MODALIDAD DE CONTRATACIÓN- ACUERDO MARCO DE PRECIOS (Ley 80 de 1.993; Ley 1150 de 2007; Ley 1474 de 2011 y Decreto 1082 de 2015) (Artículo 2.2.1.2.1.2.7 del Decreto 1082 de 2015).
DEPENDENCIA: Oficina de Tecnologías de la Información
FECHA: 21 de marzo de 2024

I. DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD PRETENDE SATISFACER CON LA CONTRATACIÓN

Que el artículo 113 de la Constitución Política dispone que: "(…) *Son Ramas del Poder Público, la legislativa, la ejecutiva, y la judicial. Además de los órganos que las integran existen otros, autónomos e independientes, para el cumplimiento de las demás funciones del Estado. Los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus fines*"

Que el artículo 209 de la Constitución Política establece que: "(…) *La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones*".

Que mediante la Ley 2281 de 2023, se creó el Ministerio de Igualdad y Equidad como organismo principal del sector central de la Rama Ejecutiva en el orden nacional, rector del sector administrativo de Igualdad y Equidad y de sus entidades adscritas o vinculadas, y de los órganos de asesoría, coordinación y articulación señalados legal o reglamentariamente.

Que el Ministerio de Igualdad y Equidad tiene como objeto, en el marco de los mandatos constitucionales, de la Ley y de sus competencias, diseñar, formular, adoptar, dirigir, coordinar, articular, ejecutar fortalecer y evaluar, las políticas, planes, programas, estrategias, proyectos y medidas para contribuir en la eliminación de las desigualdades económicas, políticas y sociales; impulsar el goce del derecho a la igualdad; el cumplimiento de los principios de no discriminación y no regresividad; la defensa de los sujetos de especial protección constitucional, de población vulnerable y de grupos históricamente discriminados o marginados, incorporando y adoptando los enfoques de derechos, de género, diferencial, étnico - racial e interseccional.

Asimismo, mediante el artículo 5° de la Ley 2281 de 2023, establece el ámbito de aplicación del Ministerio, a saber: "(…) en todo el país con énfasis en los territorios excluidos y marginados, protegerá los derechos, con enfoque de género, transversal, focalizado y de empoderamiento de las mujeres y las niñas, diferencial e interseccional, de los sujetos de especial protección constitucional, entre otros: 1. Mujeres en todas sus diversidades. 2. Población LGBTIQ+. 3. Pueblos afrodescendientes, negros, raizales, palanqueros, indígenas y Rrom. 4. Campesinos y campesinas. 5. Jóvenes. 6. Miembros de hogares en situación de pobreza y pobreza extrema. 7. Personas con discapacidad. 8. Habitantes de calle. 9. Población en territorios excluidos. 10. Mujeres cabeza de familia. 11. Adultos Mayores. 12. Familias. 13. Niñez. 14. Población migrante regular, irregular, refugiado, en tránsito y retornado.

Que el Decreto 1075 de 2024 adoptó la estructura del Ministerio de Igualdad y Equidad, definiendo la creación de viceministerios (Viceministerio de las Mujeres, el Viceministerio de la Juventud, el Viceministerio para las Poblaciones y Territorios Excluidos y la Superación de la Pobreza, el Viceministerio de las Diversidades y el Viceministerio de Pueblos Étnicos y Campesinos) encargados entre otros, de diseñar, formular, adoptar, dirigir, coordinar, articular, ejecutar, fortalecer y evaluar las políticas, planes, programas, estrategias, proyectos y medidas para contribuir en la eliminación de las desigualdades económicas, políticas y sociales; impulsar el goce del derecho a la igualdad; el cumplimiento de los principios de no discriminación y no regresividad; la defensa de los sujetos de especial protección constitucional, de población vulnerable y de grupos históricamente discriminados o marginados, incorporando y adoptando los enfoques de derechos, de género, diferencial, étnico - racial e interseccional; así como dependencias adscritas al despacho de la Ministra, orientadas a realizar acciones de apoyo, asesoría en la formulación, ejecución de las diferentes funciones del Ministerio.

Que es de resaltar las funciones asignadas a la Oficina de Tecnologías de la Información, mediante el artículo 9° del referido Decreto 1075 de 2023, la cual tiene como propósito principal aportar en el logro de los objetivos en cada una de las dependencias del ministerio, es responsable de aplicar los lineamientos y procesos de arquitectura tecnológica en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación, soporte especializado y mantenimiento de los equipos, crear y fortalecer los servicios y sistemas de información a cargo del Ministerio de Igualdad y Equidad, puede entonces enmarcarse como una implementación tecnológica, esencial para que la planta de personal pueda cumplir con sus objetivos y promover la misión del Ministerio de lograr una sociedad más equitativa.

Que en el marco de los programas por parte del Ministerio, relacionados con información de población víctima de diferentes formas de violencias, así como población en riesgo, tales como Jóvenes en Paz, el Sistema Nacional de Registro, Atención, Seguimiento y Monitoreo, el Mecanismo articulador para la prevención y atención de violencias por prejuicio contra población LGBTIQ+, y otros que cuentan con información nominal, como el Sistema de Seguimiento y Monitoreo para la superación del hambre y la malnutrición, recopilan, almacenan y administran información sensible, que requiere niveles de protección acordes con la protección de los derechos humanos de las personas que accedan a la respuesta del Ministerio de Igualdad y Equidad. Si bien la mayoría de estos programas actualmente están en diseño, deberán entrar en operación con sus respectivos mecanismos de información, y otros como Jóvenes en Paz, ya se encuentra en implementación, cuya fase de caracterización no se ha iniciado, por cuenta de la necesidad de las herramientas para la protección de los datos que se recopilen.

Que en el Plan Nacional de Desarrollo (Ley 2294 de 2023) se plantea el catalizador 5. "*Fortalecimiento institucional como motor de cambio para recuperar la confianza de la ciudadanía y para el fortalecimiento del vínculo Estado Ciudadanía*" en particular el literal d. "*Gobierno digital para la gente se fortalecerá el Gobierno Digital del país para tener una relación eficiente entre el Estado y el ciudadano, para ello: i) se acelerará la digitalización de trámites y la masificación de servicios ciudadanos digitales. ii) Se tendrán en cuenta los*

desafíos y oportunidades que trae consigo la evolución tecnológica, social e institucional de la identidad digital, con el objeto de crear confianza y una interacción fiable, eficiente y segura entre el Estado y los habitantes del territorio. iii) Se impulsará la modernización de las entidades a través de incentivos para el uso de datos y la adopción de herramientas y tecnologías digitales, así como la implementación de pilotos de compra pública innovadora."

Que para consolidar una cultura digital entre el Ministerio de Igualdad y Equidad y las/los ciudadanas/ciudadanos, se avanzará en la incorporación del componente de transformación digital conforme los estándares establecidos por el Ministerio de Tecnologías de la Información, en la la Ley 1955 de 2019 y demás normas concordantes.

Así las cosas, el artículo 147 de la referida Ley 1955 de 2019, establece que: "(…). *Transformación digital pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. (…)*" y establece los proyectos estratégicos de transformación digital los cuales están orientados a: *"(…) 3. Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información. (…)*".

En el marco de la necesidad de contar con soluciones para la protección de los sistemas de información del Ministerio de Igualdad y Equidad, es oportuno la adquisición de herramientas de ciberseguridad que permitan mitigar la materialización de riesgos cibernéticos sobre la infraestructura de Datacenter (nube privada), conectividad y equipos de cómputo del Ministerio de Igualdad y Equidad.

Esto incluye las siguientes capacidades:

- Proteger los perímetros de la nube privada ante accesos no autorizados.
- Proteger los perímetros de la red interna de la entidad ante accesos no autorizados.
- Protección de servicios web (http, https) publicados en las nubes públicas,
- Monitoreo, correlación, automatización y orquestación de eventos de seguridad y estado de salud de la infraestructura.
- Protección de Kubernetes en las nubes privadas.
- Soluciones de ciberseguridad que ayudan a las organizaciones a detectar, investigar y responder a incidentes de seguridad.
- Soluciones que permitan controlar e identificar el acceso de usuarios a la red, bajo el cumplimiento de parámetros mínimos establecidos por el Ministerio.
- Soluciones de protección, detección y respuesta de la red con inteligencia artificial, análisis conductual y humano para analizar el tráfico de red para que los equipos de seguridad puedan detectar el comportamiento del atacante y remediar la amenaza, proporcionando análisis de tráfico de red basado en archivos, identificación de la

causa raíz, alcance de los incidentes y las herramientas para remediar los incidentes rápidamente.

- Soluciones que permitan monitorear el estado de los servicios informáticos del Ministerio, así como la correlación de eventos de seguridad y respuesta automatizada ante incidentes cibernéticos.
- Herramientas de protección de seguridad para el servicio de correo electrónico diseñado para proteger contra spam, malware, phishing, y otras amenazas de seguridad del correo electrónico.

En consecuencia, el presente documento contiene la justificación y anexos que sirven de fundamento para la emisión de la orden de compra bajo el amparo del INSTRUMENTO DE AGREGACIÓN DE DEMANDA de Colombia Compra Eficiente CCE-139-IAD-2020, vigente hasta el 31 de marzo de 2024, con una vigencia máxima para la ejecución de órdenes de compra hasta el 30 de septiembre de 2024.

https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/software-por-catalogo

De otra parte, teniendo en cuenta que es obligación de las entidades del orden nacional y territorial efectuar las compras a través de esta modalidad, el Ministerio de Igualdad y Equidad realizará la adquisición de una licencia SaaS (Software como Servicio) requerido por medio del Acuerdo Marco de Precios mencionado.

Por consiguiente, el objeto del instrumento de agregación de demanda es establecer las condiciones para la adquisición de software por catálogo al amparo del instrumento de agregación de demanda; por parte de los proveedores vinculados; las condiciones para la adquisición de software por catálogo por parte del Ministerio como Entidad compradora; y las condiciones para el pago del software por catálogo por parte de las entidades compradoras.

Así las cosas, mediante este instrumento de agregación de demanda se proporciona el derecho de uso de los productos de seguridad, con el objetivo de abastecer en la Entidad una solución específica o el servicio que deba renovar. El instrumento no pretende proporcionar un entorno para la venta de proyectos o desarrollos, razón por la cual este tipo de servicios no están incluidos. Las entidades que requieran implementar una solución basada en productos de seguridad definidos en los catálogos del instrumento deben contratarla a través de la modalidad que consideren más apropiada por fuera del instrumento; sin embargo, existen algunos servicios básicos que son indispensables para el funcionamiento de los productos de seguridad por catálogo, razón por la cual hacen parte integral del instrumento de agregación de demanda.

En este sentido, se da cumplimiento al Decreto Ley 4170 de 2011, que creó la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente –, con el objeto de impulsar políticas públicas y herramientas orientadas a la organización y articulación de los partícipes en los procesos de compras y contratación pública, con el fin de lograr una mayor eficiencia, transparencia y optimización de los recursos del Estado y que dentro de las funciones

asignadas a Colombia Compra Eficiente, deberá “diseñar, organizar y celebrar los Acuerdos Marco de Precios y demás mecanismos de agregación de demanda de que trata el artículo 2º de la Ley 1150 de 2007, de acuerdo a los procedimientos que se establezcan para el efecto”.

Que los numerales 1, 3, 4, 7 y 8 del artículo 12 del Decreto Ley 4170 de 2011, asigna como funciones de la Subdirección de Negocios, adelantar estudios de mercado sobre las compras y contratación pública; identificar y promover mecanismos de adquisición y agregación de demanda dirigidos a la eficiencia y celeridad en las compras y contratación pública; diseñar, organizar y celebrar los acuerdos marco de precios y promover y desarrollar los procesos de selección para la celebración de los acuerdos marco de precios y demás mecanismos de agregación de demanda, a cargo de la agencia; desarrollar mecanismos que permitan una mayor y mejor participación de oferentes en los procesos de compras y contratación pública; y diseñar parámetros que permitan a las entidades estatales definir adecuadamente los bienes y servicios de características técnicas.

En este sentido teniendo en cuenta que Colombia Compra Eficiente adelantó el estudio de mercado, elaboró estudios y documentos previos que recogen el trabajo de planeación del proceso de contratación e invitó a vincularse al instrumento de agregación de demanda contenido en los documentos del proceso a todos los proveedores, el presente proceso de contratación deberá realizarse a través de dicho instrumento de Agregación de Demanda por catálogo a través de la plataforma dispuesta para tal fin por Colombia Compra Eficiente, para lograr los objetivos mencionados, puesto que el Ministerio de Igualdad y Equidad como Entidad Estatal requiere la protección contra ataques cibernéticos para los sistemas de información alojados en el Datacenter (nube privada), protección para la red de datos y equipos de cómputo del Ministerio.

Así las cosas, dentro del instrumento de Agregación de Demanda por Catálogo de Software, se identificó que se cuenta con un único fabricante que ofrece una solución SaaS (Software como servicio) y que cumple con los criterios para la protección de la red de datos, correo electrónico y los equipos de cómputo lo cual satisface los altos estándares de seguridad requeridos.

Así las cosas, el proceso de contratación, al realizarse a través del instrumento de Agregación de Demanda por Catálogo de Colombia Compra Eficiente, no solo cumple con los objetivos de eficiencia y transparencia, sino que también respalda al Ministerio de Igualdad y Equidad en su misión de proteger su capital informático contra cualquier forma de ataque cibernético-, lo que adicionalmente, resulta coherente con los principios rectores de Colombia Compra Eficiente y con la responsabilidad del Ministerio de salvaguardar su infraestructura tecnológica.

Por lo anterior, dentro de las necesidades que tiene identificadas el Ministerio de Igualdad y Equidad para mitigar los riesgos de seguridad de TI, a continuación se relaciona los requisitos técnicos y tecnológicos que debe contemplar el servicio a contratar:

El Servicio debe contemplar:

1. Monitoreo continuo: para detectar actividades maliciosas y otras amenazas a la seguridad.
2. Alertas de seguridad: para notificar a los administradores de seguridad sobre posibles amenazas.
3. Capacidad de respuesta: como la contención de incidentes y la remediación, que pueden incluir aislar un endpoint de la red o eliminar malware.
4. Recopilación de datos: Agrega datos de registros (logs) de muchos sistemas diferentes dentro de la entidad, incluyendo dispositivos de red, sistemas de seguridad, servidores, bases de datos y aplicaciones.
5. Consolidación y análisis: Normaliza y analiza los datos recopilados para identificar tendencias y patrones que puedan indicar una amenaza o un incidente de seguridad.
6. Detección de amenazas: Utiliza reglas, correlaciones, y, en algunos casos, inteligencia artificial y aprendizaje automático para identificar actividades sospechosas o anómalas que podrían sugerir una amenaza de seguridad.
7. Capacidad para manejo centralizado de logs y análisis en la nube.
8. Integración con los tipos de log y servicios de detección de amenazas.
9. Herramientas para gestión de acceso a la red y soporte para políticas de acceso granulares.
10. Acceso a expertos técnicos y soporte con tiempos de respuesta rápidos.
11. Capacidad de red y gestión para soportar hasta 500 endpoints concurrentes.
12. Integración con Microsoft Office 365 (para el correo electrónico)
13. Capacidad de soporte de seguridad de correo electrónico para 101-1000 buzones.
14. Soporte y capacidad para la detección y respuesta en endpoints, incluyendo la gestión de hasta 25 de ellos.
15. Soporte y recursos para optimizar el rendimiento hasta 1,000 endpoints o usuarios.
16. manejar al menos 50 dispositivos, con cada uno procesando hasta 10 eventos de seguridad por segundo.

Teniendo en cuenta lo anterior, el Ministerio de Igualdad y Equidad, requiere adquirir las siguientes soluciones de ciberseguridad para la protección del Datacenter en nube privada, correo electrónico, red y equipos de cómputo de la sede principal y servicios asociados para la implementación y soporte.

- Subscriptions license for FortiGate-VM (16 CPU) with UTP Bundle included:

  Esta solución es de vital importancia dado que se enfoca a la base de la seguridad perimetral de próxima generación que brinde la protección, control y seguridad en las conexiones entre las redes corporativas y el acceso a y desde internet, con el fin de proteger la entidad, se requiere de una solución que proporcione protección contra amenazas y descifrado líder en la industria a escala con una arquitectura ASIC personalizada. También debe ofrecer redes seguras con funciones integradas como SD-WAN, conmutación e inalámbrica, y 5G. debe permitir converger sus soluciones de seguridad con y punto de red en una consola de administración

centralizada y fácil de usar potenciada por un único sistema operativo y facilite la administración de TI.

- FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service:

  Necesaria para la gestión centralizada de registros (logs) y análisis en la nube. Ofrece una visión integral y detallada de la seguridad de la red y los eventos, facilitando a la entidad la detección de amenazas y la respuesta a incidentes.

- FortiNAC Control and Application next-gen VM Server (VMWare/Hyper-V/AWS/Azure/KVM).

  Control y visibilidad completos sobre todos los dispositivos conectados a la red de la entidad:

  Control: FortiNAC permitira a la Entidad controlar el acceso a su red. Puede identificar y clasificar automáticamente todos los dispositivos que intentan conectarse a la red, asegurándose de que solo los dispositivos autorizados puedan acceder a los recursos de la red.

  Application next-gen: Esto se refiere a que FortiNAC utiliza aplicaciones de última generación para gestionar el acceso a la red. Esto incluye características modernas como la integración con soluciones de seguridad de terceros, soporte para políticas de acceso granulares y la capacidad de adaptarse a las cambiantes demandas de seguridad.

  VM Server (VMWare/Hyper-V/AWS/Azure/KVM): FortiNAC está disponible como una Máquina Virtual (VM) que puede ser implementada en diversos entornos de virtualización como VMware, Hyper-V, y también en servicios de nube pública como Amazon Web Services (AWS), Microsoft Azure y plataformas que soportan el hipervisor KVM. Esto ofrece flexibilidad para que la Entidad implementen FortiNAC de una manera que mejor se ajuste a su infraestructura existente o futura.

  La combinación de estas características permite proporcionar una seguridad de red robusta y adaptable, garantizando que sólo los dispositivos autorizados y conformes con las políticas de seguridad puedan acceder a la red y sus recursos, lo que reduce el riesgo de brechas de seguridad y mejora el cumplimiento normativo.
- FortiCare Premium Support:

  Se tendrá acceso directo a expertos técnicos: acceso directo a un equipo de expertos técnicos que conocen profundamente los productos del fabricante

Tiempo de respuesta más rápido: Las solicitudes de soporte bajo el servicio premium tienen tiempos de respuesta garantizados más rápidos, lo cual es crucial en situaciones de emergencia.

- FortiNAC Subscription Visibility+Control (PLUS) License for 500 concurrent endpoints. MOQ 500:
  Visibility: Permite a los administradores de red obtener visibilidad completa de todos los dispositivos conectados a la red en tiempo real. Esto incluye dispositivos IoT, dispositivos móviles, usuarios y sistemas operativos.

  Control: Proporciona herramientas para controlar el acceso a la red de los dispositivos detectados. Puede incluir la capacidad de autorizar, bloquear o limitar dispositivos según políticas de seguridad.

  500 concurrent endpoints: La licencia permite la gestión de hasta 500 dispositivos o puntos finales que pueden estar activos y conectados a la red al mismo tiempo.

- FortiMail Cloud - Gateway Premium w. Office365 API support (101-1000 mailboxes). Price per mailbox

  El servicio FortiMail Cloud - Gateway Premium con soporte para la API de Office 365 es una solución de seguridad de correo electrónico que está diseñada para integrarse con Microsoft Office 365. Este servicio está enfocado en brindar protección adicional contra amenazas y ataques dirigidos a buzones de correo electrónico:

  Integración con Office 365: Utiliza APIs específicas de Office 365 para una integración más profunda y para proporcionar seguridad adicional sobre las características que ya ofrece Office 365.

  Protección de correo electrónico: FortiMail Cloud proporciona filtrado de spam, protección contra malware, phishing y ataques dirigidos, así como prevención de pérdida de datos (DLP) y encriptación de correo electrónico.

  Escala de 101-1000 buzones: cubre entre 101 y 1000 buzones de correo, lo que la hace adecuada para la Entidad.

  Teniendo en cuenta que la Entidad cuenta con la suite de Microsoft E5 office 365, el uso de este servicio puede ayudar a cumplir con regulaciones de cumplimiento al MSPI, mejorar la seguridad de su correo electrónico y proteger contra amenazas avanzadas que podrían eludir las protecciones estándar de Office 365. Además, el soporte de API para Office 365 puede permitir una integración más fluida y funciones de administración mejoradas directamente dentro del entorno de Office 365.

- FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 25 endpoints

El servicio "FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 25 endpoints" es una solución de seguridad integral que combina varias capacidades y soporte para la protección de endpoints en una red y que incluye cada componente:

- FortiEDR (Endpoint Detection and Response):

  Discover: Tiene la capacidad de identificar y catalogar todos los activos de endpoint en una red, proporcionando visibilidad completa de los sistemas conectados.
  Protect: Protección en tiempo real contra amenazas conocidas y desconocidas, incluyendo malware y ataques de día cero, utilizando técnicas avanzadas como machine learning y comportamiento de análisis.
  Respond: Herramientas y flujos de trabajo para responder rápidamente a incidentes de seguridad detectados, lo que puede incluir aislamiento de endpoints, remediation, y análisis forense.

- Standard MDR (Managed Detection and Response) Cloud Subscription:

  Contempla servicios gestionados para la detección y respuesta a amenazas que típicamente incluyen monitoreo 24/7, análisis de seguridad, y respuesta a incidentes por parte de expertos en seguridad del fabricante.

- FortiCare Premium Support:

  Soporte avanzado para 25 endpoints, incluye acceso a asistencia técnica, tiempos de respuesta garantizados, y opciones de reemplazo de hardware acelerado y recursos de formación.

- FortiEDR Best Practice Service for up to 1,000 Endpoints/users

  Esta solución incluye:

  - Best Practice Guidance: Asesoramiento para configurar y mantener FortiEDR, asegurando que la solución esté optimizada para la detección y respuesta a amenazas avanzadas en hasta 1,000 endpoints o usuarios.

  - Configuration Assistance: Ayuda en la configuración inicial de FortiEDR para alinearla con las políticas de seguridad específicas de la Entidad y para asegurarse de que todos los endpoints están protegidos eficazmente.

- Ongoing Support: Soporte continuo para garantizar que la solución FortiEDR sigue las mejores prácticas a medida que evolucionan las amenazas y cambian los entornos de TI.

- Training Resources: Recursos de formación para que los equipos de seguridad estén actualizados en el uso de FortiEDR y en las estrategias de respuesta ante incidentes.

- Performance Optimization: Monitoreo y ajuste de la solución para mantener el rendimiento óptimo a medida que cambia el entorno de amenazas y se agregan o eliminan endpoints.

Este tipo de servicio es vital para maximizar la efectividad de las soluciones de seguridad, ya que no basta con tener las herramientas; también es esencial que estén configuradas y se utilicen correctamente para proporcionar la máxima protección. La entidad podrá beneficiarse de la experiencia y conocimiento del fabricante para asegurar que están siguiendo las mejores prácticas y obteniendo el mayor rendimiento de su inversión en seguridad de endpoints.

- Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support

  La licencia permite la gestión de al menos 50 dispositivos en donde cada dispositivo puede procesar hasta 10 eventos de seguridad por segundo, Los eventos por segundo es una medida común en las operaciones de seguridad, especialmente en la gestión de información y eventos de seguridad (SIEM), donde se recopilan y analizan grandes cantidades de datos de registro en tiempo real.

- FortiCare Premium Support (1 - 50 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.
  Proporciona visibilidad integral y capacidades de respuesta automatizadas a través de la infraestructura de TI de la Entidad, combinando capacidades de SIEM y gestión de la respuesta ante incidentes.

  La asignación de puntos funciona de la siguiente manera:

  - 1 "Device": La gestión de un dispositivo de red, como un firewall o un switch, equivale a 1 punto en el sistema de soporte.

  - 2 "End points": Dos endpoints, que podrían ser estaciones de trabajo o servidores, valen 1 punto.

  - 3 "Advanced Agents - Log & FIM": Tres agentes avanzados, que ofrecen funcionalidades como registro (Logging) y monitoreo de

integridad de archivos (File Integrity Monitoring - FIM), también equivalen a 1 punto.

- 10 "Advanced Agents - UEBA Telemetry": Diez agentes avanzados que proporcionan telemetría para la analítica de comportamiento del usuario y entidades (User and Entity Behavior Analytics - UEBA), valen 1 punto.

Este sistema de puntos permitirá a la Entidad personalizar su nivel de soporte según sus necesidades específicas y el tamaño de su despliegue. Los clientes pueden elegir añadir más puntos para cubrir dispositivos adicionales, endpoints o capacidades de agentes avanzados dentro de su entorno de FortiSIEM.

- Configuración y parametrización de los Productos, Paquete de 20 horas (configuración de Herramienta Básica) Servicio ejecutado por profesional especialista certificado NSE4 Bolsa de 20 Horas

  Corresponde al paquete de soporte técnico, que incluye un total de 20 horas de trabajo por parte de un profesional con certificación NSE4 (Network Security Expert Level 4). La certificación NSE4 indica que el técnico tiene un conocimiento avanzado de los productos de seguridad y está capacitado para configurar y parametrizar dichos productos:

  - Configuración y Parametrización: Configuración inicial y la parametrización de los productos, esto involucra la configuración de firewalls, switches, puntos de acceso inalámbrico, y otras soluciones de seguridad de la red.

  - Configuración y parametrización de los Productos, Paquete de 20 horas (configuración de Herramienta Avanzada) Servicio ejecutado por profesional especialista certificado NSE5 Bolsa de 20 Horas.

Incluye la configuración y ajuste (parametrización) de los productos según las necesidades de la Entidad. Esto asegura que los productos están adecuadamente configurados para funcionar en el entorno del Ministerio y cumplir con los requisitos de seguridad y rendimiento.

Si bien es cierto que en el mercado mundial existen muchos fabricantes para soluciones de ciberseguridad, a continuación se muestra una imagen del cuadrante de Gartner donde refleja los principales lideres en este campo:

Figure 1: Magic Quadrant for Network Firewalls

Source: Gartner (December 2022)

[Cuadrante Mágico de Gartner de 2020 para firewalls de red (virtualgraffiti.co.uk)]

De acuerdo a lo anterior, de los diferentes fabricantes señalados como líderes en soluciones de Seguridad informática, y entre otros adicionales en el mercado mundial, se realizó una indagación en los diferentes portales web de los servicios SaaS ofrecidos respecto a las necesidades específicas que requiere dicho Ministerio:

Solución de seguridad de correo electrónico otros fabricantes que ofrecen servicios similares incluyen:

- Mimecast Advanced Email Security: Proporciona una pasarela de correo electrónico segura con características de anti-spam/anti-malware, prevención de pérdida de datos, envío de archivos grandes, entre otros.

- Barracuda Essentials: Ofrece soluciones de seguridad de correo electrónico con un enfoque en pequeñas y medianas empresas, con una alta puntuación de satisfacción del usuario.

- Cisco Cloud Email Security: Esta es una opción para empresas que buscan una solución de seguridad de correo electrónico en la nube con una buena reputación en el mercado

Competidores y alternativas a FortiAnalyzer:

- Palo Alto Networks:
  Un servicio de prevención de malware que aborda las amenazas de día cero a través de análisis dinámicos y estáticos, aprendizaje automático y entornos avanzados de pruebas de sandbox.

- Splunk Enterprise Security (ES):
  Recopilación centralizada de datos de eventos y registros, y la gestión de informes y cumplimiento.

- IBM Security QRadar SIEM:
  Un software que proporciona una recopilación centralizada de datos de eventos y registros, y detección de intrusiones basada en host y red.

- Trellix Intelligent Sandbox (anteriormente McAfee Advanced Threat Defense):

  Detecta malware avanzado y evasivo y convierte la información de amenazas en acciones y protección inmediatas, con la capacidad de compartir información de amenazas en todo el entorno para mejorar la protección y la investigación.

- Plataforma LogRhythm NextGen:
  Un software SIEM de LogRhythm que incluye la funcionalidad SOAR a través de los complementos de automatización SmartResponse, el módulo de análisis de seguridad DetectX y AnalytiX como solución de gestión de registros.

Para la Solución FortiNAC se identifican los siguientes fabricantes con soluciones equivalentes:

- Check Point Harmony Endpoint:
  Proporciona una solución de seguridad robusta con un solo software para múltiples tareas.

- F5 BIG-IP Access Policy Manager (APM):
  Gestiona el acceso global a las redes empresariales y a los proveedores de la nube.

- Twingate :
  Una plataforma basada en la nube que proporciona acceso seguro a las aplicaciones corporativas.

- ThreatLocker Protect:

Solución de seguridad de endpoints Zero Trust contra ransomware, malware y amenazas cibernéticas.

- Control de acceso a la red de Sophos:
  Protege las redes de las amenazas que plantean los equipos no conformes o comprometidos.

Para soluciones de detección y respuesta en endpoints (EDR) y servicios gestionados de detección y respuesta (MDR) similares a FortiEDR Discover, Protect & Respond y Standard MDR Cloud, hay varios otros fabricantes en el mercado que ofrecen productos similares:

- CrowdStrike Falcon: Ofrece protección avanzada contra amenazas, detección y respuesta para endpoints, con una plataforma basada en la nube.

- SentinelOne: Proporciona una plataforma de defensa autónoma para endpoints que combina prevención, detección, respuesta y caza de amenazas.

- Carbon Black (ahora parte de VMware): Ofrece soluciones de EDR y protección de endpoints con capacidades de análisis y respuesta a incidentes.

- FireEye Endpoint Security: Incluye capacidades de detección y respuesta a amenazas avanzadas con una plataforma de operaciones de seguridad integrada.

- Palo Alto Networks Cortex XDR: Combina datos de red, endpoints y nube para prevenir ataques sofisticados y automatizar las operaciones de seguridad.

- Microsoft Defender for Endpoint: Proporciona prevención de amenazas, detección poscompromiso, investigación automatizada y respuesta.

- Sophos Intercept X: Ofrece protección avanzada para endpoints con detección de amenazas basada en inteligencia artificial y respuesta automática.

De acuerdo a lo anterior, se puede identificar que en el mercado existen diferentes fabricantes que ofrecen una o varias soluciones que requiere la Entidad; sin embargo, no se identificó alguno que ofrezca la solución integral a las necesidades del Ministerio y tampoco se encuentra dentro del INSTRUMENTO DE AGREGACIÓN DE DEMANDA de Colombia Compra Eficiente CCE-139-IAD-2020, por tal razón, desde la pertinencia estratégica podemos indicar que varios de los productos, subproductos y servicios relacionados anteriormente que hacen parte del INSTRUMENTO DE AGREGACIÓN DE DEMANDA de Colombia Compra Eficiente CCE-139-IAD-2020, fueron seleccionados

integralmente para suplir la necesidad con los demás servicios tecnológicos, entre los cuales se encuentran Nube privada, Conectividad, equipos de cómputo y sistemas de información que tiene la Entidad para garantizar la seguridad y operación con la mayor disponibilidad posible, disminuyendo la materialización de riesgos cibernéticos que puedan causar la pérdida o robo de información o afectar la información y reputación de la Entidad.

Así las cosas, más que una necesidad es un licenciamiento de gestión de seguridad de la información que tenga como objetivo proteger la información que la Entidad necesita para realizar sus actividades estratégicas garantizando la confidencialidad, integridad, disponibilidad, autenticación, no repudio y trazabilidad de esta, permitiendo además que se gestionen los riesgos asociados a ella.

También es de vital importancia recalcar que el Ministerio de Igualdad y Equidad dentro de sus programas Misionales está manejando información sensible como lo son “jóvenes en Paz” y todos los demás programas que tienen que ver con violencias entre otros; de tal manera, que para proteger dicha información y los sistemas de información que se generen por parte del Ministerio es vital importancia contar con licencias y herramientas de seguridad informática que protejan la información que se genera y se procesa al interior de la Entidad.

En consecuencia, con la implementación de esta solución, también se impacta positivamente el cumplimiento los componentes de seguridad y privacidad de la información establecidos en la Estrategia de Gobierno Digital – GD (Decreto 1008 del 14 de junio de 2018), bajo el sistema de gestión de seguridad de la información en el marco del estándar ISO 27001:2013; dando además apoyo al cumplimiento a controles establecidos por dicha norma como: “A.6.2 Dispositivos móviles y teletrabajo”, “A.7.2 Durante la ejecución del empleo”, “A.7.3 Terminación y cambio de empleo”, “A.8.1 Responsabilidad por los activos”, “A.9.1 Requisitos del negocio para control de acceso”, “A.12.2 Protección contra códigos maliciosos”, “A. 12.4 Registro y seguimiento: Registrar eventos y generar evidencia”.

En otro análisis se infiere que el presente proceso beneficia la operación de procesos y procedimientos institucionales como son la Gestión de Tecnologías de la Información y su Procedimientos, y demás áreas transversales que impactan todo el parque computacional de la Entidad, y beneficiando a todo el personal de planta del Ministerio, así como a las actividades y operación técnica de las Gestiones y su operación TI en sede principal del Ministerio.

Finalmente se resalta que, con la adquisición de los productos de seguridad, se obtendrán los siguientes beneficios, entre otros:

- Garantizar la protección de los sistemas de información alojados en la nube privada.
- Garantizar la protección de los usuarios remotos y el acceso a la red corporativa desde cualquier ubicación.
- Garantizar la identificación y control sobre el acceso a la red corporativa de usuarios internos y externos.

- Contar con el monitoreo de la infraestructura tecnológica que soporta los servicios de información de la entidad, su estado de salud, correlación de eventos de seguridad y respuesta automatizada ante ataque cibernéticos

Lo anterior opera en el marco de los principios orientadores de las actuaciones contractuales del Estado, la Ley 1341 de 2009, que incluye el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones como política de Estado, que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político, incrementar la productividad y la competitividad, y fortalecer el respeto por los derechos humanos y la inclusión social.

Así mismo, de acuerdo con las Bases del Plan Nacional de Desarrollo 2022 – 2026 “Colombia potencia mundial de la vida”, se considera el gobierno digital indispensable para avanzar en el cierre de brechas poblacionales y territoriales para el acceso a bienes, a servicios e información, aprovechando las posibilidades que la tecnología ofrece como instrumento de transformación social para innovar, reducir costos, educar y compartir información, adicionalmente, describe la seguridad de la conectividad como un elemento esencial para llevar la presencia del estado a las zonas más apartadas y fortalecer el uso de las tecnologías de información y comunicaciones.

De acuerdo a lo anterior, damos cumplimiento a lo establecido en el modelo de seguridad y privacidad de la información definido por MinTIC, garantizando la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital, teniendo en cuenta el tratamiento de la información que debe realizar la Entidad.

Que bajo este marco estratégico, y con el propósito de aportar en el logro de los objetivos planteados, como se ha indicado, la Oficina de Tecnologías de Información es responsable de fortalecer los servicios y sistemas de información a cargo del Ministerio de Igualdad y Equidad, en aras de consolidar una gestión pública moderna eficiente, transparente, focalizada, participativa y al servicio de los grupos de valor; lo anterior, mediante la aplicación de los lineamientos y procesos de arquitectura tecnológica en materia de software, hardware, redes y telecomunicaciones, centros de datos e infraestructura y diseñando estrategias, instrumentos y herramientas con aplicación de tecnologías de la información y las comunicaciones.

Que para llevar a cabo lo planteado anteriormente es necesario continuar, con el trabajo que la Oficina de Tecnologías de la Información ha venido realizando en la adquisición y estabilización de los servicios tecnológicos, de los sistemas de información y de gestión, de las políticas de seguridad tecnológica, y el soporte de herramientas, para atender la demanda de actividades en el cumplimiento de la misión institucional de la Entidad.

Que buscando una mayor eficacia, eficiencia y efectividad en la prestación de servicios de tecnología, el Ministerio de Igualdad y Equidad empezó a funcionar el segundo semestre

de 2023 y al ser Entidad nueva no ha realizado la adquisición de ningún sistema de seguridad perimetral, que los funcionarios actualmente contratados están realizando sus labores con los equipos personales, lo cual es un alto riesgo de seguridad de la información.

Ahora bien, teniendo en cuenta el informe presentado por la empresa SonicWall, experta en el mundo en temas de ciberseguridad, Colombia y Brasil son los 2 países de Latinoamérica que aparecen en el listado de los 10 países del mundo con más ataques de ransomware, por lo cual, llama la atención la importancia de la ciberseguridad para las organizaciones colombianas en el 2024.

Esto nos demuestra que los ciberdelincuentes no tienen preferencia por ningún sector económico, atacando instituciones grandes y medianas de todas las industrias y causando periodos de inactividad de sus sistemas, pérdidas económicas, pérdidas por no operación y deterioro de la reputación, situaciones como las presentadas el miércoles 13 de septiembre de 2023, con el ciberataque que sufrieron las páginas del Ministerio de Salud, la Superintendencia de Salud, la Superintendencia de Industria y Comercio y el Consejo Superior de la Judicatura de Colombia y que han afectado las operaciones digitales de estas entidades del Estado y han dificultado sus servicios con la ciudadanía

En el año 2023, el diario La República, informó que 27 organizaciones del país sufrieron algún tipo de robo de información, sobre todo de robo de credenciales para acceso a su plataforma de correo corporativo, de las cuales 17 organizaciones pertenecen al sector gobierno e instituciones de educación, como lo son la Personería de Bogotá, la Fiscalía General de la Nación, la farmacéutica Audifarma, la Universidad Abierta y a Distancia (UNAD), la Universidad de Pamplona, IFX, entre otras.

Respetando su autonomía, el Ministerio es responsable de la estructuración de sus Procesos de Contratación, lo cual incluye realizar estudios del sector que informen sus decisiones de compra. Esta independencia permite al Ministerio adaptarse a las especificidades de sus operaciones, seleccionando sistemas de información que no solo cumplan con los requerimientos técnicos, sino que también se alineen con los principios de transparencia y eficiencia fiscal. Al hacerlo, el Ministerio no solo cumple con su mandato de servir al público, sino que también se posiciona como un ejemplo de integridad y diligencia en la administración de los fondos públicos.

Al seleccionar proveedores de sistemas de información que ofrecen soluciones innovadoras y rentables, el Ministerio no solo garantiza un uso eficiente de los recursos públicos, sino que también fomenta una competencia justa y transparente en el mercado. Este enfoque refleja una visión moderna y responsable de las compras públicas, asegurando que cada inversión contribuya significativamente a la mejora de los servicios ofrecidos a la ciudadanía.

Para esta contratación, el Ministerio de Igualdad y Equidad plasmó la necesidad de adelantar el proceso de selección en su Plan Anual de Adquisiciones de conformidad con lo establecido en el artículo 2.2.1.1.1.4.1 del Decreto 1082 de 2015. Se deja constancia que el ID asignado dentro del mencionado código UNSPSC 81111800 y 81112000

II. CONDICIONES DEL CONTRATO

OBJETO:

Adquisición instalación, configuración y puesta en marcha de solución de seguridad perimetral y de servicios de seguridad, incluyendo servicio de soporte técnico, para la sede principal y Datacenter externo del Ministerio de Igualdad y Equidad.

OBLIGACIONES DEL CONTRATISTA:

1. Realizar la entrega, instalación y configuración requeridas para dar cumpliendo con las especificaciones técnicas descritas en los estudios previos y la ficha técnica.
2. Suministrar personal idóneo para el cumplimiento del objeto del contrato, suscribir el compromiso de confiabilidad y reserva de la información. Esta obligación deberá incluirse en los contratos que el contratista celebre con el personal que prestará el servicio y estará dirigido a la obligación de guardar reserva de lo que llegue a su conocimiento por o con ocasión del desarrollo de las actividades contratadas.
3. Designar el personal de operarios(as) con la debida identificación que implica el porte de carné que los acredite como empleados del CONTRATISTA, dicha identificación deberá ser portada en lugar visible. Así mismo, el contratista proveerá a los operarios de uniformes o dotación nueva para el inicio de la labor, conforme a las siguientes indicaciones, en adelante realizará la entrega de dotaciones de acuerdo con la periodicidad dispuesta en la ley.
4. Efectuar la prestación del servicio ordinario de acuerdo con las actividades e insumos solicitados.
5. Garantizar los medios de comunicación y la infraestructura logística que permita en todo momento el seguimiento a la prestación del servicio. Para el efecto, el contratista deberá suministrar al Supervisor del contrato un esquema detallado del personal de apoyo (contactos, medios de comunicación y directorios telefónicos), a través del cual podrá controlarse la operación y la facturación.
6. Cumplir con todos y cada uno de los requerimientos establecidos en la ficha técnica del Acuerdo Marco de Precios establecido por Colombia Compra Eficiente, para el servicio a contratar.
7. Suministrar el listado de las personas asignadas y notificar al Ministerio de Igualdad y Equidad de cualquier cambio que se produzca en el personal.
8. Cumplir con las disposiciones laborales contenidas en la ley 2101 de 2021, ley 50 de 1990, la ley 100 de 1993 y demás normas vigentes y concordantes de la legislación laboral colombiana como empleador con sus trabajadores que, en virtud del presente contrato, presten servicio al Ministerio de Igualdad y Equidad.
9. Reemplazar inmediatamente cualquiera de las personas destinadas a prestar este servicio cuando el Ministerio de Igualdad y Equidad se lo requiera o cuando las circunstancias lo ameriten para que no se presente interrupción del servicio.
10. Acatar todas las disposiciones e instrucciones impartidas por el Ministerio de Igualdad y Equidad con relación a la distribución de operarias (os) y todo lo concerniente con la prestación efectiva del servicio.

11. Responder por las pérdidas o daños que el personal a su cargo cause al Ministerio de Igualdad y Equidad, en ejercicio de las funciones que le sean asignadas y cuando sus actuaciones sean contrarias al objeto del contrato, a las buenas costumbres y la Ley. Esta obligación será amparada por la póliza de Responsabilidad Civil Extracontractual conforme a las condiciones que se exijan.
12. Guardar la debida y completa reserva y confidencialidad de la información y los documentos de que tenga conocimiento a los que tenga acceso en virtud del presente contrato.
13. Presentar los informes que requiera el supervisor del contrato, y en específico aquel que se requiera para la realización de los pagos, señalando las actividades realizadas.
14. Obtener y presentar para su aprobación las garantías en las condiciones, plazos y con el objeto y montos establecidos en el presente contrato, así como mantener vigentes sus amparos y prorrogarlos en los términos señalados.
15. Dar respuestas a los requerimientos de información en los tiempos establecidos.
16. Cumplir con todas las demás obligaciones a su cargo que se deriven de la naturaleza del presente contrato y de las exigencias legales, entre ellas, aquellas de carácter tributario, en caso de que se generen.
17. Cumplir con el sistema de Gestión de Seguridad y Salud en el Trabajo conforme a lo estipulado en el Decreto 1072 de 2015 y Resolución 0312 de 2019 del Ministerio de Trabajo.
18. El contratista se obliga a cumplir las disposiciones normativas de la política de Tratamiento de datos personales, Políticas de Operación Institucionales, Política de seguridad de la información y Políticas técnicas de seguridad de la información adoptadas por la Entidad. Adicionalmente deberá guardar absoluta reserva sobre la información PÚBLICA RESERVADA, PÚBLICA CLASIFICADA, DATOS SENSIBLES, DATOS PRIVADOS, DATOS SEMIPRIVADOS, SECRETO EMPRESARIAL COMERCIAL, durante toda la vigencia del contrato y hasta 2 años después de la liquidación (si aplica) del mismo".
19. Dar cumplimiento a las obligaciones previstas en el Acuerdo Marco de Precios CCE–139-AID-2020, la ley 80 de 1993, Ley 1150 de 2007 y demás que aclaren, modifiquen, reglamenten o adiciones, el contratista se obliga con la Entidad en su generalidad en los términos de la cláusula No 7 – Actividades de los proveedores durante la operación secundaria y cláusula 12 “Obligaciones de los Proveedores” y en especial en las “Obligaciones derivadas de la orden de compra” contempladas en el Instrumento de Agregación de Demanda para la adquisición de Software por Catálogo que requieran las entidades estatales, el cual se identifica con el número CCE–139-AID-2020.
20. Las demás obligaciones que se deriven del Acuerdo Marco de Precios CCE-116-IAD-2020.

OBLIGACIONES DEL MINISTERIO DE IGUALDAD Y EQUIDAD

1. Realizar la supervisión y seguimiento a la ejecución del contrato.
2. Desembolsar los recursos financieros acordados para el desarrollo del contrato, en los montos y términos establecidos en el presente documento.

3. Prestar colaboración constante en la ejecución del contrato, suministrando la información requerida para el logro del objeto contractual.
4. Proponer los lineamientos a seguir en cumplimiento del objeto del contrato.
5. Cumplir las demás actividades que le sean encomendadas y que se encuentren relacionados con el objeto del contrato.

III. FICHA TÉCNICA:

De acuerdo con las condiciones técnicas del servicio de seguridad que requiere la Entidad, las especificaciones técnicas se encuentran establecidas en el catálogo del presente acuerdo marco, donde se realizó el simulador correspondiente. Las cuales se especifican a continuación:

Ítem	Catalogo	Descripción	Tipo	Cantidad
1	FC5-10-FGVVS-990-02-12	Subscriptions license for FortiGate-VM (16 CPU) with UTP Bundle included.	Licencia Suscripción	2
2	FC2-10-FECLD-423-02-12	FortiMail Cloud - Gateway Premium w. Office365 API support (101-1000 mailboxes). Price per mailbox	Licencia Suscripción	412
3	FC5-10-FGVVS-585-02-12	FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service.	Licencia Suscripción	1
4	FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server (VMWare/Hyper-V/AWS/Azure/KVM).	Licencia Suscripción	1
5	FC-10-FNVXM-248-02-12	FortiCare Premium Support	Licencia Suscripción	1
6	FC2-10-FNAC1-213-01-12	FortiNAC Subscription Visibility+Control (PLUS) License for 500 concurrent endpoints. MOQ 500.	Licencia Suscripción	1
7	FC1-10-FEDR1-349-01-12	FortiEDR Discover, Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 25 endpoints	Licencia Suscripción	4

Ítem	Catalogo	Descripción	Tipo	Cantidad
8	FC1-10-EDBPS-310-02-12	FortiEDR Best Practice Service for up to 1,000 Endpoints/users	Licencia Suscripción	1
9	FC1-10-FSM98-180-02-12	Per Device Subscription License that manages minimum 50 devices, 10 EPS/Device. Does not include Maintenance & Support	Licencia Suscripción	50
10	FC1-10-FSM97-248-02-12	FortiCare Premium Support (1 - 50 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.	Licencia Suscripción	1
11	RT-FSERV-BASIC2	Configuración y parametrización de los Productos, Paquete de 20 horas (configuracion de Herramienta Basica) Servicio ejecutado por profesional especialista certificado NSE4 Bolsa de 20 Horas	Servicios	2
12	RT-FSERV-ADVANCED2	Configuración y parametrización de los Productos, Paquete de 20 horas (configuracion de Herramienta Avanzada) Servicio ejecutado por profesional especialista certificado NSE5 Bolsa de 20 Horas	Servicios	12

IV. VALOR ESTIMADO DEL CONTRATO Y FORMA DE PAGO

El valor estimado para el presente proceso de selección asciende a la suma de: **QUINIENTOS OCHENTA Y OCHO MILLONES DOSCIENTOS TREINTA Y TRES MIL DOSCIENTOS DOS PESOS CON SETENTA Y OCHO CENTAVOS ($588.233.202,78) M/CTE** incluido IVA y demás gastos asociados a la ejecución del contrato, los cuales serán cubiertos con cargo al presupuesto de inversión de la presente vigencia fiscal, de conformidad con el Certificado de Disponibilidad Presupuestal No. 1524 del 29 de febrero de 2024, expedido por la Ministra del Ministerio de Igualdad y Equidad.

Nota 1: Las cifras se establecieron de acuerdo a los valores disponibles en el catálogo que se encuentra en la página de Colombia Compra Eficiente. CCE–139-AID-2020 Software por Catalogo, de acuerdo a la necesidad de la Entidad.

Item	Código Catálogo	Descripción del Producto	Tipo	cantidad	Precio Unitario	Precio Unitario + Gravamen	Descuento adicional	Precio con Descuento	Subtotal	IVA	Vr IVA	Precio Total
1	FC5-10-FGVVS-390-02-12	Subscriptions license for FortiGate-VM (16 CPU) with UTP Bundle included.	Licencia Suscripción	2	$ 75.755.204,26	$ 75.755.204,26		$ 75.755.204,26	$ 151.510.408,52	Si	$ 28.786.977,62	$ 180.297.386,14
2	FC2-10-FECLD-423-02-12	FortiMail Cloud - Gateway Premium w. Office365 API support (101-1000 mailboxes) Price per mailbox	Licencia Suscripción	412	$ 114.213,13	$ 114.213,13		$ 114.213,13	$ 47.055.809,56	No	$ -	$ 47.055.809,56
3	FC5-10-FGVVS-595-02-12	FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types IOC Service Security Automation Service and FortiGuard Outbreak Detection Service.	Licencia Suscripción	1	$ 21.667.467,17	$ 21.667.467,17		$ 21.667.467,17	$ 21.667.467,17	No	$ -	$ 21.667.467,17
4	FNC-CAV-VM	FortiNAC Control and Application next-gen VM Server (VMWare&Hyper-V/AWS/Azure/KVM).	Licencia Suscripción	1	$ 13.343.244,65	$ 13.343.244,65		$ 13.343.244,65	$ 13.343.244,65	Si	$ 2.535.216,48	$ 15.878.461,13
5	FC-10-FNVM4-249-02-12	FortiCare Premium Support	Licencia Suscripción	1	$ 2.668.664,53	$ 2.668.664,53		$ 2.668.664,53	$ 2.668.664,53	Si	$ 507.046,26	$ 3.175.710,79
6	FC2-10-FNAC1-213-01-12	FortiNAC Subscription Visibility+Control (PLUS) License for 500 concurrent endpoints. MOQ 500.	Licencia Suscripción	1	$ 19.495.000,31	$ 19.495.000,31		$ 19.495.000,31	$ 19.495.000,31	Si	$ 3.704.050,06	$ 23.199.050,37
7	FC1-10-FEDR5-349-01-12	FortiEDR Discover Protect & Respond and Standard MDR Cloud Subscription and FortiCare Premium for 25 endpoints	Licencia Suscripción	4	$ 11.322.853,71	$ 11.322.853,71		$ 11.322.853,71	$ 45.291.414,84	No	$ -	$ 45.291.414,84
8	FC1-10-EDBPS-310-02-12	FortiEDR Best Practice Service for up to 1,000 Endpoints/users	Licencia Suscripción	1	$ 25.599.495,35	$ 25.599.495,35		$ 25.599.495,35	$ 25.599.495,35	Si	$ 4.863.904,12	$ 30.463.399,47
9	FC1-10-FSM86-180-02-12	Per Device Subscription License that manages minimum 50 devices 10 EPS/Device. Does not include Maintenance & Support	Licencia Suscripción	50	$ 686.877,55	$ 686.877,55		$ 686.877,55	$ 34.343.877,50	Si	$ 6.525.336,73	$ 40.869.214,23
10	FC1-10-FSM97-248-02-12	FortiCare Premium Support (1 - 50 points) for FortiSIEM Software deployments. 1 "Device" or 2 "End points" or 3 "Advanced Agents - Log & FIM" or 10 "Advanced Agents - UEBA Telemetry" equals 1 point.	Licencia Suscripción	1	$ 11.774.192,51	$ 11.774.192,51		$ 11.774.192,51	$ 11.774.192,51	Si	$ 2.237.096,59	$ 14.011.289,09
11	RT-FSERV-ADVANCED2	Configuración y parametrización de los Productos, Paquete de 20 horas (configuracion de Herramienta Avanzada Fortinet) Servicio ejecutado por profesional especialista certificado NSE5 Etcita de 20 Horas	SERVICIOS	2	$ 17.000.000,00	$ 17.000.000,00		$ 17.000.000,00	$ 34.000.000,00	Si	$ 6.460.000,00	$ 40.460.000,00
12	RT-FSERV-BASIC2	Configuración y parametrización de los Productos, Paquete de 20 horas (configuracion de Herramienta Basica Fortinet) Servicio ejecutado por profesional especialista certificado NSE4 Etcita de 20 Horas	SERVICIOS	12	$ 8.000.000,00	$ 8.000.000,00		$ 8.000.000,00	$ 105.600.000,00	Si	$ 20.064.000,00	$ 125.664.000,00
1. Si requiere agregue o elimine fila											Valor Total	$ 500.233.282,79

Nota 2: Teniendo en cuenta que los procesos que se publiquen del 1 al 15 llevan la TRM del último día del mes anterior, y para procesos publicados entre el 16 y el 30 llevan TRM del 15 del mes en que se publique, por lo tanto, para este caso se tomó la TRM del 15 de marzo del 2024 la cual fue de $3.899,39.

FORMA DE PAGO:

El Ministerio de Igualdad y Equidad pagará el valor del contrato, de conformidad con las condiciones estipuladas por Colombia Compra Eficiente en el Acuerdo Marco de Precios, No. CCE–139-AID-2020, Software por catálogo, a saber:, cláusula 10 facturación y pago "(…) ii) De contado, dependiendo de las condiciones del producto adquirido en los términos señalados en el catálogo (…)".previa presentación de la respectiva factura y expedición del certificado de recibido a satisfacción por parte del Supervisor del Contrato, sin que el monto total de los servicios suministrados pueda exceder la cuantía total del contrato.

El Ministerio de Igualdad y Equidad como requisito previo para autorizar los pagos del contrato, verificará:

1. Formato único para pago de contratistas y/o proveedores.
2. Informe de Ejecución Contrato y/o Convenio
3. Documentos que el supervisor considere necesarios para validar la ejecución técnica del contrato (entregables, documentos soporte y/o productos, de acuerdo al contrato suscrito).
4. La factura Electrónica si la persona es responsable de IVA en su RUT y el Código CUFE para la validación de la factura ante la DIAN, conforme a los requisitos señalados en el artículo 617 Estatuto Tributario.
5. Certificado de aportes al Sistema Integral de Seguridad Social en Salud, Pensión y Riesgos Laborales, así como los propios del Sena, ICBF y Cajas de Compensación Familiar, siempre y cuando no se encuentre exento de este pago, según lo establecido en el artículo 50 de la Ley 789 de 2002, y lo establecido en el artículo 114-1 del Estatuto Tributario, de acuerdo con las obligaciones que por este concepto deba cumplir. Registro Único Tributario RUT – DIAN.
6. Registro de Identificación Tributaria RIT – Secretaría Distrital de Hacienda de lo contrario se aplicará la mayor tarifa de descuento conforme al artículo 70 del Decreto 362 de 2002. El trámite se puede realizar a través del siguiente link: https://www.shd.gov.co/shd/asi-puedessolicitar-el-rit, por parte del Contratista.

7. Ingreso al Almacén para compras de bienes (Si aplica)

Nota 1: El contratista debe expedir y enviar su factura electrónica al correo Siifnacion.facturaelectronica@minhacienda.gov.co con el asunto #$46-01-01; Contrato **"Colocar el numero"; correo de supervisor@minigualdad.gov.co** #$ ejemplo #$46-01-01; Contrato 001-2024; pepitoperez@minigualdad.gov.co #$ conforme a las Circulares Externas 016 y 019 suscritas por el Administrador de SIIF Nación.

Nota 2: Si la factura no ha sido correctamente elaborada o no se acompaña de los documentos requeridos para el pago, el término para este solo empezará a contarse desde la fecha en que se presenten debidamente corregidas o desde que se haya aportado el último de los documentos solicitados. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrá por ello derecho o pago de intereses o compensación de ninguno naturaleza.

Todos los pagos estarán sujetos al Programa Anual Mensualizado de Caja P.A.C y al cumplimiento de los procedimientos presupuestales.

V. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será hasta el treinta (30) de septiembre del 2024, inicia a partir del perfeccionamiento del contrato, expedición del registro presupuestal, aprobación de pólizas y suscripción del acta de inicio, de conformidad con las condiciones estipuladas por Colombia Compra Eficiente en el Acuerdo Marco de Precios, No. CCE–139-AID-2020.

Plazo del licenciamiento: Doce (12) meses contados a partir de la legalización y perfeccionamiento de la orden de compra y la suscripción del acta de inicio.

VI. LUGAR DE EJECUCIÓN

El Contratista realizará las actividades propias del objeto, en la ciudad de Bogotá D.C.

VII. SUPERVISIÓN DEL CONTRATO

Teniendo en cuenta las características del servicio a contratar y dado que el mismo atañe a las funciones propias del Ministerio de Igualdad y Equidad, la supervisión del contrato será efectuada por el Jefe de la Oficina de Tecnologías de la Información, o del funcionario que para el efecto designe la Ordenadora del Gasto del Ministerio de Igualdad y Equidad.

El supervisor tendrá las siguientes atribuciones para el caso:

1. El supervisor deberá estar registrado en el SECOP II como comprador, de tal manera que le sea posible verificar el cumplimiento, integridad, autenticidad, veracidad y fidelidad de la información y/o productos de ejecución contractual publicada por EL CONTRATISTA pactados en el presente contrato, en la plataforma Sistema Electrónico de Contratación Pública SECOP II.

2. El supervisor deberá a dar inicio de la ejecución del contrato en la plataforma de SECOP II.
3. Ejercer un estricto control para el cumplimiento de la totalidad de las obligaciones del CONTRATISTA.
4. Disponer lo necesario para asegurar el cumplimiento de las obligaciones de los contratistas estipulados en el documento.
5. Elaborar y tramitar el acta y/o cierre del expediente contractual.
6. Informar a la Ordenadora del gasto cualquier novedad que proceda de la ejecución del contrato, o cualquier circunstancia que haga temer por la cumplida y oportuna ejecución del contrato y sus actividades.
7. Comunicar a la Ordenadora del gasto con la debida sustentación técnica la elaboración de prórrogas, adiciones y/o cualquier cambio en el desarrollo del contrato.
8. Verificar previo a la iniciación de los contratos en SECOP II, el cumplimiento de los requisitos de ejecución del contrato
9. Verificar, la realización de los aportes por parte del contratista al Sistema de Seguridad Social y dejar constancia del cumplimiento de las obligaciones de los contratistas frente a los aportes mencionados durante toda su vigencia.
10. Efectuar la verificación sobre la vigencia de los permisos, licencias, autorizaciones, contratos y pólizas que el CONTRATISTA requiera para el desarrollo del objeto del contrato.
11. Solicitar información sobre el cumplimiento de las obligaciones tributarias, parafiscales y prestacionales a cargo del CONTRATISTA.
12. Expedir las certificaciones de cumplimiento del objeto del contrato, para efectos del pago correspondiente.
13. Responder porque en el expediente del contrato se encuentre toda la documentación que se produzca durante la ejecución del contrato y relacionada con su ejecución.
14. Elaborar el acta de liquidación del contrato y velar porque se suscriba dentro de los plazos legales establecidos para el efecto, acta que será firmada además por el Ordenador del Gasto o por quien éste delegue para tal efecto.
15. Velar por que se mantengan los amparos presupuestales del contrato durante la vigencia contractual.
16. Realizar la evaluación y reevaluación de proveedores al contratista durante la ejecución del contrato acorde con los términos establecidos en la Guía de Supervisión del Ministerio de Igualdad y Equidad.
17. Las demás que se requieran en desarrollo del objeto contractual.

VIII. LIQUIDACIÓN

Las órdenes de compra son contratos estatales en los términos del artículo 32 de la ley 80 de 1993, en cuanto son actos jurídicos generadores de obligaciones, que constan por escrito.

De conformidad con lo establecido en el artículo 60 de la ley 80 de 1993, respecto de la ocurrencia y contenido de la liquidación contempla: "(…) Los contratos de tracto sucesivo, aquellos cuya ejecución o cumplimiento se prolongue en el tiempo y los demás que lo

requieran, serán objeto de liquidación (…)". Las órdenes de compra que no cumplan con las condiciones citadas y que sólo tengan una entrega, no deben ser liquidadas

De conformidad con lo anterior, se determina respecto del contrato derivado de este proceso se liquidará bilateralmente dentro de los seis (6) meses siguientes a la terminación del plazo de ejecución.

IX. VERIFICACIÓN DE INHABILIDADES, MULTAS, SANCIONES E INCOMPATIBILIDADES DEL PROVEEDOR

De conformidad a lo establecido en el numeral 7 de la guía para comprar en la Tienda Virtual del Estado Colombiano (TVEC) a través del Acuerdo Marco de Precios para la compra y alquiler de computadores y periféricos ETP III, la Entidad es responsable de realizar la verificación de las inhabilidades, multas, sanciones e incompatibilidades en que pueda estar en curso el proveedor que presento la oferta más económica antes del momento de la adjudicación de la Orden de Compra, para lo cual se revisará la información consignada en el aplicativo RUES, sin que ello sea la única fuente de verificación.

Adicionalmente la Entidad verificará directamente los antecedentes fiscales, disciplinarios, judiciales y policivos de la persona natural o el representante legal de la firma oferente y el oferente, mediante la consulta de las páginas de la Contraloría General de la República, Procuraduría General de la Nación y Policía Nacional, respectivamente por lo que solicitará al proveedor que presentó la oferta de menor valor el Certificado de Existencia y Representación Legal Vigente a la fecha de presentación de la oferta con una expedición no mayor a 30 días y la cédula de ciudadanía del representante legal a través del correo electrónico registrado en la Tienda Virtual del Estado Colombiano.

En ese sentido, en caso tal de identificar que el proveedor se encuentra incurso en alguna de las causales de inhabilidad o incompatibilidad previstas en la legislación vigente, es informará de inmediato a la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente para el trámite respectivo y tomar las acciones que se consideren necesarias por la Entidad Compradora.

X. GARANTÍAS

Para el presente proceso, de conformidad con el acuerdo marco de precios vigente, el contratista debe constituir una garantía de cumplimiento dentro de los tres (3) días hábiles siguientes a la colocación de la Orden de Compra, por el valor, amparos y vigencia establecidos en la siguiente tabla:

Amparo	Suficiencia	Vigencia
Cumplimiento del contrato	Quince por ciento (15%) del valor de la Orden de Compra	Duración de la Orden de Compra y seis (6) meses más, En todo caso de conformidad al decreto 1082 de 2015 la garantía de cumplimiento debe estar vigente hasta la liquidación.

Calidad de los Bienes	Veinte por ciento (20%) del valor de la Orden de Compra	Duración de la Orden de Compra y Un (1) año más, En todo caso de conformidad al decreto 1082 de 2015 la garantía de cumplimiento debe estar vigente hasta la liquidación.
Pago de salarios, prestaciones sociales legales e indemnizables laborares	Cinco por ciento (5%) del valor de la Orden de Compra	Duración de la Orden de Compra y tres (3) años más

NOTA: Se deben tener cumplimiento a las obligaciones ya establecidas por Colombia Compra Eficiente en el Acuerdo Marco de Precios No. CCE–139-AID-2020.

BRUCE DARIO VARGAS VARGAS
Jefe Oficina de Tecnologías de la Información

Elaboró: Edwin Sánchez Rozo / Profesional Especializado Oficina de Tecnologías de la Información
Revisó: Diana Carolina Martínez / Asesora Oficina Jurídica
Revisó: Diana Olmos / Asesora Secretaría General
Aprobó: Bruce Darío Vargas Vargas - Jefe Oficina de Tecnologías de la Información