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 detección, protección y contención de las amenazas avanzadas, así como la implementación del NOC y SOC para complementar la plataforma actual de seguridad informática de la ANH.*"*

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 detección, protección y contención de las amenazas avanzadas, así como la implementación del NOC y SOC para complementar la plataforma actual de seguridad informática de la ANH.".

Para tales efectos, le informo que la Entidad realizará una Audiencia Pública con todos los interesados en participar, el día veintecuatro (24) de octubre del presente año a las 10:00 a.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 Deben enviar su cotización, a más tardar el día veinticinco (25) de octubre del presente año, a los correos electrónicos juan.vila@anh.gov.co y carlos.bastidas@anh.gov.coalos 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 Tecnologías 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:	Se requiere adquirir una solución integral de seguridad informática la cual permita Proactivamente la detección, monitorización y contención de amenazas avanzadas multivector asociando las plataformas tecnológicas de seguridad y TI de la Agencia Nacional de Hidrocarburos, así como la protección adicional contra riesgos informáticos que puedan afectar los sistemas de información en general, tal como se describe en el presente anexo Técnico, compuesta por múltiples plataformas de seguridad, las cuales se definen en el presente documento. De acuerdo con las necesidades de la entidad, se requieren complementar los mecanismos actuales de seguridad de la entidad con los mecanismos y soluciones a continuación descritas, de tal forma que se puedan fortalecer la entidad en el ámbito de NOC/SOC/Monitorización de la red y la seguridad informática de la entidad.
OBJETO A CONTRATAR:	Adquirir la infraestructura de detección, protección y contención de las amenazas avanzadas, así como la implementación del

	NOC y SOC para complementar la plataforma actual de seguridad informática de la ANH.
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 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): 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:

UNSPSC	CLASE
43222500	Equipo de seguridad de red
43222600	Equipo de servicio de red
43231500	Software funcional específico de la empresa
43232300	Software de consultas y gestión de datos
80101500	Servicios de consultoría de negocios y administración corporativa
80101600	Gerencia de proyectos
81111500	Ingeniería de software o hardware
81111800	Servicios de sistemas y administración de componentes de sistemas
81112000	Servicios de datos
81112200	Mantenimiento y soporte de software
81161500	Servicios de administración de acceso
81161700	Servicios de telecomunicaciones

	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 puede estar inscrito, clasificado y calificado en por lo menos uno de los Códigos anteriormente establecidos.
Plazo de Ejecución:	El plazo de ejecución del contrato es de **VEINTE (20) DIAS SIN QUE EXCEDA EL 31 DE DICIEMBRE DE 2017** para la implementación del sistema, contadas a partir de la fecha del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento del contrato. Periodo de Soporte y Mantenimiento: Un (3) años posteriores a la implementación.
Modalidad de selección:	La Entidad acudirá a la modalidad de SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES POR SUBASTA INVERSA, prevista en el literal a) del numeral 2 del artículo 2 de la Ley 1150 de 2007 y el Capítulo II de la Sección I Modalidades de Selección, y lo dispuesto en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015. **La selección se efectuará bajo la ponderación de menor precio**, debido a que se trata de servicios con características técnicas uniformes y común utilización.

REQUERIMIENTOS TCNICOS MINIMOS

COMPONENTES

1. **SOLUCION PARA MITIGACION DE AMENAZAS AVANZADAS MULTIVECTOR PARA PUNTO FINAL**

ITEM	REQUERIMIENTOS TECNICOS
1	**Generalidades** Adquisición de un sistema de protección proactiva y mitigación de amenazas avanzadas a nivel de red y de Punto Final del tipo Breach Detection System BDS. La Solución Debe contar con: - Un (1) Servidor o appliance centralizado - Seiscientos (600) Agentes para EndPoint La Solución Debe actuar: - Como Snifer de red: De tal forma que pueda recolectar, analizar y escanear todos los archivos que por los switches de core transiten. - Como centralizador de archivos: De tal forma que los agentes implementados en los endpoints envíen archivos / muestras en tiempo real a la plataforma para su análisis, recolección y escaneo en busca de malware avanzado. Debe Integrarse con los agentes de seguridad para punto final La solución Debe 100% compatible con las plataformas de seguridad actuales de la entidad, de tal forma que en caso de requerirse analizar archivos provenientes de los WAF actuales de la entidad, esta plataforma apoye este escaneo para garantizar mayor capacidad al análisis de amenazas avanzadas. Debido a la información manejada por la entidad, la solución debe ser del tipo servidor o appliance de propósito específico, por ende no se aceptan soluciones en la nube. Debe contar con API por medio del método RESTful sobre HTTPS.
2	**Análisis Proactivo de plataforma Centralizada:**

	• Debe realizar un escaneo de todos los recursos compartidos de la entidad vía (CIFS/SMB) en busca de amenazas de dia-0 que ya se encuentren residentes en dichos repositorios. • Debe realizar el análisis de tráfico por medio de un Port Span de los segmentos que la entidad defina, en busca de brechas de seguridad, botnets o amenazas que a se encuentren residentes en la entidad, dicho análisis Debe contemplar como mínimo los protocolos, HTTP, SMTP, POP3, IMAP, FTP, SMB. • Debe entregar información específica de los análisis realizados, esto debe ser sobre una interfaz gráfica con filtros predeterminados como eventos, malware, entre otros. • Debe poder analizar los tipos de Archivos: exe, dll, PDF y Javascript. En modo integrado debe poder analizar tar, gz, tar.gz, zip, bz2, tar.bz2, bz, tar. • Debe presentarse información completa del análisis de amenazas del ambiente virtual incluyendo Actividades del sistema, acción del exploit, trafico web, intentos de comunicación entre otros. • Debe clasificar los archivos de acuerdo al nivel de riesgo como alto, medio o bajo. Esta clasificación se hará de acuerdo a un score y la cantidad de puntos que tenga cada archivo en su análisis, para lo cual semanal mente se Debe presentar un informe a la entidad con el detalle de los archivos analizados, el cual para el caso de los archivos sospechosos Debe tener como mínimo: o Descarga de Virus. o Modificación de registro. o Conexiones externas a IPs maliciosas. o Infección de procesos. •	
3	**Rendimiento para el Servidor o Appliance Centralizado** • Debe soportar una capacidad de mínimo Capacidad de análisis de archivos para detección de amenazas de día cero de mínimo mil (1000) archivos por hora en ejecución en tiempo real en máquina virtual.	

4	**Caracteristicas** • Debe contar con mínimo 2 interfaces SFP+ (10 Gbps) y 2 GE. • Storage de Minimo 3 x 2 TB • Debe estar en la capacidad de detectar amenazas avanzadas en sistemas operativos Windows 7, Windows 8.1, Windows 10 y Android, mediante el uso de mínimo treinta (30) máquinas virtuales concurrentes totalmente licenciadas.
5	**Agentes para Endpoint** - La solución debe ser compatible para ser integrada de forma el appliance solicitado en el presente capitulo - Debe contar con Agentes de seguridad de “Punto Final” para servidores y estaciones de trabajo. - La solución debe capturar y grabar comportamientos anómalos en tiempo real, detectar amenazas, detenerlas y remediarlas, dicho evento debe ser centralizado para que los ingenieros de monitoreo de forma inmediata tomen acciones de corrección. - La solución debe ser implementada en modo On premise sobre la infraestructura de la Agencia Nacional de Hidrocarburos. - A nivel Administración, almacenamiento y control centralizado, la solución debe realizar búsqueda de comportamientos sospechosos, filtrado de actividad, investigación profunda, descubrimiento de actividad maliciosa, evaluación de alcance de la amenaza, remediación, actualización de las bases de conocimiento.
6	**Rendimiento / Cantidades para EndPoint** - Se requiere la solución para 600 agentes de punto final.
7	**Analisis y Remediación en EndPoint** - La solución debe permitir como mínimo: o Hacer detección y grabación de ataques en tiempo real o Validación y clasificación de alertas de seguridad. o Aislar ataques de seguridad.

		○ Hacer caza de amenazas que burlan la capa de seguridad perimetral de la entidad. ○ Hacer remediación. ○ Visualizar la cadena de ataque. ○ Registro continuo de la actividad del punto final ○ Mitigación de ataques futuros ○ Integración nativa de doble chequeo con soluciones de mitigación de amenazas avanzadas de red ○ Realizar inventario de archivos del Entorno ○ Protección Man-in-the-middle a través de la autenticación SSL bidireccional con el servidor ○ Visualización de la cadena del ataque de seguridad, por lo cual debe permitir ver la trazabilidad del ataque, lo que se afectó y lo que se debe reparar. ○ Caza de amenazas en tiempo real permitiendo la visibilidad de lo que pasa en el servidor en tiempo real (Zero-gap) para encontrar amenazas o comportamientos anómalos antes de que un ataque se lleve a cabo. ○ Debe manejar una única consola para el manejo de detección y remediación de un ataque. Una vez el mismo es detectado, se debe poder aislar y acceder de forma remota al servidor para realizar remediación.	
8	**Compatibilidad y Rendimiento en los EndPoint** • Debe soportar sistemas operativos: ○ Windows. ○ Apple. ○ Linux Read Hat. ○ Linux CentOS. • El Software de punto final o agente utilizado no debe consumir más de: ○ 1% del CPU. ○ 20 MB de RAM. ○ 50 bytes del ancho de banda de la conexión a red. ○		

9	**Garantía y Soporte** • La garantía y los servicios de soporte post venta deben ser directos del fabricante por Tres (3) años de suscripción de software en un esquema de Soporte 24x7 para los endpoint. • La garantía y los servicios de soporte post venta deben ser directos del fabricante por Tres (3) años en un esquema de Soporte 24x7 para el servidor o appliance central • La solución propuesta debe ser de tecnología actual por parte del fabricante por lo cual no se aceptarán propuestas que incluyan tecnologías que hayan sido descontinuadas por su fabricante. • Se debe incluir una transferencia de conocimiento en la solución ofertada para mínimo dos personas. La transferencia de conocimiento debe incluir la administración y operación de la herramienta.

2. SOLUCION PARA MONITOREO AVANZADO DE SERVICIOS

ITEM	REQUERIMIENTOS TECNICOS
1	**Generalidades** La solución de Monitoreo avanzado de Servicios Debe contar como mínimo con las siguientes funcionalidades para apoyar el proceso NOC / SOC de la entidad las cuales Deben prestarse desde una única plataforma: SOC - Monitoreo Avanzado de Amenazas de Punto Final - Monitoreo Avanzado de Modificación de Archivos NOC

		- Monitoreo Avanzado de Aplicaciones Web y Servicios de Usuario Final - Monitoreo Avanzado de Cambios y Configuraciones - Monitoreo Avanzado de Servicios de Datacenter y Conectividad La plataforma Debe ser del tipo Virtual Appliance, servidor físico o appliance totalmente licenciada con el fin de que la entidad pueda asignar recursos virtuales a la misma a medida que se requieran. La solución Debe contar con un sistema de bases de datos hibrida, lo que quiere decir que esté basado en **NoSQL (BigData) y SQL**, no se aceptan soluciones basadas únicamente en motores de bases de datos del tipo SQL, esto con el fin de asegurar que la solución soporte grandes volúmenes de datos sin afectar la estabilidad de la solución. Por temas de estrategia TI de la entidad, se requiere que la solución cuente con características multitenant. La plataforma Debe contar con características NOC y SOC, por lo cual Debe realizar: ▪ Actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados. ▪ Análisis constante el desempeño de las aplicaciones lo cual permita realizar un triage de la seguridad. ▪ Visor personalizado de log de tráfico. ▪ Herramienta de búsqueda sobre los logs de tráfico. La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante. Se requiere Transferencia de conocimiento Certificada por el Fabricante en la administración avanzada de esta plataforma para 2 personas de la entidad. Se Debe adjuntar certificación de fabricante indicando las plataformas ofertadas y nivel de membresía del oferente	

	2	**Desempeño** La solución debe dar soporte a las siguientes características: ▪ Numero de Dispositivos o Aplicaciones 400. ▪ HyperVisor Soportado: VMware ESX, Microsoft Hyper-V, KVM, Xen, Amazon Web Services AMI, OpenStack, Azure ▪ Numero de Eventos por Segundo (EPS): 4000 ▪ Número de Monitoreadores de Integridad de Archivos: 100	
	3	**Monitoreo Avanzado de Amenazas de Punto Final** ▪ Debe poder recolectar los logs de seguridad y eventos que se presenten en la solución de MITIGACION DE AMENAZAS AVANZADAS MULTIVECTOR PARA PUNTO FINAL de tal forma que en un dashboard centralizado se pueda visualizar todos los incidentes y alertamientos provenientes de esta solución, identificando fuentes, destinos y amenazas identificadas ▪ Debe tener la capacidad colectar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones. ▪ Debe tener la capacidad de Colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones. ▪ Debe contar con la característica de detección automática de los cambios en la configuración de red de las plataformas monitoreadas. ▪ Debe contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas. ▪ Debe contar con la característica de detección automática en cambios en archivos y carpetas, de las plataformas Windows y Linux monitoreadas, donde se detalle el “Quien” y el “Que”. ▪ Debe contar con la característica de detección automática basada en agente, de cambios en el registro de los sistemas Windows monitoreados. ▪ Debe contar con la característica de Monitoreo del sistema via SNMP, WMI y PowerShell. ▪ Debe contar con la característica de Monitoreo de aplicaciones via JMX, WMI y PowerShell.	

		▪ Debe contar con la característica de Monitoreo de Hipervisor tales como VMWARE y Hype-V. ▪ Debe poder Monitorear plataformas de almacenamiento tales como EMC, NetAPP, Nutanix, Nimble, ORACLE etc a nivel de desempeño y uso de almacenamiento. ▪ Debe poder Monitorear sistemas del tipo Directorio Activo y Exchange basado en WMI y PowerShell. ▪ Debe poder Monitorear motores de Bases de datos SQL Server, Oracle, MySQL entre otras via JDBC. ▪ Debe poder Monitorear Infraestructura VoIP via IPSLA, SNMP, CDR y CMR. ▪ Debe realizar Análisis del desempeño y flujo de las aplicaciones via NetFlow, Sflow, Cisco AVC y NBAR. ▪ Debe tener la Capacidad de definir metricas definidas por el usuario. ▪ Debe tener la Capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada. ▪ Debe tener la Capacidad de monitorear dispositivos del entorno tales como Liebert UPS, HVAC, FPC y APC. ▪ Debe monitorear las caídas y reinicios de los sistemas vía Ping, SNMP, WMI, así como análisis del reinicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage. ▪ Debe hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos.	
4	**Monitoreo Avanzado de Modificación de Archivos** - Debe monitorear modificación de archivos en por lo menos 100 servidores. - Debe monitorear los cambios en los archivos de configuración de los servidores que la entidad defina. - Debe contar con la característica de detección automática en cambios en archivos y carpetas, de las plataformas Windows y Linux monitoreadas, donde se detalle el “Quien” y el “Que”. - Debe hacer Monitoreo de la Integridad de Archivos o FIM basada en agente tanto para Windows como Linux.	

	- Debe contar con un módulo para la administración de los agentes Windows FIM. - Debe contar con la característica de detección automática basada en agente, de cambios en el registro de los sistemas Windows monitoreados. - Debe generar un informe mensual de los incidentes detectados a nivel de alteraciones 4sospechosas que se hayan podido presentar en los activos de información monitoreados.	
5	**Monitoreo Avanzado de Aplicaciones Web y Servicios de Usuario Final** - Debe hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos. - Debe poder correlacionar los eventos de seguridad y monitorear el servicio de Office 365 donde la entidad tiene el correo electrónico, permitiendo la identificación de incidentes de seguridad que Office 365 alerte a nivel de logs. Para esto la plataforma de forma nativa Debe tener integración o conector con office 365.	
6	**Monitoreo Avanzado de Cambios y Configuraciones** - Debe ser capaz de detectar anomalías en la línea base definida. - Por temas de administración y operación, todas las funciones requeridas en el presente Deben poder configurarse y operarse desde una única consola web de un único fabricante. - Debe tener la capacidad colectar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones. - Debe tener la capacidad de Colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones. - Debe contar con la característica de detección automática de los cambios en la configuración de red de las plataformas monitoreadas.	

	- Debe contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas.
7	**Monitoreo Avanzado de Servicios de Datacenter y Conectividad** - Debe poder crear dashboards personalizables para monitorear los SLAs de servicio para la conectivdad de la entidad identificando caidas del operador o saturación de sus activos de red que soportan el servicio. - Debe poder crear dashboards personalizables para monitorear los SLAs de servicio los servicios de Datacenter de la entidad identificando caidas del operador o saturacion de sus activos de red que soportan el servicio. - Debe poder crear dashboards personalizables para monitorear los KPIs asociados a los servicios.
8	**Dispositivos y Aplicaciones Soportados** En caso de que se requiera, la solución Debe como mínimo poder hacer monitorización de las siguientes plataformas o dispositivos, dependiendo de las definiciones de la entidad y los nuevos servicios que se requieran. ▪ **Application Servers** o Microsoft ASP.NET o Oracle WebLogic o IBM WebSphere o Red Hat JBoss o Sun GlassFish o Apache Tomcat ▪ **Authentication Servers** o Cisco Access Control Server (ACS) o Juniper Steel-Belted Radius o Microsoft Internet Authentication Service (IAS)

- Alcatel AAA RADIUS

- **Blade Servers**
  - Cisco Unified Computer System (UCS)
  - HP BladeSystem
  - Dell Blade Server

- **Cloud Services**
  - Amazon EC2

- **Databases**
  - IBM DB2
  - MySQL
  - Microsoft SQL Server
  - Oracle Database Server

- **Directory Services**
  - Microsoft Active Directory 2000, 2003, 2008, 2012

- **DNS/DHCP Servers**
  - Infoblox DNS/DHCP
  - BIND DNS
  - Linux DHCP
  - Microsoft DHCP/DNS 2003, 2008

- **Email**
  - Microsoft Exchange
  - Postfix Mail Server
  - Sendmail
  - Office 365

- **Environmental**
  - APC UPS
  - Liebert UPS, HVAC, FPC
  - APC NetBotz
  - Generic UPS

- **File Monitoring**
  - Linux
  - Microsoft Windows

- **Firewalls**
  - Cisco ASA, IOS
  - Cisco Firewall Services Module (FWSM), Private Internet eXchange (PIX)
  - Juniper Networks Secure Services Gateway (SSG), Integrated Security Gateways (ISG)
  - Palo Alto Networks
  - Check Point FireWall-1, Provider-1, IPSO
  - Check Point VSX
  - Fortinet FortiOS
  - Linux ipchains
  - McAfee Enterprise (Sidewinder)
  - Dell SonicWALL SonicOS
  - WatchGuard
  - Microsoft Internet Security and Acceleration (ISA) Server
  - Astaro

- **Hardware Monitoring**
  - Dell servers
  - HP servers
  - IBM servers
  - VMware ESX servers
  - Network devices
  - Storage devices

- **Host OS**
  - Microsoft Windows 2000, 2003, 2008, 2012, XP, Vista, Windows 7
  - CentOS Linux
  - Fedora Linux
  - Red Hat Linux
  - Debian Linux
  - SUSE Linux
  - HP-UX
  - IBM AIX
  - IBM OS/400
  - Oracle Solaris, SunOS

- **Internet Security Gateways**

- Blue Coat ProxySG
- Cisco IronPort Mail and Web
- Barracuda Spam Firewall
- McAfee Web Gateway
- Websense Web Filter
- Websense Email Security Gateway
- Microsoft Internet Security and Acceleration (ISA) Server
- Squid
- Untangle Secure Gateway
- Astaro Security Gateway

- **Network Intrusion Prevention Systems (IPS)**
  - Cisco IPS
  - Snort IPS
  - FireEye
  - Juniper IDP
  - IBM Security/ISS SiteProtector
  - McAfee IntruShield
  - HP TippingPoint Next-Generation Intrusion Prevention System (IPS)
  - Check Point SmartDefense
  - ForeScout
  - SourceFire IPS appliances and DefenseCenter

- **Load Balancers / Application Firewall**
  - F5 BIG-IP Local Traffic Manager
  - F5 BIG-IP WebAccelerator
  - F5 BIG-IP Application Security Manager
  - Citrix NetScaler

- **Network Flow**
  - Cisco NetFlow v5, v9
  - sFlow
  - Cisco Application Visibility and Control (AVC)

- **Routers and Switches**
  - Cisco IOS, Nx-OS, CatOS
  - Juniper Junos
  - Alcatel-Lucent TiMOS, AOS
  - Brocade/Foundry IronWare

- HP ProCurve
- Cisco MDS
- Avaya (Nortel) ERS, Nortel Passport
- HP/3Com Comware
- Huawei VPR
- Extreme ExtremeWare XOS
- Mikrotik Router
-

- **Antivirus**
  - Symantec Endpoint Protection
  - McAfee EPO
  - Trend Micro OfficeScan

- **Vulnerability Scanners**
  - McAfee Foundstone
  - Qualys QualysGuard
  - Rapid7 Nexpose
  - Tenable Nessus
  - nCircle

- **Storage**
  - EMC Data Domain
  - EMC Isilon
  - EMC VNX
  - NetApp Data ONTAP Filer
  - EMC CLARiiON
  - EMC VNX
  - Dell EqualLogic
  - VMware and Host attached storage

- **Virtualization**
  - VMware ESX, ESXi, vSphere, vCenter

- **Wireless LAN**
  - Cisco WLAN
  - Aruba ArubaOS
  - NetMotion Mobility XE

	Protocolos Soportados La solución Debe soportar los siguientes protocolos de colección y/o monitoreo: ▪ Web – HTTP/HTTPS ▪ DNS ▪ FTP/SCP ▪ Generic TCP/UDP ▪ ICMP ▪ IMAP4 ▪ JDBC ▪ LDAP ▪ POP3 ▪ POP3S ▪ SMTP ▪ SOAP ▪ SSH ▪ Telnet/SSH ▪ SNMP ▪ WMI ▪ JMX	
9	**Características de Análisis de Seguridad en Tiempo Real.** El módulo de analítica de eventos de seguridad debe cumplir con mínimo las siguientes características: ▪ Debe soportar Correlación cruzada de eventos. ▪ Integración por medio de API's con fuentes de información externa sobre amenazas, tales como Dominios de Malware, IPs, URLs, Hash y Nodos de Tor. ▪ Integración Nativa con fuentes de información de terceros tales como ThreatStream, CyberArk, SANS y Zeus ▪ Debe tener la Capacidad de Colección de logs, parsing de logs, indexación de logs a la tasa de eventos por segundo (EPS) que sean licenciados.	

		▪ Capacidad de hacer Monitoreo de la Integridad de Archivos o FIM basada en agente Windows. ▪ Debe tener la capacidad de modificar los parsers por medio de interface gráfica, sin que esta modificación afecte la colección de logs o genere caídas en los servicios de la solución. ▪ Debe permitir la creación de Parsers customizados a partir de platillas XML. ▪ Debe tener la capacidad de Colectar logs de forma segura, desde dispositivos remotos. ▪ Debe contar con un framework de notificación de incidentes el cual Debe estar basado en políticas de monitoreo de cada componente. ▪ Debe tener la capacidad de ejecutar scripts de remediación cuando un incidente ocurra. ▪ Debe contar con un sistema propio de tickets ▪ Debe tener la capacidad de integrarse con sistemas de tickets externos en caso que la entidad lo requiera, dicha integración Debe ser por API. ▪ Debe ser capaz de detectar anomalías en la línea base definida. ▪ La detección de incidentes Debe ser en tiempo real anterior al almacenamiento del evento, utilizando técnicas del tipo “Correlación Distribuida”. ▪ Debe contar con una consola de visualización de logs y eventos correlacionados la cual cuente con un sistema para el filtrado de los mismo por medio de condiciones Boleanas. ▪ Deben poder realizarse filtros por medio de expresiones regulares. ▪ El reporte de incidentes Debe poder ser priorizado por los servicios críticos. ▪ Debe permitir la identificación dinámica de usuarios.	
10	**Administración y Reportes.** La solución Debe contar con las siguientes características de administración y reportes: ▪ La plataforma debe poder ser administrada vía HTTPS. ▪ La plataforma debe tener una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cual permita tener una visión global de los incidentes de seguridad. ▪ La comunicación de los módulos Debe ser asegurada por temas de confidencialidad por medio de HTTPS. ▪ Debe contar con un módulo para el cálculo de los SLA.	

	▪ Debe contar con un módulo grafico que muestre la infraestructura existente, las conexiones de las mismas y los eventos generados en cada activo. ▪ Debe contar con un dashboard que permita identificar en un mapa los incidentes y su ubicación geográfica. ▪ Debe contar con un módulo para administrar las políticas de correlación. ▪ Debe contar con un módulo para la administración de los agentes. ▪ Debe contar con un módulo de administración para la característica de "base de datos de la gestión de configuración" o CMDB. ▪ La plataforma Debe tener un gran número de reportes predefinidos y Debe permitir crear reportes customizados.

3. SOLUCION DE BALANCEO DE DATACENTERS Y CANALES

ITEM	REQUERIMIENTOS TECNICOS
1	**Generalidades.** Contar con una solución de Datacenters y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un esquema de alta disponibilidad de datacenters y canales, donde se Deben ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento. • Solución en alta disponibilidad, dos equipos de la misma referencia funcionando en modo clúster en el DataCenter primario y standalone en el secundario. • El dispositivo debe ser un equipo de propósito específico. • Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. • La solución debe ser desarrollada por el fabricante y no debe incluir desarrollos de terceros

2	**Rendimiento.** El equipo Debe cumplir con las siguientes características MINIMAS de desempeño ya activas y funcionales: • Rendimiento Capa 4: 15 Gbps • Rendimiento Capa 7: 12 Gbps • Rendimiento Compresión: 8 Gbps • Conexiones por Segundo SSL: 12.000 • Transacciones por Segundo Capa 4: 300.000 • Dominios Virtuales: 5	
3	**Conectividad** El equipo Debe contar con las siguientes interfaces de conexión: o 4 puertos de 10Gbps SPF+. o 4 puertos de 1Gbps SPF. o 4 puertos de 1Gbps RJ45.	
4	**Funcionalidades básicas de Balanceo.** ▪ La solución debe estar diseñada para proveer aceleración en Layer-4 y Layer-7. ▪ La solución debe ser capaz de balancear tráfico ICMP,UDP,TCP y poseer entendimiento de protocolos como HTTP/s, FTP y RADIUS. ▪ La solución debe ser capaz de balancear carga de manera transparente o utilizando NAT basándose en información obtenida de Layer-7 como URL, Cookie, SSL ID, etc. ▪ La solución debe poseer distintos métodos de balance como round robin, weighted round robin, least connection y shortest response. ▪ La solución debe ser capaz de hacer routing/switching inteligente de contenido en Layer-7 basándose en la información enviada por el cliente (URL, HTTP header, cookie, URL, etc). ▪ La solución debe proveer persistencia en Layer-4 basándose en la dirección IP de origen y puerto. Adicionalmente la persistencia en Layer-7	

		debe poder ser configurada basándose en la información del cliente como URI, HTTP headers, hostname, SSL session ID y Cookies. ▪ La solución debe ser capaz de hacer SSL Offloading ▪ La solución debe ser capaz de realizar balance entre datacenters (GSLB) ▪ La solución debe poseer la capacidad de proteger aplicaciones y servidores de ataques SYN-Flood y cantidad de conexiones. Además, debe ser capaz de integrar tabla de conexiones statefull para IPv4 e IPv6. ▪ La solución debe poder ser administrada vía interfaz gráfica (GUI) e interfaz de línea de comandos (CLI). ▪ La Solución propuesta Debe proveer alta disponibilidad, failover transparente y escalabilidad para las aplicaciones. ▪ La solución propuesta Debe contar con un servicio de protocolo virtual para los siguientes protocolos HTTP, HTTPS, TCP, TCPS, FTP, FTPS, UDP, DNS, SIP UDP, SIP TCP, RTSP, RDP, IP, L2IP, este servicio virtual también Debe funcionar en modo proxy reverso, proxy transparente y proxy en modo de triangulación. ▪ La solución propuesta Debe reenviar los paquetes IP a diferentes destinos MAC para distribuir la carga a nivel de capa 2 puerto físico, a nivel de capa 3 dirección IP y rango de puertos TCP/UDP. ▪ La solución propuesta Debe ofrecer un sistema de almacenamiento de contenido Web completamente integrado con funcionalidades de HTTP/HTTPS, compresión y funciones de administración de tráfico para almacenar y enviar objetos validando las peticiones de los clientes sin tener que consultar a los servidores reales acelerando la respuesta de las aplicaciones, reduciendo el ancho de banda y la carga de los servidores. ▪ Debe proveer estadísticas detalladas del acceso al cache basándose en IP o en http hosts como mínimo, las coincidencias de los objetos almacenados podrán estar basadas en URL parciales. ▪ Debe tener reglas configurables para tamaño máximo de objetos, TTL y la forma de acceso, soporte del set de caracteres extendidos. ▪ La solución propuesta Debe tener un sistema de compresión dinámico en línea basado en hardware, en donde de forma automática Debe comprimir archivos de texto, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT y XLS, también Debe contemplar reglas para no comprimir URL seleccionados que contengan RegEx y objetos web seleccionados para el servicio virtual seleccionado y proporcionar estadísticas detalladas de la compresión.	

	▪ La plataforma ofertada debe permitir hacer balanceo y enrutamiento personalizado por medio de scripts, basados en lenguajes abiertos tales como LUA. ▪ La plataforma ofertada Debe tener un sistema de aceleración de SSL basado en hardware soportando HTTPS, NNTPS, SMTPS, POPS, IMAPS y LDAPS. Soporte de SSLv3 y TLSv1 con un cifrado máximo de 2048-bits, redirección automática de HTTP a HTTPS, Debe poder actuar como servidor de SSL o como cliente de SSL al mismo tiempo, hasta 64 servicios virtuales podrán utilizar el mismo certificado.

4. PUNTOS DE ACCESO WIFI

Ítem	**Requerimiento Técnico** **AMPLIACION SOLUCION DE RED INALAMBRICA.**
2.1	**Generalidades.** Se requieren 9 equipos que sirvan de puntos de acceso inalámbrico para la sede principal de la entidad. Los equipos físicamente Deben tener presentación para interiores y Deben unirse sin inconvenientes de compatibilidad a las redes LAN de la entidad. Igualmente los equipos Deben integrase de forma nativa a los NGFW ofertados de forma nativa, lo cual permitirá administrar sus políticas de seguridad de acceso y de encripción de la información así como las características típicas de seguridad desde una consola que lo haga de manera general y de manera particular. Todos los equipos de punto de acceso inalámbrico Deben ser administrados de forma centralizada a través de la solución de seguridad perimetral ofertada. La solución de red inalámbrica Debe permitir la implementación de un portal cautivo sin necesidad de equipos o software adicional. La solución de red inalámbrica ofertada Debe integrarse de forma nativa a la plataforma de reportes de seguridad actual de la entidad, permitiendo la generación de reportes centralizados y recolección de logs desde esta plataforma centralizada.

	La solución debe poder implementar políticas de seguridad tipo WIDS/WIPS. La solución Debe permitir establecer políticas de seguridad para acceso a la red basadas en dispositivo, sistema operativo o control por MAC. La solución Debe contar con Extensiones Multimedia Wireless la cual permita control de aplicaciones y uso de ancho de banda. La solución Debe contar con el aprovisionamiento automático de recursos de radio para optimización de rendimiento. La solución Debe contar con detección de access points intrusos Los dispositivos son requeridos por un periodo de 3 años en un esquema 7 x 24 ante fabricante. Uno de lo radios de cada Access Point Debe poderse configurar como monitor del espectro en búsqueda de access points intrusos La solución Debe tener la capacidad de detectar un access point intruso cuando es puesto en la red cableada
2.2	**Número de Radios.** Dos radios: 2.4 GHz / 5 GHz – (802.11 a/n/ac y 802.11 b/g/n)
2.3	**Ganancia de las Atenas:** 5 dbi a 2,4 Ghz y 6 dbi a 5 Ghz.
2.4	**Tecnología de Transmisión.** 3 x 3 MIMO
2.5	**Velocidad.** Radio 1 hasta 450 Mbps **–** Radio 2 hasta 1300 Mbps
2.6	**Puertos Ethernet.** 2 puerto 10/ 100/1000
2.7	**Alimentación.** Power Over Ethernet PoE, ESTANDAR: 802.3af o Adaptador, Se requiere que todos los equipos vengan con los dispositivos de inyección de poder. El cual Debe estar incluido en la oferta.

2.8	**SSID.** Los equipos Deben soportar hasta 14 SSIDs para el acceso de los clientes
2.9	**Seguridad.** El equipo Debe soportar los protocolos de encripción WPA, WPA2-PSK, WPA2 Enterprise con AES.
2.10	**Autenticación.** Radius,WPA y WPA2 para 802.1x con Preshared key y Web portal cautivo.
2.11	**Calidad de Servicio.** Los equipos Deben manejar calidad de servicio avanzada, usando técnicas de limitación de servicio por usuario.
2.12	**Tipo de Antenas.** Se requiere que todos los equipos vengan con mínimo 6 antenas de tipo internas, no dejando expuesto ningún componente de las mismas.
2.13	**Kit de Instalación.** Todos los equipos Deben contar con sus aditamentos y componentes físicos para su fácil la instalación. Se debe proveer el punto cabledo para su correcta instalación.
2.14	**Módulo de invitados.** Los equipos Deben contar con un módulo de usuarios y seguridad para el manejo de invitados que permita asignar acceso temporal a usuarios esporádicos que se presenten en la red inalámbrica de tal manera que manejen el tráfico aislado.
2.15	**Voz sobre IP.** Los Puntos de Acceso deben soportar mecanismos de QoS como WME/WMM.
2.16	**Soporte a Smartphone.** Todos los puntos de acceso inalámbrico deben soportar el uso de Smartphone.
2.17	**Soporte de Vlans.** Los equipos deben poder mapear Vlans a SSIDs.
2.18	**Certificaciones.** CE, FCC, IC, Wifi Alliance Certified

5. INSTALACION y EQUIPO MINIMO DE TRABAJO

ITEM	REQUERIMIENTOS TECNICOS
1	• Instalación, Implementación y puesta en marcha de las soluciones ofertadas. • El oferente Debe entregar los equipos en el sitio indicado por la entidad, Bogotá. • La implementación Debe comprender los siguientes puntos.

	• Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio. • Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante. • Implementación de la solución de acuerdo a las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura. • Pruebas de Servicio de las plataformas ofertadas. • Puesta en Producción de las plataformas ofertadas. • Estabilización de las plataformas ofertadas. • Se debe incluir todo el cableado necesario para la Implementación, asi y en caso de requerirse un gabinete con 2 PDU,	
2	Dentro de los servicios se debe tener en cuenta la Instalación, configuración y puesta en producción de los dispositivos ofertados ubicados en la sede principal.	
3	Las plataformas ofertadas Deben quedar totalmente configuradas y cumpliendo con las condiciones y requerimientos de configuración definidas por la entidad.	
4	El oferente Debe adjuntar con su propuesta una carta emitida por el fabricante donde evidencie el nivel de membresía y las plataformas ofertadas para la entidad indicando el tiempo de soporte ofertado.	
5	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. Adicionalmente se debe incluir actividades de mantenimiento las cuales se realizarán de manera preventiva para minimizar problemas y mantener los sistemas actualizados, cuando este sea requerido por la entidad, durante un periodo de tres años.	
6	El contratista Debe realizar y documentar entre otras, las siguientes actividades cada 6 meses previa coordinación con el supervisor del contrato en desarrollo: • Revisar y afinar, las plataformas ofertadas. • 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 las herramientas de reportes y almacenamiento de Logs. • Mantener actualizados los niveles de Firmware de los componentes ofertados de acuerdo con las últimas versiones estables liberadas por el fabricante.
7	El horario de atención para el mantenimiento correctivo debe ser de 7x24x4, en sitio debe ser requerido por el supervisor del contrato, sin costo adicional para la entidad.
8	El contratista debe garantizar soporte y garantía de repuestos para los Dispositivos Ofertados en un esquema 7 x 24 x 4 para 3 años en sitio. La entidad hará revisión de los repuestos y/o equipos de soporte para garantizar este requerimiento.
9	Al finalizar cada visita correctiva y/o preventiva el contratista generará un informe de servicio en la que constará 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 y/o en la configuración.
10	El oferente debe contemplar una transferencia de conocimiento en modalidad de transferencia de conocimientos para 2 funcionarios de la entidad, la cual debe incluir como mínimo temas de administración, Monitoreo y resolución de problemas de las plataformas objeto del presente contrato.
11	**Equipo Mínimo de Trabajo.** El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por el personal a continuación descrito:

GERENTE DE PROYECTO

- Un (1) Profesional
- Ubicación: en las instalaciones de la entidad en la modalidad bajo demanda. 50% de Dedicación.
- Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones, o afines.
- Cinco (5) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia.
Experiencia especifica de tres (3) años como Gerente de Proyectos y/o Líder de Servicio.

GERENTE DE CALIDAD

- Un (1) Profesional
- Ubicación: Remota y en las Instalaciones del cliente con dedicación al 50% bajo el esquema bajo demanda.
- Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones, o afines. -
Cinco (5) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia.
- Experiencia especifica de cinco (5) años como líder técnico de proyectos de Infraestructura y/o seguridad de información.

EQUIPO DE INGENIERIA (PERFIL 1)

- Un (1) Profesional / Experto
- Ubicación: Remota y en las Instalaciones del cliente con dedicación al 50% bajo el esquema bajo demanda.
- Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones ó afines.
- Dos (2) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. Experiencia

	especifica: de cinco (5) años como Ingeniero Líder de Redes / Seguridad de Información y SOC. **EQUIPO DE INGENIERIA (PERFIL 2)** - Un (1) Profesional - Ubicación: Remota y en las Instalaciones del cliente con dedicación al 50% bajo el esquema bajo demanda. - Tecnólogo en Sistemas, Electrónica o en culminación de Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones ó afines. - Un (1) año de experiencia en proyectos de Seguridad y/o Redes. En caso de estar culminando Pregrado de Ingeniería de Sistemas, Ingeniería de Telecomunicaciones o Afines, debe aportar carta de la universidad donde certifique estado actual.

6. CERTIFICACIONES

El oferente debe proporcionar certificación escrita directamente del fabricante donde conste que es distribuidor autorizado para comercializar los equipos y contratos de servicio de soporte para los equipos cubiertos con este contrato.

Adicionalmente el oferente Debe anexar el Datasheet de los equipos ofertados.

PROPUESTA ECONÓMICA						
"Adquirir la infraestructura de detección, protección y contención de las amenazas avanzadas, así como la implementación del NOC y SOC para complementar la plataforma actual de seguridad informática de la ANH."						
tem	**Descripción**	**Cantidad**	**Valor Unitario**	**SubTotal**	**IVA sobre el Total**	**Valor Total IVA Incluido**
1	Solución para mitigación de amenazas avanzadas multivector para punto final	**1**	$	$	$	$
2	Solución para monitoreo avanzado de servicios	**1**	$	$	$	$
3	Solución de balanceo de datacenters y canales	**1**	$	$	$	$
4	Puntos de acceso wifi	**10**	$	$	$	$
5	Instalación y equipo mínimo de trabajo	**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 Deben 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 25 de octubre de 2017.