**PARA:** **OFERENTE**

**DE:** **INGRID YANETH MEJIA CHAPARRO**
VICEPRESIDENTE ADMINISTRATIVO Y FINANCIERO

**ASUNTO:** Sondeo de Mercado para la contratación cuyo objeto es *"*Adquirir la infraestructura de conectividad de acceso lógico para las redes de la ANH, (Cableado Estructurado, Certificación y demás elementos necesarios).*"*

La Agencia Nacional de Hidrocarburos – ANH se encuentra adelantando el Análisis del Sector con el fin de obtener, entre otros aspectos, los valores estimados para la contratación de objeto "Adquirir la infraestructura de conectividad de acceso lógico para las redes de la ANH, (Cableado Estructurado, Certificación y demás elementos necesarios).".

Para tales efectos, le informo que la Entidad realizará una Audiencia Pública con todos los interesados en participar, el día lunes veintiocho (28) de agosto del presente año a las 3:00 p.m. en la Entidad – 2º piso, con la finalidad de exponer los aspectos técnicos del proyecto y resolver las observaciones e inquietudes de los participantes de la misma, de tal manera que la ANH realice el Análisis del Sector y establezca un valor estimado del proyecto que garantice, entre otros aspectos, un presupuesto acorde con los valores actuales del mercado y una participación plural de oferentes en el proceso de contratación.

Anexo a la presente comunicación, nos permitimos enviar la información técnica de requerimiento para el proceso.

Es de resaltar que posterior a la celebración de la Audiencia Pública, los interesados en participar en el sondeo de mercado deberán enviar su cotización, a más tardar el día martes veintinueve (29) de agosto del presente año, a los correos electrónicos juan.vila@anh.gov.co y carlos.bastidas@anh.gov.coa los mismos correos, se podrán hacer llegar las inquietudes o aclaraciones.

Es de precisar que la presente consulta de precios no obliga ni compromete la responsabilidad de la Agencia Nacional de Hidrocarburos y se constituye en uno de los instrumentos para establecer el presupuesto oficial estimado del proyecto a contratar.

Atentamente,

**INGRID YANETH MEJIA CHAPARRO**
VICEPRESIDENTE ADMINISTRATIVO Y FINANCIERO
Revisó: Juan Carlos Vila Franco – Jefe Oficina de Tecnologias de la Información / Componente Técnico
Proyectó: Carlos Abel Bastidas Cubides -Experto G6 Grado 3 / Componente Técnico

## SONDEO DE MERCADO

La Agencia Nacional de Hidrocarburos – ANH está adelantando el presente sondeo de mercado, con el fin de realizar el análisis económico y financiero que soportarán la determinación del presupuesto oficial de un posible proceso de selección contractual, si su Empresa se encuentra interesada en participar le agradecemos remitir la información solicitada, bajo los parámetros establecidos a continuación.

**NOTA:** *La Agencia Nacional de Hidrocarburos – ANH, aclara que ni el envío de esta comunicación ni la respuesta a la misma generan compromiso u obligación de contratar, habida cuenta que no se está formulando invitación para participar en un concurso o proceso selectivo, sino, se reitera, se está realizando un sondeo de mercado del que eventualmente se puede derivar un proceso de selección para la elaboración de un contrato que permita ejecutar el proyecto*

| | |
|---|---|
| **DESCRIPCIÓN DE LA NECESIDAD:** | La Entidad requiere adquirir la infraestructura de conectividad de acceso lógico para las redes de la ANH, (Cableado Estructurado, Certificación y demás elementos necesarios), para renovar los switch de acceso de las redes internas, así como fortalecer la seguridad de conexión de los diferentes periféricos de su red LAN. |
| **OBJETO A CONTRATAR:** | Adquirir la infraestructura de conectividad de acceso lógico para las redes de la ANH, (Cableado Estructurado, Certificación y demás elementos necesarios). |
| **IDENTIFICACION DEL CONTRATO A CELEBRAR:** | Compra venta. |

| | |
|---|---|
| **CÓDIGO UNSPSC (The United Nations Standard Products and Services Code® - UNSPSC, Código Estándar de Productos y Servicios de Naciones Unidas), correspondiente al bien, obra o servicios a contratar:** | Con Con arreglo a los artículos 2.2.1.1.1.5.1. al 2.2.1.1.1.5.7. del Decreto Reglamentario 1082 de 2015, los Proponentes Individuales deben encontrarse inscritos, clasificados y calificados en el Registro Único de Proponentes – RUP de la Cámara de Comercio de su domicilio principal, en al menos uno (1) de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC):<br><br>Con arreglo a los artículos 2.2.1.1.1.5.1. al 2.2.1.1.1.5.7. del Decreto Reglamentario 1082 de 2015, los Proponentes Individuales deben encontrarse inscritos, clasificados y calificados en el Registro Único de Proponentes - RUP de la Cámara de Comercio de su domicilio principal, en alguno (s) o en todos de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC), dentro del tercer o cuarto nivel:<br><br>UNSPSC: 43222500 — Equipo de seguridad de red<br>UNSPSC: 43233200 — Software de seguridad y protección<br>UNSPSC: 81111800 — Servicios de sistemas y administración de componentes de sistemas<br><br>En el caso de propuestas presentadas por consorcios, uniones temporales o promesas de sociedad futura, al menos uno o más de uno de los integrantes debe estar inscrito, clasificado y calificado en por lo menos uno de los Códigos anteriormente establecidos. |

**ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN:**

| **ÍTEM 1: Red de Datos** | | |
|---|---|---|
| **SUBÍTEM 1.1: Equipos SWITCH Acceso** | | |
| **Denominación del Bien:** | | Switch |
| **Denominación Técnica:** | | Switch de Acceso |
| **Unidad de Medida:** | | Unidad |
| **ÍTEM** | **CARACTERÍSTICA** | **MINIMO REQUERIDO** |
| 1.1 | Cantidad | 15 |
| 1.2 | Marca | Especificar |

| | | |
|---|---|---|
| 1.3 | Tipo | Stackable |
| 1.4 | Modelo | Especificar |
| 1.5 | Tamaño | 1 Unidad de Rack Máximo |
| 1.6 | Puertos | Cada switch debe incluir mínimo:<br>• 48 puertos 10/100/1000BASE-T (RJ-45)<br>• 4 puertos a 1GBASE-X SFP, actualizables a 10Gb Ethernet vía licencia.<br>• 2 puertos de cobre en combo a 1GbE, actualizables a 10GbE<br>• 4 puertos a 1GBASE-X SFP, actualizables a 10Gb Ethernet vía licencia.<br>• 2x7 puerto RPS |
| 1.7 | Interfaces 10GE | Incluir al menos:<br>• 6 transceivers SFP+ SR (fibra multimodo).<br>• 6 Licencias para habilitar dos puertos a 10G |
| 1.8 | Puertos de Administración | • 1 puerto serial de consola RJ-45 con RTS/CTS<br>• 1 puerto fuera de banda 1 x 10/100/1000BASE-T (Gestión) |
| 1.9 | PoE | Debe soportar PoE Plus:<br>• IEEE 802.3at<br>• RFC 3621 Power over Ethernet |
| 1.10 | Rendimiento | Soportar como mínimo:<br>• Rendimiento: 130.9 Mpps,<br>• Capacidad de conmutación: 176 Gbps.<br>• El equipo debe ser Non-Blocking y full dúplex en todas sus interfaces. |
| 1.11 | Apilamiento y Crecimiento | • Debe incluir dos puertos de stack<br>• Los equipos que son parte del stack deberán trabajar como si fuesen elementos de un solo chasís, en funcionalidad, administración, operación, configuración y monitoreo.<br>• El stack debe ser capaz de crecer al menos hasta ocho (8) equipos de la misma serie.<br>• El stack se debe conectar por medio de cables de 10Gbps. Capacidad de conectarse en stacking local o geográfico.<br>• Los equipos deben traer dos puertos de stack (SFP+)<br>• El stack debe permitir conexiones de hasta 40 KM (Distribución geográfica)<br><br>**Nota:** Se debe incluir un cable de apilamiento de 1M por cada switch. |
| 1.12 | Velocidad Apilamiento | El equipo debe ser capaz de soportar apilamiento con un ancho de banda de al menos 40 Gbps fullduplex. Proporcionando conectividad de apilamiento a largas distancias de hasta 40 km. |
| 1.13 | Alta Disponibilidad del Apilamiento | Se debe comportar como una única entidad de administración. Se debe comportar como una única entidad lógica de enrutamiento.<br><br>Incluir mecanismo de protección IP y VLANs a través de anillos ópticos 1/10G con tiempo de recuperación máximo de 50milisegundos de manera natural y sin licenciamiento extra permitiendo la rápida de las aplicaciones como son VoIP y Video esto es bajo los estándares RFC 3619 e ITU G.8032. |
| 1.14 | Enlace Agregados | Se debe poder realizar enlaces agregados, mínimo un enlace desde cada unidad del apilamiento. |
| 1.15 | Soporte USB | Los switches deben incluir un puerto USB 2.0 |
| 1.16 | Fuentes de Poder | Debe incluirse fuente de poder redundante de 1005W |

| | | |
|---|---|---|
| | | **Nota:** Energy Efficient Ethernet (EEE) soportado en todos los puestos de cobre Base-T. |
| 1.17 | Latencia | Menor a 4 microsegundos |
| 1.18 | Características de Procesamiento y Memoria | • 64-bit MIPS Processor, 1 GHz clock, single core<br>• 1GB ECC DDR3 DRAM<br>• 4GB eMMC Flash<br>• 3.0MB packet buffer on 48 port switches |
| 1.19 | Voltajes / Frecuencia soportados | • Rango de voltaje de entrada: 100-240 VAC<br>• Rango de frecuencia de línea: 50 - 60 Hz +/- 5%<br>• Power Supply Input Socket: IEC 320 C14<br>• Power Cord Input Plug: IEC 320 C13<br>• Rango de temperatura de operación: 0º C to 50º C (En normal operación) |
| 1.20 | Sistema Operativo | Todos los switches deben ejecutar la misma versión del sistema operativo, lo que ayuda a desplegar, operar y mantener la red y reducir los costos operativos.<br>• Sistema operativo modular<br>• Arquitectura de alta disponibilidad<br>• Capa 2 y Capa 3<br>• Seguridad Integrada con NetLogin, Seguridad MAC, Seguridad IP<br>• Políticas de seguridad dinámicas basadas en el usuario, la ubicación y el tiempo<br>• Soporte de redes definidas por software<br>• Compatible con OpenFlow y OpenStack<br>• Ethernet Audio Video Bridging (AVB) habilitado<br>• IPV6: Capa 2/3 IPv6 forwarding, protocolos de enrutamiento y túneles. |
| 1.21 | Jumbo Frames | Soportar tramas de hasta 9216 bytes |
| 1.22 | Tamaña de la tabla de enrutamiento | • IPv4 Host: 1000<br>• IPv4 LPM Entries: 480<br>• IPv6 LPM Entries: 240 |
| 1.23 | Tamaño de la tabla de direcciones MAC | Soportar al menos 16K Direcciones |
| 1.24 | Vlan | Soportar al menos 4092 VLANs |
| 1.25 | Audio Video Bridging (AVB) | Los equipos deben soportar el protocolo IEEE 802.1 Audio Video Bridging, para el manejo de tráfico en tiempo real de audio y video con calidad de servicio. |
| 1.26 | Protocolos Soportados | • IEEE 802.3AT<br>• Soporte de múltiples instancias del Protocolo STP (Spanning Tree Protocol).<br>• Soporte de IEEE 802.1w RSTP<br>• Soporte de IEEE 802.3ad, Configuración de compartición de carga estática y configuración dinámica basada en LACP<br>• Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol<br>• Soporte de IEEE 802.1ag Connectivity Fault Management<br>• Soporte de RFC 3619 Ethernet Automatic Protection Switching (EAPS) Version 1<br>• OpenFlow Protocol 1.0 (Por medio de Licencia)<br>• RFC 2131 BOOTP/DHCP relay agent and DHCP server<br>• RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs<br>• RFC 3410 – 3415 SNMPv3, basada en la seguridad del usuario, cifrado y autenticación<br>• RFC 2668 802.3 Medium Attachment Units (MAU) MIB |

| | | |
|---|---|---|
| 1.27 | Protocolos de Enrutamiento IPv4 | Debe incluir enrutamiento estático<br>• RFC 3376 IGMP v3<br>• RFC 2338 Virtual Router Redundancy Protocol (Por medio de Licencia)<br>• Autenticación MD5 OSPF (Por medio de Licencia) |
| 1.28 | Protocolos de Seguridad | • Secure Shell (SSH-2), Secure Copy (SCP-2) and SFTP client/server with encryption/authentication<br>• SNMPv3 user based security, with encryption/ authentication<br>• RFC 1492 TACACS+<br>• RFC 2138 RADIUS Authentication<br>• RFC 2139 RADIUS Accounting<br>• RFC 3579 RADIUS EAP support for 802.1x<br>• RADIUS Per-command Authentication<br>• Access Profiles on All Routing Protocols<br>• Access Policies for Telnet/SSH-2/SCP-2<br>• Network Login – 802.1x, Web and MAC-based mechanisms<br>• IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login<br>• Multiple supplicants with multiple VLANs for Network Login<br>• Fallback to local authentication database (MAC and Web-based methods)<br>• Guest VLAN for 802.1x<br>• RFC 1866 HTML<br>• MAC Security – Lockdown and Limit<br>• IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID<br>• IP Security – Trusted DHCP Server<br>• Layer 2/3/4 Access Control Lists (ACLs)<br>• RFC 2267 Network Ingress Filtering<br>• RPF (Unicast Reverse Path Forwarding) Control via ACLs –<br>• Wire-speed ACLs<br>• Rate Limiting/Shaping by ACLs<br>• IP Broadcast Forwarding Control<br>• ICMP and IP-Option Response Control<br>• SYN attack protection<br>• CPU DoS Protection with traffic rate-limiting to management CPU<br>• IP Security – DHCP enforcement via Disable ARP Learning<br>• IP Security – Gratuitous ARP Protection<br>• IP Security – DHCP Secured ARP/ARP Validation<br>• Routing protocol MD5 authentication<br>• CLEAR-Flow, threshold-based alerts and actions<br>• Identity Manager |
| 1.29 | Funcionalidades de Seguridad | • Políticas por usuario y host<br>• Perfiles de seguridad dinámicos por puerto<br>• Detección y respuesta a amenazas. (CLEAR-Flow Security Rules Engine)<br>• Protección contra ataques de negación de servicio (DDoS)<br>• Políticas basadas en perfiles: 63<br>• Reglas por perfil: Hasta 440<br>• Policitas de autenticación de usuario por switch: Hasta 256<br>• Policitas de autenticación de usuario por puerto: Hasta 256<br>• Reglas Permit/Deny por switch: 440<br>• Reglas basadas en IPv4: 256 |

| | | |
|---|---|---|
| | | • Reglas basadas en L2: 184<br>• Tasa de Limitación: Por Clase de Servicio |
| 1.30 | Otras funcionalidades | • 128 troncales de carga compartida, hasta 8 miembros por troncal<br>• Políticas de ancho de banda de ingresos y egreso limitadas por flujos/ACLs<br>• 8 colas de ingreso y egreso por puerto (QoS)<br>• Ancho de banda de egreso limitado por cola de egreso y por puerto<br>• Granularidad de limitación de velocidad: 8 Kbps |
| 1.31 | Certificaciones Internacionales (EMC) | • CISPR 22: 2006 Ed 2.2, Class A (International Emissions)<br>• CISPR 24: A2:2003 Class A (International Immunity)<br>• IEC 61000-4-2:2008/EN 61000-4-2:2009 Electrostatic Discharge, 8kV Contact, 15 kV Air, Criteria A<br>• IEC 61000-4-3:2008/EN 61000-4-3:2006+A1:2008 Radiated Immunity 10V/m, Criteria A<br>• IEC 61000-4-4:2004 am1 ed.2. /EN 61000-4-4:2004/A1:2010 Transient Burst, 1 kV, Criteria A<br>• IEC 61000-4-5:2005 /EN 61000-4-5:2006 Surge, 2 kV L-L, 2 kV L-G, Level 3, Criteria A<br>• IEC 61000-4-6:2008/EN 61000-4-6:2009 Conducted Immunity, 0.15-80 MHz, 10V/m unmod. RMS, Criteria A<br>• IEC/EN 61000-4-11:2004 Power Dips & Interruptions, >30%, 25 periods, Criteria C |
| 1.32 | Estándares Ambientales | • EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage<br>• EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation<br>• EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational<br>• EN/ETSI 300 753 (1997-10) - Acoustic Noise<br>• ASTM D3580 Random Vibration Unpackaged 1.5 G |

| **ÍTEM 2: Red de Datos** | | |
|---|---|---|
| **SUBÍTEM 2.1: Equipos SWITCH de control operativo** | | |
| **Denominación del Bien:** | | Switch |
| **Denominación Técnica:** | | Switch de Acceso |
| **Unidad de Medida:** | | Unidad |
| **ÍTEM** | **CARACTERÍSTICA** | **MINIMO REQUERIDO** |
| 2.1 | Cantidad | 3 |
| 2.2 | Marca | Especificar |
| 2.3 | Tipo | Standalone |
| 2.4 | Modelo | Especificar |
| 2.5 | Tamaño | 1 Unidad de Rack Máximo |
| 2.6 | Puertos | Cada switch debe incluir mínimo:<br>• 48 puertos 10/100/1000BASE-T (RJ-45)<br>• 4 puertos a 1GBASE-X SFP. |

| | | |
|---|---|---|
| 2.7 | Puertos de Administración | • 1 puerto serial de consola RJ-45 con RTS/CTS |
| 2.8 | Rendimiento | Soportar como mínimo:<br>• Rendimiento: 77,4 Mpps,<br>• Capacidad de conmutación: 104 Gbps.<br>• El equipo debe ser full dúplex en todas sus interfaces. |
| 2.9 | Fuentes de Poder | Debe incluirse fuente de poder interna y puerto adicional para conexión de fuente redundante.<br><br>**Nota:** Energy Efficient Ethernet (EEE) soportado en todos los puestos de cobre Base-T. |
| 2.10 | Voltajes / Frecuencia soportados | • Rango de voltaje de entrada: 100-240 VAC<br>• Rango de frecuencia de línea: 50 - 60 Hz +/- 5%<br>• Power Supply Input Socket: IEC 320 C14<br>• Power Cord Input Plug: IEC 320 C13<br>• Rango de temperatura de operación: 0º C to 50º C (En normal operación) |
| 2.11 | Sistema Operativo | Todos los switches deben ejecutar la misma versión del sistema operativo, lo que ayuda a desplegar, operar y mantener la red y reducir los costos operativos.<br>• Sistema operativo modular<br>• Capa 2<br>• Seguridad Integrada a través de autenticación por MAC, 802.1x<br>• 802.3x Flow Control<br>• IPV6: Capa 2 IPv6 forwarding, protocolos de enrutamiento y túneles. |
| 2.12 | Tamaño de la tabla de direcciones MAC | Soportar al menos 16K Direcciones |
| 2.13 | Vlan | Soportar al menos 4094 VLANs Estáticas<br>Soportar al menos 255 VLANs Dinámicas |
| 2.14 | Protocolos Soportados | • IEEE 802.3AT<br>• Soporte de múltiples instancias del Protocolo STP (Spanning Tree Protocol).<br>• Soporte de IEEE 802.1w RSTP<br>• Soporte de IEEE 802.3ad, Configuración de compartición de carga estática y configuración dinámica basada en LACP<br>• Soporte de IEEE 802.1AB – LLDP Link Layer Discovery Protocol<br>• Soporte de IEEE 802.1ag Connectivity Fault Management<br>• Soporte de RFC 3619 Ethernet Automatic Protection Switching (EAPS) Version 1<br>• RFC 3176 – sFlow<br>• RFC 2131 BOOTP/DHCP relay agent and DHCP server<br>• RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs<br>• RFC 3413 – 3415 SNMPv3, basada en la seguridad del usuario, cifrado y autenticación<br>• RFC 2668 802.3 Medium Attachment Units (MAU) MIB |
| 2.15 | Protocolos de Enrutamiento IPv4 | Debe incluir enrutamiento estático<br>• RFC 2933 – IGMP MIB |
| 2.16 | Protocolos de Seguridad | • Secure Shell (SSH-2, TFTP client/server with encryption/authentication<br>• SNMPv3 user based security, with encryption/ authentication<br>• RFC 1492 TACACS+<br>• RFC 2138 RADIUS Authentication<br>• RFC 2139 RADIUS Accounting<br>• RFC 3579 RADIUS EAP support for 802.1x |

| | | |
|---|---|---|
| | | • RADIUS Per-command Authentication<br>• Access Profiles on All Routing Protocols<br>• Access Policies for Telnet/SSH-2<br>• Network Login – 802.1x, Web and MAC-based mechanisms<br>• IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login<br>• Multiple supplicants with multiple VLANs for Network Login<br>• Fallback to local authentication database (MAC and Web-based methods)<br>• Guest VLAN for 802.1x<br>• RFC 1866 HTML<br>• MAC Security – Lockdown and Limit<br>• IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID<br>• IP Security – Trusted DHCP Server<br>• Layer 2/3/4 Access Control Lists (ACLs)<br>• RFC 2267 Network Ingress Filtering<br>• RPF (Unicast Reverse Path Forwarding) Control via ACLs –<br>• Wire-speed ACLs<br>• Rate Limiting/Shaping by ACLs<br>• IP Broadcast Forwarding Control<br>• ICMP and IP-Option Response Control<br>• SYN attack protection<br>• CPU DoS Protection with traffic rate-limiting to management CPU<br>• IP Security – DHCP enforcement via Disable ARP Learning<br>• IP Security – Gratuitous ARP Protection<br>• IP Security – DHCP Secured ARP/ARP Validation |
| 2.17 | Otras funcionalidades | • Políticas de ancho de banda de ingresos y egreso limitadas por flujos/ACLs<br>• 8 colas de ingreso y egreso por puerto (QoS)<br>• Ancho de banda de egreso limitado por cola de egreso y por puerto |
| 2.18 | Certificaciones Internacionales (EMC) | • CISPR 22: 2006 Ed 2.2 , Class A (International Emissions)<br>• CISPR 24: A2:2003 Class A (International Immunity)<br>• IEC 61000-4-2:2008/EN 61000-4-2:2009 Electrostatic Discharge, 8kV Contact, 15 kV Air, Criteria A<br>• IEC 61000-4-3:2008/EN 61000-4-3:2006+A1:2008 Radiated Immunity 10V/m, Criteria A<br>• IEC 61000-4-4:2004 am1 ed.2. /EN 61000-4-4:2004/A1:2010 Transient Burst, 1 kV, Criteria A<br>• IEC 61000-4-5:2005 /EN 61000-4-5:2006 Surge, 2 kV L-L, 2 kV L-G, Level 3, Criteria A<br>• IEC 61000-4-6:2008/EN 61000-4-6:2009 Conducted Immunity, 0.15-80 MHz, 10V/m unmod. RMS, Criteria A<br>• IEC/EN 61000-4-11:2004 Power Dips & Interruptions, >30%, 25 periods, Criteria C |
| 2.19 | Estándares Ambientales | • EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage<br>• EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation<br>• EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational<br>• EN/ETSI 300 753 (1997-10) - Acoustic Noise<br>• ASTM D3580 Random Vibration Unpackaged 1.5 G |

| **ÍTEM 3: Red de Datos** |
|---|

| **SUBÍTEM 3.1: Software de Administración, Gestión y Monitoreo** | | |
|---|---|---|
| **Denominación del Bien:** | | Sistema de Gestión de Red |
| **Denominación Técnica:** | | Solución de Administración de Red |
| **Unidad de Medida:** | | Unidad |
| **ÍTEM** | **CARACTERÍSTICA** | **MINIMO REQUERIDO** |
| 3.1 | Cantidad | 1 |
| 3.2 | Marca | Especificar |
| 3.3 | Modelo | Especificar |
| 3.4 | Plataforma | La solución se requiere virtualizada. La entidad proveerá las máquinas virtuales requeridas para la implementación bajo ambientes VMware o Microsoft Hyper-V. |
| 3.5 | Dimensionamiento | La solución de cumplir con las siguientes características:<br>• Numero de Dispositivos 50<br>• Numero de APS: 500 |
| 3.6 | Versión | La plataforma debe estar licenciada en su máxima versión para soportar la gestión unificada de los módulos de acceso seguro a la red (NAC) y analítica. |
| 3.7 | Integración | Esta plataforma debe ser la única consola de administración que se use para la gestión de la red cableada, la solución de acceso seguro a la Red, la solución de analítica y las interfaces (API) a otras herramientas (SDN).<br><br>**Nota:** No se aceptarán propuestas que usen más de una consola de gestión para administrar las plataformas antes referidas. |
| 3.8 | Características Especificas | • Debe soportar el uso del SNMP v1/v2/v3 para monitoreo y configuración de los equipos.<br>• Debe Soportar análisis de OpenFlow, NetFlow o sFlow<br>• Gestión de dispositivos sobre el protocolo IPv6<br>• Autodescubrimiento de equipos en la red por rangos de direcciones IP.<br>• Control y gestión de los usuarios administradores, definiendo diferentes niveles de acceso y privilegios.<br>• Mostrar en forma gráfica y estadística parámetros generales de los elementos de red mediante tablas, graficas de pastel o de barras que permitan su exportación en formatos JPG, BMP y PNG.<br>• La autenticación de usuarios administradores podrá realizarse a través de: credenciales del sistema operativo, LDAP y RADIUS.<br>• Gestionar elementos de red de diferentes fabricantes en base a MIBs.<br>• Unificar y centralizar el monitoreo y gestión de infraestructura de red alámbrica e inalámbrica.<br>• Proporcionar mapas topológicos de la red mostrando información en capas 2 y 3, tales como VLANs, OSPF, 802.1ad, Spanning Tree, 802.1s.<br>• Desde la misma herramienta acceder a los dispositivos de red vía Web, Telnet o SSH dependiendo de las capacidades de gestión que soporte el elemento administrado.<br>• Contar con una interface gráfica de gestión de monitoreo básico compatible con dispositivos móviles como Smartphones y Tablets. |

| | | |
|---|---|---|
| | | • Proporcionar una vista gráfica de los equipos que muestre tarjetas, puertos, así como el estado operativo de los mismos (puertos administrados/no administrados, link de los puertos, estadísticas)<br>• Tener la capacidad de realizar búsquedas de elementos en la red, basadas en los siguientes criterios:<br>  o Dirección IP/Subred<br>  o Dirección MAC<br>  o Nombre de usuario<br>• Administrar listas de control de acceso de los dispositivos que por sus características así lo permitan.<br>• Administrar los dispositivos para que estos puedan ser configurados para el envío de traps y logs.<br>• Realizar respaldos de la configuración sobre múltiples elementos de red en forma automática y programada de forma:<br>  o Manual o por único evento<br>  o Diaria<br>  o Semanal<br>• Realizar la descarga de los archivos de configuración de los elementos de red de forma directa en la máquina desde la cual se esté haciendo la sesión a la herramienta.<br>• Actualizar la versión de sistema operativo o firmware de los elementos de red, calendarizar actualizaciones de los mismos en forma programada ya sea individual o en grupos.<br>• Mostrar un historial de las actualizaciones de firmware y/o configuración que se han realizado.<br>• Realizar un inventario de los equipos proporcionando la siguiente información: número de serie, versión de sistema operativo (firmware), memoria, tipo de CPU.<br>• Comparar archivos de configuración de los equipos de red, indicando las diferencias entre los mismos en caso de que se hayan registrado cambios.<br>• Navegador de MIBs que permita inspeccionar variables en los dispositivos de red además de tener la capacidad de compilar MIBs nuevas o de otros fabricantes.<br>• Crear alarmas basadas en diferentes eventos tales como:<br>  o Caída de un equipo<br>  o Severidad de evento (informational, warning, critical, emergency, etc)<br>  o Notificación trap<br>  o Sobrepasar umbrales de parámetros de los elementos de red<br>• Al generar una alarma el sistema debe tener la capacidad de realizar las siguientes acciones:<br>  o Envío de e-mail<br>  o Envío de Syslog<br>  o Envío de trap SNMP<br>  o Ejecutar scripts de configuración o programas<br>• Tener la capacidad para definir y aplicar políticas de QoS, prioridades, anchos de banda y seguridad en la red.<br>• Configurar los siguientes métodos de autenticación por puerto de switch:<br>  o 802.1x<br>  o MAC<br>  o Web |

| | | |
|---|---|---|
| | | • Capacidad para especificar la(s) MAC address(es) que tiene(n) acceso por cada puerto de switch. Se especificará el método en como el equipo aprenderá las MAC address por puerto:<br>  o De forma dinámica (primera en conectarse)<br>  o De forma estática<br>  o Por autenticación<br>• Definir clases de servicio con los siguientes componentes:<br>  o 802.1p<br>  o ToS<br>  o Drop precedence<br>  o Rate-limits<br>  o Transmit Queue<br>• Crear rate limits para establecer el máximo índice de trasmisión por puerto o tráfico especifico por:<br>  o Porcentaje del total de ancho de banda disponible por puerto<br>  o Paquetes por segundo (pps)<br>  o Kilobits por segundo<br>  o Megabits por segundo<br>  o Gibabits por segundo<br>• Especificar el re-marcado de ToS/DSCP en los paquetes que hagan match con reglas de clasificación, para su tratamiento por Clases de Servicio.<br>• Tener la capacidad de configurar y administrar múltiples controladoras inalámbricas y access points del mismo fabricante.<br>• Tener la capacidad de configurar y administrar múltiples Switches del mismo fabricante, sin necesidad de abrir consolas por cada dispositivo<br>• La comunicación entre la consola y las controladoras Inalámbricas deberá realizarse mediante túneles SSL/TLS y shared secrets (claves)<br>• Crear y administrar plantillas de configuración para controladoras inalámbricas, así como plantillas de configuración para puntos de acceso<br>• Crear grupos de access points, incluso cuando no pertenezcan al mismo controlador, para aplicar la misma configuración a los access points que forman parte del grupo.<br>• Contará con un módulo de visualización de mapas, para ubicación de equipo y APs. Mostrará alarmas, información del dispositivo y permitirá realizar búsquedas de: dispositivos, APs, clientes alámbricos e inalámbricos.<br>• Podrá descubrir nuevos dispositivos de red, aplicar plantillas de configuración y actualizar los dispositivos a la última versión disponible de sistema operativo (firmware)<br>• Podrá realizar las siguientes funciones de monitoreo:<br>  o Mostrar vistas topológicas de un dispositivo de red<br>  o Analizar detalles de flujos, aplicaciones, fuentes y destinos por puerto<br>  o Analizar en tiempo real estatus, utilización, errores y paquetes por puerto<br>  o Analizar un histórico de utilización y disponibilidad por puerto<br>  o Mostrar todos los endpoints conectados a un puerto<br>• Realizara capturas de tráfico en tiempo real en puntos de acceso, para facilitar diagnósticos y solución de problemas.<br>• Generará reportes que proporcionen la siguiente información sobre los dispositivos:<br>  o Alarmas<br>  o Disponibilidad |

| | | |
|---|---|---|
| | | ○ Inventario<br>○ Rastrear cambios realizados en los dispositivos<br>○ CPU<br>○ Memoria<br>• Generará reportes que proporcionen la siguiente información sobre las interfaces:<br>○ Flujos<br>○ Ancho de banda<br>○ Uso de PoE<br>○ Utilización<br>• Generará reportes que proporcionen la siguiente información sobre la red inalámbrica:<br>○ APs<br>○ Clientes<br>○ Controladoras<br>○ Top de APs y clientes por utilización de ancho de banda<br>• Deberá contar con un visor de flujos el cual mostrará la siguiente información:<br>○ Dirección IP cliente, quien origina el flujo<br>○ Dirección IP servidor, que recibe o maneja el flujo<br>○ Puerto TCP/UDP del servidor<br>○ Protocolo<br>○ Conteo de flujos<br>○ Duración<br>○ Cantidad de bytes transmitidos<br>○ Cantidad de bytes recibidos<br>○ DSCP ( Diffserv Codepoint)<br>○ TTL (Time to Live)<br>• Deberá realizar búsquedas de actualizaciones de sistema operativo (firmware) para los dispositivos de Red en el website del fabricante.<br>• Deberá obtener información de equipos de seguridad como IDS o IPS, para localización del atacante en la red (switch/puerto) y aplicar acciones para contener la amenaza de forma automática.<br>• La funcionalidad de respuesta automática contra ataques o amenazas en la red, tendrá las siguientes opciones de configuración:<br>○ Rangos de días y hora<br>○ Notificaciones por mail, trap, syslog y script<br>○ Subredes y VLANs<br>○ Dispositivos de red y grupos de dispositivos<br>○ Exclusión de puertos de dispositivos de red<br>• La funcionalidad de respuesta automática contra ataques o amenazas, realizara las siguientes acciones de contención:<br>○ Apagar puerto<br>○ Aplicar política de cuarentena<br>○ Cambiar VLAN<br>○ Notificar solución<br>• Deberá poseer un módulo que permita interactuar y administrar la solución de Identidad en el acceso, así como la solución de NAC si se está ofertando.<br>• Mostrar datos provenientes de la solución de control de acceso a la red (NAC) y gestión de funciones de dicha solución, tales como:<br>○ Dirección IP del dispositivo |

| | | |
|---|---|---|
| | | ○ Dirección MAC<br>○ Sistema operativo del dispositivo<br>○ Username<br>○ Dirección IP del elemento de red al cual está conectado<br>○ Perfil o política<br>○ Nivel de riesgo o salud del dispositivo<br>○ Tipo de autenticación<br>○ Registro u hora en la que se detectó por el NAC dicho dispositivo.<br>• El sistema de monitoreo centralizado para la red alámbrica e inalámbrica debe incluir una herramienta de monitoreo mediante un acceso basado en web, en donde se puedan generar reportes de la solución monitoreada, así como que sea de utilidad para resolver problemas reportados con respecto a la red en las mesas de servicio (helpdesk).<br>• La interface web de monitoreo que muestre:<br>○ Dashboards de red alámbrica/inalámbrica<br>○ Reportes<br>○ Mapas de topología<br>○ Identificación de aplicaciones<br>○ Visor de dispositivos y syslog<br>○ Visor de flujos<br>○ Búsquedas por MAC address, dirección IP, username, hostname<br>• Los reportes que se pueden obtener de la herramienta tienen que ser históricos o en tiempo real<br>• Debe tener la capacidad de búsqueda para encontrar un dispositivo, APs y ubicarlos en un mapa, así como a algún usuario alámbrico o inalámbrico.<br>• Debe incluir la funcionalidad de mostrar un dashboard donde muestre los detalles de la red inalámbrica.<br>• Que tenga opción de integración ambientes de virtualización data center de VMware, Citrix y Microsoft, para aprovisionamiento automático y seguro de servicios.<br>• Que tenga opción de integración con consolas MDM (Mobile Device Management) como Airwatch, MobileIron, etc. Para control de acceso a los recursos de la red desde dispositivos móviles<br>• Capacidad de integración con soluciones de seguridad de terceros como: Next generation firewalls, filtrados de contenido y appliance de seguridad. |

| **ÍTEM 4: Red de Datos** | | |
|---|---|---|
| **SUBÍTEM 4.1: Acceso Seguro a la Red** | | |
| **Denominación del Bien:** | | NAC |
| **Denominación Técnica:** | | Solución de Acceso Seguro a la Red |
| **Unidad de Medida:** | | Unidad |
| **ÍTEM** | **CARACTERÍSTICA** | **MINIMO REQUERIDO** |
| 4.1 | Cantidad | 1 |
| 4.2 | Marca | Especificar |

| | | |
|---|---|---|
| 4.3 | Modelo | Especificar |
| 4.4 | Plataforma | La solución se requiere virtualizada. La entidad proveerá las máquinas virtuales requeridas para la implementación bajo ambientes VMware o Microsoft Hyper-V. |
| 4.5 | Dimensionamiento | La solución de cumplir con las siguientes características:<br>• Numero de Eventos por Segundo: 3K |
| 4.6 | Versión | La plataforma debe estar licenciada en versión Enterprise. |
| 4.7 | Integración | Esta plataforma debe estar integrada nativamente a la consola de administración del NMS del punto anterior, para realizar su gestión y administración. |
| 4.8 | Características Especificas | • Debe operar con acceso de usuarios a la red cableada, inalámbrica y VPN.<br>• Soportar al menos 3000 endpoints concurrentes en un solo appliance, los cuales podrán contar con un agente NAC en operación.<br>• Soportar un esquema de alta disponibilidad.<br>• Gestión centralizada de la solución de control de acceso para simplificar la implementación y administración de la misma.<br>• La solución debe combinar autenticación, escaneo de vulnerabilidades y localización, para autorizar el acceso a la red con un perfil adecuado para cada dispositivo.<br>• La solución debe contar con funcionalidades de BYOD (Bring Your Own Device), que incluya registro de dispositivos sesiones basadas en login de usuarios.<br>• La funcionalidad de BYOD debe cumplir con lo siguiente:<br>o Auto-descubrimiento<br>o Perfilamiento multinivel de dispositivos<br>o Flexibilidad<br>o Gestión de políticas<br>o Acceso de invitados<br>o Integración con MDM (Mobile Device Management)<br>o Integración con VDI (Virtual Desktop Infraestructure)<br>• Debe realizar un registro automático de invitados, que permita un acceso seguro de invitados en la red.<br>• Debe contar con un esquema para limitar la visualización de endpoints, para que en ambiente multi-tenant o enterprise pueda limitarse la información y estadísticas de grupos de endpoints entre usuarios administradores.<br>• La solución tendrá la capacidad de integrarse a una arquitectura de seguridad preventiva y reactiva, por lo tanto, deberá ser capaz de interactuar con:<br>o Consola MDM (Mobile Device Management)<br>o Correlacionador de eventos SIEM (Security Information and Event Manager)<br>o Sistema de detección de intrusos (IPS)<br>o Firewall de siguiente generación (NGFW)<br>• La solución debe ser capaz de integrarse con terceros, tales como:<br>o Firewall de última generación<br>o IF-MAP<br>o OS LIA<br>o Polycom<br>o Avaya<br>o MS SCCM – MS System Center Configuration Manager<br>• Tener la capacidad de ser un RADIUS Proxy<br>• Soportar RFC 3580<br>• Soportar las siguientes autenticaciones: |

| | | |
|---|---|---|
| | | ○ 802.1X (Extensible Authentication Protocol)<br>○ MAC<br>○ Web-based<br>○ Kerberos<br>• Soportar IPv6<br>• Debe ser interoperable con Microsoft NAP y Trusted Computing Group TNC.<br>• Debe contar con un esquema de balanceo de carga para una solución compuesta por más de un appliance de NAC.<br>• La solución debe ser capaz de manejar los siguientes protocolos de autenticación RADIUS:<br>○ PAP<br>○ CHAP<br>○ MS-CHAP<br>○ PEAP<br>○ EAP-MSCHAPv2<br>○ EAP-TLS<br>○ EAP-TTLS<br>○ EAP-MD5<br>• La solución debe ser capaz de usar un registro RADIUS accounting, para determinar en tiempo real estado de la conexión.<br>• La solución debe ser capaz de ofrecer un control granular de acceso con los siguientes criterios:<br>○ Tipo de autenticación<br>○ Grupos de endpoints por MAC address, dirección IP o Hostname<br>○ Tipo de dispositivo por sistema operativo<br>○ Ubicación en la red del endpoint<br>○ Hora y día<br>○ Grupo de usuario, en LDAP, RADIUS, etc.<br>• La solución deber contar con las funcionalidades de: permitir, negar, priorizar, etiquetar, redirigir, aplicar rate-limit y auditar tráfico de red, con base en identidad del usuario, tipo de dispositivo, hora y ubicación de acceso.<br>• La solución debe contar con funcionalidades de servidor de escaneo propias y tendrá la posibilidad de integrarse con servidores externos de assessment.<br>• La solución debe permitir realizar un escaneo de los endpoints en al menos tres modos:<br>○ Informacional: en la cual se valoren los endpoints, se reporten resultados, permita el acceso de enpoints aun cuando no cumplan las políticas y permita colectar información del nivel de cumplimiento.<br>○ Precautorio: la cual reporte los resultados del escaneo, notifique al usuario las políticas no cumplidas y les permita el acceso aun cuando no cumplan las políticas.<br>○ Obligatorio: la cual reporte los resultados del escaneo, aplique cuarentena a los dispositivos que no cumplen con las políticas y le notifique al respecto; solo los dispositivos que cumplan las políticas obtendrán acceso a la red.<br>• · La solución debe ser capaz de realizar los modos de escaneo informacional, precautorio y obligatorio de enpoints:<br>○ Sin agente<br>○ Mediante un agente |

| | | |
|---|---|---|
| | | • El agente de escaneo o revisión de endpoints, será compatible con los siguientes sistemas operativos:<br>  ○ Windows 2000<br>  ○ Windows 2003<br>  ○ Windows 2008<br>  ○ Windows XP<br>  ○ Windows Vista<br>  ○ Windows 7<br>  ○ Windows 8<br>  ○ Mac OS X (Tiger, Leopard)<br>  ○ Mac OS X 10.8 (Mountain Lion)<br>• El agente deberá ofrecer las siguientes opciones de instalación en endpoints Windows:<br>  ○ Permanente<br>  ○ Temporal<br>  ○ Permanente como Servicio<br>• El agente tendrá la posibilidad de comunicarse con un server Nessus versión 3 o superior, para la revisión de los endpoints.<br>• La solución debe contar con remediación asistida, la cual informe al usuario cuando se encuentre en cuarentena debido al incumplimiento de políticas y le permita al usuario remediar su endpoint sin necesidad de la intervención del personal de TI.<br>• Debe incluir una función de registro de endpoints a través de una página web, la cual debe contemplar lo siguiente:<br>  ○ Determinar la validez de los usuarios en una base de datos.<br>  ○ Ofrecer un patrocinador, usuario confiable de la organización, quien podrá autorizar y asignar el nivel de acceso de los endpoints<br>  ○ Especificar el número máximo de MAC address registradas por usuario<br>  ○ A través de un portal seguro (HTTPS) se podrán: visualizar, agregar, eliminar y modificar los registros. El portal estará disponible para patrocinadores y administradores de la solución.<br>• La solución debe contar con un portal para registro de invitados, en el cual el usuario introduzca la dirección de correo electrónico del patrocinador, quien será notificado por correo electrónico y asignara el acceso. El registro de invitados contara con las opciones de acceso:<br>  ○ Sin patrocino<br>  ○ Patrocinio opcional<br>  ○ Patrocinio obligatorio<br>• La solución debe contar con la funcionalidad de verificar los datos de contacto del usuario que se registra a través del portal de invitados, dicha validación se realizará mediante un código que se enviará al usuario a través de e-mail y/o SMS.<br>• La solución debe tener la capacidad de cerrar el acceso de una MAC address dada a un solo puerto de un switch, para que el dispositivo solo tenga acceso a la red mediante el switch y puerto especificado.<br>• La solución debe ser capaz de mostrar la siguiente información de los enpoints conectados a la Red:<br>  ○ MAC Address<br>  ○ IP Address<br>  ○ Dirección IP y puerto del switch acceso |

| | | |
|---|---|---|
| | | ○ Estatus en la revisión del endpoint<br>○ Username<br>○ Hostname<br>○ Tipo de dispositivo<br>○ Tipo de autenticación<br>○ Autorización<br>○ Perfil<br>○ Fecha de primera vez que se detecto<br>○ Fecha de ultima vez que se detecto<br>○ Fecha ultima en que se escaneo<br>• El Agente debe ser capaz de validar en los endpoints lo siguiente:<br>○ Sistema operativo<br>○ Versión mínima de agente<br>○ Antivirus<br>○ Firewall<br>○ Actualizaciones automáticas<br>○ Software P2P<br>○ Parches<br>○ Archivos<br>○ Procesos<br>○ Llave de registro<br>○ Servicios<br>• La solución debe ofrecer una opción de escaneo de endpoints sin agente, en la cual existan al menos cuatro distintos niveles de revisión de endpoints.<br>• La solución deberá permitirle al administrador crear grupos de endpoints en base a:<br>○ MAC address<br>○ Dirección IP o subredes<br>○ Hostname<br>○ Grupos en LDAP<br>• La solución permitirá al administrador crear grupos de ubicación, los cuales restrinjan el acceso de los endpoints por:<br>○ Dirección IP de switch y puerto<br>○ Dirección IP de controladora, access point y SSID<br>• La solución debe ser capaz de restringir endpoints en base al día y hora en que el usuario solicita el acceso a la red.<br>• La solución deberá permitirle al administrador crear grupos de usuarios en base a:<br>○ Username<br>○ Grupo LDAP<br>○ Grupo RADIUS<br>• Para sistemas operativos MAC, el agente será capaz de validar los siguientes antivirus:<br>○ McAfee 8.6<br>○ McAfee 9.0<br>○ Sophos 4.9<br>○ Sophos 7.x<br>○ Norton 11<br>○ Symantec AV 10<br>○ Symantec Endpoint 11 |

| | | |
|---|---|---|
| | | ○ ClamX AV 2.2.2<br>• La solución debe ser capaz de detectar de forma automática los endpoints por familia de sistema operativo:<br>○ Android<br>○ Apple iOS<br>○ Blackberry<br>○ Linux<br>○ MAC<br>○ Windows<br>• La solución debe ser capaz de retener información y estadísticas de los endpoints y su actividad al menos por 90 días, el administrador podrá modificar el periodo de retención de dicha información.<br>• La solución debe permitir agregar, editar y probar reglas de notificación, las cuales se activen por eventos de NAC, permitiendo acciones como:<br>○ Envío de e-mail<br>○ Syslog<br>○ SNMP trap<br>○ Ejecutar script<br>• Las reglas de notificación de NAC podrán ser activadas por los eventos siguientes:<br>○ Cuando un enpoint sea agregado o removido<br>○ Cuando el estatus de un endpoint cambie<br>○ Cuando el tipo de autenticación o un tipo de dispositivo cambie<br>○ Cuando se produzca un cambio en un grupo de usuarios<br>○ Cuando se produzca un cambio en un grupo de endpoints<br>○ Cuando en el registro un usuario o dispositivo sea agregado, actualizado o removido<br>• Debe contar con una herramienta capaz de proporcionar:<br>○ Reportes<br>○ Dashboard<br>○ Identificación de los endpoints conectados a la red<br>○ Información sobre los endpoints y eventos asociados<br>○ Salud o nivel de cumplimiento de cada endpoint<br>• La solución debe ser capaz de mostrar un listado de los endpoints conectados, aplicar filtros por fecha y de búsqueda en la información siguiente:<br>○ Estatus, por ejemplo: en revisión, desconectado, cuarentena, etc.<br>○ Dirección IP<br>○ MAC Address<br>○ Hostname<br>○ Tipo de dispositivo por sistema operativo<br>○ Username<br>○ Política aplicada al endpoint<br>○ Dirección IP y puerto del equipo de red por donde accede el endpoint<br>○ Tipo de Autenticación<br>○ Appliance NAC al cual está asociado<br>○ VLAN por RFC 3580<br>○ Ultima vez que se observó conectado en la red<br>○ Primera vez que se observó conectado en la red<br>○ Resultado de la última revisión al endpoint |

| | | |
|---|---|---|
| | | ○ Compatibilidad con NAP<br>• Debe contar con una herramienta de análisis que muestre detalles del endpoint registrado por NAC y sus flujos (Netflow), tanto para red alámbrica como inalámbrica. Debe permitir al administrador:<br>○ Visualizar la topología de los dispositivos de red y endpoint en cuestión.<br>○ Analizar detalles de flujos, aplicaciones, emisor y receptor por puerto<br>○ Analizar en tiempo real el estatus, utilización, errores y paquetes por puerto<br>○ Análisis histórico de la utilización y disponibilidad de un puerto |
| 4.9 | Integración | La solución debe estar homologada para integrarse con la plataforma de seguridad (firewall) de Fortinet. Esto permitirá trasladar las políticas de seguridad que la entidad actualmente tiene en el perímetro con equipos Fortinet al interno de la red de datos, generando políticas de seguridad end to end.<br><br>**Nota:** Se debe adjuntar a la oferta el documento donde se certifique la integración de la plataforma ofertada con el fabricante de equipos de seguridad Fortinet, |

| **ÍTEM 5: Red de Datos** | | |
|---|---|---|
| **SUBÍTEM 5.1: Solución de Analítica** | | |
| **Denominación del Bien:** | | Analítica |
| **Denominación Técnica:** | | Solución de Analítica para la Red de Datos |
| **Unidad de Medida:** | | Unidad |
| **ÍTEM** | **CARACTERÍSTICA** | **MINIMO REQUERIDO** |
| 5.1 | Cantidad | 1 |
| 5.2 | Marca | Especificar |
| 5.3 | Modelo | Especificar |
| 5.4 | Plataforma | La solución se requiere virtualizada. La entidad proveerá las máquinas virtuales requeridas para la implementación bajo ambientes VMware o Microsoft Hyper-V. |
| 5.5 | Dimensionamiento | La solución de cumplir con las siguientes características:<br>• Numero de Flujos por Minuto: 50K |
| 5.6 | Versión | La plataforma debe estar licenciada en versión Enterprise. |
| 5.7 | Integración | Esta plataforma debe estar integrada nativamente a la consola de administración del NMS del punto anterior, para realizar su gestión y administración. |
| 5.8 | Características Especificas | • Debe manejar millones de flujos y operar a nivel de terabit/s<br>• No ser intrusivo en toda la red<br>• Proveer información contextual, más allá del usuario de la aplicación, rol, ubicación, hora, dispositivo.<br>• Debe detectar y decodificar aplicaciones independientes de la capa de transporte<br>• Debe medir el tiempo de respuesta de aplicaciones y redes y recopilación de contextos de aplicación<br>• Debe utilizar tecnología DPI (Deep Packet Inspection) con un amplio conjunto de fingerprints de aplicaciones para detectar aplicaciones internamente alojadas (SAP, SOA, Exchange, SQL, etc.), aplicaciones de nube pública (Salesforce, Google, Email, |

| | | |
|---|---|---|
| | | YouTube, P2P, etc.) y las aplicaciones de redes sociales (Facebook, Twitter, etc.) en la capa 7 del modelo OSI.<br>• Contar con una arquitectura capaz analizar información de: acceso, wireless, distribución, core, data center y perímetro<br>• Debe contar con la capacidad de identificar aplicaciones internas (SQL,Exchange,etc.) , aplicaciones en la nube (Google, Youtube, etc.)y aplicaciones de redes sociales (Facebook, Twitter, etc. ) a nivel de capa 7 del modelo OSI<br>• Debe determinar la siguiente información: la aplicación, URL, información del certificado, versión del browser, medir tiempo de respuesta y capaz de obtener información contextual del acceso como: usuario, rol o perfil, tipo de dispositivo y ubicación<br>• La solución debe presentar la información analizada con múltiples dashboards con funcionalidad drill-down para mostrar información más detallada.<br>• El dashboard debe contar con al menos cuatro distintos tipos de grafica para mostrar la información (p.e. grafica de pay, etc.)<br>• Debe mostrar los servidores y clientes activos durante las últimas 24 horas, así como el top de clientes y servidores por ancho de banda.<br>• Mostrará el top de aplicaciones en diversos tipos de gráfica, así también permitirá revisar por aplicación los clientes y datos relacionados.<br>• Mostrará los flujos de comunicación de las aplicaciones, con las siguientes opciones:<br>o Flujos con los tiempos de respuesta TCP más altos (peores)<br>o Aplicaciones con tiempos de respuesta más altos (peores)<br>o Top de aplicaciones, clientes o servers con base al ancho de banda empleado, paquetes o cantidad de conexiones<br>• Contará con un visor de flujos que permita obtener la siguiente información:<br>o Dirección IP del cliente<br>o Dirección IP del servidor<br>o Puerto del servidor<br>o Aplicación<br>o Tiempo de respuesta de la red<br>o Tiempo de respuesta de la aplicación<br>o Ubicación<br>o Username del cliente<br>o Protocolo empleado para la conexión<br>o Ubicación del cliente (Switch/puerto, Access Point/SSID)<br>o Ancho de banda promedio del flujo<br>o Paquetes transmitidos/recibidos<br>o Bytes transmitidos/recibidos<br>• Deberá permitir exportar los datos mostrados en formato CSV<br>• Debe contar con la funcionalidad de interconectarse a otros sistemas para análisis de tráfico (Big Data processing) a través de interface XML/SOAP<br>• La solución debe incluir la capacidad de identificar al menos13,000 huellas de aplicaciones y además esta base debe contar con actualizaciones de forma continua<br>• La solución debe contar con una base de identificación de aplicaciones (fingerprints) abierta y personalizable, para que el administrador pueda crear y personalizar la identificación de aplicaciones |

| | | |
|---|---|---|
| | | • Para simplificar la resolución de problemas de aplicaciones, la solución debe mostrar el tiempo de respuesta de la red y de las aplicaciones, para que el administrador distinga entre problemas de desempeño de la red o de la aplicación.<br>• Debe mostrar el número de veces que han sido detectados flujos que concuerden con el fingerprint de una aplicación con (hits)<br>• Debe permitir al administrador agrupar segmentos de red para asociarlos con un edificio, oficina o áreas geográficas, para así identificar el análisis de tráfico relacionado con alguna ubicación especifica<br>• La solución debe soportar la implementación como appliance físico o virtual compatible con VMware ESX/ESXi 4.0 o superior<br>• La solución debe ser capaz de procesar un mínimo de 100 mil flujos por minuto<br>• La solución debe utilizar tecnología Coreflow2 o su equivalente |
| 5.9 | Gestión de Informes | La herramienta debe permitir presentar la información en múltiples cuadros de mando, proporcionan capacidad de exploración e informes detallados. Los paneles de control deben presentar resúmenes de alto nivel, así como información específica por vertical de negocio. Además de los cuadros de mando, debe incluir una serie de informes como TopN para aplicaciones, grupos, clientes, etc. Estos deben poder programarse para que se ejecuten de forma regular y estar disponibles en formato pdf |
| 5.10 | Sensor | El sensor o equipo de recolección de datos debe ser basado en hardware y ser totalmente no intrusivo en la red. Para esto debe capturar la información vía un puerto SPAM desde el Core de la Red, y procesar toda esta data en un equipo propietario que no requiera recursos compartidos de la red para el procesamiento de la información.<br><br>Especificaciones Técnicas:<br><br>• Dos fuentes de poder de 480 Watt (15A, 100-240VAC input)<br>• 4 Puertos SFP+. (Incluir al menos 2 1000BASE-T, RJ45 MINI GBIC)<br>• Temperatura de operación: 5° to 40°C (41° to 104°F)<br>• Cumplimiento de estándares:<br>• UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSA C22.2, No. 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Low Voltage Directive)<br>• 2002/95/EC (RoHS Directive), 2002/96/EC (WEEE Directive)<br>• El sensor debe trabajar con tecnologia de Puerto espejo tipo MirrorN o su equivalente. |

| **PROPUESTA ECONÓMICA:** | | | | | | |
|---|---|---|---|---|---|---|
| "Adquirir la infraestructura de conectividad de acceso lógico para las redes de la ANH, (Cableado Estructurado, Certificación y demás elementos necesarios)." | | | | | | |
| **Ítem** | **Descripción** | **Cantidad** | **Valor Unitario** | **SUBTOTAL** | **IVA sobre el Total** | **Valor Total IVA incluido** |
| 1 | Equipos switch acceso | 15 | | | | |
| 2 | Equipos SWITCH de control operativo | 3 | | | | |
| 3 | Software de Administración, Gestión y Monitoreo | 1 | | | | |
| 4 | Acceso Seguro a la Red | 1 | | | | |
| 5 | Solución de Analítica | 1 | | | | |
| **VALOR TOTAL** | | | | **$** | **$** | **$** |

NOTA: Por favor abstenerse de modificar el formato de la propuesta económica arriba mencionada.

De acuerdo al principio de transparencia basado en el artículo 24 de la ley 80 de 1993, que reza…" Facilitar el control social sobre la gestión pública contractual.

- Hacer públicas todas las actuaciones que refieren a la contratación de la ANH.
- Garantizar el acceso a la información de la contratación de la ANH, utilizando para el efecto las páginas electrónicas institucionales definidas para ello…"

La ANH requiere que la cotización contenga la siguiente información para la validación de datos:

Nit de la Persona Jurídica:

Nombre de la Empresa:

Teléfono :

Dirección Sitio Web:

Email de contacto:

Al igual se debe anexar el Rut, de quien presenta la cotización.

Firma Representante Legal: _____

**Validez de la Oferta 60 días.**
**Los valores deberán presentarse en Pesos Colombianos**.

ENTREGA DE INFORMACIÓN DEL SONDEO DE MERCADO: Las firmas invitadas deben entregar la información solicitada en el presente sondeo de mercado al correo electrónico: carlos.bastidas@anh.gov.co antes del día 29 de agosto de 2017.