FECHA: DD/MM/AAAA

Fecha de la ficha técnica definitiva

1. NECESIDAD:

El Ministerio de Ambiente y Desarrollo Sostenible es el rector de la gestión del ambiente y de los recursos naturales renovables, encargado de orientar y regular el ordenamiento ambiental del territorio y de definir las políticas y regulaciones a las que se sujetarán la recuperación, conservación, protección, ordenamiento, manejo, uso y aprovechamiento sostenible de los recursos naturales renovables y del ambiente de la nación, a fin de asegurar el desarrollo sostenible, sin perjuicio de las funciones asignadas a otros sectores. Corresponde al Ministerio de Ambiente y Desarrollo Sostenible dirigir el Sistema Nacional Ambiental -SINA-, organizado de conformidad con la Ley 99 de 1993, para asegurar la adopción y ejecución de las políticas, planes, programas y proyectos respectivos, en orden a garantizar el cumplimiento de los deberes y derechos del Estado y de los particulares en relación con el ambiente y el patrimonio natural de la Nación. Art 1. Decreto 3570/2011.

Es por lo anterior que el Ministerio para la vigencia 2025 debe continuar dando cumplimiento al Plan Nacional de Desarrollo 2022-2026 (PND 2022-2026) *Colombia potencia mundial de la vida*, donde se concreta el inicio de una transición que debe desembocar en la paz total, que no es otra cosa que la búsqueda de una oportunidad para que todos podamos vivir una vida digna, basada en la justicia; es decir, en una cultura de la paz que reconoce el valor excelso de la vida en todas sus formas y que garantiza el cuidado de la casa común. En esta transición hacia la paz, basada en el fortalecimiento de la democracia, el PND 2022-2026 pone sus mayores énfasis en la disminución de las desigualdades y en la superación de las injusticias que les son propias, por lo que la redistribución de los recursos prioriza a los sectores de la sociedad y a las regiones que producen la riqueza pero no se han beneficiado con ella.

De conformidad con lo anterior, desde el Despacho de la Ministra se han establecido programas como categorías que agrupan las acciones prioritarias de este Gobierno, las cuales provienen de las bases del PND, asociados a las transformaciones y catalizadores del mismo. Para el caso de la Oficina de Tecnologías de la Información y las Comunicaciones – OTI tiene la responsabilidad de participar en el programa de la Ministra denominado Justicia ambiental y gobernanza inclusiva, apuntando al componente del PND: Democratización del conocimiento, la información ambiental y de riesgo de desastres.

En consecuencia, la Oficina de Tecnologías de la Información y las Comunicaciones – OTI debe integrar estratégicamente la gestión de Tecnologías de la Información y las Comunicaciones al servicio de la misión de la entidad, brindando la continuidad operacional y agregando valor a los servicios mediante la implementación de estándares, buenas prácticas y principios para la gestión de la información estatal y políticas en materia de tecnologías de la información del gobierno nacional, que permitan el manejo efectivo y seguro de la información, con lo cual a su vez se da cumplimiento a las funciones legalmente asignadas a esta oficina en el artículo 13 del Decreto 3570 de 2011, principalmente las siguientes: *"(...)1. Garantizar la aplicación a nivel sectorial de los estándares, buenas prácticas y principios para la información estatal. (...) 4. Desarrollar estrategias de generación y promoción del flujo eficiente de información sectorial e intersectorial y de servicio al ciudadano, en la difusión de la información y la promoción del Sector, hacia los ciudadanos y organizaciones para rendición de cuentas. (...) 7. Lograr acuerdos entre las entidades del Sector Administrativo para compartir información y mejorar la eficiencia en la producción, recolección, uso y disposición de la información de acuerdo con los lineamientos estratégicos emitidos por Departamento Nacional de*

Planeación, el Ministerio de las Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo Nacional de Estadística (DANE). 9. Organizar los procesos internos del sector en producción de información para cumplir con las políticas, planes, programas y proyectos sectoriales teniendo en cuenta los lineamientos para la información estatal.(...) 16.Atender las peticiones y consultas relacionadas con asuntos de su competencia. 17. Las demás funciones asignadas que correspondan a la naturaleza de la dependencia (...)"

En consecuencia, la Oficina de Tecnologías de la Información y las Comunicaciones – OTI para la presente vigencia hace parte del proyecto de inversión denominado: "*Modernización Institucional para la gestión y transformación ambiental Nacional* - BPIN: 202400000000095", el cual tiene como meta: *Fortalecer el desempeño institucional y la gestión estratégica del Ministerio de Ambiente y Desarrollo Sostenible, dentro del cual la Oficina tiene a su cargo el objetivo específico "Fortalecer la capacidad de gestión de TI en la entidad", con el producto: "Servicios tecnológicos"* y cuya actividad principal se estableció en: *" Actualizar la infraestructura tecnológica (licenciamiento y equipos o servicios) conforme a la planeación estratégica que se priorice en el PETI".*

En este sentido, el Ministerio de Ambiente y Desarrollo Sostenible siendo consiente que para dar cumplimiento y desarrollo a la misión institucional de acuerdo con su normatividad vigente y competencias se apoya en una base tecnológica que opera en una arquitectura híbrida de nube on premise combinando la infraestructura TI existente dentro de la entidad, alojada en el centro de cómputo (on premise) con recursos y servicios en la nube pública (Amazon Web Services - AWS).

De lo anterior, esta arquitectura cuenta con unas características de seguridad. En la nube, está optimizada para diversas amenazas cibernéticas, mientras que la infraestructura on premise puede mantener la privacidad de datos sensibles. No obstante, hoy día el mundo está expuesto a diferentes amenazas mediante medios informáticos que exponen y atentan de manera permanente los ambientes corporativos.
El Ministerio de Ambiente y Desarrollo Sostenible desde la OTIC ha tenido dentro de su infraestructura TI on premise una solución de seguridad perimetral marca FORTINET que desde finales del año 2014 fue adquirida y ha sido objeto de renovaciones periódicas para preservar la función de detección, disuasión y freno a los intrusos que pretenden acceder de manera fraudulenta a los sistemas de información, aplicaciones, servidores, base de datos y servicios de la red interna del ministerio desde internet.

Estos componentes tecnológicos de seguridad han jugado un rol importante e indispensable para garantizar la protección y operación de los servicios de TI que ofrece la entidad vía WEB. Es por ello por lo que, la infraestructura de TI y la información allí almacenada, son susceptibles a diversos ataques, que de no lograr repelerse pueden llegar a afectar la disponibilidad, confidencialidad e integridad de la información y la continuidad de los servicios que allí se alojan y se ofrecen a la ciudadanía.



Top Attacks

Attack	SPP	Direction	Drops	Events
Source flood	[redacted]	Inbound	645,933	4
ICMP flood	[redacted]	Inbound	457,713	8
State Anomalies: Foreign packet (Out of State)	[redacted]	Inbound	169,081	7,108
SYN flood from source	[redacted]	Inbound	91,693	3
L4 anomalies	[redacted]	Inbound	78,922	4,949
UDP checksum error	[redacted]	Inbound	54,311	8,747
Possible UDP reflection flood	[redacted]	Inbound	46,880	59
TCP invalid flag combination	[redacted]	Inbound	4,680	2,431
TCP port flood	[redacted]	Inbound	3,776	19
SYN flood	[redacted]	Inbound	2,166	4
TCP checksum error	[redacted]	Inbound	1,561	986
Invalid HTTP Version Anomaly	[redacted]	Inbound	477	45
Invalid ICMP Type/Code	[redacted]	Inbound	24	3
ICMP checksum error	[redacted]	Inbound	1	1

Imagen 1. Reporte parcial de ataques registrados.

En la imagen 1, se visualiza un pequeño aparte de un reporte que entrega la solución perimetral y la contención que realiza en amenazas al mantener las licencias de seguridad activas para cada uno de los componentes perimetrales. Esta protección se realiza de manera permanente en la red con el fin de asegurar ambientes de trabajo de tipo corporativo cumpliendo las políticas de seguridad que se encuentran previamente establecidas bajo los tres pilares de la seguridad: disponibilidad, confidencialidad e integridad. Cada uno de estos dispositivos tiene una especialidad y forma de proteger la red pues corresponden a equipos de propósito específico respaldados de fábrica.

En este sentido, la entidad cuenta con los siguientes componentes tecnológicos de seguridad, así:

MODELO	NÚMERO DE SERIE	CANTIDAD
Fortigate 600E	FG6H0E5819902723	2
Fortigate 600E	FG6H0E5819903277	
FortiAnalyzer 200F	FL-2HFTB19000612	1
FortiWeb-1000D	FV-1KD3A16800107	2
FortiWeb-1000D	FV-1KD3A17800187	
FortiDDoS 200F	FI-2HFTE22000044	1
TENABLE	CustomerID-373113	100 licencias.nodos VM 30 licencias de WAS
Prefijo IPv6 (*)	2801:1c:a800::/48	1

Tabla 1. Solución de Seguridad Ministerio de Ambiente y Desarrollo Sostenible.

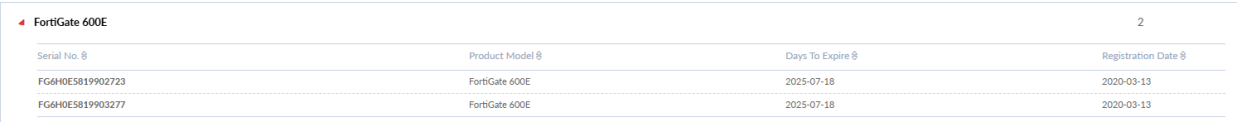
*El pool de IPv6 no es un componente de seguridad, sino que forma parte de la red.

Dichos componentes, son de uso frecuente para el control de la seguridad de la red y de los nuevos servicios que se publican en internet. Sin embargo, dado el tiempo de operación, la OTIC evidencia lo siguiente por cada componente:

FIREWALLS

Se cuenta con dos equipos cortafuegos en HA (High Availability) adquiridos a finales de 2019 bajo el modelo **FortiGate 600E** que monitorea, filtra y controla el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas para la entidad. Esto, manteniendo una arquitectura de alta disponibilidad tanto en hardware como de forma lógica.

La actual solución de firewall NGFW (Next Generation Firewall) cuenta con controles de antivirus, antispam, botnet / IP domain, filtro de contenidos WEB, firmas de IPS (Intrusión Prevention System), control de Aplicaciones, Sandbox Cloud (unified UTM protection), Anti DDoS, analítica, entre otros; dicha solución opera en modo Alta Disponibilidad con equipos redundantes lo cual garantiza tolerancia a fallas y en la continua protección ante ataques provenientes desde internet o internos.



FortiGate 600E — 2

Serial No.	Product Model	Days To Expire	Registration Date
FG6H0E5819902723	FortiGate 600E	2025-07-18	2020-03-13
FG6H0E5819903277	FortiGate 600E	2025-07-18	2020-03-13

Figura 1. Hardware lifecycle – FortiGate 600E.

Estos equipos cuentan aún con vida útil, su capacidad en disponibilidad de puertos de alta velocidad está limitada, dado que sus interfaces están ocupadas y limita el crecimiento a nuevos servicios que se requieran implementar, lo que retrasaría proyectos de mayor demanda en transferencia de datos y generando cuellos de botella, impactando así el desempeño de nuevos servicios, lo que se traduciría en lentitud para los usuarios finales que consumen y demanden servicios desde y hacia la entidad.

Por otra parte, dado al proceso de modernización que se ha venido realizando en el ministerio, se hace propicio contar con una solución de seguridad que permita escalar a nivel de velocidad y capacidad, permitiendo tasas de transferencia de datos mayores bajo la demanda de aplicaciones nuevas y que exigen

un ancho de banda más elevado, las cuales son consumidas por los usuarios interna y externamente a la entidad. Los equipos actuales FortiGate 600E cuentan con múltiples interfaces o puertos para la conectividad de servicios (página 7), donde se evidencia que la capacidad es muy limitada frente a puertos de alta transferencia de datos ULL (ultra-low latency) impidiendo la conexión de servicios misionales que requieren de este tipo de características a muy baja latencia para el correcto funcionamiento de aplicaciones.

Otro hito relevante, y posterior a la pandemia ocurrida en el año 2020, se hace necesario la capacidad de conectar usuarios remotos o teletrabajadores (Vía Virtual Private Network – VPN) que requieran de los servicios o aplicativos internos del ministerio, por ello, es indispensable que la plataforma de seguridad perimetral garantice los recursos necesarios para la conexión de miles de usuarios conectados simultáneamente, con la capacidad de soportar e implementar el segundo factor de autenticación (2MF) bajo una única plataforma, con la finalidad de proyectar la implementación de reglas de Zero Trust Network Access (ZTNA).

Frente a las actualizaciones de firmware, las cuales son ideales mantener y evitar malfuncionamientos, vulnerabilidades emergentes, bugs y errores; se limitan al hecho que el contrato suscrito de soporte y mantenimiento se encuentra próximo a finalizar exponiendo los dispositivos a vulnerabilidades críticas que no se pueden remediar pues para ejecutar las mencionadas se hace necesario evaluar técnicamente la versión de firmware que interopere con los demás componentes de seguridad para así mantener la salud y buen funcionamiento operacional de estos equipos.

Frente a las actualizaciones de firmware, las cuales son ideales mantener y evitar malfuncionamientos, vulnerabilidades emergentes, bugs y errores; se limitan al hecho que el contrato suscrito de soporte y mantenimiento se encuentra próximo a finalizar exponiendo los dispositivos a vulnerabilidades críticas que no se pueden remediar pues para ejecutar las mencionadas se hace necesario evaluar técnicamente la versión de firmware que interopere con los demás componentes de seguridad para así mantener la salud y buen funcionamiento operacional de estos equipos.

Para la solución FORTINET, es preciso evidenciar que se cuenta con ventajas competitivas que permiten robustecer la seguridad perimetral de las organizaciones, una de estas ventajas es que se ofrece una arquitectura llamada FORTINET SECURITY FABRIC, que permite integrar diferentes componentes de seguridad (firewalls, antivirus, VPNs, control de acceso, switches y otros elementos de red.) en una única plataforma coordinada. Esto mejora la visibilidad y la respuesta ante amenazas. De igual forma, FORTINET permite administrar múltiples dispositivos desde una sola consola mediante herramientas como FortiManager

(gestión) y FortiAnalyzer (análisis y reportes), lo que facilita la administración a gran escala, permitiendo a los administradores detectar, mitigar y resolver eventos que se puedan llegar a presentar en un futuro.

En cuanto a la integración con terceros, FORTINET se integra con otras tecnologías y plataformas, tanto a nivel on-premise como en la nube (AWS, Azure, Google Cloud), lo que la hace ideal para entornos híbridos y multi-nube.

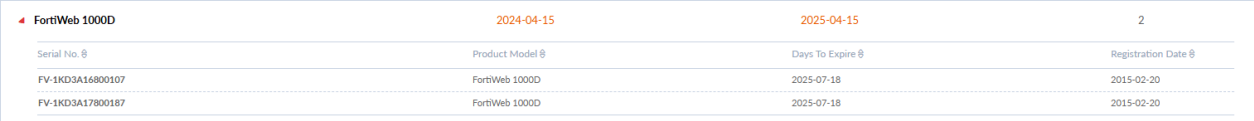
En consecuencia, cabe resaltar que la administración y gestión de la solución ofrece una facilidad frente a otras marcas para ajustar y parametrizar sus configuraciones pues sus reglas están basadas en objetos, grupos y agrupaciones individuales y/o conjuntas que agiliza y permite gestionar los cambios deseados en tiempo real, por lo que se tendría un tiempo eficaz de atención y respuesta a eventos o incidentes que se puedan llegar a presentar en la infraestructura del ministerio. Por otra parte, el equipo de ingenieros que operan las herramientas de seguridad perimetral posee conocimiento previo al uso y configuración de las soluciones FORTINET y por ello se facilitaría el manejo de la operación de la suite de seguridad y en el caso que se requiera de soporte especializado, FORTINET cuenta con un soporte técnico sólido a nivel local y mundial y una comunidad activa de usuarios y profesionales certificados (como NSE), lo cual es útil para resolución de problemas y buenas prácticas.

Teniendo en cuenta los tiempos actuales y la premura con la que cuenta el ministerio para la renovación del licenciamiento FORTINET, sea hace evidente que implementar otro fabricante o marca de seguridad perimetral que supla las necesidades actuales traería consigo tiempos más amplios de implementación, estabilización de la solución y capacitación en las herramientas, de igual forma, se tendría que tener en cuenta la curva de aprendizaje para operar las soluciones por parte de los administradores de la entidad.

Adicionalmente, el soporte actual contratado con fábrica expirará en el mes de julio y con el proveedor igualmente, esto es altamente riesgoso debido que de presentarse una incidencia o fallo en los equipos, no se tiene una opción para reponer o restaurar su parte física, de tal manera que se expone la Entidad a una posible interrupción de servicio dependiendo del daño o perder la alta disponibilidad que aunque se mantendría el servicio, al fallar este último se afectaría el acceso a los servicios de la Entidad en un gran porcentaje.

FIREWALLS DE APLICACIONES

Se cuenta con dos equipos WAF en HA (High Availability) adquiridos a finales de 2014 bajo el modelo **FortiWeb 1000D**. Estos equipos perimetrales operan en conjunto con los anteriormente mencionados firewalls, pues aumenta la protección contra ataques a las aplicaciones WEB de la entidad al inspeccionar el tráfico a un nivel más profundo, como su contenido y estructura de peticiones que son dirigidas a la aplicación.



FortiWeb 1000D	2024-04-15	2025-04-15	2
Serial No.	Product Model	Days To Expire	Registration Date
FV-1KD3A16800107	FortiWeb 1000D	2025-07-18	2015-02-20
FV-1KD3A17800187	FortiWeb 1000D	2025-07-18	2015-02-20

Imagen 2. Hardware lifecycle – FortiWeb 1000D.

Estos equipos que forman parte de la estrategia de seguridad de la entidad finalizan su capacidad de renovación por licenciamiento este año y su soporte físico el próximo, por lo que se hace necesario evaluar una nueva opción de capacidades para estos componentes de seguridad manteniendo arquitecturas que permitan una disponibilidad de servicio permanente.

Por otro lado, las capacidades por puerto en estos equipos requieren ser aumentadas dado que sus capacidades actuales están limitadas a 1Gbps, así como su throughput. Esto, sin mencionar que el hardware ha sido reemplazado dos veces durante los 10 años en que ha operado y que gracias a los contratos de soporte suscritos se ha logrado mantener la disponibilidad y estabilización de la solución de seguridad.

Como lo muestra la imagen 2, este hardware no presenta posibilidad de renovar licenciamiento y su soporte con fábrica se agotó, para lo cual se hace necesario adquirir una nueva solución que permita proteger y mantener las aplicaciones de forma segura.

Debido a que esta plataforma es especializada principalmente en el control del tráfico HTTP/HPTTS y entre otros protocolos, se hace necesario la renovación de la solución a fin de proteger y mitigar las aplicaciones misionales de la entidad, la no actualización de los equipos FortiWeb implicaría un alto riesgo a la seguridad perimetral, permitiendo que los intentos de ataques generados hacia la infraestructura critica se pudiesen perpetrar y ocasionar daños y perjuicios económicos y reputacionales.

Respecto a las actualizaciones de estos equipos (FortiWeb 1000D), de acuerdo con lo anterior se encuentra limitado la obtención de nuevas versiones de firmware pues este modelo de equipo no tiene más versiones liberadas por el fabricante exponiendo a un riesgo importante la seguridad y protección de las aplicaciones de la entidad.

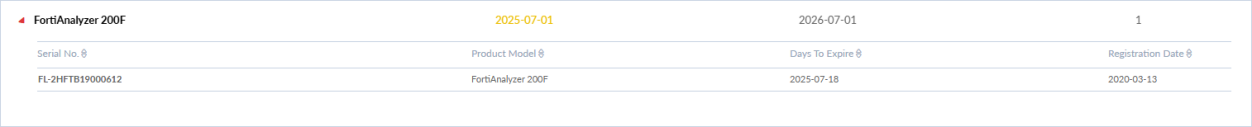
Frente a la gestión o administración, esta solución es práctica y flexible haciendo de la solución de WAF (Web Application Firewall) de FORTINET la más adecuada y adaptada a las necesidades de negocio de la entidad, permitiendo su integración con el firewall marca Fortinet, automatizando la generación de reglas y políticas en pro de robustecer la seguridad en ambos elementos.

Por otra parte, existen otras herramientas en el mercado local y global que permiten brindar un control de tráfico HTTP/HTTPS, sin embargo, estas otras plataformas no cuentan con integración nativa con el ecosistema Fortinet con el que actualmente la entidad cuenta, lo que permite a los administradores desarrollar tableros de visualización integrados en un único panel y despliegue de políticas automáticas en las herramientas de seguridad perimetral. En consecuencia y teniendo en cuenta los tiempos actuales y la premura con la que cuenta el ministerio para la renovación del licenciamiento FORTINET, sea hace evidente que implementar otro fabricante o marca de seguridad perimetral que supla las necesidades actuales traería consigo tiempos más amplios de implementación, estabilización de la solución y capacitación en las herramientas, de igual forma, se tendría que tener en cuenta la curva de aprendizaje para operar las soluciones por parte de los administradores de la entidad.

Es importante mencionar igualmente que el soporte actual con fábrica expirará en el mes de julio así como con el proveedor, y de presentarse un daño en el hardware, el fabricante no tendría responsabilidad y la Entidad asumiría un riesgo importante en la protección de sus aplicativos on premise, considerando que algunos de estos tienen lenguajes tipo legacy, fácilmente vulnerables.

ANALÍTICA DE LA SOLUCIÓN

Esta solución está conformada por un equipo, adquirido a finales de 2019 bajo el modelo **Fortianalyzer 200F**, el cual gestiona la seguridad recopilando, almacenando y analizando logs de dispositivos FORTINET, proporcionando visibilidad, análisis y automatización para mejorar la detección de amenazas y respuesta a incidentes.



FortiAnalyzer 200F	2025-07-01	2026-07-01	1
Serial No.	Product Model	Days To Expire	Registration Date
FL-2HFTB19000612	FortiAnalyzer 200F	2025-07-18	2020-03-13

Imagen 3. Hardware lifecycle – FortiAnalyzer 200F.

Esta solución ha sido un apoyo importante en la identificación de eventos de seguridad, pues dada su configuración se logra consolidar reportes detallados y personalizados mediante plantillas prestablecidas, según la necesidad y disponibilidad de estos. Este equipo, al recopilar un importante caudal de información se vuelve lento al ingreso de la gestión, teniendo niveles altos de respuesta y consumos de CPU.

La solución que opera en la Entidad cuenta con una capacidad de 1.6TB con una frecuencia de reporte según la necesidad, pues esta información es de tipo clasificada y solo se proporciona por directriz de la jefatura de la OTIC o por requerimiento de la Oficina de Control Interno. Ahora bien, con el incremento de servicios de tecnología el número de registros va en aumento lo que genera que cada día haya más DATA para verificar y de esta forma se pueda hacer una verificación más detallada, lo que genera que cada día el almacenamiento sobre este equipo sea más recurrente y se aplique una política de almacenamiento que permita tener una retención recomendada según los especialistas que corresponde a 60 días para la capacidad dispuesta.

De acuerdo con la imagen 3, el equipo solo se podría renovar por un año más previo a la salida de soporte por parte de fabricante. En otras palabras, el hardware actual que posee la entidad no tiene posibilidad de extender licencia y soporte por más de 1 año, lo que obliga a efectuar un cambio de hardware necesario en el componente de seguridad.

La integración de la solución FortiAnalyzer permite a la entidad, recopilar, almacenar y analizar registros (logs) de múltiples dispositivos Fortinet, asegurando correlacionar eventos de seguridad, Identificar patrones de ataque e Investigar incidentes de forma más rápida y eficiente. Por medio de los paneles de visualización la correlación de eventos y alertas, FortiAnalyzer puede ayudar a detectar amenazas que un dispositivo individual podría pasar por alto, de igual forma la herramienta permite crear reportes personalizados y automáticos para cumplir con auditorías, métricas de desempeño de seguridad, SLA, y normativas (ISO 27001, GDPR, NIST y entre otras).

En cuanto a la automatización el FortiAnalyzer puede integrarse con otros productos Fortinet para ejecutar acciones automáticas (por ejemplo, activar bloqueos) cuando se detecta una amenaza, mediante playbooks o reglas predefinidas.

Bajo lo anteriormente expuesto, el FortiAnalyzer ofrece cubrir las necesidades de la entidad en cuanto a la plataforma de análisis y reportes, permitiendo garantizar las capacidades de funcionamiento y operación por parte de los administradores de la entidad.

Otro aspecto, corresponde que estos guardan relación con las soluciones mencionadas pues el soporte con fábrica expirará en el mes de julio, así como con el proveedor que brinda el soporte y mantenimiento necesario para garantizar su funcionalidad. Estos componentes de seguridad son relevantes para la protección de los repositorios de información de la entidad por lo que no se recomienda dejarlos expuestos o sin la protección requerida ya que se pierde efectividad en la contención de ataques y visibilidad en la red para eventos de seguridad.

PREFIJO IPv6

El Ministerio de Ambiente y Desarrollo Sostenible dispone de un pool o grupo de direcciones asignadas por LACNIC desde 2019 bajo el prefijo **2801:1c:a800::/48**. Este direccionamiento ha venido siendo renovado con la finalidad de ejercer propiedad y control sobre este para las labores internas y externas de los servicios tecnológicos que desarrolla la entidad.

IPv6 es la última versión del protocolo IP y el sucesor de IPv4. Esencialmente, IPv6 proporciona un sistema de numeración más amplio y ofrece características mejoradas para la comunicación en red.

- Mayor capacidad de direcciones
- Mayor eficiencia en la red
- Redes más seguras
- Configuración de red más sencilla

Es necesidad de la entidad renovar la suscripción de este grupo de direcciones dado que, de no hacerlo, se tendría que reemplazar nuevamente en toda la red un nuevo direccionamiento haciendo la tarea mucho más dispendiosa y complicada.

SOLUCIÓN ANTI-DDoS

Se cuenta con un equipo de seguridad adquirido a finales de 2023 bajo el modelo **FortiDDoS 200F**. Esto, para contrarrestar los ataques de denegación de servicio distribuido (DDoS) y evitar que grandes cantidades de tráfico no confiable, saturen la red de la entidad. Esta solución perimetral fue adquirida en el año 2014 y recientemente fortalecida en capacidad y protección mediante una licencia activa que expirará en la actual vigencia.

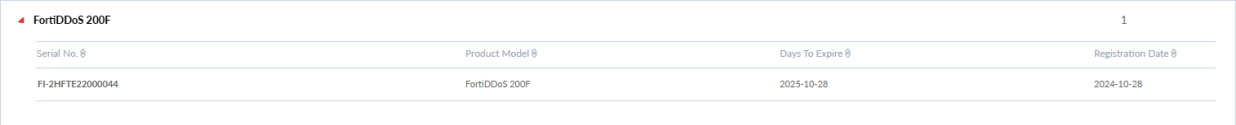


Imagen 4. Hardware lifecycle – FortiDDoS 200F.

El soporte con fábrica expirará en octubre, así como con el proveedor que brinda el soporte y mantenimiento necesario para garantizar su funcionalidad. Sin embargo, este equipo exclusivamente requiere renovación de licenciamiento de seguridad para ejercer su protección a cabalidad.

Esta solución de propósito específico de la marca FORTINET ha sido bastante efectiva en la contención de ataques desde su adquisición inicial; pues aparte del hardware, el licenciamiento de seguridad es necesario e importante, así como mantenerlo activo dado que con esta se mantiene actualizadas las bases de datos para la identificación y bloqueo de nuevas ciberamenazas que pueden cursar en el tráfico hacia las aplicaciones y sistemas de información de la entidad.

Para la administración de esta solución, esta resulta ser autónoma pues en su lógica de diseño y operación el dispositivo DDoS actúa de forma inmediata al detectar patrones no usuales, empleando umbrales específicos. Por ello, el equipo DDoS actuará de manera inmediata sin requerir de una acción u orden desde el administrador.

De acuerdo a lo anteriormente expuesto el Ministerio de Ambiente y Desarrollo Sostenible lleva operando con la marca FORTINET por más de 10 años, tiempo en el cual ha brindado una protección oportuna a la infraestructura TI que se tiene dispuesta para la adecuada prestación de los servicios informáticos, así como, una defensa proactiva mediante la evolución que han presentado las soluciones de seguridad adquiridas, lo que facilita la administración de las mismas, generando una rápida adaptación y comprensión de las herramientas y utilidades que dispone.

Otro aspecto para tener presente corresponde a que es una marca enfocada y especializada en seguridad, según Gartner; pues más del 30% de los dispositivos firewall instalados a nivel mundial son de esta marca, cuenta con más de 700 patentes que son empleadas y dispuestas en los dispositivos que se comercializan y muchas casas consultoras someten a los dispositivos FORTINET a múltiples pruebas de uso rudo y estrés, tales como: las pruebas de NSS Labs donde se elogia el Security Fabric, una suite de aplicaciones de siguiente generación que permite extender la ciberseguridad a toda la red mediante Forti-OS 7.0 el sistema

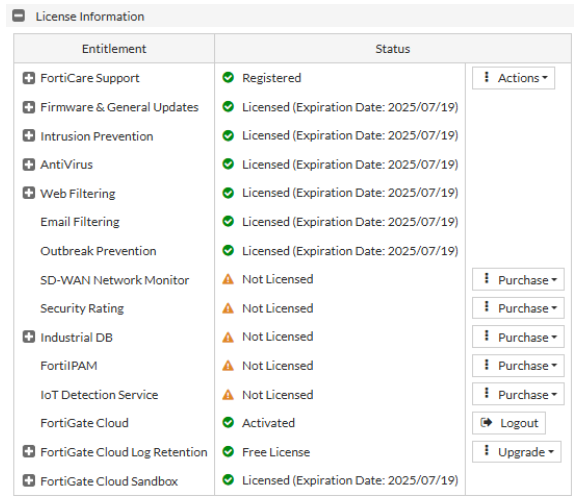
operativo de ciberseguridad más vanguardista e innovador, el cual se emplea en la gestión y administración actual del Ministerio.

Para la Entidad es importante que su plataforma tecnológica, con la que presta servicios a toda la ciudadanía de manera continua esté respaldada por marcas que generen confianza, calidad, confiabilidad, capacidad de integración y escalabilidad, de tal manera que proporcionen protección completa, resiliencia operativa y un alto nivel de rendimiento. FORTINET ha logrado para el Ministerio de Ambiente y Desarrollo Sostenible una solución especializada en ciberseguridad avanzada que brinda soluciones integrales para proteger redes, dispositivos, aplicaciones y datos frente a amenazas cada vez más sofisticadas, que garantiza la seguridad integral de las infraestructuras digitales dispuestas.

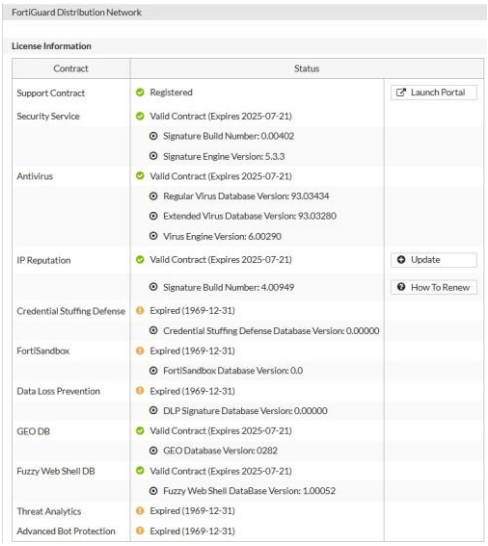
Ahora bien, la alta demanda de servicios en Internet genera plataformas más amplias de ataque y así mismo vislumbra fallas de seguridad que se convierten en vulnerabilidades esperando el momento menos esperado para que un actor malicioso explote una de ellas y ponga en riesgo la integridad, disponibilidad y confidencialidad de la información (activo de alto valor).

Así las cosas, esta necesidad no solo está dada por la capacidad de recursos y medios de los equipos, sino por el cercano vencimiento del licenciamiento de seguridad y de contratos de soporte y mantenimiento especializado que se tiene, ya que de no renovar esto, se expone a la Entidad de manera peligrosa a que sus activos de información y de misión crítica sean fácilmente vulnerables. Esto, sin mencionar que este componente perimetral y de seguridad forma parte del cumplimiento normativo y el apoyo necesario en la gestión institucional, así como la disponibilidad de herramientas a los servidores públicos en el cumplimiento de su labor.

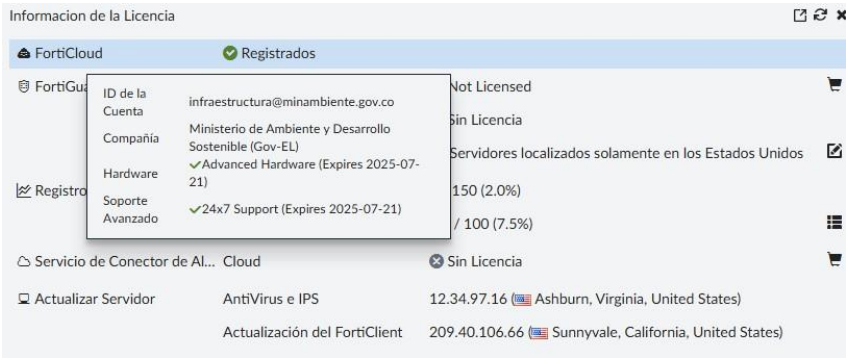
En conclusión, FORTINET ofrece cubrir las necesidades de la entidad en cuanto a la plataforma de seguridad perimetral, permitiendo garantizar las capacidades de funcionamiento y operación por parte de los administradores de la entidad.



Estado de licenciamiento – Fortigate 600E.



Estado de licenciamiento – FortiWeb 1000D.



Estado de licenciamiento – FortiAnalyzer 200F.

License Informations

Name	Status	
Firmware	Firmware: Hardware:	Web/Online (Expires: 2025-11-12) Web/Online (Expires: 2025-11-12)
Enhanced Support	Enhanced Support:	24/7 (Expires: 2025-11-12)
IP Reputation	Expiry: Version: Last Successful Check:	Web/Online (Expires: 2025-11-12) 4.949 (2025-05-13) 2025-01-14 13:34:12
Domain Reputation	Expiry: Version: Last Successful Check:	Web/Online (Expires: 2025-10-31) 00007.421 (2025-05-22) 2025-01-14 13:34:12

Estado de licenciamiento – FortiDDoS 200F.

HERRAMIENTA DE VULNERABILIDADES

Esta herramienta denominada TENABLE brinda una solución en la gestión de exposición y vulnerabilidades, identificando y permitiendo mitigar riesgos en la infraestructura de TI, así como en los servicios WEB publicados del Ministerio de Ambiente y Desarrollo Sostenible.

Esta fue inicialmente adquirida en 2020 y por los resultados que se obtuvieron, se ha mantenido un proceso de renovación del licenciamiento mediante los contratos suscritos por la entidad, permitiendo así año tras año, fortalecer mediante buenas prácticas el procedimiento de publicación de nuevos servicios en internet, evitando exponer la disponibilidad e integridad de los aplicativos, sistemas de información, servidores e información.

Actualmente la suscripción cuenta con cubrimiento para 100 máquinas virtuales o nodos y 30 licencias de WAS (Web Application Scanning) para las aplicaciones objeto de evaluación. Estas últimas, han permitido identificar vulnerabilidades y remediarlas empleando ajustes de código por parte del personal de desarrollo y así cerrar brechas en seguridad. Por otro lado, se ha logrado evidenciar que existen varios aplicativos antiguos, con lenguajes de código obsoleto y para lo cual no es posible remediar las vulnerabilidades detectadas; por lo que se hace necesario adoptar nuevas medidas con estos aplicativos.

En virtud de lo anterior, el Ministerio de Ambiente y Desarrollo Sostenible requiere fortalecer su arquitectura de seguridad perimetral con la adquisición de nuevos componentes de Firewall Perimetrales, Firewall de Aplicaciones y de Analítica de Solución con mejores capacidades y licenciamiento de seguridad así como la renovación del licenciamiento para la solución de DDoS y herramienta de vulnerabilidades TENABLE y prefijo IPv6, permitiendo mantener el framework de seguridad de la información con el que cuenta actualmente la Entidad, contando con una plataforma renovada y disponible para la prestación de nuevos servicios.

Esta contratación se encuentra incluida en el Plan de Adquisiciones de la vigencia 2025 en la línea 056.

2. OBJETO:

15-0056 Garantizar la continuidad, soporte, garantía y mantenimiento de la solución de seguridad perimetral, así como la adquisición de los componentes tecnológicos necesarios para la protección de la infraestructura tecnológica, con el fin de fortalecer la seguridad perimetral y la gestión de vulnerabilidades del Ministerio de Ambiente y Desarrollo Sostenible.

2.1 ALCANCE:

LOTE 1 – SOLUCIÓN PERIMETRAL

- Adquirir mediante equipos de propósito específico y suscripción de licenciamiento y soporte con fabricante, nuevas capacidades para la gestión de seguridad perimetral del Ministerio de Ambiente y Desarrollo Sostenible
- Debe integrarse nativamente con las plataformas de seguridad perimetral que tiene la entidad garantizando su interoperabilidad y máximo nivel de integración con los demás componentes de infraestructura TI.
- Los equipos de propósito específico tendrán una garantía por periodo de un (1) año en un esquema 7 x 24 ante fabricante.
- Servicios de instalación, configuración, puesta en marcha y afinamiento de cada uno de los equipos de propósito específico.
- Renovación de la suscripción de licenciamiento de la solución DDoS deberá quedar activa a partir del momento del perfeccionamiento del contrato, el nuevo periodo será de un (1) año en un esquema 7 x 24 ante fabricante.
- Soporte técnico por demanda y transferencia de conocimiento a mínimo tres (3) personas responsables de la administración de herramienta.
- El centro de atención al cliente del proveedor debe asegurar el cumplimiento del servicio de garantía solicitado por la entidad hasta que se haya terminado y solucionado, luego solicitará a la entidad la autorización para cierre a través de una notificación.
- Garantizar una disponibilidad de mínimo el 98% de la solución tecnológica, excluyendo horarios de actualizaciones, los cuales deben ser informados con mínimo 72 horas de anticipación), 24 horas al día 7 días a la semana, por el termino establecido de la licencia en la presente ficha técnica.
- ANS se determinarán en conjunto con el oferente adjudicado y en conjunto con el supervisor del contrato.
- Evaluaciones de seguridad para garantizar la correcta implementación de la solución perimetral.
- Evaluaciones de seguridad a la red durante el tiempo de la vigencia de la garantía.

LOTE 2 – Solución de Herramienta de Análisis de Vulnerabilidades

- Renovación por un (1) año de la consola en nube con la que cuenta la Entidad y con los recursos definidos por el fabricante para gestionar los siguientes activos de manera óptima.
- Renovación de las suscripciones un (1) año de la Herramienta de Análisis de Vulnerabilidades Tenable IO cien (100) en total.
- Renovación de treinta (30) suscripciones Tenable WAS para analizar los diferentes portales y servicios de la Entidad.
- La activación de la suscripción de la licencia debe quedar activa a partir del momento del perfeccionamiento del contrato y con vigencia de 12 meses.
- Servicios de activación y puesta en marcha de las suscripciones, configuración y parametrización de la herramienta y sus componentes, soporte técnico por demanda y transferencia de conocimiento a mínimo tres (3) personas responsables de la administración de herramienta.
- El centro de atención al cliente del proveedor debe asegurar el cumplimiento del servicio de garantía solicitado por la entidad hasta que se haya terminado y solucionado, luego solicitará a la entidad la autorización para cierre a través de una notificación.
- Garantizar una disponibilidad de mínimo el 98% de la solución tecnológica, excluyendo horarios de actualizaciones, los cuales deben ser informados con mínimo 72 horas de anticipación), 24 horas al día 7 días a la semana, por el termino establecido de la licencia en la presente ficha técnica.

- ANS se determinarán en conjunto con el oferente adjudicado y en conjunto con el supervisor del contrato.

3. CARACTERÍSTICAS O ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO A CONTRATAR:

El objeto contractual se desarrollará de acuerdo con la descripción, especificaciones y demás condiciones establecidas en el pliego de condiciones, las fichas técnicas, adendas y la propuesta presentada por el contratista, los cuales hacen parte integral de este contrato.

Con el presente objeto, el Ministerio de Ambiente y Desarrollo Sostenible recibirá:

LOTE 1 – SOLUCIÓN PERIMETRAL

ÍTEM A	DESCRIPCIÓN
MARCA – ESPECIFICAR POR EL PROPONENTE	
MODELO – ESPECIFICAR POR EL PROPONENTE	
Subítem	**Generalidades**
1.1	Adquisición de dos (2) appliances de seguridad informática perimetral con sistema operativo propietario del fabricante, que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento.
1.2	La solución debe estar en la capacidad de soportar alta disponibilidad.
1.3	El dispositivo debe ser equipos de propósito específico, no se aceptan implementaciones en sistemas de propósito general como PC o servidor, usando sistemas operativos genéricos como Windows, Linux, BSD, Solaris, Apple MacOS o GNU
1.4	El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de trafico
1.5	El dispositivo debe ser nuevo de fábrica, no se aceptan soluciones remanufacturadas. Se debe proveer certificación del fabricante donde se evidencie que los equipos son nuevos, esta debe estar dirigida a la entidad especificando el número y objeto del proceso. La certificación debe ser expedida con una fecha de al menos 30 días antes de la presentación de la propuesta.
1.6	La solución deberá pertenecer al cuadrante de líder de Gartner para Network Firewall en los tres (03) últimos reportes.
1.7	La solución deberá pertenecer al cuadrante de líder de Gartner para SDWAN en el último reporte.
1.8	El dispositivo debe soportar e incluir las funcionalidades de: Firewall, IPS, Control de Aplicaciones, Filtrado Web, Antivirus perimetral, SDWAN y DLP.
1.9	Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad podrá dar seguimiento a los casos abiertos por el oferente.
1.10	Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad podrá acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante.
1.11	La solución debe contar con Fuente de poder redundante incluida en la oferta no por separado.
2.	**Rendimiento**

2.1	El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
2.2	• Rendimiento de Firewall en Ipv4 150 Gbps o superior
2.3	• Rendimiento de Firewall en Ipv6 150 Gbps o superior
2.4	• Rendimiento de IPS 42 Gbps o superior
2.5	• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 30 Gbps o superior
2.6	• Rendimiento Protección de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 30 Gbps o superior
2.7	• Rendimiento IPSec VPN 55 Gbps o superior
2.8	• Soporte de 16 Millones sesiones concurrentes o superior
2.9	• Rendimiento de Inspección SSL 16 Gbps o superior
2.10	• Soporte de 10.000 usuarios concurrentes VPN SSL o superior
2.11	• Rendimiento de VPN SSL 10 Gbps o superior
3.	**Conectividad**
3.1	El equipo deberá contar con las siguientes interfaces de conexión:
3.2	• 2 puertos USB
3.3	• 1 x GE RJ45 puerto de consola (Administración)
3.4	• 1 x 2.5/1 GE RJ45 interfaz (dedicada a la alta disponibilidad). (El proponente deberá incluir los cables de conexión UTP CAT 6A)
3.5	• 16 interfaces de 1 GE RJ45 (El proponente deberá incluir los cables de conexión UTP CAT 6A)
3.6	• 8 interfaces de 1 GE SFP - Transceivers requeridos mínimo ocho (8) SFP multimodo por equipo. (El proponente deberá incluir los cables de conexión en fibra óptica tipo LC-LC)
3.7	• 4 interfaces de 10 GE SFP+ - Transceivers requeridos mínimo cuatro (4) SFP+ multimodo por equipo. (El proponente deberá incluir los cables de conexión en fibra óptica tipo LC-LC)
3.8	• 4 x 25GE/10GE SFP28/SFP+ ULL (ultra-low latency) interfaces - Transceivers requeridos mínimo cuatro (4) SFP+ 25GE multimodo por equipo. (El proponente deberá incluir los cables de conexión en fibra óptica tipo LC-LC)
3.9	Para la conexión de los Firewalls a los Switches Core Actuales de la entidad el proponente deberá suministrar ocho (08) de la marca HPE JL293A X190 25G SFP28 LC SR 100m MM Transceiver, con el objetivo de garantizar que todas conexiones puedan ser exitosas en la etapa de implementación.
4.	**Address Traslation**
4.1	La plataforma debe soportar e incluir los siguientes tipos de traducción de direcciones:
4.2	• NAT y PAT
4.3	• NAT estático
4.4	• NAT: destino, origen
4.5	• NAT, NAT64 persistente
5.	**Funciones básicas de Firewall**
5.1	El NGFW debe incluir la capacidad de operar en los siguientes modos: * Sniffer: Usando un puerto SPAN o mirror de la red.

	* Capa 2: Ubicado en línea con el tráfico, haciendo inspección del tráfico que cursa a través de él, sin ser un salto IP en el mismo. * Capa 3 o Modo Gateway: Ubicado en línea con el tráfico, comportándose como un salto de enrutamiento en la red y haciendo inspección del tráfico que cursa a través de él.
5.2	Las reglas de firewall deben analizar las conexiones que pasen por el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
5.3	La solución debe integrarse con el directorio activo y soportar políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acu3.3erdo con el grupo de pertenencia de los usuarios.
5.4	Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada
5.5	Debe estar en la capacidad de integrase con plataforma Cloud IaaS como: AWS, Azure, Google etc. Con el fin de generar y actualizar objetos de direcciones de manera automática basado en los parámetros de red (IP, TAG etc) de las instancias desplegadas en la nube y estas ser usadas como objetos de reglas o políticas de firewall
5.6	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface) como por GUI (Graphical User Interface).
5.7	La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP
5.8	El dispositivo será capaz de crear e integrar políticas contra ataques DoS (Denial of service) las cuales se deben poder aplicar por interfaces
5.9	El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
5.10	Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
5.11	El equipo firewall debe permitir limitar el número de dispositivos asociados a un mismo invitado.
5.12	Debe soportar e incluir la identificación de dispositivos y sistemas operativos, con clasificación automática, y permitir la visualización de esta información.
5.13	Soporte de reglas basadas en servicios cloud populares de Internet, en donde se tiene una base de datos que se actualiza dinámicamente. Esta base de datos puede usarse también en enrutamiento y balanceo de enlaces o SD-WAN. Sin costo adicional a la entidad o sin dependen de suscripciones para su activación.
5.14	Permitir almacenar localmente versiones de configuración después de acceder al equipo, y permitir hacer rollback a una configuración anterior en caso de ser necesario. Debe ser posible comparar dos versiones de configuración para per las diferencias entre las mismas, en la GUI del Firewall. El histórico de versiones de configuración debe ser visible tanto por GUI como por CLI.
5.15	La solución de firewall deberá permitir la visibilidad de la red a través de una interfaz simple, flexible y de acceso vía web. Deberá estar en capacidad de almacenar un historial detallado de atributos de todos los puntos finales que se conectan a la red, usuarios (incluidos tipos como invitados, empleados, contratistas, etc.) en la red hasta los detalles de la aplicación de punto final.
6.	**Conectividad y Enrutamiento**

6.1	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
6.2	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
6.3	Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP
6.4	La solución podrá habilitar políticas de ruteo en IPv6
6.5	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
6.6	El dispositivo debe realizar balanceo de carga de enlaces mediante el uso de los siguientes algoritmos: - Ancho de banda - Sesiones - Spillover - IP fuente – destino - IP fuente
6.7	La Solución deberá soportar e incluir el balanceo de enlaces WAN inteligente (SD-WAN Seguro) sin licencia o suscripciones adicionales basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)
7.	**VPN IPSEC**
7.1	El equipo deberá soportar las siguientes características:
7.2	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
7.3	Soporte para IKEv2 y IKE Configuration Method.
7.4	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
7.5	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
7.6	Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN client-to-site.
7.7	Se deben soportar VPNs basadas en rutas y VPNs basadas en políticas.
8.	**VPN SSL**
8.1	Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
8.2	Soporte a SSL 2.0 y 3.0, TLS 1.0,1.1 y 1.2
8.3	Soporte para modo de operación basado en web o modo túnel.
8.4	Debe soportar Split Tunel, de tal forma que el tráfico hacia internet no se enrute por la VPN
8.5	Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
8.6	Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
8.7	Capacidad de realizar SSL VPNs por usuarios sin incurrir en costos adicionales.
8.8	Soporte a certificados PKI X.509 para construcción de VPNs SSL.
8.9	Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
8.10	Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
8.11	Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios.
9.	**Autenticación**

9.1	El dispositivo deberá manejar los siguientes tipos de autenticación:
9.2	Capacidad de soporta autenticación local y remota integrándose con Servidores de Autenticación RADIUS, LDAP o TACACS+.
9.3	Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
9.4	Soporte de Token Físicos o Mobile sobre Smartphone basado en IOS o Android, token de SMS, email o con plataformas de terceros como RSA SecurID.
9.5	Capacidad de soportar autenticación de acceso de usuario a través de 802.1x y portal cautivo.
9.6	Capacidad de realizar 2FA mediante tokens que se integren a la plataforma de mínimo 5000.
9.7	Debe estar en capacidad de proporcionar autenticación fuerte por medio de software token para al menos los siguientes entornos: A. Portales Web de la Entidad. B. VPNs IPSec y SSL Actuales de la Entidad. C. Logon de estaciones Windows.
9.8	La solución ofertada de Token Móviles deberá ser desarrollada por el mismo proveedor de la solución de Firewall propuesta en este proceso contractual. Los Tokens deben poder usarse tanto para Autenticación de VPNs actuales. En el caso del uso para autenticación de VPNs deben tener integración directa con la plataforma del Firewall VPNs IPSec y SSL ofertada. Se deberá suministrar 200 tokens como mínimo disponible por la marca ofertada.
9.9	Debe estar en capacidad de administrar switches y Access point para servir como plataforma de una red Secure SD-LAN.
9.10	La solución debe estar en capacidad de integrarse con el Directorio Activo de la entidad
9.11	Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
9.12	Debe soportar la identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server.
10.	**Manejo de tráfico y calidad de servicio.**
10.1	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix, por ejemplo), se requiere que la solución incluya la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.
10.2	El equipo debe soportar e incluir traffic shaper basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs.
10.3	Capacidad de poder asignar parámetros de traffic shapping a través de reglas de manera independiente
10.4	Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión

10.5	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación y categoría URL de las mismas para la regla en general.
10.6	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kilobits por segundo
11.	**Antimalware**
11.1	Debe soportar e incluir granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
11.2	Capacidad de realizar filtrado por interceptación de tráfico DNS Sinkhole para el bloqueo de tráfico hacia dominios maliciosos.
11.2	El IPS debe tener la posibilidad de tomar las siguientes acciones: permitir, monitorear, bloquear, resetear la sesión, guardar copia de los paquetes que coincidan con las firmas, hacer cuarentena con base en dirección IP del atacante y tiempo basado en días, horas o minutos
11.3	Debe estar en capacidad de detener más de 11000 amenazas, incluyendo evasiones.
11.4	El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
11.5	El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA.
11.6	La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.
11.7	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP, MAPI
11.8	El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.
11.9	Debe soportar la inspección de archivos comprimidos como los son: GZIP, RAR, LZH, IHA, CAB, ARJ; ZIP entre otros con el fin de proteger contra estas técnicas de evasión.
11.10	El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.
12.	**Filtrado WEB**
12.1	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.
12.2	Debe poder categorizar contenido Web requerido mediante IPv6.
12.3	Será posible exceptuar la inspección de HTTPS por categoría.
12.4	Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID
12.5	El firewall deberá contar con bloquea de dominios asociados con phishing, malware, botnets y otras categorías de alto riesgo (criptominería, dominios recién vistos, etc.)
12.6	Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.

12.7	El filtrado debe ser sobre tráfico http y https.
13.	**Protección contra intrusos (IPS)**
13.1	El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
13.2	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico Ipv6. A través de sensores.
13.3	Capacidad de detección de más de 7000 ataques.
13.4	El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
13.5	Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.
14.	**Control de Aplicaciones**
14.1	La solución debe soportar e incluir la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
14.2	Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como: - Tecnología utilizada en las aplicaciones (Client-Server, Browser Based, Network Protocol). - Nivel de riesgo de las aplicaciones. - Categoría y sub-categoría de aplicaciones.
14.3	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
14.4	La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.
14.5	Reconocer por lo menos 4000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
14.6	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log y resetear conexión
14.7	Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.
14.8	Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
15	**Inspección de Contenido SSL/SSH**

15.1	La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3 y FTP en su versión segura
15.2	Debe ser posible definir perfiles de inspección SSL donde se definan los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad.
15.3	La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection.
16	**Alta Disponibilidad**
16.1	El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6
16.2	Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.
16.3	Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
16.4	La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.
16.5	El equipo debe soportar hasta 4 equipos en esquema de HA.
16.6	Debe incluir doble fuente
16.7	Debe tener máximo 1 unidad de Rack por equipo.
17	**Visibilidad**
17.1	La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.
17.2	El sistema deberá contar con una gestión centralizada que permita la configuración, el registro, la supervisión e informes de eventos.
17.3	Deber tener la capacidad de poder validar con que política la sesión se está coincidiendo y un link hacia la misma.
17.4	De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.
18	**Características de Administración**
18.1	Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)
18.2	Interfase basada en línea de comando (CLI) para administración de la solución.
18.3	Debe permitir exportar las reglas de seguridad en al menos dos de los siguientes formatos: CSV, JSON y PDF
18.4	Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
18.5	La solución de firewall deberá permitir la creación de políticas y ver informes por usuario (Directorio Activo), red (por IP), dispositivo de red, subred interna.

18.6	Debe tener la capacidad de gestionar todas las políticas de seguridad, además de poder gestionar Switches y APs dentro de una única consola de gestión Debe estar en capacidad de administrar switches y Access point para generar una red SD- LAN administrada y gestionada desde el mismo Firewall.
19.	**Virtualización**
19.1	El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"
19.2	Debe soportar e incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
19.3	Cada instancia virtual debe poder tener un administrador independiente
19.4	Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red
19.5	Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.
20	**Licenciamiento y actualizaciones**
20.1	El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
20.2	La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos un (1) año.
20.3	La plataforma es requerida por un periodo de un (1) año en un esquema de soporte 7x24 ante el fabricante.
20.4	El equipo debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono

ÍTEM B	**ANALÍTICA DE LA SOLUCIÓN** **DESCRIPCIÓN**
MARCA – ESPECIFICAR POR EL PROPONENTE	
MODELO – ESPECIFICAR POR EL PROPONENTE	
Subítem	**Generalidades**
1.1	Adquisición de un equipo tipo appliance físico que permita registrar cada transacción de la plataforma de seguridad perimetral, para poder identificar y reaccionar a cualquier informe emitido por un log o registro de los dispositivos de seguridad perimetral ofertados
1.2	El dispositivo debe ser nuevo de fábrica, no se aceptan soluciones remanufacturadas. Se debe proveer certificación del fabricante donde se evidencie que los equipos son nuevos, esta debe estar dirigida a la entidad especificando el número y objeto del proceso. La certificación debe ser expedida con una fecha de al menos 30 días antes de la presentación de la propuesta.
1.3	El equipo deberá recolectar y emitir el reporte de e ventos, actividades y tendencias ocurridas en las plataformas de seguridad perimetral ofertadas.
1.4	Debe ser de la misma marca que todas las soluciones ofrecidas para garantizar optima seguridad e integración nativa entre todos los componentes.
1.5	La solución de análisis de logs debe dar soporte a las siguientes características:

1.6	Capacidad de recibir hasta 100 GB o superior de logs diarios.
1.7	Capacidad de Almacenamiento de 8 Terabytes, después de RAID 4 TB o superior.
1.8	4 interfaces de red de 1Gbps Mbps Cobre (El proponente deberá incluir los cables de conexión UTP CAT 6A).
1.9	Capacidad de recibir logs hasta de 180 equipos sin necesidad de licencias adicionales.
1.10	Los discos deben soportar arreglos de al menos RAID 0/1
2.	**Funciones y configuraciones requeridas para el analizador de red**
2.1	Visor de tráfico en tiempo real.
2.2	Visor de tráfico histórico.
2.3	Visor personalizado de log de tráfico
2.4	Herramienta de búsqueda sobre los logs de tráfico.
3.	**Análisis de logs y reportes requeridos**
3.1	Vista de búsqueda y manejo de logs.
3.2	Reportes basados en perfiles.
3.3	Inventario de plantillas predefinidas para reportes regulares
3.4	Debe soportar de forma predefinida los reportes:
3.5	Eventos del sistema
3.6	Análisis de riesgo y aplicaciones
3.7	Reporte de Aplicaciones y Ancho de Banda
3.8	Reputación de Clientes
3.9	Análisis de seguridad
3.10	Reporte de Amenazas
3.11	Reportes de VPN
3.12	Reportes de uso de Web
3.13	Reportes de WiFi
3.14	Debe ser posible calendarizar los reportes
3.15	La plataforma deberá permitir integrar los logs de las plataformas de Firewall ofertadas.
4.	**Licenciamiento requerido para la solución de analítica de logs.**
4.1	La solución deberá ser licenciada con soporte y garantía ante el fabricante por un (1) año.
4.2	El equipo debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono
4.3	La solución deberá incluir módulos de indicadores de compromiso y servicio de detección de propagación de amenazas por un (1) año.
4.4	La solución deberá incluir un servicio de respuesta de seguridad automatizada por un (1) año.
4.5	La solución deberá incluir un servicio para el reporte y descubrimiento de aplicaciones no avaladas por TI, tipo Shadow IT.
4.6	La solución deberá incluir un servicio que permita evaluar y puntuar las configuraciones de seguridad en los equipos integrados y entregar un reporte de las mejores prácticas recomendadas para la mitigación de brechas con la finalidad de poder robustecer las funcionalidades de seguridad.

ÍTEM C	**SOLUCIÓN DE FIREWALL DE APLICACIONES WEB**
	DESCRIPCIÓN
MARCA – ESPECIFICAR POR EL PROPONENTE	
MODELO – ESPECIFICAR POR EL PROPONENTE	
Subítem	**Generalidades**
1.2	Adquisición de dos (2) Firewall de propósito específico para la protección de aplicaciones web (HTTP/HTTPS).
1.3	El dispositivo debe ser nuevo de fábrica, no se aceptan soluciones remanufacturadas. Se debe proveer certificación del fabricante donde se evidencie que los equipos son nuevos, esta debe estar dirigida a la entidad especificando el número y objeto del proceso. La certificación debe ser expedida con una fecha de al menos 30 días antes de la presentación de la propuesta.
1.4	Las plataformas deberán ser de propósito específico en las premisas de la entidad (físico).
1.5	La solución debe brindar protección para aplicaciones web y APIs contra ataques externos, internos y exploits conocidos y zero-day.
1.6	La solución debe tener capacidad de Machine Learning para la contención de ataques y/o vulnerabilidades de zero-day.
1.7	La solución debe tener capacidad de protección para aplicaciones web, protección de APIs y Mitigación contra bots.
1.8	La solución debe operar en los siguientes modos, sin que incurra en gastos extras para entidad: -Reverse Proxy -Inline Transparent -True Transparent Proxy -Offline Sniffing -WCCP
1.9	La solución debe estar en la capacidad de aplicar reglas de seguridad web, tales como: -AI-based Machine Learning -Automatic profiling (white list) -Web server and application signatures (black list) -IP address reputation -IP address geolocation -HTTP RFC compliance -Native support for HTTP/2 -WebSocket protection and signature enforcement -Man in the Browser (MiTB) protection
1.10	La solución debe tener protección contra ataques de aplicación: -OWASP Top 10 -Cross Site Scripting -SQL Injection -Cross Site Request Forgery -Session Hijacking

	-Built-in Vulnerability Scanner -Third-party scanner integration (virtual patching) -File upload scanning with AV and sandbox.
1.11	La solución debe permitir la autenticación por medio de: -Active and passive authentication -Site Publishing and SSO -RSA Access for 2-factor authentication -LDAP -RADIUS and SAML support -SSL client certificate support -CAPTCHA and Real Browser Enforcement (RBE)
1.12	La solución debe permitir la protección de APIs: -Machine Learning based API Discovery and Protection -XML and JSON protocol conformance -CI/CD integration -Schema verification -API Gateway -Web services signatures
1.13	La solución debe permitir la protección contra ataques de Bots: -Machine Learning based Bot Mitigation -Biometrics Based Detection -Threshold Based Detection -Bot Deception -Know Bots
1.14	La solución debe permitir funcionalidades de capa 7: -Layer 7 server load balancing -URL Rewriting -Content Routing -HTTPS/SSL Offloading -HTTP Compression -Caching
1.15	La solución debe permitir servicios de seguridad embebidos en el dispositivo tales como: -Detección de Malware -Parchado Virtual -Validación de protocolos -Protección contra ataques de fuerza bruta -Encripción y protección de cookies. -Puntuación y criticidad de las amenazas -Detección con XSS y SQLi -Seguridad en cabeceras de HTTP. -Personalización de mensajes de error y código. -Firmas de intrusión en el S.O. -Protección contra amenazas conocidas y de Zero-Day. -Prevención de DoS. -Correlación con multiples elementos de seguridad. -Protección contra la desconfiguración de sitios web.

1.16	La solución debe proporcionar módulos de alertas y monitoreo: --Notificaciones SNMP, email, reporte a Dashboard, Registro y almacenamiento de logs. Además, la solución debe contar con módulos para la administración de la plataforma y visualización de eventos. -Web user interface -Command line interface -View graphical analysis and reporting tools -Central management for multiple FortiWeb devices -Active/Active HA Clustering -REST API -Centralized logging and reporting -User/device tracking -Real-time dashboards -Bot dashboard -OWASP Top 10 attack categorization -Geo IP Analytics -SNMP, Syslog and Email Logging/ Monitoring -Administrative Domains with full RBAC
1.17	La solución debe cumplir con los siguientes requerimientos de hardware: -Interfaces de red: 8 x GE RJ45 bypass, 4x SFP GE (no bypass), 2xSFP+ 10GE (se deben incluir todos los tranceivers de la misma marca del fabricante y cables UTP CAT 6ª para las conexiones de RJ45). -Storage – 2 X 480 GB SSD o superior. -Maxímo 2 Unidades de Rack por equipo. -Throughput 2.5 Gbps o superior -Latency menor o igual a 5ms -Administrative Domains 64 o superior -Alta disponibilidad - Clusterizado en Active/Passive y/o Active/Active -Fuente de poder redundante por equipo (Dual Hot Swappable). -Certificaciones de seguridad: FCC Class A Part 15, RCM, VCCI, -CE, UL/CB/cUL
1.18	Debe integrarse a la plataforma de reportes FORTIANALYZER a adquirir por el Ministerio.
1.19	Debe integrarse nativamente con el Firewall de nueva generación a adquirir por el Ministerio
2.	**Licenciamiento de la solución**
2.1	La solución deberá ser licenciada con soporte y garantía ante el fabricante por un (1) año.
2.2	El equipo debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 1 año en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono
2.3	La solución debe licenciar por 1 año los siguientes módulos: -Web Security -IP Reputation -Antimalware -Cloud Sandbox

	-Credential Stuffing Defense -Threat Analytics

ÍTEM D	**RENOVACIÓN PREFIJO IPv6**	
Subítem	**Descripción**	
1.1	El Ministerio de Ambiente y Desarrollo Sostenible, requiere renovar el registro de direcciones IPV6 (2801:1c:a800::/48) con el que cuenta actualmente.	
1.2	El contratista debe realizar todas los tramites técnicos, administrativos y financieros que sean necesarios ante el organismo LACNIC - Latin America & Caribbean Network Information Center (en Español Registro de Direcciones deInternet de América Latina y Caribe) para la renovación del prefijo de direcciones IPV6 que tiene asignado al Ministerio de Ambiente y Desarrollo Sostenible	
1.3	El contratista debe cumplir con los requisitos y exigencias definidas por LACNIC para realizar todos los trámites de renovación.	
1.4	El contratista debe cumplir con la política de seguridad de la información definida por el Ministerio.	
1.5	El contratista debe entregar a la Entidad la documentación técnica y administrativa que se derive del objeto contractual incluidos los comprobantes de pago efectuados a LACNIC.	

ÍTEM E	**RENOVACIÓN DE LICENCIAMIENTO - FORTIDDoS**		
Subítem	**DESCRIPCIÓN**		**Cumple Si/No**
1.2	Especificaciones	El oferente deberá entregar y activar las renovaciones de licenciamiento y de soporte del siguiente equipo: **FortiDDoS 200F** bajo serial **FI-2HFTE22000044**	
1.3	Vigencia	La renovación es requerida por un periodo de 12 meses en un esquema 7x24 ante fabricante con las mismas características y servicios actuales con que cuenta la plataforma actual. La renovación de las plataformas y los servicios de soporte deben tener una única fecha de vigencia, para el servicio de soporte ante el fabricante y soporte con partner (canal), la garantía, licenciamiento y actualizaciones para todos los productos, deberá aplicarse y quedar activa a partir del perfeccionamiento del contrato o posterior y con vigencia de 12 meses.	
1.4		El oferente (Partner Expert o advance del fabricante) deberá realizar afinamiento, configuración y activación del licenciamiento, así mismo, el oferente será el primer nivel de atención para el MINISTERIO DE AMBIENTE Y	

		para el servicio de soporte, además el oferente será quien mediará cualquier interacción con el fabricante en caso de ser necesario.	
1.5		El oferente deberá presentar al menos tres (3) especialidades técnicas correspondientes al mismo fabricante, tal como fue definido desde el estudio de mercado y conforme con el alcance técnico y el monto de inversión del proceso.	
1.6		Presentar plan de trabajo 5 días después de firmada el acta y cumplimiento de los requisitos del perfeccionamiento del contrato para realizar cada una de las actividades requeridas para la activación de las licencias en conjunto con el supervisor del contrato.	
1.7		Realizar durante la ejecución del contrato, el diagnóstico inicial de configuración de la infraestructura actual y plantear las mejoras sugeridas, actividad que realizará personal certificado en la marca sin que esto genere gastos o cobros adicionales para el MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. Realizar la verificación del estado actual del modo de operación/umbrales/objetos configurados en los equipos, informar sobre los hallazgos encontrados y realizar las recomendaciones para mejorar la optimización de las políticas configuradas, debe entregarse informe con los diagnósticos emitidos al supervisor del contrato.	
1.8		El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas, consultas sobre funcionamiento y/o configuración de los dispositivos y requerimientos de soporte por cualquier medio (correo electrónico, sesiones remotas y atención en sitio en caso de requerirse) en horario 24/7/365/4. (Las 24 horas del día, los siete días de la semana, los 365 días del año, con un tiempo máximo de atención de cuatro (4) horas, soporte proactivo, reactivo. Todo con respecto a las plataformas ofertadas y objeto del presente contrato.	
1.9		El proveedor deberá realizar dos (2) mantenimientos preventivos al total de los equipos sujetos a la renovación, mientras dure la garantía, los cuales deben ser acordados con el supervisor del contrato.	
1.10		Al finalizar cada visita correctiva y/o preventiva el contratista deberá generar un informe de servicio/acta en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. Se deberá realizar una transferencia de conocimiento sobre las configuraciones y mejoras realizadas en las plataformas objeto de renovación.	
1.11		El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto	

		pueda cumplir sus funciones. Estos valores no incurrirán en costos adicionales para el Ministerio	
1.12		En caso de cambio de cambio del hardware, software o licenciamiento por daño, el proveedor deberá atender y resolver en un esquema 24/7 garantizando la operatividad de los servicios y realizar las configuraciones correspondientes de manera posterior a la entrega del equipo de reemplazo.	

ÍTEM F	
Subítem	**Descripción**
1.1	El oferente deberá entregar todas las soluciones o equipos en el sitio indicado por la entidad.
1.2	Instalación, Implementación, configuración, puesta en marcha y afinamiento de las soluciones de seguridad y conectividad ofertadas.
1.3	El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
1.4	Todas las plataformas deberán ser de propósito específico, no se aceptan soluciones genéricas.
1.5	El oferente deberá presentar certificación de distribuidor autorizado del fabricante donde se evidencie que tiene el nivel de membresía EXPERT o ADVANCED. Lo anterior con el fin de garantizar la experiencia en la implementación de las soluciones que requiere la entidad. Este documento debe ser expedido por el fabricante de los equipos objeto de esta renovación con fecha no mayor a 30 días. El oferente deberá presentar certificación emitida directamente por el fabricante Fortinet y dirigida a la entidad haciendo referencia al número del proceso a la cual está aplicando.
1.6	El oferente deberá presentar al menos tres (3) especialidades técnicas correspondientes al mismo fabricante, tal como fue definido desde el estudio de mercado y conforme con el alcance técnico y el monto de inversión del proceso. Lo anterior con la finalidad de garantizar que el equipo técnico cuenta con la certificaciones e ingeniería calificada para la implementación y puesta en marcha de las soluciones ofertadas.
1.7	El oferente debe entregar junto con la propuesta una certificación emitida directamente del fabricante de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con soporte por mínimo 5 años, estos documentos deben ser dirigidas a la Entidad y deben ser expedidas con una fecha de al menos 30 días antes de la presentación de la propuesta.
1.8	El contratista debe entregar el plan de trabajo para todas las actividades de migración que deban contemplarse en la ejecución del contrato, en un término que no supere los quince (15) días calendario a partir de la suscripción del acta de inicio del contrato

1.9	El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil por el tiempo contratado.
2	**Implementación y puesta en marcha solución de seguridad**
2.1	El proponente seleccionado deberá entregar implementada y funcionando las soluciones completas, de acuerdo con los requerimientos y políticas.
	La implementación deberá contemplar: -Planeación de cada una de las actividades, validadas en conjunto con el Ministerio de Ambiente y Desarrollo Sostenible. -Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas. -Afinamiento y estabilización de las plataformas. -Pruebas de servicio de las plataformas. -Entrega de las plataformas a satisfacción del Ministerio de Ambiente y Desarrollo Sostenible.
2.2	Las actividades de afinamiento de las plataformas deberán ser realizadas por personal certificado por el fabricante.
2.3	La entidad requiere que se realicen pruebas / muestras de las plataformas donde se evidencie la correcta configuración y afinamiento de cada plataforma.
3	**Soporte solución de seguridad**
3.1	El contratista deberá garantizar soporte y garantía para las plataformas ofertadas en un esquema 7x24 por un (1) año, con soporte remoto o en sitio en caso de requerirse.
3.2	El soporte deberá contemplar: -El servicio de soporte debe incluir atención de incidentes sobre las plataformas ofertadas. -Consultas a través de llamadas telefónicas, correo electrónico. -Sesiones remotas y atención en sitio (En caso de requerirse) en horario Hábil y No Hábil. Todo con respecto a las plataformas ofertadas y objeto del presente contrato.
3.3	

PRIORIDAD		DESCRIPCIÓN
1	CRITICA	La producción está parada o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.
2	ALTA	Experimenta perdida del servicio, algunas características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.
3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.
4	BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.

	PRIORIDAD		DESCRIPCION	
	1	CRITICA	De manera remota (2) horas de atención y (3) horas de traslado a sitio.	
	2	ALTA	De manera remota (3) horas de atención y (4) horas de traslado a sitio.	
	3	MEDIA	De manera remota (8) horas y de ser necesario traslado a sitio	
	4	BAJA	De manera remota (24) horas y de ser necesario traslado a sitio	
	Nota: Ver documento anexo ANS.Minambiente.pdf El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo: -Revisar la consistencia de los Backups realizados a la solución implementada. Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma, en forma escrita. -Configurar, afinar y revisar los reportes / logs de las plataformas. -Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.			
3.4	El horario de atención para el mantenimiento correctivo y preventivo deberá ser de 7x24 en sitio, sin costo adicional para la entidad.			
3.5	Se deben incluir en la oferta dos (2) actividades de mantenimiento preventivo/correctivo en el año y afinamiento con el fin de minimizar problemas y mantener los sistemas actualizados, estas actividades deberán ser con previa aprobación del responsable TI de la entidad.			
3.6	El oferente debe contemplar una transferencia de conocimientos para 3 funcionarios de la entidad de al menos 24 horas, la cual debe incluir como mínimo temas de administración, configuración y afinamiento de las plataformas.			
3.7	Al finalizar cada visita correctiva y/o preventiva el contratista deberá: -Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. -El oferente deberá consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.			
3.8	El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.			
4	**Servicios adicionales requeridos**			
4.1	Para la ejecución del servicio, el oferente debe contemplar un mínimo de dos mil (2.000) direcciones IP activas y/o 4 Gbps de Throughput, que serán objeto del análisis durante el desarrollo del assessment. El oferente deberá realizar dos (2) evaluaciones de seguridad al año, enfocadas en el análisis a nivel de red, con el objetivo de entender el comportamiento del tráfico y de los usuarios, y con ello fortalecer la seguridad perimetral de la Entidad.			

	Con el fin de garantizar la correcta implementación de las plataformas, el oferente deberá realizar (2) assessment o evaluaciones de seguridad en conjunto con el fabricante de las soluciones ofertadas para garantizar el correcto funcionamiento de las plataformas. Estas deben incluir un reporte detallado de la implementación realizada, mejores prácticas, hardering, conclusiones y planes de mejoramiento y acción para la entidad.
4.2	El oferente debe realizar (2) evaluaciones de seguridad en el año a nivel de red para entender el comportamiento de tráfico y de usuarios para robustecer la seguridad perimetral de la entidad. Estas evaluaciones se realizarán netamente como un servicio por parte del oferente, por lo cual en caso de ser necesario no se aprovisionarán recursos por parte de la entidad para el despliegue de agentes en estaciones de trabajo o servidores, el servicio debe ser lo menos intrusivo posible para la entidad, implicando la menor cantidad de cambios o tiempo de administración posible para realizar el diagnostico de red. Se debe utilizar una herramienta para el análisis de red que cuente con licenciamiento vigente y soporte oficial del fabricante por 12 meses a partir de la suscripción del contrato. Además, se requiere que la solución empleada para el assessment utilice técnicas basadas en inteligencia artificial y análisis de comportamiento de usuarios, con el fin de identificar patrones anómalos y posibles amenazas de manera proactiva. Es importante mencionar que se requiere que la herramienta se encuentre incluida categorizada como líder en Gartner o IDC para Detección y Respuesta en Redes a nivel global, lo que garantizará la calidad, reconocimiento y confiabilidad de la solución propuesta.
4.3	Todos los equipos y elementos ofertados deberán ser nuevos, originales u homologados por el fabricante. No se admitirán equipos o componentes usados así sean reconstruidos en fábrica (refurbished) (remanufacturado).

4.4	El equipo ofertado y demás componentes tecnológicos deberán entregarse en un término que no supere cuarenta y cinco (45) días calendario a partir de la legalización del contrato.	
4.5	Suministrar la Documentación Técnica de la solución instalada, así como suministrar la documentación de buenas prácticas y recomendaciones de uso para la solución implementada.	
4.6	El contratista deberá remitir la evidencia de datasheets del fabricante, en donde se resalte el ítem al que hace cumplimiento de este anexo técnico y su numeral.	
4.7	**Equipo Mínimo de Trabajo**	
Equipo	Título / Certificaciones / Cursos	Experiencia Profesional relacionada
Un Gerente de Proyecto	-Título Ingeniero Eléctrico o electrónico o sistemas, telecomunicaciones, industrial o carreras afines: -Tarjeta Profesional -Especialización en Gerencia de Proyectos y/o Certificación PMP. -Certificación ITIL Foundation v3 o superior	Experiencia mínima de diez (10) años a partir de la expedición de la Tarjeta Profesional. Mínimo cinco (5) proyectos gerenciando y/o coordinando proyectos de TI y/o seguridad informática. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un Líder Técnico	Título Ingeniero Eléctrico, electrónico, sistemas telecomunicaciones o carreras afines: Tarjeta profesional de mínimo 8 años Especialización o maestría en Seguridad de la Información o informática. Certificación Vigente en Auditor Líder ISO 27001:2022 o superior Certificación en SCRUM Foundations o superior Certificación vigente como especialista en el fabricante de la solución. emitida directamente por dicho fabricante.	Experiencia general de cinco (5) años en proyectos de TI, de los cuales mínimo tres (3) años como líder o coordinador o gerente de servicio de TI. Certificaciones de Experiencia especifica de mínimo años (4) años en implementación o administración en plataformas de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un Ingeniero Implementador	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines: Certificación Vigente en Auditor Líder ISO 27001:2022 o superior Tarjeta profesional de mínimo 8 años Certificación vigente como especialista en el fabricante de la solución. Emitida por el fabricante con el cual se esté presentado el proponente	Experiencia Profesional relacionada: Experiencia general de mínimo cuatro (4) años en implementación, soporte y monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Un Ingeniero de	Título Ingeniero Eléctrico o electrónico o sistemas, telecomunicaciones o carreras afines.	Experiencia general de ocho (8) años en proyectos de TI, de los cuales mínimo de cuatro (4) años en

soporte II	Certificación vigente como Especialista en seguridad de redes. Emitida por el fabricante con el cual se esté presentado el proponente. Certificación vigente como Auditor Interno en la norma ISO/IEC 20000 :2018 o superiores.	implementación, soporte y monitoreo de soluciones de seguridad La experiencia se cuenta a partir de la expedición de la tarjeta profesional.
Dos ingenieros de soporte I	Ingeniero Eléctrico, electrónico, sistemas, telecomunicaciones o carreras afines. Certificación vigente como especialista en el fabricante. Emitida por el fabricante con el cual se esté presentado el proponente. Experiencia general de dos (2) años en proyectos de TI, de los cuales mínimo de un (1) año en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.	Experiencia general de dos (2) años en proyectos de TI, de los cuales mínimo de un (1) año en implementación, soporte y monitoreo de soluciones de seguridad. La experiencia se cuenta a partir de la expedición de la tarjeta profesional.

LOTE 2 – SOLUCIÓN DE HERRAMIENTA DE ANÁLISIS DE VULNERABILIDADES

ÍTEM	**DESCRIPCIÓN**		
A	**RENOVACIÓN DE LICENCIAMIENTO**		
Subítem	**Numero de Parte**	**DESCRIPCIÓN**	**Cantidad**
1.1	TIOVM	Standard Tenable Vulnerability Management Container TIOVM-STNDC Term: 12 Months Order Type: Renewal	100
1.2	TIO-WAS	Tenable Web App Scanning TIO-WAS, Term: 12 Months Web Apps: 30 Order Type: Renewal	30
1.4	La solución ofertada deberá soportar un licenciamiento flexible, el cual permita asignar el licenciamiento de acuerdo con las necesidades de evaluación y modificar dicha asignación siempre que sea necesario.		
1.5	La solución ofertada deberá ser de licencia exclusiva de la Entidad, no se aceptarán soluciones de uso compartido, licenciamiento open source y reúso de licenciamiento.		
1.6	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.		
1.7	La solución ofertada permitirá anticipar las amenazas y priorizar los esfuerzos de mitigación con el fin de evitar ataques.		
1.8	La solución ofertada permitirá comunicar el riesgo cibernético, con la finalidad de tomar mejores decisiones.		
1.9	La solución ofertada deberá contar con una vista de exposición, la cual permita enfocar los esfuerzos de seguridad brindando información clara y concisa de la exposición con respecto a la seguridad de la Entidad.		

	De la misma forma deberá proporcionar una puntuación global unificada de la exposición obtenida a partir de diferentes fuentes de datos.
1.10	La solución ofertada deberá tener capacidades que permitan análisis, visualización y priorización de rutas de ataques proporcionando una respuesta enfocada de forma preventiva con el fin de interrumpir las rutas que pueden ser utilizadas por un atacante. Dicho análisis deberá ser soportado bajo las criticidades expuestas en el marco MITRE ATT&CK.
1.11	La solución ofertada deberá contar con un Inventario de Activos centralizado, con el objetivo de proporcionar una visibilidad completa hacia todos los activos independientemente de la fuente de datos (Activos TI, Activos Nube, Aplicaciones Web, Identidades del Directorio Activo), permitiendo la agrupación por medio de etiquetas.
1.12	La solución ofertada permitirá gestionar la superficie de ataque externa, con el fin de identificar y reducir riesgo, brindando a la entidad la visión de un atacante.
1.13	La solución ofertada deberá realizar una gestión de vulnerabilidades basadas en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas.
1.14	La solución ofertada deberá realizar una evaluación de vulnerabilidades en entornos web de manera automatizada de manera completa y precisa.
1.15	La solución ofertada permitirá la protección de la infraestructura en la nube, permitiendo una visibilidad completa y de manera continua de exposiciones, vulnerabilidades y permisos de acceso; priorizando tareas de remediación.
1.16	La solución ofertada permitirá la protección del Directorio Activo, permitiendo identificar brechas de seguridad, malas prácticas de configuración y ataques en tiempo real.
1.17	La solución ofertada permitirá proveer métricas de evaluación de los programas de evaluación y remediación de los sistemas de información de la función pública asignada de Ministerio de Ambiente
1.18	La solución ofertada permitirá realizar una evaluación de la exposición de manera comparativa entre unidades de negocio o ubicaciones a nivel interno de la entidad; de la misma forma con competidores de la industria de manera externa. Con el fin de obtener información que permitan una toma de decisiones certeras.
1.19	La solución ofertada deberá soportar funcionalidades de seguridad de doble factor de autenticación.
1.20	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).
1.21	Con la presentación de la oferta se deberá presentar certificación de fabricante indicando las tecnologías consideradas en la presentación de oferta y adjuntar datasheets públicos de fabricante donde se evidencie el cumplimiento de los requerimientos técnicos.
1.22	La solución ofertada deberá ser provista por un partner perteneciente al programa de canales de la fábrica que provea la solución y pertenecer por lo menos a uno de los dos niveles más altos del mismo.
1.23	El oferente deberá presentar certificación dirigida a la entidad con los datos del proceso y expedida en un tiempo no mayor a 30 días al momento de la entrega del proceso. Con fin de garantizar el cumplimiento de los requisitos plasmados en el presente documento, el oferente deberá entregar junto con la oferta, los datasheet u hojas de datos y/o manuales de usuario que avalen el cumplimiento técnico de la solución ofertada.
1.24	Se deberá presentar certificación del fabricante indicando productos y cantidades ofertadas.
1.25	El oferente deberá estar en uno de los dos máximos niveles de partner de la solución ofertada y además deberá para fines de soporte contar con su propio SOC en la ciudad de Bogotá y ser miembro de FIRST.
2	**Características Gestión de Vulnerabilidades**

2.1	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de los activos TI de la función pública asignada de Ministerio de Ambiente y hacer parte de una plataforma de gestión de ciber exposición.
2.2	La solución ofertada deberá estar en la capacidad de cubrir más de 199.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.
2.3	La solución ofertada podrá gestionar vulnerabilidades de sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores Web e infraestructuras esenciales y las infracciones de cumplimiento.
2.4	La solución ofertada deberá proporcionar una consola de gestión en la nube para la gestión de la información de seguridad.
2.5	La solución ofertada deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de: -Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Dicha tecnología deberá estar patentada. -Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes.
2.6	La solución ofertada deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo.
2.7	La solución ofertada deberá contar con un esquema de perfiles de usuarios basados en roles y garantizar los niveles adecuados de acceso a la plataforma.
2.8	La solución ofertada deberá permitir una evaluación de vulnerabilidades y/o postura de seguridad de manera autenticada, por de los siguientes sets de credenciales y sin limitarse a Windows, SSH y SNMPv3.
2.9	La solución ofertada deberá contar con un módulo que permita la creación de filtros para mejorar las búsquedas. Estos filtros deberán poder ser por lo menos: protocolo, IP, activo, identificador de la vulnerabilidad, identificador CVE, CVSS, vulnerabilidades por su puntaje dinámico, explotabilidad, severidad.
2.10	La solución ofertada deberá permitir la clasificación de activos identificados de manera manual o dinámica, con base en diferentes atributos encontrados en el análisis con base en etiquetas o en grupos de trabajo, para poder usarse en escaneos posteriores.
2.11	La solución ofertada deberá proporcionar información de capacidad de explotación contra las plataformas de validación como Metasploit, CoreImpact y Canvas.
2.12	La solución ofertada deberá tener la capacidad de integrarse con sistemas tipo SIEM para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a vulnerabilidades. Por defecto debe tener la capacidad de integrarse al menos con las siguientes soluciones: Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic.
2.13	La solución ofertada deberá proporcionar una integración con los sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Por lo menos se deben soportar: Microsoft WSUS/SCCM, Red Hat Satellite, HCL BigFix, Symantec Altiris, Dell KACE K1000.
3	**Características Gestión de Vulnerabilidades en Aplicaciones Web**
3.1	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la función pública asignada de Ministerio de Ambiente; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciber exposición.
3.2	La solución ofertada deberá poder escanear aplicaciones modernas desarrolladas en frameworks JavaScript, AJAX, HTML5 and Single Page Applications.
3.3	La solución ofertada permitirá observar las vulnerabilidades a lo largo del tiempo, según su nivel de riesgo, clasificación en OWASP Top 10, de la misma forma que sus descripciones e instrucciones de remediación.
3.4	La solución ofertada deberá ser tipo SaaS, de la misma forma tendrá capacidad para ser desplegada como un contenedor de Docker, permitiendo el escaneo de sitios públicos y privados.

3.5	La solución ofertada permitirá realizar escaneos sin degradación de performance en el sitio, por medio de escaneos seguros, permitiendo definir sitios que no deben ser escaneados a partir de la URL, o extensiones de archivos
3.6	La solución ofertada deberá contar con dos escaneos predefinidos que permitan detectar rápidamente problemas de ciberhigiene: -SSL/TLS Scan -Config Audit Scan
3.7	La solución ofertada deberá permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.
3.8	La solución ofertada deberá soportar escaneos con autenticación avanzada como: -HTTP Server Authentication -Web Application Authentication (Login Form, Cookie Authentication, Selenium Authentication, API Key, Bearer Authentication. - Client Certificate Authentication
3.9	La solución ofertada deberá contar con las siguientes plantillas de escaneo: -API -Config Audit -Log4Shell -Overview -PCI -Quick Scan -Scan -SSL/TLS
3.10	La solución ofertada permitirá conocer el estado y progreso de una tarea de escaneo; de la misma forma generar tareas de escaneo programadas y envío de resultados por medio de correo electrónico.
3.11	La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura.
3.12	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad.
4	**Transferencia de conocimiento**
Se debe realizar una transferencia de conocimiento de mínimo 8 horas. Esta se realizará una vez sea entregado el licenciamiento y tendrá lugar una nueva capacitación cada que exista una actualización a la herramienta que amerite otra transferencia de conocimiento.	
5	**Soporte Técnico**
El contratista deberá estar en la capacidad de prestar soporte remoto para la herramienta por el tiempo de adquisición de la licencia, este requisito no ocasionará costo adicional para la Entidad. El contratista clasificará los incidentes, problemas y solicitudes y les dará resolución en horario 5x8.	
CARACTERÍSTICAS A TENER EN CUENTA DE LA GARANTÍA DE FABRICA Debe autorizar de manera explícita a la Entidad el uso de versiones y actualizaciones posteriores que se liberen durante el periodo de la garantía. Realizar el seguimiento de las solicitudes del servicio de garantía desde el centro de soporte al cliente, desde el momento de recibir la llamada hasta la prestación del servicio, en los casos de soporte en sitio deberá asegurar y verificar que el trabajo de los ingenieros de campo se está haciendo de acuerdo con los estándares técnicos y de servicio ofrecidos a la entidad.	

Asegurar que el centro de atención al cliente cumpla con el servicio de garantía solicitado por la entidad hasta que se haya terminado y solucionado el caso, luego solicitará a la entidad la autorización para cierre a través de una notificación.

De requerirse un técnico en las oficinas de la entidad, este arribará para atender los eventos de servicio reportados, de acuerdo con el horario de cubrimiento y tiempos de respuesta solicitados.

Prestar soporte técnico para reconfiguración de los equipos, migraciones o nuevas implementaciones que surjan durante el periodo de vigencia de la garantía, según las necesidades de la entidad, sin costo adicional para el Ministerio de Ambiente y Desarrollo Sostenible.

Los repuestos empleados para reemplazar elementos defectuosos serán de la misma calidad al existente y se realizara su reemplazo previa autorización por parte del supervisor del contrato.

6	**Canales de Atención**
El Contratista debe contar como mínimo con los siguientes canales de atención a requerimientos: -Telefónico -Correo electrónico	
7	***Entrega y Activación***
El Contratista deberá realizar la entrega de la suscripción de manera remota y/o en las Instalaciones del Ministerio.	
8	***Equipo mínimo de trabajo***

Gerente del Proyecto	El oferente debe contar con un equipo de trabajo para la ejecución del proyecto, el cual debe contar con los siguientes perfiles: -Título Ingeniero de Sistemas o Electrónico o Eléctrica o Redes o de Telecomunicaciones y/o afines. -Posgrado y/o Maestría en Gerencia de Proyectos de Tecnologías de la Información -Certificación PMP vigente. -Tarjeta Profesional con expedición mínimo de cinco (5) años **Experiencia General** Experiencia mínima general de siete (7) años de experiencia profesional. **Experiencia Específica** Experiencia mínima de siete (7) años orientada a implementación y/o experiencia específica como gerente o gestor o coordinador o director de proyectos relacionados con: Seguridad de la información y/o seguridad informática y/o seguridad digital y/o ciberseguridad y/o centro de operaciones de seguridad Deberá contar con al menos cinco (5) de las siguientes certificaciones: - ITIL V4 Certification - **CEH** (CERTIFIED ETHICAL HACKER) - AUDITOR LIDER 27001:2013/2022 - ISO27035:2016 (INCIDENT MANAGER) - **CISM** (CERTIFIED INFORMATION SECURITY MANAGER) - **GIAC** Security Operations Certified (GSOC) - **CISSP -** Certified Information Systems Security Professional Nota 1: El oferente deberá presentar todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso de adquisición. La NO presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación
Líder de Seguridad	Profesional en Ingeniería de Sistemas o Electrónica o Eléctrica o de Redes o de Telecomunicaciones y/o afines. Deberá contar como mínimo con una Especialización y/o Maestría en Seguridad Informática y/o Administración de Riegos Informáticos y/o Gerencia de Proyectos de TI. -Tarjeta Profesional con expedición mínimo de ocho (8) años Deberá contar con al menos cinco (5) de las siguientes certificaciones: - **CISM** (CERTIFIED INFORMATION SECURITY MANAGER) - **CISSP -** Certified Information Systems Security Professional - **CEH-** Certified Ethical Hacker - **ISO22301:** 2012 (SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO - **ISO31000: 2018 (Lead Risk Manager)** - **CISA-** Certified Information Systems Auditor **Experiencia Específica**

	Experiencia mínima de ocho (8) años orientad como Ingeniero de Seguridad y/o Auditor de Seguridad y/o Coordinador de Seguridad y/o Consultor de Seguridad y/o Oficial de Seguridad.
Ingeniero de soporte	Título Ingeniero electrónico o sistemas o telecomunicaciones. **Experiencia General** Cuatro (4) años de experiencia a partir de la expedición de la tarjeta profesional Deberá contar con al menos dos (2) de las siguientes certificaciones: TENABLE ENGINNER CLOUD SECURITY TENABLE ENGINNER NESSUS TENABLE ENGINNER OPERATIONAL TECHNOLOGY

4. CLASIFICADOR DE BIENES Y SERVICIOS:

LOTE 1 – SOLUCIÓN PERIMETRAL

Clasificación UNSPSC	Producto
43233200	Software de seguridad y protección
43222500	Equipo de seguridad de red
43222600	Equipo de servicio de red
81111800	Servicios de sistemas y administración de componentes de sistemas
81112100	Servicios de Internet
81112200	Mantenimiento y soporte de Software

LOTE 2 – SOLUCIÓN DE HERRAMIENTA DE ANÁLISIS DE VULNERABILIDADES

Clasificación UNSPSC	Producto
43222600	Equipos de servicio de red

43233205	Software de Seguridad de Transacciones y de Protección contra Virus
80101600	Gerencia de Proyectos
81111800	Servicios de Sistemas y Administración de Componentes de Sistemas
81112200	Mantenimiento y soporte de Software

5. REGULACIONES ESPECÍFICAS:

1. Dar cumplimiento a la normatividad vigente relacionada con la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), aportando para el inicio de la ejecución, certificación suscrita por el representante legal en la que manifieste que cuenta con los documentos y registros que permitan corroborar el cumplimiento de lo establecido en el Decreto 1072 de 2015 y sus normas concordantes, conforme al anexo que hace parte del presente estudio previo.

2. Entregar al supervisor al inicio de la ejecución constancia de la autoevaluación del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) autoevaluación de los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST conforme a la Resolución 0312 del 2019. La cual debe ser igual o superior al 60% (Moderadamente Aceptable), de acuerdo a los criterios de valoración de la Resolución 0312 de 2019, Articulo 28.

RESOLUCIÓN 0312 DE 2019 Art. 28	
CRITERIO	VALORACIÓN
Puntaje obtenido menor al 60%	CRITICO
Puntaje obtenido entre el 60% y el 85%	MODERADAMENTE ACEPTABLE
Puntaje obtenido mayor o igual al 85%	ACEPTABLE

6. OBLIGACIONES DEL CONTRATISTA

6.1 Obligaciones Generales

1. Acatar la Constitución, la ley, las normas legales y procedimentales establecidas por el Gobierno Nacional y el Ministerio de Ambiente y Desarrollo Sostenible.
2. Cumplir con el objeto del contrato de manera responsable e idónea, realizándolo de acuerdo con las condiciones pactadas en el pliego de condiciones, su propuesta y demás documentos que los integran.
3. Constituir las garantías pactadas en la presente convocatoria.
4. Mantener indemne a la entidad por las reclamaciones que se deriven con ocasión a la ejecución contractual.
5. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y entrabamientos.
6. Cumplir con lo estipulado en la cláusula Forma de Pago y requisitos para el Pago, con respecto a los documentos

requeridos para el mismo y el plazo establecido para la presentación de la facturación.

7. Dar cumplimiento a las obligaciones con los sistemas de seguridad social en salud, pensión, sistema general de riesgos laborales y aportes parafiscales, cuando haya lugar a ello, y presentar los documentos respectivos que así lo acrediten, conforme lo establecido en el artículo 50 de la Ley 789 de 2002, en la Ley 828 de 2003, la Ley 1562 de 2012, y demás normas que regulen la materia.
8. Concurrir con el Ministerio de Ambiente y Desarrollo Sostenible a la liquidación formal del contrato
9. Reportar al supervisor, de manera inmediata, cualquier novedad o anomalía que pueda afectar la ejecución del contrato.
10. Responder ante las autoridades competentes por los actos u omisiones que ejecute en desarrollo del contrato cuando con ellos se cause perjuicio a la administración o a terceros en los términos del artículo 52 de las Ley 80 de 1993.
11. Reparar los daños de forma inmediata o cualquier falla o error que se comenta en la ejecución del objeto contractual e indemnizar los perjuicios (si a ello hubiere lugar) que cause al Ministerio por el incumplimiento del contrato.
12. Dar aplicación a la política del Sistema Integrado de Gestión (Sistema de Gestión de Calidad, Sistema de Gestión Ambiental, Sistema de Seguridad y Salud en el Trabajo, Sistema de Seguridad de la Información y el Modelo Integrado de Planeación y Gestión) establecida en el Ministerio de Ambiente y Desarrollo Sostenible, implementado los documentos y lineamientos exigidos en las diferentes etapas de contratación.
13. Guardar total reserva de la información que por razón de la prestación del servicio y desarrollo de sus actividades obtenga, pues en virtud del presente contrato dicha información se considera de propiedad del Ministerio y solo salvo expreso requerimiento de autoridad competente podrá ser divulgada, para lo cual deberá dar cumplimiento a lo contenido en la circular de confidencialidad e integridad de la información expedida por la entidad. Así mismo deberá asistir a las socializaciones que sobre la materia programe el Ministerio.
14. Dar aplicación a las políticas y emplear los formatos del Sistema Integrado de Gestión, Sistema de Seguridad de la Información y demás, aprobados por la Entidad.
15. Responder por la salvaguarda y preservación de los equipos y elementos que le sean asignados para el cumplimiento de sus actividades contractuales.
16. Acatar las instrucciones que durante el desarrollo del contrato le imparta el Minambiente, a través del supervisor del contrato.
17. El contratista deberá cumplir con todos los procedimientos y exigencias establecidos para los contratos y sus modificaciones en la plataforma SECOP II de manera inmediata.
18. Suscribir, juntamente con el Supervisor, el Acta de confidencialidad de la información establecido en el MADSIG cuando aplique según el objeto del contrato y lo establecido en el Manual de Contratación de la Entidad (cuando aplique).
19. Las demás inherentes al objeto y a la naturaleza del contrato y aquellas indicadas por el Supervisor para el cabal cumplimiento del objeto del contrato.

7. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

LOTE 1 – Solución Perimetral

1. Dar cumplimiento a todas las especificaciones del anexo técnico, las cuales hacen parte integral del presente proceso.
2. Efectuar entrega de los bienes adquiridos objeto de contratación al almacén, según el procedimiento establecido por la entidad.
3. Entregar al Ministerio los documentos (licenciamiento legal y de uso) soporte donde se especifique el detalle de los productos que están descritos en las especificaciones técnicas.
4. Realizar la renovación del licenciamiento de seguridad y soporte de los equipos con fábrica.
5. Realizar la renovación del licenciamiento de los equipos Fortinet, configuración, puesta en marcha y afinamiento de la solución de acuerdo con lo establecido en el presente proceso y la ficha de especificaciones técnicas.
6. Realizar la renovación ante LACNIC del pool IPv6 de propiedad de la entidad por un periodo de mínimo un (1) año, generar documento de evidencia de la renovación digital la cual debe ser entrega al supervisor contractual.
7. Realizar el trámite pertinente para la propagación y/o publicación del pool IPv6 sobre la red del proveedor de Internet de la Entidad. Así como las configuraciones a que haya lugar para el correcto funcionamiento.
8. Realizar los ajustes pertinentes en el portal de https://milacnic.lacnic.net/lacnic para que se vea reflejado la renovación por el nuevo periodo contratado.
9. Elaborar y entregar la documentación de instalación, activación del licenciamiento, configuración y puesta en marcha, así como los afinamientos realizados.
10. Realizar las actualizaciones de software de manera periódica o por demanda de la solución de tal forma que se solucionen posibles bugs, vulnerabilidades y/o activación de nuevas funcionalidades sin que esto genere costos adicionales para el Ministerio, durante el término de la vigencia de las licencias, se deberá entregar informe de la revisión finalizando la vigencia de las actualizaciones aplicadas.
11. Brindar los servicios de soporte técnico remoto o en sitio, mantenimiento, configuración y afinamiento por demanda de acuerdo con lo establecido en el presente proceso y la ficha de especificaciones técnicas.
12. Entregar un cronograma de trabajo con las actividades a realizar en cuanto a planeación, ejecución y entrega final de los productos y servicios establecidos; este cronograma deberá ser entregado para revisión y aprobación del supervisor del contrato dentro de los ocho (8) días siguientes al perfeccionamiento del contrato. El cronograma deberá estar ajustado al plazo máximo de ejecución del contrato.
13. Entregar el cronograma de mantenimiento preventivo de los equipos adquiridos por el tiempo contratado para su debida actualización en el Plan de Mantenimiento a la infraestructura TI de la entidad.
14. Acordar con el supervisor la fecha y hora, en caso de que las labores a realizar requieran de interrupción total del servicio informático del Ministerio de Ambiente y Desarrollo Sostenible.
15. Atender todas las sugerencias y recomendaciones que realice el Ministerio de Ambiente y Desarrollo Sostenible para el correcto desarrollo del contrato y particularmente aquellas dadas por el supervisor.
16. Mantener la confidencialidad de la información entregada por el Ministerio, en reserva o secreto, dándole a la misma el carácter estrictamente confidencial, y mantenerla debidamente protegida de accesos no autorizados a terceros, con el fin de no permitir su conocimiento o manejo por parte de tales terceros no autorizados. Así mismo, a no permitir la copia o reproducción total o parcial de la misma y devolverla una vez utilizadas para los fines estrictamente necesarios para la consultoría objeto del contrato.
17. Firmar el Acuerdo de Confidencialidad para contratistas que tiene establecido el Ministerio de Ambiente y Desarrollo Sostenible, el cual se entrega por parte de la Entidad al Contratista al momento de firmar el acta de inicio y debe ser firmado y devuelto por éste dentro de los 5 días hábiles siguientes a esa firma.

18. Guardar total reserva de la información recibida del Ministerio de Ambiente y Desarrollo Sostenible debido al servicio que presta en desarrollo de sus actividades, ya que es propiedad del Ministerio, salvo requerimiento de autoridad competente.
19. Presentar formalmente dentro de los 2 dias hábiles siguientes a la suscripción del contrato, el personal mínimo solicitado que ejecutará las actividades objeto de la contratación y el cual debe contar con disponibilidad permanente y capacidad de decisión, el cual solo podrá ser reemplazado por personal de igual o superiores condiciones, habiendo mediado fuerza mayor que deberá acreditar ante el supervisor del contrato quien autorizará el cambio respectivo.
20. Generar reportes de servicios, cuando se realicen visitas técnicas programadas por el supervisor del contrato, en el que conste el resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software o en la configuración de los equipos, se debe generar al menos una visita de revisión y mantenimiento antes de terminar la vigencia y dejar informe del diagnostico o estado salud de la revisión realizada.
21. Ejecutar transferencia de conocimiento cuando sea requerido por el supervisor del contrato durante las actualizaciones y mantenimientos durante el periodo de vigencia de las licencias, para mínimo tres (3) colaboradores de la entidad.
22. Garantizar el funcionamiento y continuidad de la operación de los componentes de Hardware y Software relacionados con la prestación de los servicios relacionados con el presente objeto.
23. Las demás que se deriven y que garanticen su cabal y oportuna ejecución, acorde con el anexo técnico.
24. Efectuar los procesos de borrado seguro en los componentes retirados y que son objeto de adquisición garantizando que los primeros no cuenten con información o configuraciones de la Entidad.
25. Elaborar los informes técnicos que den a lugar por concepto de ingeniería de detalle final, retiro de equipos y así generar con este último un insumo para la adecuada gestión de inventarios.

LOTE 2 – Solución de Herramienta de Análisis de Vulnerabilidades

1. Entregar al supervisor del contrato, el certificado de renovación de suscripción de la Herramienta de Análisis de Vulnerabilidades Tenable IO, así como la evidencia del acceso a la consola de gestión en la nube, ya sea por correo electrónico o de manera física durante el plazo de ejecución del contrato.
2. Entregar al supervisor del contrato, el certificado de renovación de las suscripciones Tenable WAS, para el Ministerio de Ambiente y Desarrollo Sostenible, ya sea por correo electrónico o de manera física durante el plazo de ejecución del contrato.
3. Realizar la instalación y/o activación del licenciamiento de acuerdo con lo establecido en el presente proceso y la ficha de especificaciones técnicas.
4. Realizar la configuración de acuerdo con lo establecido en el presente proceso y la ficha de especificaciones técnicas.
5. Realizar trasferencia de conocimiento a mínimo cuatro (4) usuarios que la Entidad defina, en el uso, instalación y administración del software adquirido, con una intensidad de mínimo ocho (8) horas distribuidas en máximo cuatro (4) sesiones, las cuales se realizarán dentro del primer mes siguiente a la firma del acta de inicio del contrato. Dicha transferencia se realizará remotamente y/o presencial haciendo entrega al supervisor de las memorias y/o material utilizado.
6. Realizar la programación de reportes y/o informes en la consola de acuerdo con las necesidades del Ministerio y a lo establecido en el presente proceso y la ficha de especificaciones técnicas.

7. Realizar las actualizaciones de software de manera periódica de la solución de tal manera que se solucionen posibles bugs, vulnerabilidades y/o activación de nuevas funcionalidades sin que esto genere costos adicionales para el Ministerio.
8. Brindar los servicios de soporte técnico remoto o en sitio, mantenimiento, configuración y afinamiento por el periodo de un año a partir de la entrega y activación de las suscripciones de acuerdo con lo establecido en el presente proceso y la ficha de especificaciones técnicas.

5.4 Obligaciones en materia ambiental y de gestión de calidad

Dar cumplimiento a los criterios ambientales establecidos por el Ministerio y entregar los debidos soportes de ejecución conforme a los establecido en la ficha técnica.

5.5 Obligaciones en materia de seguridad de la información

1. Dar aplicación y cumplimiento a la política del Sistema Integrado de Gestión establecida en el Ministerio de Ambiente y Desarrollo Sostenible, en lo relacionado al Sistema de Gestión de Seguridad de la Información.
2. Conocer, dar aplicación y cumplimiento a 2.1.5.1.1 Política de protección de datos, dispuesta en: https://www.minambiente.gov.co/wp-content/uploads/2023/03/DS-E-GET-01.pdf
3. Conocer y dar aplicación y cumplimiento a 2.1.5.1.6 Manual de Políticas Específicas de Seguridad de la Información, dispuestas en: https://www.minambiente.gov.co/wp-content/uploads/2023/04/M-E-GET-04_V1_copia_controlada.pdf
4. Suscribir junto con el Supervisor, el Acta de compromiso de confidencialidad de la información F-A-CTR-36 establecido en el Sistema Integrado de Gestión, lo anterior, en los casos en los cuales se deba permitir al proveedor o contratista el conocimiento y acceso a información confidencial de la entidad.

8. PLAZO DE EJECUCIÓN:

El plazo de ejecución del contrato será de tres (3) meses a partir de la suscripción del acta de inicio y perfeccionamiento del contrato.

Nota: Sin perjuicio del plazo de ejecución establecido, la vigencia del licenciamiento para los sistemas de seguridad Fortinet (Fortigate, fortianalyzer,y Fortiweb) serán de un (1) año contado a partir de la entrega del certificado presentado por el contratista y recibido a satisfacción por la Entidad. Así como para el licenciamiento del sistema DDoS y Herramienta de vulnerabilidades, el cual será activo inmediatamente siguiente a la fecha de expiración de la licencia actual.

9. LUGAR DE EJECUCIÓN:

El lugar de ejecución del contrato será la Sede del Ministerio ubicada en la Calle 37 No. 8-40, Bogotá DC

10. FORMA DE PAGO:

LOTE 1 – Solución Perimetral

EL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE - MINAMBIENTE - al contratista el valor del contrato en los siguientes términos:

- Un pago por un 30% a la entrega del licenciamiento conforme a la ficha técnica. Lo anterior, previa presentación de la factura y de los soportes requeridos en la ley y los procedimientos internos para la radicación de cuentas de cobro de la entidad. (deberá generarse la relación de lo siguiente en la facturación).

  1. Renovación Ipv6 LACNIC por un año.
  2. Renovación de licencia DDOS FortiDDoS 200F licencia de uso por un año.

- Un segundo pago por un 70% a la entrega de dispositivos y licenciamiento de la siguiente forma (deberá generarse la relación de lo siguiente en la facturación).

  3. Dos (2) appliances de seguridad informática perimetral con sistema operativo propietario del fabricante, que sea del tipo Firewall de Nueva Generación más licencia de seguridad por un año de uso.
  4. Adquisición de dos (2) Firewall de propósito específico para la protección de aplicaciones web (HTTP/HTTPS). más licencia de seguridad por un año de uso.
  5. Un (1) equipo tipo appliance físico que permita registrar cada transacción de la plataforma de seguridad perimetral. Licencia por uso de un año.

- Las entregas deben de darse en sitio bajo recibo de almacén del MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE y la entrega de un documento con la información de la garantía de Fábrica conforme a la ficha técnica. Lo anterior, previa presentación de la factura y de los soportes requeridos en la ley y los procedimientos internos para la radicación de cuentas de cobro de la entidad.

Debe generarse dos facturas con el cumplimiento de los requisitos legales y según el origen de los recursos utilizados, conforme a generar el 100% del pago total.

Deberá dirigirse a nombre del EL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE - MINAMBIENTE NIT 830.115.395–1 donde se describa (**Garantías de equipos, características en los cuales se entrega el Licenciamiento y soporte a nombre del MinAmbiente**).

Para efectos del pago, el contratista deberá adjuntar la factura correspondiente y en caso de estar obligado a facturar electrónicamente deberá dar cumplimiento a lo previsto en la Resolución N° 000042 del 5 de mayo de

2020 expedida por la DIAN y a lo dispuesto en la Circular Interna No. 00008 el 30 de marzo de 2021 o aquella que la modifique o reemplace; igualmente, deberá contar con el lleno de los requisitos legales, constancia de cumplimiento a satisfacción por parte del supervisor del contrato, acreditación del pago de los aportes al sistema general de seguridad social integral del personal asignado para la ejecución del contrato, así como el pago de aportes parafiscales, según sea el caso, de conformidad con lo dispuesto en el artículo 50 de la Ley 789 de 2002, artículo 23 de la ley 1150 de 2007 y demás normas concordantes.

LOTE 2 – Solución de Herramienta de Análisis de Vulnerabilidades

Un único pago del 100% del valor total ofertado, previa certificación de cumplimiento expedida por la supervisión, de acuerdo con la entrega del licenciamiento y servicios de implementación, puesta en marcha, afinamiento, configuración, transferencia de conocimiento efectivamente realizados y recibidos a satisfacción con el cumplimiento de las características técnicas establecidas en los documentos del proceso, y de conformidad con los valores ofertados. (deberá generarse la relación de lo siguiente en la facturación de acuerdo a las condiciones establecidas en la ficha técnica).

1. Licencia por un año de TIOVM Standard Tenable Vulnerability Management Container TIOVM-STNDC Term: 12 Months Order Type: Renewal 100.
2. Licencia por un año de TIO-WAS Tenable Web App Scanning TIO-WAS Term: 12 Months Web Apps: 30 Order Type: Renewal 30.
3. Licencia Renovación por un (1) año de la consola en nube Tenable.

Para el trámite de pago, el contratista deberá allegar los siguientes documentos:

- ✓ Certificación que acredite cumplimiento por parte del contratista de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, cuando a ello haya lugar.
- ✓ Factura (s) de conformidad con lo dispuesto en el Decreto 358 del 5 de marzo de 2020 expedido por el Ministerio de Hacienda y Crédito Público por el cual se reglamentan aspectos en materia tributaria y la Resolución No. 000042 del 5 de mayo de 2020 expedida por La Dirección de Impuestos y Aduanas Nacionales–DIAN y demás normas aplicables.
- ✓ Resolución DIAN de autorización numeración de la facturación aportada*
- ✓ RUT*
- ✓ Certificación bancaria *
- ✓ Demás disposiciones legales aplicables que surjan

Los documentos señalados con * se requerirán actualizados con máximo 30 días a la fecha de radicación del primer pago.

Si las facturas no han sido bien elaboradas, no cumplen con las normas aplicables o la Entidad solicita correcciones a la misma o no se acompañan de los documentos que las respalden, el término de trámite de revisión, aprobación y pago sólo empezará a contarse desde la fecha en que quede corregida la factura o documento equivalente, o desde aquella en que se haya aportado el último de los documentos y por tal motivo no se darán lugar al pago de intereses o compensación de ninguna naturaleza a favor del contratista.

Las demoras que se presenten por estos conceptos no serán atribuibles a la Entidad, por tanto, serán de responsabilidad exclusiva del contratista, quien no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza.

En caso de que el contratista se encuentra obligado a facturar electrónicamente deberá aportar factura electrónica de acuerdo con lo establecido por la DIAN, el cual será un requisito para el pago de la respectiva negociación. Todas las facturas electrónicas para su reconocimiento tributario deberán ser validadas previo a su expedición, por la Dirección de Impuestos y Aduanas Nacionales (DIAN) o por un comitente vendedor autorizado por esta. La factura electrónica solo se entenderá expedida cuando sea validada por el contratista autorizado.

Nota: No obstante, lo señalado en la forma de pago, los mismos están sujetos a las disponibilidades del Programa Anual Mensualizado de Caja – PAC y a la ubicación de fondos en la tesorería del Ministerio de Ambiente y desarrollo sostenible, Igualmente, para la presentación de la última cuenta de cobro se tendrá presenta las fechas, requisitos y tramites establecidos en la Circular de Cierre Financiero que para tal fin expida la entidad.

11. ANÁLISIS DE EXIGENCIA DE GARANTÍAS:

El contratista deberá constituir a favor del MINISTERIO garantía de que tratan la Ley 80 de 1993, Ley 1150 de 2007, y el Decreto 1082 de 2015, considerando el objeto a contratar, las obligaciones contractuales y el valor del contrato, dicha garantía deberá constituirse con los siguientes amparos[1]:

De conformidad con los artículos **2.2.1.2.3.1.1.** y **2.2.1.2.3.1.2. del Decreto 1082 de 2015** las garantías en la contratación deben cubrir el cumplimiento de las obligaciones surgidas en favor de las Entidades Estatales con ocasión de: (i) la presentación de las ofertas; (ii) los contratos y su liquidación; y (iii) los riesgos a los que se encuentran expuestas las Entidades Estatales, derivados de la responsabilidad extracontractual que pueda surgir por las actuaciones, hechos u omisiones de sus contratistas y subcontratistas. En este orden de ideas, teniendo en cuenta la naturaleza del objeto a contratar, la forma de pago y el valor del contrato, se considera que es necesario exigir la garantía única en la presente contratación, que incluya los siguientes amparos:

LOTE 1

1 www.colombiacompra.gov.co – Guía para el manejo de garantías en procesos de contratación.

- **Cumplimiento del contrato**, por una cuantía equivalente al veinte por ciento (20%) del valor del contrato y una duración igual al plazo del contrato y seis (6) meses más, contados desde la expedición de la póliza.
- **Calidad y correcto funcionamiento de los bienes**: por una cuantía equivalente al veinte por ciento (20%) del valor del contrato y una duración igual al plazo de ejecución del contrato y dos (2) años más, contando a partir del recibo de los mismos.
- **Calidad del servicio**, por una cuantía equivalente al veinte por ciento (20%) del valor del contrato y una duración igual al plazo del contrato y un (1) año más, contados desde la expedición de la póliza.
- **Pago de Salarios Prestaciones Sociales, Legales e Indemnizaciones Laborales:** Desde la suscripción del contrato, en cuantía equivalente al cinco por ciento (5%) del valor del contrato, por el término de ejecución del mismo y tres (3) años más.

LOTE 2

- **Cumplimiento del contrato**, por una cuantía equivalente al veinte por ciento (20%) del valor del contrato y una duración igual al plazo de ejecución del contrato y seis (6) meses más.
- **Calidad del servicio**, por una cuantía equivalente al veinte por ciento (20%) del valor del contrato y una duración igual al plazo de ejecución del contrato y dos (2) años más.

Sin perjuicio de lo anterior, el contratista se obliga a mantener vigente la garantía durante el plazo que demande la ejecución del contrato, así como la liquidación de este, si aplica, tal y como lo establece el Decreto 1082 de 2015.

En cualquier evento de aumento del valor del contrato o prórroga de su vigencia, el contratista estará obligado a ampliar o prorrogar los amparos en forma proporcional de manera que se mantengan las condiciones originales.

El contratista responderá por cualquier incumplimiento de sus obligaciones y se obligará a indemnizar al MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE de cualquier perjuicio le cause por este hecho.

Se exigirán las garantías destinadas a amparar los perjuicios derivados del ofrecimiento, de conformidad con las disposiciones señaladas en la Ley 1150 del año 2007, y el Decreto 1082 del año 2015, toda vez que le permite al MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE contar con un respaldo que le garantice por parte de los proponentes u oferentes la efectividad o eficacia de suscribir el contrato en el evento de ser seleccionado dentro del presente proceso de selección.

12. MATRIZ DE RIESGOS:

SE ANEXA

13. CUADRO DE COSTOS:

Se anexa cuadro de estudio de mercado con la información del costo unitario de los ítems conforme a la siguiente información:

14. REQUERIMIENTOS PARA EL PROVEEDOR:

LOTE 1 – Solución Perimetral

Certificación Cuadrante Gartner: La solución deberá pertenecer al cuadrante de líder de Gartner para Network Firewall en los tres (03) últimos reportes.

Certificación de Garantía: El oferente debe adjuntar un certificado expedido y firmado directamente por el fabricante con una fecha de expedición no mayor a 30 días calendario anteriores a la fecha de cierre del proceso, en el que se avale el nivel y el alcance de la garantía ofrecida de los productos adquiridos, y así mismo, que esta cumpla con lo indicado en la ficha técnica.

Certificación con el Fabricante: El oferente debe ser canal (Partner) certificado con alguno de los dos máximos niveles de membresía del fabricante de las soluciones principales de seguridad perimetral propuestas y estar en capacidad técnica de configurar, mantener y dar soporte técnico a los equipos. Este documento debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días.

Certificación de Especialidades: El oferente deberá presentar al menos tres (3) especialidades técnicas correspondientes al mismo fabricante, tal como fue definido desde el estudio de mercado y conforme con el alcance técnico y el monto de inversión del proceso.

Lo anterior con la finalidad de garantizar que el equipo técnico cuenta con la certificaciones e ingeniería calificada para la implementación y puesta en marcha de las soluciones ofertadas.

Certificación de Fabricante: El oferente debe entregar junto con la propuesta una certificación emitida directamente del fabricante de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta y contaran con soporte por mínimo 5 años, estos documentos deben ser dirigidas a la Entidad y deben ser expedidas con una fecha de al menos 30 días antes de la presentación de la propuesta.

LOTE 2 – Solución de Herramienta de Análisis de Vulnerabilidades

Certificación de Garantía: El oferente debe adjuntar un certificado expedido y firmado directamente por el fabricante con una fecha de expedición no mayor a 30 días calendario anteriores a la fecha de cierre del proceso en el que se avale el nivel y el alcance de la garantía ofrecida de los productos adquiridos, y así mismo, que esta cumpla con lo indicado en la ficha técnica.

Certificación de Fabricante: El oferente deberá presentar certificación de fabricante indicando las tecnologías consideradas en la presentación de oferta y adjuntar datasheets públicos de fabricante donde se evidencie el cumplimiento de los requerimientos técnicos.

15. ACEPTACIÓN CUMPLIMIENTO DE REQUIRIMIENTOS TÉCNICOS

Señor proveedor o contratista potencial: Al remitir cotización, usted está aceptando que la misma cumple con la totalidad de los requerimientos incluidos en el presente documento y que incluye los impuestos, tasas, gravámenes y contribuciones establecidas por las diferentes autoridades nacionales, departamentales o municipales y dentro de estos mismos niveles territoriales, las contribuciones, tasas, derechos, tarifas, y multas establecidos por las diferentes autoridades, que afecten la celebración, ejecución y liquidación del contrato y las actividades que de él se derive, y entiende que la misma se asume como una oferta irrevocable en los términos del artículo No. 846 del Código de Comercio. Así mismo, que, en caso de resultar adjudicatario del proceso de selección correspondiente, podrá prestar el servicio y/o entregar el bien, con las condiciones técnicas descritas en el presente documento.

NOTA 1: El proponente con la firma del presente documento se compromete a cumplir con todos los requerimientos técnicos descritos en los estudios previos y el pliego de condiciones y así mismo manifiesta expresamente que cumple con la totalidad de los requerimientos técnicos diseñados y solicitados por la Entidad.

NOMBRE DEL PROPONENTE: _____

FIRMA DEL REPRESENTANTE LEGAL:

_____

Nombre del Representante Legal:

_____

C.C.: _____

Autorizo la notificación electrónica a la dirección de correo electrónico

_____

Elaborado por: Yeison Chaparro Ayala – Profesional OTIC
Revisado componente jurídico: Luz Karime Jaimes Bonilla -Contratista OTIC
Aprobado por: Álvaro Caro Toloza – Jefe Oficina Tic