SONDEO DE MERCADO PARA AMPLIAR Y ACTUALIZAR LA PLATAFORMA DE SEGURIDAD INFORMÁTICA DE LA AGENCIA NACIONAL DE HIDROCARBUROS – ANH.

TABLA DE CONTENIDO

1 OBJETO, DESARROLLO, PRODUCTOS SOLICITADOS, CARACTERISTICAS TÉCNICAS ESPERADAS.

1.1 Objetivo

La adquisición, instalación, configuración y puesta en marcha de infraestructura tecnológica para la ampliación y actualización de la plataforma de seguridad, de acuerdo a lo requerido por la ANH en este estudio.

1.2 Objeto

CONTRATAR LA AMPLIAR Y ACTUALIZAR LA PLATAFORMA DE SEGURIDAD INFORMÁTICA DE LA AGENCIA NACIONAL DE HIDROCARBUROS – ANH.

1.3 Lugar de Ejecución

El lugar de ejecución del presente contrato se realizará en la sede principal de la Agencia Nacional de Hidrocarburos en la Avenida Calle 26 No. 59-65 | Bogotá, Colombia - Edificio Cámara Colombiana de la Infraestructura.

1.4 Plazo de Ejecución

El tiempo de ejecución estimado del contrato es de **sesenta (60) días calendario** después del perfeccionamiento del mismo.

1.5 Solicitud de Mercado

- Se requiere un presupuesto detallado del valor. Los costos deben ser calculados por análisis de precios unitarios y por el valor total de cada producto que se debe registrar en las tablas a continuación: “CUADRO PROPUESTA ECONOMICA”, dicho valor será presentado en pesos Colombianos y debe tener incluido todos los costos directos e indirectos, con sus respectivas tasas e impuestos.

- No se permite realizar modificaciones al cuadro “PROPUESTA ECONOMICA” (agregar y/o eliminar, ítems, filas, columnas o modificar el contenido de las celdas), conducirá a la exclusión de la cotización del proponente y no se tendrá presente en el sondeo realizado.

- Los factores de costos y gastos a incluir, corresponden a todos aquellos que resulten necesarios para la ejecución del contrato en las condiciones de tiempo requeridos.

- Los valores deben ser sumas fijas, no sujetas a reajuste o modificaciones de ninguna clase, en función de eventuales variaciones que puedan experimentar los factores de costos y gasto que las integren, durante la ejecución del contrato.

- Disponibilidad: La firma participante en el presente sondeo de mercado, debe especificar si tiene la disponibilidad inmediata para la prestación del servicio requerido para ejecutar el presente contrato o la fecha más próxima para disponer de los mismos.

1.6 Entrega de Información del Sondeo de Mercado

Las firmas invitadas deberán entregar la información solicitada en el presente sondeo de mercado al correo electrónico: gloria.cruz@anh.gov.co, antes del día 06 de marzo de 2015.

1.7 Productos y servicios a cotizar:

1.7.1 Especificaciones Técnicas

La necesidad de mejoramiento de la plataforma de seguridad informática que requiere la Agencia Nacional de Hidrocarburos se resume en los siguientes puntos principales:

- Mejorar las características de los firewalls de perímetro, mediante la adquisición de un cluster de Next Generation Firewalls a 3 años que soporten configuración de firewalls virtuales, los cuales incluyan prevención de intrusos (IPS), filtrado web (URL Filtering), control de aplicaciones, inspección de tráfico cifrado, inspección profunda de paquetes, detección de malware basada en reputación, visibilidad y protección APT
- Adicionar un segundo anillo de seguridad mediante la configuración de un firewall virtual interno en cluster para controlar las conexiones de la red de usuarios hacia la red de servidores.
- Agregar seguridad para dispositivos móviles por medio del uso de políticas de firewall basadas en dispositivo o usuario y la configuración de portal cautivo.

- Adquirir una plataforma para almacenamiento de logs y generación de reportes a 3 años, de tal forma que se puedan centralizar los logs y reportes de los firewalls perimetrales e internos del Centro de Datos Principal.
- Renovar el licenciamiento de dos de los firewalls existentes a 1 año con coterm de tal forma que la fecha de vencimiento sea 31 de diciembre de 2016, para instalarlos como firewalls perimetrales en el Centro de Datos Alterno.
- Renovar el licenciamiento existente de las suites TDA (Total Protection Data) y EPA (Endpoint Protection Advanced) con coterm de tal forma que la fecha de vencimiento sea 31 de diciembre de 2016 y adquirir licencias nuevas para ambas suites a 1 año para tener un total de 500 licencias por cada suite.
- Renovar el licenciamiento de la herramienta DAM (Database Activity Monitoring) de McAfee para 16 instancias de bases de datos a 1 año con coterm de tal forma que la fecha de vencimiento sea 31 de diciembre de 2016.
- Renovar el licenciamiento de las herramientas SIEM (McAfee Enterprise Security Manager), MVM (McAfee Vulnerability Manager) con coterm de tal forma que la fecha de vencimiento sea 31 de diciembre de 2016 y RSA Archer Incident Management Solution y Enterprise Management solution a 1 año.
- Tener visibilidad y protección de APTs (amenazas avanzadas persistentes), por medio de la adquisición de un appliance dedicado para este tipo de amenazas a 1 año.

A continuación se relacionan las características de los elementos a cotizar:

1.7.1.1 *NGFW (Next Generation Firewall)*

Característica	**Especificaciones técnicas mínimas requeridas**
Cantidad	2
Funcionalidades activas	Firewall, IPS, Control de aplicaciones, Antivirus, control de bots, Filtrado Web y VPN.
Rendimiento	**Especificaciones técnicas mínimas requeridas**
Rendimiento de Firewall	20 Gbps
Rendimiento de IPS	6 Gbps
Rendimiento VPN IPSec	3.5 Gbps para AES-128
Sesiones concurrentes	4.000.000
Conexiones por segundo	100.000
Políticas de Firewall	10.000
Usuarios VPN	500
Configuración Base	**Especificaciones técnicas mínimas requeridas**

Característica	Especificaciones técnicas mínimas requeridas
Interfaces 10 Gb aprovisionadas con transceivers	2
Interfaces 10/100/1000 RJ45	8
Interfaces 1Gb en Fibra aprovisionadas con transceivers	4
Protocolos soportados	IPv4 e IPv6
Característica	**Especificaciones técnicas mínimas requeridas**
Manejo de tráfico y calidad de servicio	Capacidad de asignar parámetros de traffic shapping.
	Capacidad de definir parámetros de traffic shapping que apliquen para cada dirección IP, usuario o grupos de usuario en forma independiente.
Funciones básicas de Firewall	Analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
	Soportar definición de nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
	Soporte de configuración de creación de políticas y objetos en doble stack (IPv4-IPv6)
Inspección de trafico cifrado	Soporte de políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios del Directorio Activo
	Captura de paquetes para luego ser exportado en formato PCAP o CAP.
Conectividad y Enrutamiento	Funcionalidad de DHCP: como cliente DHCP, Servidor DHCP y reenvio (relay) de solicitudes DHCP
	Soporte a etiquetas de VLAN (802.1Q) y creación de zonas de seguridad en base a VLANs.
	Soporte de rutas estáticas, incluyendo distancia y prioridad.
	Soporte de enrutamiento dinámico RIP V1, RIP V2, OSPF y BGP.
	Capacidad de enrutamiento tanto en IPV4 como en IPv6
	La solución debe soportar 6to4 NAT o 6to4 Tunnel
	La solución debe soportar los siguientes RFC IPv6 • RFC 1981 Path Maximum Transmission Unit Discovery for IPv6 • RFC 2460 IPv6 Basic specification • RFC 2464 Transmission of IPv6 Packets over Ethernet Networks • RFC 3596 DNS Extensions to support IPv6 • RFC 4007 IPv6 Scoped Address Architecture • RFC 4193 Unique Local IPv6 Unicast Addresses

Característica	Especificaciones técnicas mínimas requeridas
	• RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported. • RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884) • RFC 4443 ICMPv6 • RFC 4861 Neighbor Discovery • RFC 4862 IPv6 Stateless Address Auto-configuration
VPN IPSec	Soporte para método de configuración IKE e IKEv2.
	Soporte de VPNs con algoritmos de cifrado: AES, DES y 3DES.
	Soporte de longitudes de llave para AES de 128, 192 y 256 bits.
	Soporte de grupos Diffie-Hellman 1, 2, 5 y 14.
	Soporte de los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
	Posibilidad de crear VPNs entre gateways y clientes con IPSec (VPNs IPSEC site-to-site y VPNs IPSec client-to site)
VPN SSL	Soporte a certificados PKI X.509 para construcción de VPNs SSL.
	Permitir la definición de varios portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
Autenticación	Debe permitir los siguientes esquemas de autenticación: tokens (SecureID, TACACS, RADIUS, certificados digitales)
	Capacidad de integrarse con LDAP o Microsoft Active Directory tanto en IPv4 como IPv6.
	Capacidad de crear certificados propios, en caso que la ANH requiera realizar autenticación de dos factores.
Módulos de seguridad	**Especificaciones técnicas mínimas requeridas**
Filtrado Web	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios. Por flexibilidad, el filtro de URLs debe cubrir más de 90 millones de sitios web en al menos 60 categorías preconfiguradas.
	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
	Soportar como mínimo los 400 usuarios actuales de la entidad y el crecimiento anual de usuarios durante 3 años posteriores.

Característica	Especificaciones técnicas mínimas requeridas
	Como apoyo a las políticas de seguridad empresariales, se solicita que la solución tenga la capacidad de desplegar alertas en tiempo real (informativas o de pregunta) cuando los usuarios traten de ingresar a sitios restringidos.
	Categorizar contenido Web requerido tanto en IPv4 como IPv6.
Protección contra intrusos (IPS)	El sistema IPS debe poder ser habilitado para prevenir los ataques (bloqueo) y ante carga alta maneje un sistema que le permita generar bypass o cerrar las conexiones que no puedan ser garantizadas. Debe permitir que el administrador de la solución lo pueda configurar en modo de Detección.
	IPS debe estar basado en los siguientes mecanismos de detección: exploits de firmas, anomalías de protocolos, control de aplicaciones y detección basada en comportamiento.
	IPS debe estar en la capacidad de detectar y bloquear ataque a nivel de red y de aplicación, al menos en los siguientes servicios: Email, DNS, servicios de Windows y SNMP (los cuales se han identificado por estadísticas que son los mas frecuentes en las redes de datos)
	IPS debe estar integrado en la plataforma de firewalls virtuales de nueva generación que se está adquiriendo.
	La solución debe proporcionar protección a protocolos VoIP
	Capacidad de analizar en detener ataques de tráfico tanto en IPv4 como IPv6
	El IPS debe contar con un mecanismo que permita la identificaión de servidores según tipo de servicio (web, DNS, Mail, ente otros) para aplicarle las firmas según el perfil de servicio.
	Se debe garantizar que el IPS inspeccione toda la sesión, para todas las firmas aplicadas.
	Debe tener la capacidad de generar excepciones a firmas basado en fuente, destino, servicio o la combinación de las tres.
	Permitir configuración de firmas nuevas para cualquier protocolo.
	Debe permitir al administrador de la solución activar o desactivar firmas de acuerdo a parámetros configurables como impacto al desempeño de la plataforma, severidad de la amenaza o niveles de confidencialidad.

Característica	Especificaciones técnicas mínimas requeridas
	Actualización automática de firmas en tiempo real para el detector de intrusos durante la duración del contrato. La solución debe estar en la capacidad de permitir administrar (activar o no) las nuevas firmas.
	Detección de ataques por variaciones de protocolo y además por firmas de ataques conocidos.
	IPS debe contar con un mecanismo de fail-open, el cual debe ser configurable basado en los umbrales de recursos físicos de la máquina.
Control de aplicaciones	Capacidad de identificar la aplicación que origina el tráfico a partir de la inspección del mismo.
	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
	La solución debe tener un listado de al menos 3000 aplicaciones definidas y verificables en el sitio web del fabricante
	La solución debe contar con categorías predefinidas que al menos incluya Web 2.0, IM (instant messaging), P2P, Voice & Video y File Share
	El listado de aplicaciones debe actualizarse periódicamente y de forma automática.
	Las aplicaciones identificadas o no identificadas deben poder permitirse, bloquearse o registrarse.
	Se debe poder controlar el consumo de ancho de banda usado por las aplicaciones.
	Control de aplicaciones granular. Por ejemplo: Bloqueo de Google Talk sin tener que bloquear Gmail o Bloqueo de Chat de Facebook sin tener que bloquear Facebook.
	Como apoyo a las políticas de seguridad empresariales, se solicita que la solución tenga la capacidad de desplegar alertas en tiempo real (informativas o de pregunta) cuando los usuarios traten de ingresar a aplicaciones no autorizadas. En caso de no tenerlo dentro de la solución, se podrán ofertar de forma adicional soluciones de terceros que se integren a la plataforma de Next Generation para cumplir con este requerimiento
	Las aplicaciones deben estar categorizadas basadas en nivel de riesgo
	Se debe tener la capacidad de crear políticas de acceso a aplicaciones basados en usuarios o grupos de usuarios del AD del ANH
Protección contra amenazas avanzadas (APTs)	Debe ser capaz de analizar, establecer control de acceso, detener ataques y hacer antivirus en tiempo real.
	Detección APT en tiempo real, integrado a la plataforma de seguridad “appliance” de Next Generation.

Característica	Especificaciones técnicas mínimas requeridas
	La detección APT debe soportar la capacidad de inspeccionar y detectar malware tanto en tráfico IPv4 como IPv6.
	Debe tener la capacidad de detectar y bloquear patrones de conexiones a botnets y patrones de comportamiento
	El antivirus deberá hacer inspección y bloqueo de archivos transferidos
	Debe realizar las actualizaciones de antibot y antivirus en tiempo real.
	Inteligencia de seguridad en tiempo real mediante el uso de un repositorio que contenga las actualizaciones de firmas
	Prevención de daño por bloqueo de la comunicación entre los hosts infectados y el operador remoto.
	Inteligencia de seguridad en tiempo real mediante el uso de un repositorio que contenga las actualizaciones de firmas.
	Prevención de daño por bloqueo de la comunicación entre los hosts infectados y el operador remoto.
Característica	**Especificaciones técnicas mínimas requeridas**
Inspección de contenido SSL	Soporte de inspección de tráfico que este siendo cifrado mediante SSL
	Análisis de contenido cifrado para el tráfico que circula por la solución.
Alta disponibilidad	La solución deberá ofertarse en Alta disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.
	Capacidad de funcionar en Alta disponibilidad en modo Activo-Pasivo o en Activo-Activo
	Se debe garantizar que la conexión para sincronía se pueda realizar con la cantidad de interfaces necesarias que garantice el ancho de banda necesario que le de estabilidad al cluster
Virtualización	La solución ofertada deberá tener como mínimo 2 firewalls virtuales incluidos en clúster. Los cuales son: Firewall de Perímetro en HA y Firewall de Core en HA.
	El dispositivo deberá poder virtualizar los servicios de seguridad mediante firewalls virtuales, sistemas virtuales o dominios virtuales.
	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.

Característica	Especificaciones técnicas mínimas requeridas
	Cada firewall virtual deberá tener la posibilidad de administrarse por separado con usuarios, operadores y administradores por separado.
Cliente VPN	Se debe suministrar el software de cliente para VPN, sin costo
	La solución debe tener acceso para 500 usuarios de VPN desde dispositivos móviles, portátiles o equipos de escritorio.
	El cliente VPN debe estar en la capacidad de evitar la fuga de información del ANH. Esto implica que el cliente VPN debe evitar la descarga de información corporativa no autorizada.
	Debe poderse administrar el borrado remoto de los agentes configurados en los dispositivos móviles de los usuarios.
	El cliente VPN debe poder ser instalado en sistemas operativos Windows, MacOS, IOS, Android.
	En los casos en donde el cliente VPN sea instalado en dispositivos móviles (tabletas o telefónos inteligentes), debe estar en la capacidad de separar los datos de negocio de los personales.
Seguridad para dispositivos móviles	La solución deberá permitir la configuración de políticas basadas en dispositivo o usuario y la configuración de portal cautivo para manejar la seguridad de dispositivos móviles.

1.7.1.2 *Renovación licenciamiento Fortigates 310B (Fortinet)*

Elemento	Tipo	Descripción	Especificaciones Ofrecidas
Fortigate 310B **Cantidad: 2**	**Licencias**	Antivirus: Renovación hasta el 31 de Diciembre de 2016.	
		IPS & Application Control: Renovación hasta el 31 de Diciembre de 2016.	
		Web Filtering, Vulnerability Scan y Email Filtering: Renovación hasta el 31 de Diciembre de 2016.	

Elemento	Tipo	Descripción	Especificaciones Ofrecidas
	Soporte	Hardware hasta el 31 de Diciembre de 2016.	
		Firmware hasta el 31 de Diciembre de 2016.	
		Enhanced Support hasta el 31 de Diciembre de 2016.	
		Comprehensive Support hasta el 31 de Diciembre de 2016.	
		Soporte remoto 7X24 hasta el 31 de Diciembre de 2016.	
		Soporte en sitio 7X24 hasta el 31 de Diciembre de 2016.	
		Soporte de cambio de equipos por RMA 7X24 hasta el 31 de Diciembre de 2016.	
	Garantía	Garantía 7X24 tanto de Fábrica como del Proveedor hasta el 31 de Diciembre de 2016.	

1.7.1.3 *Adquisición de plataforma para almacenamiento de logs y generación de reportes*

Característica	Especificaciones técnicas mínimas requeridas
Generalidades	La solución propuesta deberá cumplir con las siguientes funcionalidades: - Sistema de Almacenamiento de Logs y Reportes para la solución de Seguridad Perimetral e Interna (Firewalls de Nueva Generación). - Deberá contar con Sistema operativo propietario. - Deberá contar con Interface de administración gráfica (GUI) o vía Web (HTTPS).
	- Deberá contar Interface de administración vía CLI (Línea de comando), vía ssh y consola serial. - Deberá tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas.

Característica	Especificaciones técnicas mínimas requeridas
Generación de reportes	Permitir la generación de reportes personalizados, permitiendo al administrador de la solución determinar el contenido de los reportes de la solución de seguridad perimetral e interna (Firewalls de Nueva Generación).
	Generar reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
	Generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
	Generar reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
	Permitir la generación de un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.
	Permitir la personalización de los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.
	Permitir la especificación del período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
	Generación de reportes en formato. PDF, .DOC, o HTML
	Opción de generar reportes en idioma inglés o en idioma español.
	Deberá permitir enviar el reporte vía correo electrónico.
	Deberá permitir hacer búsquedas por nombre de usuario o dirección IP, para que toda la información almacenada de dicho usuario o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.
Otras consideraciones	Almacenamiento incluido como mínimo de 1 TB.
	Mínimo cuatro (4) interfaces Ethernet 10/100/1000.
	El Equipo debe ser montable en rack.

1.7.1.4 *Renovación y adquisición de licenciamiento para suites EPA y TDA McAfee*

Tipo	Detalle	Cantidad

Renovación licenciamiento	Suite McAfee Total Protection Data – TDA.	370
Renovación licenciamiento	Suite McAfee Endpoint Protection Advanced - EPA	370
Licenciamiento nuevo	Suite McAfee Total Protection Data – TDA.	130
Licenciamiento nuevo	Suite McAfee Endpoint Protection Advanced - EPA	130

1.7.2 Soporte y Garantía:

Para suites EPA y TDA McAfee Estas licencias deben estar vigentes hasta el 31 de Diciembre de 2016 para soporte y garantía 7X24X365 tanto de Fábrica como del Proveedor.

1.7.2.1 Renovación de licenciamiento DAM (Database Activity Monitoring) de McAfee

Tipo	Detalle	Cantidad
Renovación licenciamiento por cantidad de instancias de BD.	MFE Database Activity Monitoring	16

Estas licencias deben estar vigentes hasta el 31 de Diciembre de 2016 para soporte y garantía 7X24X365 tanto de Fábrica como del Proveedor.

1.7.2.2 Renovación de licenciamiento SIEM de McAfee

Tipo	Detalle	Cantidad
Renovación licenciamiento	MFE Ent Sec Mgr 5600 1Yr GL+ARMA	1

Estas licencias deben estar vigentes hasta el 31 de Diciembre de 2016 para soporte y garantía 7X24X365 tanto de Fábrica como del Proveedor.

1.7.2.3 Renovación de licenciamiento MVM de McAfee

Tipo	Detalle	Cantidad
Renovación licenciamiento	MFE Vulnerability Mgr MVM3100Appl 1Yr GL+ARMA	1

Renovación licenciamiento	MFE Vulnerability Mngr EN SW 1YrGL	300

Estas licencias deben estar vigentes hasta el 31 de Diciembre de 2016 para soporte y garantía 7X24X365 tanto de Fábrica como del Proveedor.

1.7.2.4 Renovación de licenciamiento RSA Archer Incident Management Solution y Enterprise Management Solution

Tipo	Detalle	Cantidad
Renovación licenciamiento	RSA Archer - Incident Management Solution para 1500 usuarios	1
Renovación licenciamiento	RSA Archer - Enterprise Management Solution para 1500 usuarios	1

Estas licencias deben estar vigentes hasta el 31 de Diciembre de 2016 para soporte y garantía 7X24X365 tanto de Fábrica como del Proveedor.

1.7.3 Protección de Amenazas Avanzadas Persistentes (APTs)

Característica	Especificaciones técnicas mínimas requeridas
Cantidad	1
Interfaces 10/100/1000 RJ45	4
Interfaces 1GbE en Fibra	2
Fuentes de poder	Redundantes
Capacidad de almacenamiento	4 TB
Administración	Soporte de configuraciones a través de interfaz de línea de comando (CLI) e interfaz de usuario Web (WebUI).
	Notificación vía correo electrónico cuando se detecte un archivo malicioso.
Detección proactiva y mitigación	Ejecución de código malicioso en sistemas operativos virtualizados.
	Soporte de múltiples filtros antes de la ejecución en el OS Virtual.
	Los múltiples filtros deben incluir filtros de AV, queries a base de datos en la nube y simulación de código independiente del Sistema Operativo.

Característica	Especificaciones técnicas mínimas requeridas
	La solución debe estar en la capacidad de detectar los siguientes tipos de infección y ataques: o Gusanos o Botnet: Archivos que actuan como un cliente de una red Bot. o Hijack: Archivos que tratan de modificar registros para tener acceso al sistema. o Stealer: Archivos que tratan de substraer información confidencial. o Backdoor: Archivos que tratan de instalarse como servicios nuevos de red para permitir el acceso remoto. o Injector: Archivos sospechosos que inyectan código en los procesos del sistema. o RootKit: Archivos que tratan de esconcer su comportamiento funcionando en conjunto con procesos del sistema. o Adware: Archivos tratando de acceder a sitios web. o Troyanos: Archivos con un payload malicioso. o Riskware: Software que tiene posibles procesos que puedan poner en riesgo la infraestructura. o Greayware: Archivos con comportamiento similar al de virus o Dropper: Instalación de Software malicioso. o Downloader: Intento de descarga de software malicioso. o Riskware: Funciones críticas que representan amenazas. o Desconocidos: Ataques no conocidos o catalogados.
Visibilidad	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.
Protección avanzada de amenazas	Técnicas de Anti-evasión: Sleep Calls
	Detección de modificación de archivos, comportamiento de procesos, comportamiento de registros y comportamientos de red.
	Sanbox OS Virtual: Múltiples instancias de Windows.
	Tipos de Archivos: exe, dll, PDF, Javascript, Microsoft Office, Adobe Flash, Java Archives. En modo integrado debe poder analizar tar, gz, tar.gz, zip, bz2, tar.bz2, bz, tar.
	Protocolos/Aplicaciones: HTTP-HTTPS, SMTP-SMTPS, FTP, POP3, IMAP
	Debe ser posible enviar los archivos a análisis en la nube para análisis manual y creación de firmas.

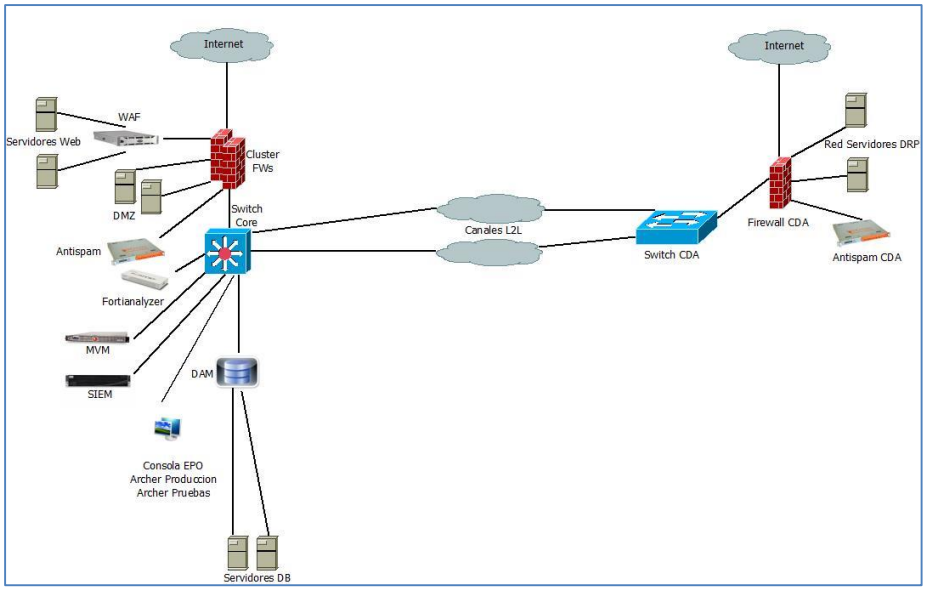
Característica	Especificaciones técnicas mínimas requeridas
	La solución debe incluir un módulo de webfiltering para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan.
	Los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características: o Descarga de Virus o Modificación de registro. o Conexiones externas a IPs maliciosas. o Infección de procesos.
	La solución debe estar en la capacidad de procesar múltiples archivos al mismo tiempo, se debe contar con múltiples VM para el análisis de Sandbox OS.
	La solución debe poder descargar de forma automática máquinas virtuales cuando estén disponibles.
	La solución debe estar en la capacidad de analizar sitios web.
	El resultado de los análisis 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.
	Debe ser posible habilitar el envió de notificaciones cada vez que el análisis detecte Malware.
	La solución debe actualizarse frecuentemente, igualmente debe estar la posibilidad de hacer consultas directas en tiempo real al laboratorio de investigación.
Modo de implementación	La solución debe poder ser implementada de una de las siguientes formas: o File Input: Debe ser posible manualmente hacer una subida de los archivos a analizar. o Sniffer: El equipo debe estar en la capacidad de recoger el tráfico de un puerto en modo espejo. o Integración con FW: En este modo la solución requerida deberá integrarse con las plataformas de firewall existentes en la Entidad.
	Se debe poder implementar en un ambiente distribuido donde múltiples dispositivos de seguridad perimetral le envían archivos para análisis.
	Soporte de rutas estáticas.

Característica	Especificaciones técnicas mínimas requeridas
Monitoreo y reportes	Monitoreo en tiempo real que contenga Top de hosts objetivo, Top de malware, Top de URLs infectadas y Top de dominios Callback.
	Generación de reportes para archivos maliciosos: Reportes detallados que incluyan modificación de archivo, comportamientos de proceso, comportamientos de registro y comportamientos de red.
	La solución debe entregar online información específica de los análisis realizados, esto debe ser sobre una interfaz gráfica con filtros predeterminados como eventos, malware, entre otros.
	La información del análisis debe poder ser descargada en un log para en posterior análisis.
	Debe ser posible descargar un archivo PCAP para revisar el comportamiento del archivo.

1.7.4 Compatibilidad

La siguiente grafica muestra la infraestructura actual de seguridad y de red que tiene la Agencia Nacional de Hidrocarburos:

1.7.5 Topología lógica:



2 INSTALACION DE HERRAMIENTAS

- El oferente debe acompañar al equipo técnico de la Agencia o a quienes ella delegue para que realice de manera adecuada la instalación de los elementos a contratar hasta que quede satisfactoriamente operativa.

- Deben entregarse a la Agencia, manuales, instructivos y en general documentación que facilite la administración y uso de las herramientas.

- Puesta en producción de la solución general, con pruebas de preproducción y producción.
- La cantidad de horas incluidas en la instalación será la necesaria para completar y probar el correcto funcionamiento de todas las herramientas sin costo adicional para la ANH.
- La instalación de los firewalls de nueva generación (NGFW) deberá comprender los siguientes puntos:
  - Creación y configuración de las políticas de seguridad acorde a los requerimientos de la ANH.
  - Creación y configuración de las VPN site to site que la ANH actualmente tiene con proveedores.
  - Creación y configuración de las VPN client-to-site.
  - Puesta en producción de todos los módulos de seguridad requeridos.

3 SERVICIOS DE IMPLEMENTACION, SOPORTE Y GARANTIA

3.1 Implementación:

- El proponente deberá realizar la instalación y configuración de los equipos por personal certificado por el fabricante.
- El proveedor debe entregar toda la solución (Hardware y Software) funcionando y con sus respectivas pruebas de aceptación.
- Los servicios de implementación deben ir acompañados de la metodología de gerencia de proyectos, por lo cual dentro del equipo de trabajo se debe entregar la Hoja de vida del gerente de proyecto con experiencia en proyectos de tecnología.
- El proponente debe entregar documentación técnica de los servicios de implementación.

- El proponente deberá incluir en su oferta los servicios de reconfiguración de los firewalls actuales de la Entidad para reacomodarlos en el Centro de Datos Alterno, realizando las debidas configuraciones requeridas a nivel de todas las políticas de seguridad. Para esto, el oferente deberá certificar (mediante certificación oficial del fabricante) que es canal autorizado del fabricante de estos firewalls garantizando así conocimiento en los servicios ofertados.
- Las soluciones de firewalls de nueva generación (NGFW), plataforma para almacenamiento de logs y generación de reportes y la herramienta para protección de APTs deben ser implementadas con la última versión de firmware estable liberada por el fabricante.

3.2 Soporte y Mantenimiento:

- El proponente deberá garantizar soporte remoto o en sitio cuando así se requiera con un esquema de atención 7 x 24 x 365
- El proponente deberá contar con una línea de soporte telefónico local para creación de casos y atención de requerimientos.
- El proponente debe tener una estructura de atención de incidentes que contemple los diferentes niveles de atención y escalamiento.
- El proponente deberá cotizar mantenimiento preventivo durante el desarrollo del contrato, dos mantenimientos anuales durante el desarrollo del contrato.
- El proponente deberá contar como mínimo con dos (2) ingenieros certificados de fabricante de la solución de seguridad a nivel Profesional.
- El proponente deberá notificar la liberación de nuevas versiones de firmware para mitigar vulnerabilidades y/o corregir bugs.
- Para las suites TDA y EPA y las soluciones DAM, SIEM, MVM de McAfee y RSA Archer Incident Management Solution y Enterprise Management Solution, el proponente debe realizar una visita de mantenimiento mensual por cada solución, en la cual se revise el estado de cada herramienta y se realicen mejoras a la operación de las mismas.

3.3 Garantía:

- Para todos los componentes de las soluciones: Garantía de soporte a 1 año o 3 años según se definió en el punto 1 (Especificaciones Técnicas).
- Para todos los elementos a adquirir y renovar: Actualización de software y firmware por 1 año o 3 años según se definió en el punto 1 (Especificaciones Técnicas).

- Para todos los componentes de las soluciones: Soporte telefónico de fabricante y en sitio de parte del proponente cuando se requiera durante 1 año o 3 años según se definió en el punto 1 (Especificaciones Técnicas).
- El proponente debe contar con la autorización del fabricante para comercializar y dar soporte del software y/o appliances ofrecidos.

4 CAPACITACIÓN

- El proponente deberá incluir dentro de su oferta, transferencia de conocimiento, capacitación básica y avanzada para las soluciones ofertadas de Firewalls de nueva generación (NGFW), plataforma para almacenamiento de logs y generación de reportes y la herramienta para protección de APTs para mínimo dos funcionarios de la ANH.
- Los cursos deberán ser dictados por personal certificado en las herramientas.

5 CUADRO PROPUESTA ECONOMICA

ITEM	DESCRIPCIÓN	VALOR UNITARIO	CANTIDAD	SUBTOTAL	IVA	TOTAL
1	Adquisición de NGFW (Next Generation Firewall)		2			
2	Renovación licenciamiento Fortigates 310B (Fortinet)		2			
3	Adquisición de plataforma para almacenamiento de logs y generación de reportes		1			
4	Renovación licenciamiento Suite McAfee Total Protection Data - TDA		370			
5	Renovación licenciamiento Suite McAfee Endpoint Protection Advanced - EPA		370			
6	Adquisición de licenciamiento Suite McAfee Total Protection Data - TDA		130			
7	Adquisición de licenciamiento para Suite Endpoint Protection Advanced - EPA		130			
8	Renovación de licenciamiento DAM (Database Activity Monitoring) de McAfee		16			
9	Renovación de licenciamiento SIEM de McAfee		1			
10	Renovación de licenciamiento MVM de McAfee		1			
11	Renovación de licenciamiento RSA Archer Incident Management Solution y Enterprise Management Solution		1			
12	Protección de Amenazas Avanzadas Persistentes (APTs)		1			
13	Servicios de Implementación, Soporte y Garantía		1			
14	Capacitación		1			
					TOTAL ITEMS	