLIMIENTO Y SEGURIDAD

- La solución debe alinearse con los estándares que garanticen la protección de la información como SOC 2 Tipo 2, GDPR, e ISO 27001 entre otras.
- Debe ofrecer un SLA de al menos 99.99%.

Acceso seguro para dispositivos no gestionados (Enterprise Browser)

- La solución debe contar con un aislamiento de datos robusto, creando un entorno de navegación seguro que evita el intercambio o filtración no autorizada de información sensible.
- La solución debe contar con una capa de protección para garantice que los datos empresariales permanezcan seguros, sin importar desde dónde se conecten los usuarios ni qué dispositivos utilicen.
- La solución debe permitir aplicar políticas de seguridad dinámicas para todo el tráfico web, protegiendo aún más el acceso tanto a aplicaciones locales como en la nube.
- Capacidad de Aislamiento del contenido web para evitar la interacción directa con datos sensibles.
- Capacidad de Protección contra descargas no autorizadas, acciones de copiar-pegar y compartición de datos.
- Proveer una solución de acceso a Aplicaciones con Confianza Cero (Zero Trust) a través de un navegador empresarial como una puerta de enlace segura de Confianza Cero, con capacidades de prevención de pérdida de datos (DLP).
- Permitir visibilidad completa de las acciones del usuario.
- Permitir la Grabación de sesiones del usuario.
- Permitir Restricciones para copiar, pegar e imprimir.
- Permitir Capturas de pantalla de acciones seleccionadas.
- Permite Monitoreo DLP para interacciones con aplicaciones web, correo electrónico, manejo de archivos y compartición de datos dentro del navegador empresarial.
- Permitir Control estricto del comportamiento del navegador (por ejemplo, restricciones a APIs web, políticas de manejo de archivos, etc.).

MOBILE THREAT DEFENSE (MTD)

- Capacidad para restringir el acceso a red privada o a datos de la organización confidenciales en dispositivos móviles cuando se determina que el dispositivo se encuentra en un estado de riesgo.
- La solución debe detectar y analizar actividades sospechosas, produce una puntuación de riesgo basada en el tipo y la severidad de la amenaza, y determina acciones automáticas de mitigación para proteger dispositivos y datos.
- Visibilidad de las versiones de los sistemas operativos.
- Definición de una versión mínima del sistema operativo sobre la que corran los dispositivos.
- Detección automatizada de sistemas operativos desactualizados para iOS.
- Detección automatizada de sistemas operativos desactualizados para Android.
- Identificar la gravedad de las vulnerabilidades en la flota de dispositivos.
- Configuraciones de dispositivos riesgosas.
- Vulnerabilidades de los sistemas operativos.
- Establece un nivel de riesgo para el dispositivo si no se comunica durante el período especificado en días.
- La solución debe permitir debe permitir políticas de seguridad para:
  - Definición forzosa de contraseña para pantalla de bloqueado
  - Encriptación forzosa de dispositivos
  - Detección de jailbreak/root
  - Detección remota de jailbreak/root
- La solución debe permitir Automáticamente categorizadas Aplicaciones Maliciosas como de alto riesgo y no pueden configurarse.
- La solución debe permitir para aplicaciones con mala reputación o riesgos de seguridad potenciales pueden tener sus niveles de riesgo establecidos por los administradores.
- La solución debe escanear y analizar las aplicaciones móviles para determinar si los permisos de la aplicación móvil son capaces de acceder como calendario o a los datos de contacto.
- La solución debe contar con tecnologías de Anti-Phishing, Navegación Segura, Filtrado de URL y Anti-bot para la Protección de Red en el dispositivo. inteligencia de amenazas con el Motor de Riesgo Conductual para el análisis de aplicaciones.
- Ataques de intermediario en redes celulares y Wi-Fi.
- Ataques de capa de sockets seguros (SSL).
- Puntos de acceso Wi-Fi falsos.

- Detecta intentos de escaneo de puertos abiertos en dispositivos móviles y establece el nivel de riesgo y la política asociada con esta técnica de ataque.
- La solución debe contar con políticas:
  - Controles de privacidad de datos.
  - Políticas personalizables para aplicaciones.
  - Políticas personalizadas para aplicaciones riesgosas.
  - Listas de aplicaciones permitidas/restringidas.
- Protección contra el Phishing de día cero para navegación web desde navegadores móviles.
- Protección contra el smishing para la ingeniería social.
- Bloqueo el acceso a enlaces de phishing en todas las aplicaciones.
- Bloqueo de servidores maliciosos, sistemas de comando y control, y ataques de watering hole.
- Detección impulsada por IA de las últimas amenazas de phishing.
- Controles de privacidad configurables para administradores.
- Privacidad y protección de DNS (SecureDNS).
- Identificación o bloqueo de acceso a contenido para adultos, violento y delictivo.
- Bloqueo sitios que afectan la productividad, el rendimiento y los costos de datos móviles.
- La solución escanea y analiza las aplicaciones móviles para proporcionar informes detallados que incluyen los posibles riesgos de seguridad y privacidad de las capacidades y permisos inherentes de la aplicación.
- Capacidad de integración con soluciones MDM o MAM para establecer políticas basadas en el estado de salud del dispositivo.
- La solución debe permitir la gestión de parches y vulnerabilidades móviles.
- Identificación de los últimos parches y actualizaciones disponibles.
- Identificación de aplicaciones vulnerables y forzar políticas sobre las mismas.
- Notificaciones para que a los usuarios a actualicen aplicaciones vulnerables.
- Búsqueda proactiva de amenazas en el contenido web y las aplicaciones de sus usuarios.
- Investigación para la respuesta a incidentes.

- Capacidad de integración con soluciones MDM o MAM para establecer políticas basadas en el estado de salud del dispositivo:
  - Protección de dual persona de Android Enterprise.
  - Integración de UEM para soporte de MDM y/o MAM.
  - Integración de la gestión de acceso a la identidad (IAM).
- Integración con solución de Detección y respuesta XDR.
- Correlación los IOC de amenazas móviles con los datos de amenazas de la plataforma existentes.
- Integración de API para integrar los datos del móvil a las herramientas de seguridad existentes.
- Integración de gestión de eventos de incidentes de seguridad (SIEM).
- El agente de seguridad único y unificado para MTD y para el Acceso de ZTNA.

GARANTÍA TÉCNICA Y SERVICIO

- El proveedor deberá brindar soporte técnico para la solución de acceso seguro objeto del presente anexo, conforme a los siguientes requisitos:
- El soporte técnico deberá prestarse en modalidad 7x24 (siete días a la semana, 24 horas al día), durante un período de veinticuatro (24) meses, contados a partir de la activación de la suscripción. Este servicio estará disponible durante toda la vigencia de la garantía y podrá ser requerido en cualquier momento por el supervisor del contrato o el administrador de la herramienta de seguridad.
- El soporte deberá brindarse de manera inmediata, a través de medios telefónicos o herramientas de acceso remoto, tan pronto se reporte cualquier novedad o incidente y si el incidente no se resuelve de forma definitiva dentro de las cuatro (4) horas posteriores a su notificación, el proveedor deberá desplegar personal técnico especializado para atención presencial en un plazo máximo de dos (2) horas, con el fin de garantizar la pronta solución del problema.
- En caso de requerirse soporte presencial, este deberá prestarse en la ciudad de Bogotá D.C., en las instalaciones del Complejo Militar CAN, sin afectar la continuidad operativa de la solución.
- El servicio de soporte deberá incluir un procedimiento de escalamiento claramente definido, que asegure la atención oportuna y eficiente de los incidentes que no puedan resolverse en el primer nivel de soporte.
- El proveedor deberá ofrecer atención ilimitada a todos los casos reportados por el COGFM, relacionados con fallas de funcionamiento, problemas administrativos, incidentes operativos o eventos de seguridad que afecten la solución.
- La atención deberá mantenerse activa hasta que se restablezca por completo el funcionamiento normal de la solución de ciberseguridad y se garantice su operatividad en condiciones óptimas.

FUNCIONAMIENTO Y CONTINUIDAD

- El contratista deberá entregar la solución de acceso seguro completamente instalada, configurada, integrada y operativa. Esta deberá ajustarse a los requerimientos técnicos definidos por la entidad y el proceso de implementación incluirá, como mínimo:
  - La instalación lógica del software en los entornos definidos (producción, pruebas, respaldo, etc.).

- La configuración personalizada de acuerdo con la arquitectura tecnológica y los protocolos de seguridad establecidos por la entidad.
- La integración con sistemas de información existentes, si así se requiere.
- La ejecución de pruebas funcionales, de rendimiento, interoperabilidad y seguridad.
- Creación de reglas de acceso.
- Configuración de políticas de seguridad.
- La entrega de un informe de resultados de las pruebas, con la validación correspondiente del supervisor del contrato.

- El contratista garantizará el funcionamiento estable y continuo de la solución, asegurando que no se presenten interrupciones atribuibles a fallas de configuración, errores del sistema, incompatibilidades o mal desempeño. La solución debe operar conforme a los niveles de servicio y desempeño definidos contractualmente.
- El contratista deberá entregar la solución completamente instalada, configurada y probar su funcionamiento, asegurando que todas las pruebas sean exitosas.

GARANTÍA LEGAL

De acuerdo con lo establecido en los artículos 7, 8, 9 y 11 de la Ley 1480 de 2011. Su período de vigencia será de veinticuatro (24) meses contados a partir de la activación de la suscripción.

Durante este período, el contratista deberá cumplir con los siguientes requisitos:

- Certificación de licencias adquiridas: Se deberá entregar un certificado que evidencie las licencias adquiridas, incluyendo su respectiva clave y las fechas de vigencia.
- Cumplimiento de estándares de calidad: Conforme a lo estipulado en la Ley 1480 de 2011, el productor y/o proveedor tiene la obligación de garantizar la calidad, idoneidad, seguridad y el buen estado y funcionamiento del software.
- Garantía de respaldo por el fabricante: Se deberá asegurar que las licencias estén respaldadas por la casa fabricante del software y correspondan a la última versión disponible en el mercado, conforme a las especificaciones técnicas exigidas.
- Soporte técnico especializado: Se deberá contar con personal técnico capacitado para atender y solucionar los incidentes de soporte reportados.

SEGURIDAD

ACUERDO DE CONFIDENCIALIDAD:

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

OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO

- El contrato debe ejecutarse a todo costo, el contratista se compromete con la instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad.
- El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
- Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
- El contratista deberá entregar los diagramas correspondientes a las conexiones lógicas de la solución de acceso seguro, de acuerdo con el alcance del contrato y la implementación general de la misma.
- El contratista deberá realizar una transferencia de conocimientos de 20 a 40 horas sobre la solución de seguridad implementada en el COGFM, para mínimo dos (02) funcionarios asegurando que el personal designado adquiera las competencias necesarias para gestionar y operar adecuadamente la solución de acceso seguro configurada para la infraestructura tecnológica del COGFM.

CRONOGRAMA

Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma para la ejecución del objeto del futuro contrato, para aprobación del supervisor del contrato.

- LOTE 7: SUSCRIPCIÓN SERVICIO DE VIDEOCONFERENCIA.

ÍTEM No.	DESCRIPCIÓN DEL BIEN / SERVICIO *(1)*	UNIDAD DE MEDIDA	CANTIDAD
1	Suscripción del Licenciamiento de videoconferencia cisco Webex para equipos con aplicación en dispositivos móviles.	UNIDAD	13
ESPECIFICACIONES TÉCNICAS MÍNIMAS DE OBLIGATORIO CUMPLIMIENTO			
1	SUSCRIPCIÓN DEL LICENCIAMIENTO DE VIDEOCONFERENCIA CISCO WEBEX PARA EQUIPOS CON APLICACIÓN EN DISPOSITIVOS MÓVILES		
Debe ser un servicio ofrecido en nube y debe tener la capacidad de tener modelo hibrido. Se debe incluir el licenciamiento para registrar 10 dispositivos Cisco Room Kit Mini de forma nativa por 4 años.			
Se deben incluir 13 licencias que permitan tener de manera simultánea 13 salas de videoconferencia activas, y por 4 años contados a partir de la activación y adicionalmente debe considerar las siguientes especificaciones técnicas:			
. La solución deberá tener su propia aplicación en dispositivos móviles tales como, iPhone, iPad y dispositivos móviles en plataformas como Android, de igual manera en plataformas como PC Windows, Apple Mac, Cromebook e incluso desde navegadores de internet usando exploradores como Google Chrome, Mozilla Firefox, Apple Safari, y Microsoft Edge en computadores con sistema operativo Windows, Mac, o Linux. . La solución deberá tener interoperabilidad con dispositivos de sala de videoconferencia del mismo fabricante, así como de terceros que estén basados en estándares base abiertos de video SIP o H.323 directamente conectándose a la nube sin necesidad de implementar equipo adicional, hardware adicional o software adicional. . La solución debe soportar la integración con plataformas de terceros tales como Microsoft Office 365, Google Calendar y workplace de Facebook. . Cada una de las 13 licencias deberá permitir organizar una sesión de hasta 1000 invitados simultáneos, sea una sesión de reunión, evento o entrenamiento. Dichos invitados no requieren ser usuarios registrados y dicha capacidad deberá ser independiente por cada usuario. . La solución debe permitir la transcripción en vivo y durante la reunión debe poder activarse o desactivarse en cualquier momento de la reunión. . La solución debe permitir subtítulos, los subtítulos proporcionan una mayor accesibilidad para los participantes con problemas de audición, que pueden elegir seguir el texto en el tercio inferior de la pantalla. . La solución debe soportar la grabación de transcripciones. Se debe soportar la habilitación de la grabación durante la reunión para capturar la transcripción posterior a la reunión; el etiquetado del orador dentro de la transcripción debe permite saber exactamente qué fue dicho por quién. . La solución debe permitir la búsqueda entre reuniones, dando la posibilidad de que después de la reunión, se puedan buscar todas las transcripciones de la reunión con palabras clave. . Agendamiento de sesiones de videoconferencia a través de portal web propio de la solución configurando nombre de la reunión o tema de esta misma, password de la sesión en caso de ser requerido, día, hora, y un apartado donde pueda colocar la lista de correos de los invitados a dicha reunión; en esta ultima el usuario podrá usar la lista del directorio activo. Se deberá tener la opción de guardar los parámetros de la sesión agendada como plantilla para ser utilizada cuando así se requiera. . Posibilidad de agendar sesiones desde la aplicación de video colaboración, ya sea integrado con Microsoft Outlook, Google Calendar o con el planificador nativo de la solución de video colaboración, el cual permitirá al organizador invitar a las personas y seleccionar la hora y este enviará automáticamente un correo electrónico a las personas que fueron invitadas con el detalle de la reunión. . Desde el agendador nativo de la solución, el organizador podrá definir un coanfitrión que sea de la misma entidad, que asista con las labores de control de participantes durante las sesiones, incluyendo la posibilidad para el coanfitrión de: - Comenzar/terminar la reunión - Silenciar a todos o algunos de los participantes - Expulsar asistentes - Iniciar la grabación de la sesión - Bloquear o desbloquear la reunión -Mover a los asistentes desde y hacia la sala de espera virtual. -Unirse al igual que el organizador a las subsesiones para ayudar a los asistentes		

. El organizador de la reunión podrá silenciar el micrófono de los participantes.
. Los participantes podrán acceder a las sesiones en dispositivos Android, Apple, Windows, Mac o a través de navegadores compatibles con WebRTC.
. Los participantes podrán acceder a las sesiones desde dispositivos SIP o H.323.
. Deberá contener una barra de control de funcionalidades:
. Activación y apagado de micrófono.
. Activación y apagado de cámara.
. Compartir contenido
. Icono para ver la lista de participantes
. Antes de comenzar la reunión, la solución deberá contar con la opción de seccionar el tipo de salida de audio desde el computador o desde el dispositivo móvil que se utilizará en la reunión.
. La aplicación de video colaboración deberá permitir acercar o alejar la visualización del contenido compartido para una mejor experiencia del usuario.
. La solución deberá de ser capaz de grabar la sesión teniendo la opción de pausar y reanudar la grabación tanto como se requiera. Las grabaciones quedarán en la nube del fabricante y se podrán descargar si en necesario.
. La solución de video colaboración deberá enviar un correo electrónico al usuario que inicio la reunión con un link y una clave de seguridad (password) para poder visualizar y compartir con los involucrados en la reunión. El máximo de tiempo para poder recibir la grabación al correo será de 24 horas.
. La solución debe permitir compartir contenido en las siguientes modalidades: Compartir todo, el escritorio, el archivo o la aplicación específica.
. La aplicación deberá brindar supresión de ruidos de fondo, eliminación de ruido y mejoramiento del habla tanto en la aplicación de escritorio como en la aplicación de dispositivos móviles y en el dispositivo de videoconferencia.
. La solución debe permitir la asignación de roles de presentador a los invitados que así desee.
. La solución deberá ser capaz de contar con mecanismos que permitan realizar encuestas y compartir cuestionarios en la reunión. Los tipos de encuestas y sondeos deben ser:
. Respuesta opción múltiple.
. Diagrama de opciones donde la opción con más votaciones incrementa de tamaño (Word Cloud)
. Otras como: Quiz, Rating, Texto abierto, Ranking
. Debe permitir al organizador dividir la sesión en sesiones tipo “breakout” o subsesiones seleccionando los participantes de cada una de forma automática o manual.
. La solución de video colaboración deberá permitir a todos los participantes de la sesión personalizar el diseño de vista de video, donde cada participante de la sesión podrá elegir que participante estará con el video en exhibición en la parte principal de la reunión (escenario).
. El organizador o co-anfitron tendrá la opción de sincronizar su vista de escenario con todos los participantes de la sesión durante la duración de la misma.
. La aplicación deberá brindar al usuario la capacidad de reaccionar con emoticones de forma manual o automática, es decir la aplicación deberá reconocer los gestos del usuario como pulgar arriba o pulgar abajo y convertirlos de manera automática en emoticones.
. Las sesiones no deberán tener un límite máximo de tiempo.
. Cada sesión ya sea agendada o en la sala personal de cada usuario, debe contar con una sala de espera virtual, la cual permite al organizador y/o a la coanfitrión aceptar o declinar usuarios que se encuentren en la sala de espera, así como mover participantes de la sesión de video conferencia a la sala de espera virtual.
. La solución deberá permitir la retransmisión en streaming en vivo a Facebook, Youtube y otras plataformas compatibles con RTMP
. El licenciamiento ofertado debe permitir organizar sesiones tipo evento o webinar que permitan un rol adicional de panelista, en dichas sesiones solo los panelistas pueden interactuar en video y audio mientras el resto de los participantes solo actúan de oyentes en la sesión.
. La solución de video colaboración propuesta debe realizar la supresión de sonido de fondo resaltando la voz de la persona que está hablando, esto permite eliminar distracciones sin perder la calidad en el audio y video de la persona que está interviniendo
. La solución de video colaboración debe contar con la posibilidad de unir usuarios externos a la entidad que no están configurados en la plataforma sin necesidad de crear cuentas de invitados manteniendo los niveles de seguridad.
. La Solución de video colaboración debe contar con la posibilidad de hacer la cifrado extremo a extremo de la sesión/audiencia/reunión teniendo la posibilidad de generar las llaves en servidores de la misma entidad. La solución de video colaboración debe poseer la capacidad de optimizar su contenido compartido para texto, imagen o video automáticamente.
. La licencia de registro del equipo de video (Room Kit mini) debe permitir el acceso a la administración web del equipo.
. La licencia de registro del equipo de video debe permitir hacer troubleshooting en tiempo real a las sesiones de video que se están teniendo en el equipo.
. Desde el management del equipo deberá poder tenerse un histórico de las sesiones a las cuales ha participado el equipo de video

. La licencia de registro debe permitir a través de la administración se activen macros en el equipo de videoconferencia.
Se deben incluir los siguientes servicios de implementación: • Configuración Plataforma. • Registro de 10 Webex room kit a nivel nacional de manera remota. • Integración calendario office 365. • Transferencia de conocimiento en Bogotá. • Integración con la plataforma de colaboración de COGFM • Pruebas de funcionalidades de la plataforma y de integración.
PRUEBAS
. El contratista deberá realizar todas las pruebas de funcionamiento necesarias para garantizar que el licenciamiento sea plenamente compatible y operativo con las plataformas de video y voz actualmente implementadas en el Comando General de las Fuerzas Militares. . Se verificará que, una vez instalado el licenciamiento en las cámaras de videoconferencia, estas operen con normalidad. Para ello, se llevarán a cabo pruebas de conectividad, operación, estabilidad, funcionalidad y disponibilidad, con el fin de asegurar su correcto desempeño.
TRANSFERENCIA DE CONOCIMIENTO
El contratista deberá realizar un proceso completo de transferencia de conocimiento sobre el licenciamiento y uso de la herramienta, dirigido a cuatro (4) funcionarios orgánicos del Departamento Conjunto de Comunicaciones. Esta capacitación deberá ser de carácter teórico-práctico, abarcando de manera detallada todos los componentes de hardware y software del sistema de comunicaciones unificadas. El objetivo es que, al finalizar el proceso, el personal capacitado sea plenamente autónomo en: La operación del sistema. El dimensionamiento y configuración de la solución. La detección y resolución de fallas durante su funcionamiento. Actualización de parches o firmware de las cámaras de videoconferencia Con ello, se busca reducir la dependencia de soporte externo y evitar gastos recurrentes en administración y mantenimiento. El contratista asumirá toda la logística necesaria para la ejecución de esta transferencia de conocimiento, sin que ello represente costos adicionales para el Comando General de las Fuerzas Militares.
ALCANCE GARANTÍA TÉCNICA
El término de la garantía técnica (o garantía legal de conformidad con el art. 7º de la Ley 1480 de 2011), de conformidad con el art. 7, 8, 9 y 11 de la Ley 1480 de 2011. Para los servicios prestados será de cuatro (04) años, contados a partir de la activación. Es la obligación, en los términos de la ley 1480 de 2011 de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad, el buen estado y funcionamiento de los productos. Durante este período, el contratista será responsable de atender cualquier falla o inconveniente relacionado con el funcionamiento de las licencias, asegurando su correcto desempeño conforme a las condiciones pactadas. . Las licencias que deberán ser suministradas, probadas y entregadas deberán ser completamente nuevas y de primera calidad, cumpliendo con todas las especificaciones técnicas pactadas en el contrato. . En consecuencia, el contratista se compromete a reemplazar, sin costo adicional, cualquier licencia que presente fallas o deficiencias durante el proceso de instalación, prueba o funcionamiento, garantizando así la continuidad y calidad del servicio. . En caso de presentarse una novedad que requiera cambio o reparación bajo garantía, el contratista deberá, en un plazo máximo de un (1) día calendario, instalar una licencia transitoria con especificaciones y funcionalidades iguales o superiores, que permita suplir la operación del equipo afectado sin afectar la continuidad del servicio. Esta acción deberá realizarse sin costo alguno para el Comando General de las Fuerzas Militares. . El proveedor deberá brindar soporte técnico para la solución de videoconferencia objeto del presente contrato, cada vez que sea requerido por el supervisor del contrato o el administrador de la solución. Este soporte deberá mantenerse activo durante toda la vigencia de la garantía, asegurando la continuidad operativa del servicio y una atención oportuna ante cualquier eventualidad.
SEGURIDAD
ACUERDO DE CONFIDENCIALIDAD: El oferente y todos los colaboradores de la ejecución del contrato se comprometen a firmar acuerdos de confidencialidad y no divulgación de equipos, elementos, configuraciones, cantidad y características de activos en hardware, software e información previos instalados y por adquirir, así como los resultados de los posibles análisis de Malware que serán usados para las pruebas, durante la ejecución del contrato, este se reserva el derecho de admisión del personal que hará del desarrollo del proyecto por parte de la empresa contratista seleccionada, lo cual será verificado por el supervisor del contrato.

Políticas de seguridad informática: El contratista debe comprometerse a conocer, aceptar y ajustarse a las políticas de seguridad de la directiva de seguridad informática de las Fuerzas Militares. El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará.
OTRAS CONDICIONES DE OBLIGATORIO CUMPLIMIENTO
El contrato debe ejecutarse a todo costo, el contratista se compromete a renovar el Licenciamiento con instalación, configuración, implementación y realizar pruebas exitosas de funcionalidad. El Contratista se compromete a cumplir lo expuesto en las políticas y directivas de Ciberdefensa y seguridad de la información del Ministerio de Defensa – Comando General de las Fuerzas Militares, durante el tiempo de ejecución, garantía y soporte que brindará. Es importante aclarar que tanto el personal, como las dedicaciones mínimas del mismo, son de referencia. en todo caso el contratista deberá efectuar el respectivo análisis del pliego de condiciones del proceso y demás documentos que lo componen, y basado en su experiencia deberá determinar el equipo y personal necesario con sus respectivas dedicaciones y cantidades para cada una de las actividades, con el fin asegurar el cumplimiento de los objetivos de los requerimientos de este proceso contractual. Con la presentación de la propuesta, el proponente acepta la información y el alcance del contrato contenido en los documentos mencionados anteriormente, lo que no dará lugar a reclamaciones por parte del contratista durante el desarrollo y ejecución del contrato por tiempos adicionales del personal o equipos.
CRONOGRAMA
Dentro de los primeros cinco (05) primeros días calendario del plazo de ejecución, el contratista seleccionado deberá presentar el cronograma de actividades para la ejecución del objeto del futuro contrato, previa aprobación del supervisor del contrato.

TC. RAMIRO ESTEBAN SILVA GUTIERREZ
Gerente de Proyecto

CT. JORGE ANTONIO GONZÁLEZ
Comité técnico estructurador