FICHA TÉCNICA

1. **OBJETO:** 10-7-14-31 - ADQUISICIÓN HARDWARE, SOFTWARE, LICENCIAS, GARANTÍA DE FÁBRICA, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DEL BALANCEADORES DE CARGA PARA LAS APLICACIONES Y SERVICIOS WEB DE LA AUTORIDAD NACIONAL DE LICENCIAS AMBIENTALES ANLA.

2. CLASIFICACIÓN DE BIENES Y SERVICIOS A ADQUIRIR

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
43201600	Difusión de Tecnologías de Información y Telecomunicaciones	Componentes para tecnología de la información, difusión o telecomunicaciones	Componentes del chasis
43222622	Difusión de Tecnologías de Información y Telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz y datos	Equipo de servicio de red
43233400	Difusión de Tecnologías de Información y Telecomunicaciones	Software	Software de controladores de dispositivos y utilidades
81111500	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Ingeniería de software o hardware
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de sistemas y administración de componentes de sistemas
81112000	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Servicios de datos
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software
81112300	Servicios Basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de hardware de computador

La entidad (ANLA) requiere cubrir la necesidad descrita en la presente ficha técnica con los requerimientos o condiciones mínimas que se deben cumplir, sin embargo, de acuerdo con los equipos que oferten estos podrán ser de mejor condición. Los balanceadores de aplicaciones debe cumplir como mínimo los siguientes Ítems:

3. BALANCEADOR DE APLICACIONES (APPLICATION DLIVERY CONTROLLER – ADC)

Se requiere la adquisición de balanceadores de aplicaciones de propósito especifico tipo appliance en alta disponibilidad para los centros de datos el cual debe contener como mínimo:

Para Datacenter principal (2 BALANCEADORES) y Datacenter Alterno (2 BALANCEADORES)

Este Balanceador debe incluir el software de administración y su respectivo licenciamiento mínimo por un (1) año, se debe contar las siguientes características:

- Ninguno de los modelos entregados a la ANLA, en cumplimiento del objeto contractual, podrá estar listado en el site del fabricante como End of Life (EoL), End of Sale o End of Support (EoS).
- Se requiere equipos de tipo “appliance”. Equipo nuevo de fábrica; no se aceptarán equipos remanufacturados o reparados. Debe ser la última versión disponible del fabricante. El sistema operativo (SO) del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web. Debe traer todos los accesorios para montaje y operación en rack estándar de 19” pulgadas (599 mm).
- El equipo debe cumplir mínimo con las siguientes características de capacidad y rendimiento:
  - Soportar Throughput de tráfico en L4 (OSI) de al menos 24 Gbps.
  - Soportar un Throughput en L7 (OSI) de al menos 17 Gbps.
  - Soportar al menos 10 Millones de conexiones simultáneas.

Debe soportar al menos el 30% del thoughput de HTTP (TLS /SSL) Requests por Segundo.

- Cada equipo debe contar con al menos las siguientes Interfaces de red:
  Al menos 4 puertos 1/10Gb RJ45.
  Al menos 4 puertos 1/10/25Gbps SFP28. Cad puerto debe incluir un SFP28 a 25Gbps multimodo.
  Puerto de administración y HA requeridos.

- El equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap) toma C13.
- Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y también tener la capacidad de funcionar las dos unidades al mismo tiempo (Activo/Activo), deberá contar con la capacidad de direccionamiento virtual. Los Equipos deben tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
- Memoria mínimo RAM de 32 GB.
- Debe incluir almacenamiento mínimo de 256GB SDD
- Debe permitir configurar cluster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda.
- Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción de balanceo.
- Debe realizar funciones de balanceo de aplicaciones en el tráfico basadas en mínimo protocolos TCP/UDP
- Debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
- Debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
- Los equipos ofertados deben ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los miembros ya existentes.
- Debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting:

  Round Robin
  Proporcional (Ratio)
  Proporcional dinámico
  Respuesta más rápida
  Conexiones mínimas
  Menor número de sesiones
  Tendencia de menor cantidad de conexiones

- El equipo debe soportar mínimo 32 y permitir crecer hasta 64 servicios virtuales que se pueden configurar (virtual servers, virtual IP, Granjas)El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
- Debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
  - Ping.
  - Chequeo a nivel de TCP y UDP a puertos específicos
  - Monitoreo http y https
  - Ejecución de scripts para determinar la respuesta emulando un cliente.
  - Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
  - Monitoreo de servicios:
    - LDAP
    - FTP
    - SMTP
    - IMAP/POP3
    - Oracle
    - MSSQL
    - MySQL
    - RADIUS
    - SIP
    - Protocolo SASP
    - SOAP
    - WMI
    - SNMP
- Debe poder realizar como mínimo estos métodos de persistencia de las conexiones:
  - Dirección IP origen
  - Dirección IP destino
  - Cookies
  - Hash
  - SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
  - Sesiones SSL Microsoft Remote Desktop.
- Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.
- El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.
- Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:
  Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.
- Soporte de REST API
- Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.
- Debe soportar el protocolo TDS para balanceo de los diferentes motores de Base de Datos: MSSQL, Oracle, Postgres, MongoDB y MySQL
- Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT
- Debe soportar el protocolo NetFlow y/o sFlow.

- El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.
- El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3
- Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP.
- Cada equipo debe soportar seguridad SSL con las siguientes características:
    - Incluir el soporte de Aceleración SSL usando Hardware Dedicado
    - Incluir mínimo 10.000 Transacciones por segundo SSL (RSA 2K Keys)
    - Incluir mínimo 10.000 Transacciones por segundo SSL (ECDSA P-256)
    - Incluir mínimo 10.000 Transacciones por segundo SSL (ECDHE P-256-RSA 2K)
    - Soportar al menos 10 Gbps SSL Bulk Encryption (Thoughput SSL)
    - Soporte de llaves SSL RSA de mínimo de 256 bits.

- Debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener las sesiones SSL ya establecidas.
- El Stack TLS del equipo debe soportar las siguientes funcionalidades/características
    - Session ID
    - Session Ticket
    - OCSP Stapling (online certificate status protocol)
    - Dynamic Record Sizing
    - ALPN (Application Layer Protocol Negotiation)
    - Forward Secrecy.
- Debe manejar como mínimo AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)
- Firmado criptográfico de cookies para verificar su integridad.
- Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales Y Entrust.
- Debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo, el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el tráfico SSL sin que el balanceador termine la sesión SSL.
- Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.
- Debe soportar HSTS (HTTP Strict Transport Security).
- Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.
    - Scanners
    - Exploits Windows
    - Denial of Service
    - Proxies de Phishing
    - Botnets
    - Proxies anónimos.
- La implementación debe incluir la capacidad de hacer aceleración de aplicación a nivel de:
    - Memoria cache.

Compresión tráfico HTTP
Optimización de conexiones a la aplicación a nivel TCP
Multiplexación de conexiones hacia los servidores.

- El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
- Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 15 Gbps o superior.
- Debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.
- Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos
- Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP.
- Se debe permitir alta disponibilidad de aplicaciones distribuidas en 2 o más datacenters, sin importar la ubicación geográfica.
- Debe permitir como un servidor DNS de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.
- Debe permitir funcionamiento como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.
- Para el balanceo global (DNS), debe permitir mínimo los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting:
  Round Robin
  Global Availability
  Geolocalización
  Capacidad del Servicio
  Least Connections
  Packets Per Second
  Round Trip Time
  Drop Packet
  Hops
  Packet Completion Rate
  User-defined QoS
  Proporcional (Ratio)
  Kilobytes Per Second
  Regreso al DNS
  Persistencia estática
  Puntuación del Servicio.
- Debe funcionar y manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión.
- Debe permitir balanceo de cargas ente Datacenters de acuerdo con la ubicación geográfica.
- Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico basado en requerimientos particulares de la infraestructura
- Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.
- Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.
- Debe permitir realizar balanceo de servidores DNS.
- Debe soportar el protocolo DNSSEC
- Debe soportar herramientas de administración grafica para el manejo de zonas DNS
- Debe soportar registros AAAA para IPv6

- Debe soportar traducción entre DNS IPv4 y DNS Ipv6.
- Soporte VLAN 802.1q, Vlan tagging
- Soporte de 802.3ad para definición de múltiples troncales
- Soporte de NAT, SNAT
- Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
- Soporte de Rate Shapping.
- Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
- Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS.
- Debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- Debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
- Debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
- Debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
- Debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales.
- Debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
  Protocolo SysLog
  Notificación vía SMTP
  SNMP versión.2.0 o superior.
- El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
- El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
- La interfaz gráfica debe contar con varias plantillas de Dashboard personalizable que permita monitorear el estado del equipo en tiempo real.
- Debe contar con un módulo de reportes con plantillas predefinidas y a su vez contar con un módulo personalizable que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
- Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.

3.1. FIREWALL DE APLICACIONES Y PROTECCIÓN DE API PARA BALANCEADORES DATACENTER ALTERNO

Para el Balanceador que se desplegará en el centro de datos alterno, se deberán incluir funcionalidades avanzadas de firewall de aplicación por cada uno de los appliances para este sitio.

- Con el fin de proteger las aplicaciones WEB y APIs expuestos a través en un entorno público, se debe contar con una funcionalidad de seguridad de capa 7 que valide toda la interacción de los usuarios y bloquee requerimientos maliciosos hacia estos servicios.
- La política de seguridad del WAF debe ser declarativa y fácil de integrar en entornos de DevSecOps por medio de pipelines de CI/CD,

- El firewall de aplicación (WAF) activado en balanceador al momento de recibir tráfico, debe soportar modo bloqueo o modo monitoreo.
- Debe incluir un módulo de Denial of Service en capa 7.
- Debe incluir un set de firmas para proteger como mínimo OWASP Top 10.
- Debe incluir firmas de ataque para diferentes tecnologías.
- Debe soportar la detección y el bloqueo de métodos de evasión, como directory transversal, caracteres escapados, como mínimo.
- Debe permitir configurar un listado de extensiones de archivo no permitidas que deben ser bloqueados
- Debe permitir configurar un listado de parámetros sensibles, cuyo valor sea enmascarado en los logs.
- Debe permitir la configuración de parámetros de tráfico JSON, como la máxima profundidad de la estructura, tamaño máximo de la data, máximo valor de parámetros, máximo tamaño de arreglos, entre otros
- Debe permitir definir como mínimo los métodos HTTP (GET, POST) para una aplicación
- El WAF debe detectar contenido gRPC malformado
- Debe permitir customizar una página de respuesta en caso de una violación
- Debe asociar a cada violación un identificador único, con el fin de tener trazabilidad en los logs
- Debe validar las cookies e identificar cookies malformadas
- Debe permitir personalizar los códigos HTTP válidos para cada aplicacion
- Debe permitir asociar una referencia a un archivo OpenAPI (swagger), con el fin de restringir todos los requerimientos realizados únicamente a lo indicado por el descriptor del API
- Debe incluir una funcionalidad básica de detección de BOT basada en firmas, incluyendo BOTs confiables y BOTs nocivos
- Debe validar también la respuesta del servidor contra firmas de ataques, no solamente el requerimiento del usuario
- Debe permitir la configuración de parámetros usados en la aplicacion web y definir el tipo de valores que cada parámetro utiliza, o permitir que este tipo de valor sea configurado de forma automática
- Debe permitir la configuración de firmas de ataque definidas por el usuario
- Debe soportar protections contra CSRF (Cross-Site Request Forgery)
- Debe soportar protección contra Clickjacking
- Debe permitir la protección de las aplicaciones de forma granular, por ejemplo, se puede decidir no activar el WAF de forma global sino para ciertas aplicaciones o para ciertas rutas dentro de cada aplicación
- Debe proteger GraphQL APIs
- Debe permitir la personalización del log de eventos y permitir enviarlos a repositorios externos

3.2. Soporte y garantía: Todos los componentes deberán estar cubierta por un contrato de soporte y garantía por un (1) año con el fabricante que incluya:

Atención 7x24x365,
Acceso a base de conocimiento.
Portal de soporte.
Reemplazo de Equipos. El oferente debe contemplar un tiempo de cambio de equipo dentro de las ocho (8) horas siguientes al diagnóstico de falla en el hardware que lo requiera.

El contratista deberá disponer de personal en sitio en un plazo máximo de ocho (8) horas ante eventos de máxima severidad.

3.3. Insumos requeridos para la plataforma de balanceo (Datacenter Principal)

- Doble fuente de poder y Cables de poder (4 unidades) con clavija C13
- Unidades de Rack: 2U
- Cables de red UTP Cat6: 8 PassCord 2mts
- Fibras FC Multimodo OM4 LC-LC: 12 unidades 2 mts
- 4 unidades de SFP-10GBASE-T SFP+ cobre RJ-45 30m
- 12 unidades de SFP-25GBASE-SR SFP28 850nm 100m

3.4. Insumos requeridos para la plataforma de balanceo (Datacenter Alterno)

- Doble fuente de poder y Cables de poder (4 unidades) con clavija C13
- Unidades de Rack: 2U
- Cables de red UTP Cat6: 8 PassCord 2mts
- Fibras FC Multimodo OM4 LC-LC: 12 unidades 2 mts
- 4 unidades de SFP-10GBASE-T SFP+ cobre RJ-45 30m
- 12 unidades de SFP-25GBASE-SR SFP28 850nm 100m

4. SWITCH ETHERNET AVANZADO PARA LA PLATAFORMA DE BALANCEO (DATACENTER ALTERNO)

La entidad actualmente cuenta con El equipo en Datacenter alterno C9500-24Y4C, por lo cual se requiere un equipo de iguales características que permita la capacidad e integrarse como Virtual Chasis con las siguientes características:

- Switching capacity: Up to 2 Tbps
- Total, number of MAC addresses: Up to 82,000
- VLAN IDs 4000
- Total, number of IPv4 routes (Address Resolution Protocol [ARP] plus learned routes): Up to 212,000 indirect + direct Up to 90,000 host/ARP
- Total number of IPv6 routes: Up to 212,000 indirect + direct Up to 90,000 host
- DRAM 16 GB

- Debe poseer motor de telemetría y analítica interno para monitoreo que permita la resolución de problemas, la identificación de anomalías y predicción de capacidad.

- Soporte de módulos y cables 1G y 10G compatibles de otras marcas de forma que se puedan reutilizar módulos existentes en la entidad.

- Soporte de sincronización de tiempo por protocolo NTP. Debe permitir funcionar como servidor NTP de la red.

- Soporte VxLAN. Deben tener soporte de VxLAN estático VTEP, VxLAN dinámico BGP-EVPN. Soporte IPV4 Multicast sobre VxLAN overlay/EVPN, IPV6 VxLAN/EVPN overlay, VxLAN distributed Anycast Gateway, VxLAN ARP/ND Supression, Segementación dinámica VxLAN GBP.

- Soporte DHCP, DHCP Relay, debe permitir servir como servidor DHCP de la red en IPV4 e IPV6. Debe permitir la coexistencia DHCP relay y DHCP Server.

- Soporte DNS. Debe soportar sistema de nombres de dominio distribuidos con soporte como cliente y como servidor.

- Soporte de Enrutamiento estático y dinámico. OSPF, BGP y PIM IPv4 e IPV6. Debe permitir Network Load Balancing (NLB)

Los switches suministrados deben incluir soporte y garantía por un periodo de 1 año. El Contratista debe garantizar un tiempo de atención en modalidad 7x24x365 durante el periodo de la garantía. El contratista debe garantizar el intercambio y reemplazo de partes dentro de las ocho (8) horas siguientes al reporte de falla de switch.

4.1. Insumos requeridos para switch ethernet avanzado para la plataforma de balanceo (Datacenter Alterno)

- Doble Fuente de poder y Cables de poder (4 unidades) con clavija C13
- Unidades de Rack: 1U
- Cables de red UTP Cat6: 2 PassCord 3mts
- Fibras FC Multimodo OM4 LC-LC: 4 unidades
- 4 unidades de SFP-10GBASE-T SFP+ cobre RJ-45 30m
- 12 unidades de SFP-25GBASE-SR SFP28 850nm 100m
- 10 unidades de SFP-10GBASE-SR SFP 850nm 100m
- 2 cables DAC SFP56 de 3 metros

5. SWITCHS ETHERNET PLATAFORMA DE BALANCEO (PARA SEDE CALLE 34)

Para la sede ANLA de calle 34 se debe contar con dos **(2)** Switches (SW), estos SW deben tener puertos ópticos con sus respectivos SFP (Ten giga) y deben ser configurados en virtual chasis.

- Cada switch debe poseer las siguientes características de rendimiento:

Se requiere el suministro, instalación y configuración de Dos (2) Switches ethernet 32Y (veintiocho puertos 1/10/25G SFP28) 4C (Cuatro puertos 100G QSFP28).

- Capacidad de Switching de mínimo 2,4Tbps.
- Packet Buffer de 32MB.
- Mac Address Capacity 210,000,
- Capacidad de tabla IPV4/PV6 145.000/145.000
- CAPACIDAD DE VLANS 4094 Simultaneas.

Para el ítem de switch se de cumplir con características:

Acceso y configuración: Al menos vía:

- Línea serial de comandos (CLI)
- HTTP/HTTPS - Web Authentication
- SSHv2 Secure Shell

Soporte de tablas ARP, como mínimo: Estático y dinámico

Montaje: Debe incluir todos los accesorios para montaje y operación en rack estándar
Fuentes de poder: El switch debe incluir al menos dos (2) fuentes de poder.

- Cada Switch debe tener la siguiente capacidad de puertos.

28 puertos 1/10/25Gbe SFP+/SFP28, de estos, debe permitir la configuración de hasta 12 Puertos 50G.
4 puertos 10/25Gbe MACsec.

4 puertos 40/100Gbe.

- Debe poseer motor de telemetría y analítica interno para monitoreo que permita la resolución de problemas, la identificación de anomalías y predicción de capacidad.

- Soporte de módulos y cables 1G y 10G compatibles de otras marcas de forma que se puedan reutilizar módulos existentes en la entidad.

- Se debe garantizar los SPF adicionales para la integración con los equipos existentes.

- Soporte de sincronización de tiempo por protocolo NTP. Debe permitir funcionar como servidor NTP de la red.

- Soporte VxLAN. Deben tener soporte de VxLAN estático VTEP, VxLAN dinámico BGP-EVPN. Soporte IPV4 Multicast sobre VxLAN overlay/EVPN, IPV6 VxLAN/EVPN overlay, VxLAN distributed Anycast Gateway, VxLAN ARP/ND Supression, Segementación dinámica VxLAN GBP.

- Soporte DHCP, DHCP Relay, debe permitir servir como servidor DHCP de la red en IPV4 e IPV6. Debe permitir la coexistencia DHCP relay y DHCP Server.

- Soporte DNS. Debe soportar sistema de nombres de dominio distribuidos con soporte como cliente y como servidor.

- Soporte de Enrutamiento estático y dinámico. OSPF, BGP y PIM IPv4 e IPV6. Debe permitir Network Load Balancing (NLB)

- Los switches suministrados deben incluir soporte y garantía por un periodo de 1 año. El Contratista debe garantizar un tiempo de atención en modalidad 7x24x365 durante el periodo de la garantía. El contratista debe garantizar el intercambio y reemplazo de partes dentro de las ocho (8) horas siguientes al reporte de falla de switch.

- Debe poseer motor de telemetría y analítica interno para monitoreo que permita la resolución de problemas, la identificación de anomalías y predicción de capacidad.

- Soporte de módulos y cables 1G y 10G compatibles de otras marcas de forma que se puedan reutilizar módulos existentes en la entidad.

- Soporte de sincronización de tiempo por protocolo NTP. Debe permitir funcionar como servidor NTP de la red.

- Soporte VxLAN. Deben tener soporte de VxLAN estático VTEP, VxLAN dinámico BGP-EVPN. Soporte IPV4 Multicast sobre VxLAN overlay/EVPN, IPV6 VxLAN/EVPN overlay, VxLAN distributed Anycast Gateway, VxLAN ARP/ND Supression, Segementación dinámica VxLAN GBP.

- Soporte DHCP, DHCP Relay, debe permitir servir como servidor DHCP de la red en IPV4 e IPV6. Debe permitir la coexistencia DHCP relay y DHCP Server.

- Soporte DNS. Debe soportar sistema de nombres de dominio distribuidos con soporte como cliente y como servidor.

- Soporte de Enrutamiento estático y dinámico. OSPF, BGP y PIM IPv4 e IPV6. Debe permitir

Network Load Balancing (NLB)

5.1. Insumos requeridos para switches ethernet avanzado para la plataforma de balanceo (sede calle 34)

- Se deben incluir los siguientes módulos SFP en total:
    - 24 módulos SFP SR de 10G para fibra multimodo.
    - 8 módulos 1G /10G SFP Rj45.
    - 2 cables DAC SFP56 de 3 metros.
    - 24 Fibras OM4 Multimodo LC LC de 1 metro.
    - Doble Fuente de poder y Cables de poder (4 unidades) con clavija C13
    - Unidades de Rack: 1U por switch

6. **GARANTÍA Y SOPORTE DE FABRICA POR UN (1) AÑO:** Toda los equipos adquiridos y detallados en los anteriores numerales deben incluir el suministro y remplazo de partes y/o equipos completos en caso de presentarse daños en su funcionamiento sin costo adicional para ANLA durante el tiempo de la garantía y soporte. Las partes que sean remplazadas por efecto de la garantía deben estar homologadas por el fabricante del equipo, deberán ser nuevas y libres de imperfecciones. En cuanto a la reparación o reemplazo de los equipos o partes en garantía, se debe realizar la configuración, y dejar los equipos en perfecto estado de funcionamiento en un tiempo no mayor a ocho (8) horas a partir de que se notifique la falla por medio de correo electrónico o a través de llamada telefónica, este deber ser reemplazado en el mismo lugar de la falla. Para evitar la indisponibilidad prolongada deben hacer uso de equipos de repuesto de iguales o superiores características mientras se deja el equipo definitivo.

El soporte técnico incluye mantenimiento correctivo cuando a los equipos suministrados y este se deberá realizar una vez al año durante el periodo de garantía.

Nota: Los equipos requeridos para el cumplimiento del objeto del contrato deben propender por ser eficientes y con rendimiento en consumo energético de acuerdo con su categoría en el mercado y que cumplan con las especificaciones técnicas exigidas

7. **IMPLEMENTACIÓN:** Se debe incluir la instalación, configuración, en integración de la nueva infraestructura y puesta en marcha de los equipos y configuración, además se de garantizar la integración o articulación con el hardware e infraestructura actual tanto en Datacenter principal y Alterno y Sede principal Calle 34 o donde se encuentren ubicados o donde se requiera de acuerdo con las ubicaciones establecidas por la entidad durante la ejecución del contrato.

8. **TRANSFERENCIA A DE CONOCIMIENTO:** Transferencia de conocimiento completa: Exige una transferencia completa de conocimiento sobre el equipo, incluyendo información sobre su funcionamiento, mantenimiento preventivo, solución de problemas comunes y cualquier otra información relevante para su uso efectivo, esta debe ser mínimo de al menos 20 horas para los profesionales que disponga la supervisión del contrato. Adicionalmente se debe entregar toda la documentación requerida como los manuales, instructivo y grabaciones de las capacitaciones. (Sin generar costo para la entidad), la documentación de las configuraciones finales se realizará de acuerdo con los lineamientos de la supervisión.

9. **PLAZO DE EJECUCIÓN DEL CONTRATO**

El plazo del del contrato será hasta el 27 de diciembre de 2024 contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.

Nota 1: La entrega de equipos se deben garantizar hasta máximo el 17 de diciembre de 2024, previo

cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato.
Nota 2: La implementación y puesta macha de la plataforma y equipos no debe superar el 17 de diciembre de 2024.
Nota 3: La entrega del certificado de garantía de fábrica de los componentes de software no debe superar el 17 de diciembre de 2024.
Nota 4: Las garantías de fábrica de los (balanceadores y switches) tendrán una vigencia de un año a partir de su activación.
NOTA 5: 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_____

Proyectó: Wilder Javier Morales - Contratista - Oficina de Tecnologías de la Información
Revisó: Edgar Daniel Sierra - Contratista - Oficina de Tecnologías de la Información
Cristian Leonardo Serna Ramirez - Contratista - Oficina de Tecnologías de la Información
Revisó: Juan David Anzola Rodriguez – Coordinador del Grupo de Infraestructura Tecnológica - Oficina de Tecnologías de la Información