SONDEO DE MERCADO para "Fortalecer la Infraestructura de Seguridad Informática, para la protección de los sistemas de información y redes de la ANH "– ANH-2015.

TABLA DE CONTENIDO

1 SONDEO DE MERCADO.

1.1 Objeto

Fortalecer la Infraestructura de Seguridad Informática, para la protección de los sistemas de información y redes de la ANH.

1.2 Lugar de Ejecución

El lugar de ejecución será 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 Piso 2.

1.3 Plazo de Ejecución

El tiempo de ejecución estimado del contrato es desde la firma del Acta de inicio hasta el 31 de diciembre de 2015.

1.4 Especificaciones Técnicas

1.4.1 Solución de Firewall de Nueva Generación.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) FIREWALL DE NUEVA GENERACION
1	**Generalidades.** Adquisición de un sistema de seguridad informática perimetral e interna que sea del tipo Firewall de Nueva Generación, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente documento. • Solución en alta disponibilidad, dos equipos de la misma referencia funcionando en modo clúster. • 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.

	• El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. • El equipo debe entregar en tiempo real estadísticas de usuarios, aplicaciones, seguridad. Debe ser posible tener en formato de drilldown este tipo de información donde sea posible por usuario verificar que aplicaciones, sitios, categorías y amenazas de seguridad se han tenido en un tiempo de 24 horas. • El equipo deberá integrarse de forma nativa con la solución de sandbox, sin requerir desarrollos adicionales. • La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante.
2	**Rendimiento** El equipo deberá cumplir con las siguientes características MINIMAS de desempeño ya activas y funcionales: • Rendimiento de Firewall 74 Gbps • Rendimiento de IPS 11 Gpps • Rendimiento IPSec VPN 45 Gbps • Rendimiento Antivirus de 4 Gbps • Soporte de 10.000.000 sesiones concurrentes • Soporte de 90.000 políticas • Soporte a 9.500 usuarios VPN
3	**Conectividad** El equipo deberá contar con las siguientes interfaces de conexión, totalmente aprovisionadas: • 16 interfaces de 1Gbps SFP • 16 interfaces de 1Gbps RJ45 • 8 interfaces de 10Gbps SFP+
4	**Address Traslation** • NAT y PAT • NAT estático • NAT: destino, origen

	• NAT, NAT64 persistente
5	**Funciones básicas de Firewall** • Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. • La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios. • La solución soportará políticas basadas en dispositivo. Esto Significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (movil, laptop) que tenga el usuario. Esta característica no requerirá ningún tipo de licenciamiento adicional. • Debe ser posible hacer políticas basados en usuarios, grupos de usuarios y dispositivos sobre una misma política, de esta forma se lo mas granular posible en la definición de políticas. • Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. • Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). • La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP. • El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. • El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico • Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
6	**Conectividad y Enrutamiento** • Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. • Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. • Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas. • Soporte a políticas de ruteo (policy routing)

	• Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP • Soporte a ruteo dinámico RIPng, OSPFv3 • Soporte de ECMP (Equal Cost Multi-Path) • Soporte a ruteo de multicast PIM SM y PIM DM. • La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow. • La solución podrá habilitar políticas de ruteo en IPv6 • La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
7	**VPN IPSEC** El equipo deberá soportar las siguientes características: • Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) • Soporte para IKEv2 y IKE Configuration Method • Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES • Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits • Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14. • Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. • Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. • La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) • En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
8	**VPN SSL** • Capacidad de realizar SSL VPNs sin necesidad de licenciamiento por usuarios. • Soporte a certificados PKI X.509 para construcción de VPNs SSL. • Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.

	• Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos o basados en software.
	
	• Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
	
	• Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
	
	• Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)
	
	• La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS
	
	• Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
	
	• Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
	
	• Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
	
	• Los portales personalizados deberán soportar al menos la definición de:
	
	  • Widgets a mostrar
	  • Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC
	  • Soporte para Escritorio Virtual
	  • Política de verificación de la estación de trabajo
	
	• La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.

9	**Autenticación** El dispositivo deberá manejar los siguiente tipos de autenticación: • Capacidad de integrarse con Servidores de Autenticación RADIUS. • Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”. • El oferente deberá incluir como mínimo un sistema de autenticación de doble factor, el cual cuente con 100 tokens **FISICOS** los cuales deben incluirse en la oferta para los

	usuarios que la entidad designe. • Soporte de Token Físicos o mobile sobre smartphone basado en IOS o Android.
10	**Manejo de tráfico y calidad de servicio.** • Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall • Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión • Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. • Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo • Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo
11	**Antimalware** • Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP. • El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. • El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión. • El Antivirus deberá integrarse de forma nativa con el sandbox, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. • Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. • El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. • La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso. • El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por

	mensajería instantánea (Instant Messaging). • La solución debe soportar la integración con soluciones de Sandbox. • La solución deberá integrarse de forma nativa con la solucion de sandbox local, si la necesidad de desarrollos adicionales o licencias adicionales. • La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.
12	**Filtrado WEB** • Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 47 millones de sitios web en la base de datos. • Debe poder categorizar contenido Web requerido mediante IPv6. • La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • La solución de Filtraje de Contenido debe soportar el forzamiento de “Safe Search” o “Búsqueda Segura” independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing. • Será posible exceptuar la inspección de HTTPS por categoría. • Debe contar con la capacidad de implementar el filtro de Educación de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube, bloqueando cualquier tipo de contenido no Educativo. • El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido. • La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios. • La solución debe estar en la capacidad de filtrar el acceso a cuentas de google, permitiendo acceso solo a cuentas corporativas de google. • El filtrado debe ser sobre tráfico http y https.

13	**Protección contra intrusos (IPS)** • El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. • Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores. • Capacidad de detección de más de 4000 ataques. • Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas) • El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. • El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / Rate base). • Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo. • Actualización automática de firmas para el detector de intrusos • El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios. • Métodos de notificación: o Alarmas mostradas en la consola de administración del appliance. o Alertas vía correo electrónico. o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. o Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

14	**Control de Aplicaciones** • Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto 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 ya definidas por el fabricante. • El listado de aplicaciones debe actualizarse periódicamente. • Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log, resetear conexión y hacer traffic shapping. • Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. • Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. • Preferentemente deben soportar mayor granularidad en las acciones. • Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.
15	**Inspección de Contenido SSL/SSH** • La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3. • Debe ser posible definir perfiles de inspección SSL donde sea posible definir los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. • Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad. • La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. • Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. • El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS

	• Debe ser posible inspeccionar tráfico SSH funcionalidades como Port-Fortward o X11.
16	**Alta Disponibilidad** • La solución deberá ofertarse en alta disponibilidad • El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 • Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. • Posibilidad de definir al menos dos interfaces para sincronía • El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red • Será posible definir interfaces de gestión independientes para cada miembro en un clúster. • Debe ser posible definir que Firewall Virtual estará activo sobre que miembro del Cluster para hacer una distribución de carga en caso se der necesario. • El equipo debe soportar hasta 4 equipos en esquema de HA.
17	**Visibilidad** La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. • Menú tipo dropdown para navegar por la información. • Visualización de las sesiones top 100 • Mostrar los origenes del tráfico o usuarios que lo generan. • Mostrar las aplicaciones y su categorización según riesgo. • Visibilidad de aplicaciones Cloud usadas por el usuario. • Visibilidad de Destinos del tráfico. • Visibilidad de los sitios web mas consultados por los usuarios. • Visibilidad de las amenazas o incidentes que han ocurriendo en la red • En la información de sources, aplicaciones, navegación debe ser posible con un doble-click

	filtrar la información para ser más específica la búsqueda. • Se debe ver aplicaciones, sitios, amenazas por cada usuario. • Se debe ver el tiempo de navegación por cada sitio o categoría de sitios. • De las aplicaciones Cloud que permitan compartir archivos como Dropbox debe ser posible ver que archivos fueron subidos y descargados por los usuarios. • De aplicaciones de contenido como youtube debe ser posible ver que videos fueron vistos por los usuarios.
18	**Características de Administración** • Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS) • Interfase basada en línea de comando (CLI) para administración de la solución. • Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. • Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH) • El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. • Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. • El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS. • El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. • Soporte de SNMP versión 2 • Soporte de SNMP versión 3 • Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos • Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para

	administración y monitoreo del Firewall. • Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red. • Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. • Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. • Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard). • Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa. • Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.
19	**Virtualización** • El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains” • La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS. • Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer, de los cuales se deberán configurar como mínimo tres acorde a los requerimientos de la entidad. • Cada instancia virtual debe poder tener un administrador independiente • La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. • Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red • Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual • Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.

	• Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. • Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente • Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.

1.4.2 Solución Plataforma de LOGS y Reportes.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) PLATAFORMA DE LOGS Y REPORTES
1	**Generalidades** Se requiere un equipo tipo *appliance* de proposito especifico que permita registrar cada transacción de la plataforma de seguridad perimetral de la entidad, para poder identificar y reaccionar a cualquier informe emitido por un log o registro de los firewalls de perímetro de la red. Tanto el software como el hardware debera ser del mismo fabricante. El equipo deberá recolectar y emitir el reporte de eventos, actividades y tendencias ocurridas en los Actuales Firewalls de aplicaciones Web, los firewalls actuales de la entidad y la plataforma de firewalls de nueva generación ofertada. La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante.
2	**Desempeño** La solución de análisis de logs debe dar soporte a las siguientes características: ▪ Capacidad de recibir hasta 70 Gbytes de logs diarios. ▪ Capacidad de Almacenamiento de 7 Terabytes ▪ 6 interfaces de red de 1000 Mbps Cobre ▪ 2 interfaces de red de 1000 Mbps SFP ▪ Capacidad de recibir logs hasta de 2000 equipos sin necesidad de licenciar ▪ Los discos deben soportar arreglos de RAID 0/1/5/10

3	**Funciones y configuraciones requeridas para el analizador de red** ▪ Visor de tráfico en tiempo real. ▪ Visor de tráfico histórico. ▪ Visor personalizado de log de tráfico ▪ Herramienta de búsqueda sobre los logs de tráfico.
4	**Análisis de logs y reportes requeridos** ▪ Vista de búsqueda y manejo de logs. ▪ Reportes basados en perfiles. ▪ Inventario de plantillas predefinidas para reportes regulares. ▪ Debe soportar de forma predefinida los reportes: ○ Eventos del sistema ○ Análisis de riesgo y aplicaciones ○ Reporte de Aplicaciones y Ancho de Banda ○ Reputación de Clientes ○ Análisis de seguridad ○ Reporte de Amenazas ○ Reportes de VPN ○ Reportes de uso de Web ▪ Debe ser posible calendarizar los reportes ▪ La plataforma deberá permitir integrar los logs de las plataformas de Firewall actuales de la entidad, los web application firewalls actuales y los firewalls de nueva generación ofertados.

1.4.3 Solución de Protección para Amenazas Avanzadas SandBox

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) PROTECCION CONTRA AMENAZAS AVANZADAS – SANDBOX
1	**Generalidades** Adquisición de un sistema de protección proactiva y mitigación de amenazas avanzadas y persistentes que permita la utilización de mecanismos combinados para la detección de virus, virus polimórficos y otras amenazas avanzadas. La solucion debera ser tipo appliance de proposito especifico. 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 no debe ser de tipo inline, no se acepta ninguna solución que agregue más puntos de falla y latencia en la red.

	La solución deberá ser 100% compatible con las plataformas de firewalls de aplicaciones web de la entidad y con la plataforma de firewalls de nueva generación ofertada y deberá integrarse de forma nativa con las mismas, por lo cual no requerirá de desarrollo adicional alguno. La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante

2	**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, Consultas a base de datos en la nube y simulación de código independiente del Sistema Operativo.
	• La solución debe estar en la capacidad de detectar los siguientes tipos de infección y ataques:
	  ○ Gusanos
	  ○ Botnet: Archivos que actúan como un cliente de una red Bot.
	  ○ Hijack: Archivos que tratan de modificar registros para tener acceso al sistema.
	  ○ Stealer: Archivos que tratan de substraer información confidencial.
	  ○ Backdoor: Archivos que tratan de instalarse como servicios nuevos de red para permitir el acceso remoto.
	  ○ Injector: Archivos sospechosos que inyectan código en los procesos del sistema.
	  ○ RootKit: Archivos que tratan de esconcer su comportamiento funcionando en conjunto con procesos del sistema.
	  ○ Adware: Archivos tratando de acceder a sitios web.
	  ○ Troyanos: Archivos con un payload malicioso.
	  ○ Riskware: Software que tiene posibles procesos que puedan poner en riesgo la infraestructura.
	  ○ Greayware: Archivos con comportamiento similar al de virus

3	**Visibilidad** • Toda la clasificación (Maliciosos, alto, medio, bajo riesgo) deben ser presentados en un dashboard intuitivo. • Debe presentarse información completa del analisis de amenazas del ambiente virtual incluyendo Actividades del sistema, accion del exploit, trafico web, intentos de

	comunicación entre otros.
4	**Protección Avanzada de Amenazas:** • Técnicas de Anti-evasión: Sleep Calls • Detección de modificación de Archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red. • OS Virtuales (Sandbox): Múltiples instancias de Windows XP y Windows 7. Es de vital importancia para la entidad que estas máquinas virtuales vengan licenciadas por Microsoft. • Las máquinas virtuales deberán crearse de forma automática en el sandbox y no requerir licenciamiento de ningún Hipervisor para la creación de las mismas. • Tipos de Archivos: exe, dll, PDF y Javascript. En modo integrado debe poder analizar tar, gz, tar.gz, zip, bz2, tar.bz2, bz, tar. • Protocolos/Aplicaciones: o Modo Sniffer – http, ftp, pop3, imap, smtp. o Modo integrado con solución de seguridad perimetral*: http, smtp, pop3, imap, mapi, ftp, im y sus equivalentes en SSL. • Debe ser posible enviar los archivos a análisis en la nube para análisis manual y creación de firmas. • Tamaño de Archivo sin límite, este valor debe poder ser configurable. • 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.

	• 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.
5	**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 el Next Generation Firewall: En este modo la solución debe integrarse con el Firewall de la entidad para que este le envié archivos sospechosos para el análisis. o Integración con el Web Application Firewall: En este modo la solución debe integrarse con el Firewall de aplicaciones web de la entidad de la entidad para que este le envié archivos sospechosos para el análisis. o Escaneo por demanda: En este modo la solucion debe poder escanear carpetas compartidas para analisis de archivos sospechosos. • Se debe poder implementar en un ambiente distribuido donde múltiples dispositivos de seguridad perimetral le envían archivos para análisis. • Soporte de rutas estáticas. • Autorización de dispositivos que quieren enviar archivos para análisis.
6	**Especificaciones:** • 6 Interfaces 10/100/1000 y 2 puertos GbE SFP. • 4 TB de capacidad de disco con capacidad de crecer a 8 TB. • Fuentes de poder redundantes. • El equipo debe soportar múltiples archivos simultáneos en análisis.

	• Se deben soportar al menos 8 máquinas virtuales. • Debe escanear como minimo 150 archivos/hora en el sandbox • Debe escanear como minimo 5000 archivos /hora en el antimalware
7	**Generación de Reportes:** • Reportes detallados en características y comportamiento. Modificación de archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red. • Debe tener reportes en línea en tiempo real, esta debe poder ser personalizable con widgets que se puedan agregar o quitar. • Se deben presentar estadísticas de TOP N, con datos de los hosts atacados, malware, URLs, Call Back Domains. • Estás estadísticas pueden ser vistas en línea con la posibilidad de seleccionar el período de tiempo que se quieren ver. • La solución debe estar en la capacidad de enviar reportes semanalmente. • 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.

1.4.4 Solución de Análisis de Vulnerabilidades y Monitoreo de Base de Datos.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) ANALISIS DE VULNERABILIDADES Y MONITOREO DE BASES DE DATOS
	Generalidades. Adquisición de un sistema de seguridad informática tipo appliance de proposito especifico la cual permita el monitoreo de actividad en las bases de datos de la entidad. 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 plataforma debera poder implementarse al menos en 3 modalidades para la recolección de datos: Sniffer, Nativo y por Agente

	La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante
	Desempeño y Conectividad. • Capacidad mínima de almacenamiento incluida 4TB • Número de Instancias de Bases de Datos: 90 • Conectividad con interfaces Cobre 10/100/1000: 4 • Conectividad con interfaces SFP 10/100/1000: 2
	Licenciamiento. • Incluye licencias para gestionar al menos 90 instancias de bases de datos.
	Soporte de Motores de Bases de Datos Debe poseer soporte para los siguientes motores de bases de datos: • DB2 UDB V8 (Solo VA) • DB2 UDB V9.x (Solo VA) • DB2 UDB V9.5 • MS SQL Server 2000 • MS SQL Server 2005 • MS SQL Server 2008 • MS SQL Server 2012 • MySQL 5.1 • Oracle 9i • Oracle 10 gR1 (Solo VA) • Oracle 10gR2 • Oracle 11g • Sybase ASE 12.5 (Solo VA) • Sybase ASE 15.x
	Análisis de Vulnerabilidades • Debe ser capaz de realizar análisis de vulnerabilidades sobre motores de bases de datos por medio de

	la red, sin la instalación de un agente o alteración en la estructura de la instancia de base de datos • Las políticas de análisis de vulnerabilidades deberán poder ser personalizadas una a una y pueden ser usados en grupos • Las políticas de análisis de vulnerabilidades pueden ser creadas desde cero mediante la construcción de sentencias SQL definidas por el administrador • Los análisis de vulnerabilidades deben tener la capacidad de ser programados a criterios del administrador de la solución. • Los análisis de vulnerabilidades deben tener la capacidad de notificar automáticamente a su administrador de acuerdo a la sección "Notificaciones y Gestión" de este documento • Los análisis de vulnerabilidades deben reportar los hallazgos basados en los siguientes criterios : Severidad (Alto, medio, bajo e informativo) y Clasificación (Host, Base de Datos, Privilegios, Contraseñas, configuración e Informativo) • Los análisis de vulnerabilidades relacionados con vulnerabilidades públicas, deben hacer referencia a bases de datos de públicas como lo son CVE u otras del mercado • Los análisis de vulnerabilidades deben reportar un resumen de los privilegios que se encuentran asignados en la instancia. Estos resúmenes deben proporcionar un listado completo de usuarios y roles descubiertos • La solución debe estar en la capacidad de descubrir de manera automática, los diferentes motores de bases de datos instalados en la red
	Monitoreo y Auditoria • Debe poseer la capacidad de realizar labores de monitoreo y auditoria sobre los motores de bases de datos mediante el uso de trazas o auditoria nativa. • Soporte para monitorear ambientes virtualizados • Debe poseer la capacidad de auditar sentencias DCL, DML y DDL • Debe ser capaz de rastrear datos sensibles: IFE, Número de Seguro Social, Número de Tarjetas de Crédito. • La solución debe ser capaz de generar políticas "Out of the box" para usuarios privilegiados, y el diseño y cambio de esquemas • Debe poseer a capacidad de hacer monitoreo y auditoria sobre los motores de bases de datos soportados y ser capaz de obtener la siguiente información sobre lectura, escritura y acceso de los siguientes objetos al interior de la instancia de base de datos: ✓ Aliases ✓ Packages ✓ Routines ✓ Stored Procedures ✓ Synonyms ✓ Tables ✓ Tablespaces ✓ Triggers ✓ Indexes

- ✓ Views
- ✓ Events
- ✓ Profiles
- ✓ Role Privileges
- ✓ Roles
- ✓ Procedures
- ✓ System Privileges
- ✓ Table Privileges
- ✓ Column Privileges
- ✓ Member Privileges
- ✓ Object Privileges
- ✓ Server Roles
- ✓ Database Privileges
- ✓ Index Privileges
- ✓ Package Privileges
- ✓ Schema Privileges
- ✓ Table and View Privileges
- ✓ Tablespace Privileges
- ✓ User Privileges
- ✓ SYS User Operation

• Debe poseer la capacidad de general alertas que puedan ser revisadas por el administrador. Estas alertas deben contener al menos tres (3) estados diferentes que permitan indicar si el evento ya ha sido notificado al administrador, si no se ha notificado o si es un problema resuelto.

Cada alerta debe contener al menos los siguientes campos:

- ✓ Nombre del Target (Host que tiene la instancia)
- ✓ Nombre de la Política
- ✓ Reglas que fueron Violadas

	✓ Severidad ✓ Acción ✓ Usuario del Sistema Operativo ✓ Usuario de Base de Datos ✓ Login ✓ Objeto usado ✓ Consulta SQL utilizada ✓ Lugar (IP /Host) ✓ Hora ✓ Aplicación Usada ✓ Las alertas pueden ser agrupadas a visualizadas a criterio del administrador • La solución de monitoreo y auditoria debe contar con al menos los siguientes tipos de grupos de alertas generados de fábrica: ✓ Alertas conocidas ✓ Alertas de errores corregidos ✓ Alertas Criticas ✓ Cambios en Metadatos (schemas) ✓ Cambios de Privilegios ✓ Violaciones de Seguridad ✓ Cambios en Tablas ✓ Alertas no conocidas

1.4.5 Solución contra Ataques de Denegación de Servicio Distribuido (DDoS).

Ítem	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)** **SOLUCION CONTRA ATAQUES DE DENEGACION DE SERVICIO DISTRIBUIDO (DDoS).**
1	**Generalidades.**

	Se requiere un sistema de seguridad informática para Controlar los ataques de denegación de servicio distribuido que puedan ser realizados contra la infraestructura de seguridad perimetral de la entidad, mediante una plataforma de propósito específico y diversos sistemas de filtrado e establecimiento de umbrales, geolocalización y demás características de funcionamiento solicitadas en el presente documento. • Todos los componentes del sistema: procesador, tarjeta principal y en general el conjunto electrónico debe ser propósito específico. • Para el sistema de contención de ataques, NO se aceptan sistemas de propósito general (PCs o servidores) 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 plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante.
2	**Rendimiento** La solución de contención y mitigación de ataques de denegación de servicio distribuido deberá contar con las siguientes características de rendimiento: • Desempeño (FullDuplex): 2 Gbps • Capacidad de virtualización para separar el appliance en mínimo 3 dispositivos lógicos con la misma granularidad. • Conexiones simultaneas en la plataforma AntiDDoS: 1 Millón • Tiempo de respuesta en mitigación de ataques: Menor a 2 Seg • Orígenes Simultáneos: 1 Millón • Latencia menor a 50 microsegundos
3	**Conectividad** El equipo deberá contar con las siguientes interfaces de conexión: • Mínimo 8 interfaces (con posibilidad de bypass) 10/100/1000 cobre, para proteger como mínimo 4 segmentos de red.
4	**Características de Funcionamiento** • Proporcionar una solución de propósito específico y dedicado para la entidad la cual permita el aseguramiento del acceso desde internet hacia la infraestructura pública del ministerio, contra ataques especializados de Denegación de Servicio Distribuido. • Esta solución deberá ser un hardware de propósito específico basado en tecnología ASIC. • Debe permitir como mínimo configurar 7 instancias virtuales las cuales permitan establecer políticas de seguridad totalmente diferentes para cada una de las instancias de tal forma que se puedan establecer diferentes niveles de seguridad acorde a cada área de red asegurada. • Deberá garantizar que se comporta como un bridge capa 2 el cual no deberá realizar ningún tipo

	de modificación en los paquetes, la IP o las MAC involucradas en la transmisión de los datos.
5	**Métodos de detección y contención de ataques.** • Filtrado granular capa 3, capa 4 y capa 7. • Protección basada en geolocalización • Listas de control de acceso, IP´s y puertos permitidos • Filtrado algorítmico • Verificación de protocolos • Mitigación packet flood • Statefull packet inspection • Filtrado Out of state • Capacidad de auto aprendizaje para adaptar políticas basadas en comportamiento. • Determinación heurística de tráfico malicioso tipo Botnet. • Soporte de controles de mitigación de SYN Flood por Servicio o VID. • Control de estado TCP por servicio o VID y globales. • Control de sobrecarga de conexiones sobre los servidores. • Controles heurísticos en capa 7.
6	**Soportar los siguientes mecanismos.** • Reconocimiento de anomalías. • Filtrado de ataques ocultos. • Protección de sobre flujo de 256 protocolos. • Excesivas conexiones TCP por destino. • Sobreflujo de SYN. • Sobreflujo de cookies. • Protección contra ataque LAND. • Combinación invalidad de banderas TCP. • Prevención de escaneo Dark Address • Verificación de encabezado incorrecta • Sobreflujo de Hosts • Anomalias de transición de estado • Versión invalidada de HTTP • Soportar el ajuste de los siguientes umbrales: ○ Paquetes fragmentados

	○ Máximos paquetes por origen ○ Protocolo ○ TOS ○ Syn Packets ○ ACK Packets ○ Sesiones TCP Simultaneas ○ Nuevas conexiones TCP por segundo. ○ ICMP por tipo y codigo
7	**Administración y Operación.** • Esta solución deberá contar con Interface gráfica de usuario (GUI), vía HTTP y HTTPS para hacer administración de las políticas de seguridad establecidas para la solución. • Para poder garantizar la disponibilidad del servicio ante fallos la plataforma debe contar internamente con Bypass Incorporado. • Reportes con estadísticas como top de ataques, top de atacantes, top de puertos TCP y UDP atacados, etc.

1.4.6 Solución de Administración centralizada de Firewalls.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) SOLUCION DE ADMINISTRACION CENTRALIZADA DE FIREWALLS PERIMETRALES
1	**Generalidades.** Se requiere una solución para la centralización de Configuración y monitoreo de todos los firewalls de nueva generación, así como todas sus funciones de protección de red. Por seguridad y eficiencia, debe ser un “appliance” físico de propósito específico para el gerenciamiento de la seguridad. No se aceptan plataformas basadas en sistemas operativos genéricos y/o hardware genérico. Se requiere que la solución ofertada administre los firewalls actuales de la entidad y los firewalls de nueva generación ofertados.

	Deberá permitir la administración de dispositivos firewalls físicos y virtuales. La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante.
2	**Desempeño** La solución de administración centralizada debe dar soporte a las siguientes características: • Capacidad de administrar hasta 30 equipos. • Capacidad de Almacenamiento de hasta 1 Terabytes • 4 interfaces de red de 1Gbps RJ45
3	**Funcionalidades** • Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos. • Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido. • Las comunicaciones entre la consola de administración y los dispositivos administrados deben ser cifradas (Encriptadas). • La interface de administración es basada en Web Seguro (HTTPS). • Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución. • Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura. • Configuración basada en scripts para una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados. • Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras. • Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos. • Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los firewalls de nueva generación. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a

	lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red. • Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo. De esta forma, se disminuye la posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados. • Capacidad de ejecución de scripts para automatización en el aprovisionamiento de dispositivos, políticas, etc. • La solución deberá proveer opciones de integración mediante APIs (XML, JSON) para la definición y personalización de entornos anexos. • Posibilidad de administrar el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos administrados por la consola, reduciendo tiempos de operación y administración del personal que administra los equipos de seguridad. • La consola de administración debe soportar la configuración en Alta Disponibilidad, de tal forma que en caso de falla pueda existir otro equipo en línea que tome las tareas del equipo dañado con una pérdida mínima en la disponibilidad del servicio. • Capacidad de creación y aplicación de configuraciones de VPN entre los dispositivos de seguridad administrados. • Debe soportar al menos 20 modelos diferentes de dispositivos o firewalls. Y especificamente debera ser totalmente compatible con los firewalls actuales de la entidad y los firewalls de nueva generacion ofertados. • Cuando se requiera, deberá poder gestionar de forma independiente o integrada puntos de acceso inalámbricos asociados a los controladores gestionados.
4	**Monitoreo y Reporteria** • Deberá incluir un subsistema de Monitoreo en Tiempo-Real, Esto permite al equipo de monitoreo y administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados. • Deberá incluir un sistema de reportes integrado con al menos los siguientes reportes predeterminados: o Logins y eventos de administración. o Anchos de Banda y aplicaciones.

	○ Reputación de clientes. ○ Reportes por usuario. ○ VPN. ○ Redes inalámbricas. ○ IPS. ○ Amenazas. • Deberá incluir un completo sistema de reportes personalizables pudiendo realizar consultas complejas a la base de datos de registro de logs. • Debe poderse integrar de forma nativa con la actual plataforma de logs de la entidad. • Subsistema de monitoreo especial para los túneles de VPN de tal forma que el área de operación puede monitorear desde una sola pantalla el estado de todos los túneles de VPN establecidos, administrados y operados desde la consola de administración. • Deberá soportar automatización y calendarización en la ejecución de reportes. • Deberá contar con un panel de monitoreo en tiempo real para las siguientes opciones: ○ Orígenes. ○ Aplicaciones. ○ Destinos. ○ Sitios Web. ○ Amenazas. ○ Eventos de sistema. ○ VPN (SSL / IPSEC).

1.4.7 Puntos de Acceso WIFI para Integrar a la Plataforma de Firewall.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) SOLUCION DE RED INALAMBRICA.
2.1	**Generalidades.**

	Se requieren 10 equipos que sirvan de puntos de acceso inalámbrico para la sede principal de la entidad. Los equipos físicamente deberán tener presentación para interiores y deberán unirse sin inconvenientes de compatibilidad a las redes LAN de la entidad. Igualmente los equipos deberán 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 deberán ser administrados de forma centralizada a través de la solución de seguridad perimetral ofertada. La solución de red inalámbrica deberá permitir la implementación de un portal cautivo sin necesidad de equipos o software adicional. La solución de red inalámbrica ofertada deberá 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 deberá permitir establecer políticas de seguridad para acceso a la red basadas en dispositivo, sistema operativo o control por MAC. La solución deberá contar con Extensiones Multimedia Wireless la cual permita control de aplicaciones y uso de ancho de banda. La solución deberá contar con el aprovisionamiento automático de recursos de radio para optimización de rendimiento. La solución deberá 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 deberá poderse configurar como monitor del espectro en búsqueda de access points intrusos La solución deberá tener la capacitadad 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 deberá estar incluido en la oferta.
2.8	**SSID.** Los equipos deberán soportar hasta 14 SSIDs para el acceso de los clientes
2.9	**Seguridad.** El equipo deberá 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 deberán 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 deberán contar con sus aditamentos y componentes físicos para su fácil la instalación.
2.14	**Módulo de invitados.** Los equipos deberán 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

1.4.8 Alta disponibilidad para el Firewall de Aplicaciones WAF actual de la Entidad.

Ítem	**Requerimiento Técnico Mínimo (de obligatorio cumplimiento)** **ALTA DISPONIBILIDAD PARA EL WAF ACTUAL DE LA ENTIDAD**
1	• Instalación, Implementación y puesta en operación de la alta disponibilidad del actual firewall de aplicaciones web de la entidad Fortinet FortiWeb 3000D, la cual se deberá dejar integrada y funcional a la plataforma de logs y a la solución de sandbox. • El oferente deberá entregar la plataforma para la alta disponibilidad del actual firewall de la entidad Fortinet FortiWeb 3000D por un periodo de 3 años en un esquema 7 x 24 ante fabricante. • El oferente deberá presentar certificado de distribuidor autorizado donde se evidencie que es partner del fabricante de las plataformas actuales de la entidad y se evidencie la plataforma ofertada.

1.4.9 Renovación del Licenciamiento de la Plataforma de Seguridad Actual de la Entidad hasta el 31 de Diciembre de 2018.

Ítem	Requerimiento Técnico Mínimo

1	• Instalación, Implementación y puesta en marcha de las renovaciones requeridas.
	• El oferente deberá entregar las renovaciones de las siguientes plataformas identificadas con los siguientes seriales:
	  • FV3KD3R13800021
	  • FG300B3911600483
	  • FG300B3911600570
	• Las renovaciones son requeridas hasta el 31 de Diciembre de 2018 en un esquema 7 x 24 ante fabricante para los seriales mencionados.

1.4.10 Servicios profesionales para la implementación, transferencia de conocimiento y soporte especializado de la solución por 3 años.

Ítem	Requerimiento Técnico Mínimo (de obligatorio cumplimiento) SERVICIOS PROFESIONALES Y DE SOPORTE

1	• Instalación, Implementación y puesta en marcha de las soluciones ofertadas.
	• El oferente deberá entregar los equipos en el sitio indicado por la entidad, Bogotá DC.
	• Todas las plataformas ofertadas deberán ser del mismo fabricante.
	• El oferente deberá realizar la instalación y configuración de los equipos con personal certificado en un nivel profesional.
	• La implementación de todas las plataformas deberá 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. • Análisis de Vulnerabilidades, sobre los diferentes ambientes (Internet, redes internas, redes remostas), que garanticen que la solución implementada, cumple con las condiciones de seguridad para las Aplicaciones y redes de la Entidad.
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	Los dispositivos ofertados deben quedar integrados a la plataforma de reportes y logs suministrada, en la cual se realizarán las configuraciones de los informes de acuerdo a las necesidades de la entidad.
4	El oferente deberá 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	Las soluciones deberan ser implementadas y puestas en producción bajo esquemas de alta disponibilidad (en las plataformas que apliquen) y stand alone en las plataformas que no las requieran.
6	La entidad requiere la implementación y puesta en marcha de la plataforma de protección SandBox, e integrar la misma a la solución de NGFW y Firewall de aplicaciones web de forma nativa, así como realizar pruebas de detección para validar su correcta configuración.
	Para la Instalación de los puntos de acceso inalámbrico: • onfiguración y alistamiento del software, hardware y firmware de cada uno de los equipos a la última versión probada del fabricante. • uesta en producción de todos los equipos y las configuraciones de seguridad y puesta en marcha y en producción de los equipos. • uministro e instalación de los puntos de cableado estructurado de datos CAT (6A) y Power Injectors necesarios para la alimentación eléctrica de los access points. en todos los casos se requiere cableado de red para los Access Points; el cual deberá ser suministrado e implementado por el oferente. • ntegración a nivel de reportes y recolección de logs con la plataforma de logs y reportes suministrados. •

	ealizar mapas de Radiación, con el fin de Garantizar el mayor cubrimiento sobre las Sede Principal de la Entidad.
7	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 (3) años.
8	El contratista deberá 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.
9	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.
10	El contratista deberá garantizar soporte y garantia de repuestos para los Dispositivos Ofertados en un esquema 7 x 24 x 4 para tres (3) años en sitio. La entidad hara revision de los repuestos y/o equipos de soporte para garantizar este requerimiento. Los repuestos suministrados por el fabricante deberán ser nuevos.
11	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.
12	El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, Entre otros) requerida para que el personal asignado al proyecto, pueda cumplir sus funciones.
13	El oferente debe contemplar una capacitación en modalidad de transferencia de conocimientos para tres (3) 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. Esta trasferencia de conocimiento deberá ser de mínimo 16 horas.
14	El oferente deberá dictar diez (10) Charlas, en concienciación sobre diferentes temas de seguridad de la Información.

15	**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: **Gerencia de Proyecto:** Un ingeniero electrónico o de sistemas, graduado con matricula profesional, esta ultima con fecha de expedición mínimo de 5 años a la fecha de cierre del proceso . Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matricula profesional y certificado de vigencia expedido por la entidad competente. El gerente de proyectos deberá ser certificado PMP con Experiencia en gerencia de proyectos de seguridad informática de por lo menos 5 años, para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia. Así mismo para garantizar las mejores prácticas en prestación de servicios de TI este deberá ser como mínimo ITIL Foundations Certified. **Especialistas en servicios:** Mínimo Dos (2) ingenieros electrónicos o de sistemas, graduados, con matricula profesional. Para su verificación deberá presentar, según lo dispuesto por la Ley 842 de 2002 y la Ley 51 de 1986, diploma o acta de grado, copia de su tarjeta o matricula profesional y certificado de vigencia expedido por la entidad competente. Experiencia en instalaciones, soporte y/o mantenimiento en soluciones de seguridad de la marca ofrecida de por lo menos 2 años, para su verificación deberá presentar las respectivas certificaciones que comprueben y soporten su experiencia. El personal propuesto debe estar certificado por el fabricante en los productos ofertados a nivel de: Firewalls de Nueva Generación (Administración o Experto) Por lo menos uno de los dos ingenieros debe estar certificado por el fabricante en los productos ofertados a nivel de: Plataforma de logs y reportes Plataforma de administración centralizada Plataforma de red inalámbrica Plataforma para contención y mitigación de DdoS Plataforma Web Application Firewall (actual de la entidad) Para comprobar la experiencia deberán adjuntar certificados del fabricante vigentes. NOTA: Para la presentación de la oferta será suficiente que el representante legal de la firma proponente manifieste por escrito que cuenta con el personal certificado y que cumplen los requisitos de ley para realizar la instalación y configuración de los equipos con personal certificado en la marca a instalar y garantizar soporte de la solución ofertada por un periodo de un año con ingenieros certificados en la plataforma ofertada. En consecuencia la Entidad realizará la verificación de la formación y experiencia del personal previa suscripción del acta de inicio, sin embargo se aclara que el proponente deberá tener en cuenta que la

	mencionada verificación de la experiencia del personal se realizará de conformidad con el Artículo 12 de la Ley 842 de 2003, que señala: *"…ARTÍCULO 12. EXPERIENCIA PROFESIONAL. Para los efectos del ejercicio de la ingeniería o de alguna de sus profesiones afines o auxiliares, la experiencia profesional solo se computará a partir de la fecha de expedición de la matrícula profesional o del certificado de inscripción profesional, respectivamente. Todas las matrículas profesionales, certificados de inscripción profesional y certificados de matrícula otorgados con anterioridad a la vigencia de la presente ley conservan su validez y se presumen auténticas…"*

1.5 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 deberá anexar el Datasheet de los equipos ofertados y el informe NSSLABS del firewall de Nueva Generación ofertado.

1.6 Entrega de Información del Sondeo de Mercado

Las firmas interesadas deberan enviar una cotización antes de las 5:45 p.m. del día 7 de Octubre de 2015 a nombre de la Oficina de Tecnologías de Información a la Avenida Calle 26 No. 59-65 Piso 1 Costado Occidental, Bogotá, o digitalmente al correo electrónico a la dirección eric.vargas@anh.gov.co y carlos.bastidas@anh.gov.co .

Agradecemos diligenciar la siguiente tabla conforme a las especificaciones técnicas definidas en el numeral ***1.4 Especificaciones Tecnicas.***

Formato de Propuesta Económica

ANH AGENCIA NACIONAL DE HIDROCARBUROS COLOMBIA

FORMATO DE PROPUESTA ECONOMICA

Objeto: Fortalecimiento de la Infraestructura de Seguridad Informática, para la protección para los sistemas de información y redes de la ANH

Item	Descripcion	Cantidad	Valor Unitario	Valor Total	IVA sobre el Total	Valor Total con IVA
1	Solución de Firewall de Nueva Generacion (Anexo Tecnico Numeral 3.1)	2				
2	Solucion Plataforma de LOGS y Reportes (Anexo Tecnico Numeral 3.2)	1				
3	Solución de Protección para Amenazas Avanzadas SandBox (Anexo Tecnico Numeral 3.3)	1				
4	Solución de Analisis de Vulnerabilidades y Monitoreo de Base de Datos (Anexo Tecnico Numeral 3.4)	1				
5	Solución contra Ataques de Denegación de Servicio Distribuido DDOS (Anexo Tecnico Numeral 3.5)	1				
6	Solucion de Administracion centralizada de Firewalls (Anexo Tecnico Numeral 3.6)	1				
7	Puntos de Acceso WIFI para Intregrar a la Plataforma de Firewall (Anexo Tecnico Numeral 3.7)	10				
8	Alta disponibilidad para el Firewall de Aplicaciones WAF actual de la Entidad (Anexo Tecnico Numeral 3.8)	1				
9	Renovacion del Licenciamiento de la Plataforma de Seguridad Actual de la Entidad hast 31 de Diciembre de 2018. (Anexo Tecnico Numeral 3.9)	1				
10	Servicios profesionales para la Implementacion, transferencia de conocimiento y soporte especializado de la solucion por 3 años. (Anexo Tecnico Numeral 3.10)	1				
Total				$0	$0	$0

Nota: Favor abstengase de modificar el presente formato.

Nombre Empresa:
NIT :
Nombre representate Legal:
Valides de la Oferta 120 dias

LOGO EMPRESA

FIRMA

La presente consulta de precios no obliga, ni compromete responsabilidad por parte de la compañía participante del sondeo o por parte de la ANH y se constituye exclusivamente en una ayuda para sondear el mercado.

Nota: *Las cotizaciones que contengan valores en monedas diferentes al Peso Colombianos (COP) no se tendrán en cuenta.*

Aprobó. Juan Carlos Vila Franco – Jefe Oficina de Tecnologías de la Información
Revisó: Carlos A. Bastidas – Experto G3-6
Proyectó: Eric Mauricio Vargas Forero – Contratista