PARA: **OFERENTE**

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

ASUNTO: Sondeo de Mercado para la contratación cuyo objeto es *"*Contratar los servicios de NOC - SOC para la infraestructura actual y así como los sistemas de detección, protección y contención de las amenazas avanzadas, para complementar la plataforma actual de seguridad informática de la ANH*"*

La Agencia Nacional de Hidrocarburos – ANH se encuentra adelantando el Análisis del Sector con el fin de obtener, entre otros aspectos, los valores estimados para la contratación de objeto "Contratar los servicios de NOC - SOC para la infraestructura actual y así como los sistemas de detección, protección y contención de las amenazas avanzadas, para complementar la plataforma actual de seguridad informática de la ANH.".

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

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

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

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

Atentamente,

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

SONDEO DE MERCADO

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

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

DESCRIPCIÓN DE LA NECESIDAD:	Se requiere un servicio integral de seguridad informática y seguridad de la información, el cual permita Monitorear la Seguridad y Disponibilidad de las plataformas tecnológicas de la Agencia Nacional de Hidrocarburos, así como la protección adicional contra amenazas avanzadas que puedan afectar los sistemas de información en general, tal como se describe en el presente anexo Técnico.
OBJETO A CONTRATAR:	Contratar los servicios de NOC - SOC para la infraestructura actual, así como los sistemas de detección, protección y contención de las amenazas avanzadas, para complementar la plataforma actual de seguridad informática de la ANH
IDENTIFICACION DEL CONTRATO A CELEBRAR:	Prestación de Servicios

CÓDIGO UNSPSC (The United Nations Standard Products and Services Code® - UNSPSC, Código Estándar de Productos y Servicios de Naciones Unidas), correspondiente al bien, obra o servicios a contratar:	Con arreglo a los artículos 2.2.1.1.1.5.1. al 2.2.1.1.1.5.7. del Decreto Reglamentario 1082 de 2015, los Proponentes Individuales deben encontrarse inscritos, clasificados y calificados en el Registro Único de Proponentes – RUP de la Cámara de Comercio de su domicilio principal, en al menos uno (1) de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC): Con arreglo a los artículos 2.2.1.1.1.5.1. al 2.2.1.1.1.5.7. del Decreto Reglamentario 1082 de 2015, los Proponentes Individuales deben encontrarse inscritos, clasificados y calificados en el Registro Único de Proponentes - RUP de la Cámara de Comercio de su domicilio principal, en alguno (s) o en todos de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC), dentro del tercer o cuarto nivel: **UNSPSC** — **CLASE** 43222500 — Equipo de seguridad de red 43222600 — Equipo de servicio de red 43231500 — Software funcional específico de la empresa 43232300 — Software de consultas y gestión de datos 80101500 — Servicios de consultoría de negocios y administración corporativa 80101600 — Gerencia de proyectos 81111500 — Ingeniería de software o hardware 81111800 — Servicios de sistemas y administración de componentes de sistemas 81112000 — Servicios de datos 81112200 — Mantenimiento y soporte de software 81161500 — Servicios de administración de acceso 81161700 — Servicios de telecomunicaciones En el caso de propuestas presentadas por consorcios, uniones temporales o promesas de sociedad futura, al menos uno o más de uno de los integrantes puede estar inscrito, clasificado y calificado en por lo menos uno de los Códigos anteriormente establecidos.

DESCRIPCION DEL SERVICIO CONTRATAR

El servicio requerido deberá estar alineado con las mejores prácticas definidas por ITIL, por lo que deberá contar con:

- Diseño del Servicio: El servicio requerido deberá contar con las características mínimas descritas en el presente documento, sin embargo, las definiciones adicionales especificas deberán contemplarse en esta fase del servicio, de tal forma que se detallen y acuerden los alcances técnicos detallados entre la entidad y el prestador del servicio. Esta fase deberá ser previa a la puesta en producción del servicio contratado y contará con el visto bueno de la entidad, de tal forma que se cubran las expectativas que la entidad requiere a nivel de ingeniería de detalle.

- Transición del Servicio: En esta fase del servicio se deberán analizar todas las actividades necesarias para aprovisionar correctamente el servicio, de tal forma que todas las programaciones, ventanas, información requerida, configuraciones detalladas y demás adicionales, se contemplen y se dejen claras para que los tiempos y el cronograma sea ejecutado correctamente y se cumplan con los tiempos acordados para cada fase.

- Operación del Servicio: Esta fase permitirá la puesta en producción del servicio, contando con la operatividad de la modalidad de servicios, subservicios y características detalladas en el presente documento, garantizando el cumplimiento de los SLAs definidos para cada servicio.

- Mejora Continua del Servicio: Se deberá contar con una fase que garantice la mejora continua de todos los servicios, subservicios, procesos y características requeridas para la prestación del servicio. Garantizando que las configuraciones, reportes, características y demás requerimientos en los servicios y plataformas que lo soportan, se encuentren totalmente afinados y configurados acorde a las definiciones acordadas en el Diseño del servicio.

- Realizar el monitoreo tipo (NOC), la correlación de eventos tipo (SOC) y la administración y soporte delegados desde la sede NOC/SOC del Contratista de cuatrocientos (400) activos

de la plataforma de red y cómputo con capacidad de cuatro mil (4000) EPS (Eventos Por Segundo). Entiéndase por activo una única dirección IP de un dispositivo como un Switch, un servidor, una URL, un enrutador, etc.

- El servicio deberá tener la capacidad de monitorear los archivos críticos definidos por la entidad para mínimo cien (100) dispositivos utilizando funcionalidades de FIM (File Integrity Monitoring).

- La totalidad del software, el licenciamiento, el hardware de cómputo y almacenamiento necesarios para soportar los servicios definidos, deberán ser provistos por el Contratista con herramientas licenciadas (no opensource), sin que ello acarre costos adicionales para la entidad.

- Entregar al supervisor del contrato dentro los cinco (5) días hábiles al inicio del plazo de ejecución del mismo, un plan de trabajo en el cual se indiquen las actividades a realizar y las fechas complementadas para la instalación de los servicios contratados.

- El proveedor deberá contar con una capacidad operativa dedicada al NOC y SOC para brindar un soporte 7x24x365 con el personal especializado solicitado y prestar el servicio acorde al modelo operativo definido en el presente documento por una duración de 12 meses.

- Para la prestación del servicio de monitoreo y la correlación de eventos, el proponente debe proveer las herramientas tecnológicas especializadas propias para la recopilación, correlación y análisis de eventos. Por lo tanto, el proveedor pondrá al servicio de la ANH la infraestructura que sea necesaria para el cumplimiento técnico del servicio, sin que esto implique costos adicionales para la entidad.

- La plataforma utilizada para el servicio de monitoreo NOC y SOC debe ser de propósito específico y con soporte del respectivo directamente del fabricante, que garantice la continuidad del producto..

- Con el fin de mantener la homogeneidad de las soluciones que prestan en el servicio de NOC y SOC, se requiere que las mismas estén totalmente integradas y que desde un mismo dashboard se puedan ver los eventos de NOC y los eventos de SOC, lo cual le garantiza a la entidad los tiempos de repuesta en temas de soporte y garantía.

- Se debe garantizar el monitoreo 7x24x365 del estado de los activos objeto del servicio NOC/SOC y se deben generar las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la información o la continuidad de servicio de la plataforma IT de la Agencia Nacional de Hidrocarburos.

- Se debe proporcionar un servicio (integrando el concepto de solución SIEM con que cuenta la entidad) que permita realizar análisis, gestión de logs y correlación de eventos de seguridad que se presenten. La herramienta que soporte este servicio de correlación debe ser especializada para esta función y administrada por personal calificado.

- Se deben parametrizar una serie de alertas específicas, clasificarlas, priorizarlas sobre la plataforma tecnológica que se está monitoreando y reportarlas a las personas designadas por la Agencia Nacional de Hidrocarburos cada vez que se encuentre en riesgo la integridad, la disponibilidad o la confidencialidad de la información. Estas alertas deben suministrar información de valor para ser analizadas en la gestión de riesgos e incidentes que hace parte del Sistema de Gestión de Seguridad de la Información, esta información debe responder como mínimo las siguientes preguntas; ¿Quién?, ¿Qué?, ¿Cuándo?, Donde? y Por qué?, el cual permita a la entidad conocer la trazabilidad detallada de un incidente de seguridad.

- La información de logs que se generen en la actividad de monitoreo será propiedad de la Agencia Nacional de Hidrocarburos y, por ende, el almacenamiento de la misma al finalizar el contrato será provisto por la Entidad. Sin embargo, el proponente deberá garantizar el almacenamiento de logs en su plataforma con retención de al menos Treinta y seis (36) meses durante toda la vigencia del contrato. La Agencia Nacional de Hidrocarburos indicará el lugar final de almacenamiento de logs en su infraestructura NAS propia en el momento de la finalización del servicio.

- Se deben elaborar reportes de monitoreo, estadísticas, alertas/eventos, trazabilidad de históricos de alertas/eventos, hallazgos/recomendaciones, remediación de vulnerabilidades, entre otros y se entregarán de manera periódica según requerimiento, los cuales estarán ajustados de acuerdo a los requerimientos de la entidad, por lo menos con una frecuencia mensual. El servicio debe incluir un portal web donde se permita ver el estado de seguridad, indicadores, reportes y datos en tiempo real con disponibilidad 7x24x365, de la siguiente manera:

- Los Dashboard deben soportar diferentes vistas acordes a las diferentes partes interesadas, incluyendo; alta dirección, equipo de operaciones, departamento de seguridad de la información.

- Los Dashboard deberán tener la capacidad de ser modificados, de tal forma que permitan configurar estilos para cada tipo de usuario del sistema.

- El portal debe presentar el estado de seguridad de la infraestructura de IT que hace parte del servicio.

- Se deberá establecer un procedimiento y un plan de comunicaciones (matriz de escalamiento) claro y preciso para notificación de eventos y gestión de alarmas. Este procedimiento definirá el trabajo conjunto entre el proveedor y el contratante como base de trabajo para operar el servicio y entregar los resultados solicitados.

- Se debe aprovisionar un servicio de monitoreo de los aplicativos web para la entidad el cual permite monitorear los portales web con técnicas de transacciones sintéticas de la Agencia Nacional de Hidrocarburos, el cual deberá estar aprovisionado por lo especificado en la tabla de requerimientos técnicos “servicio de protección y monitoreo de las aplicaciones web de la entidad”.

- Se debe aprovisionar un servicio para mitigación de amenazas avanzadas en End Points (Estaciones de Trabajo) mediante agentes.

- Se debe entregar un servicio de monitoreo y detección de brechas de seguridad, el cual permita validar la efectividad y eficiencia de las plataformas de seguridad actuales de la entidad, dicho servicio deberá estar aprovisionado por lo especificado en la tabla de requerimientos técnicos “Requerimiento Técnico servicio de monitoreo y detección de amenazas avanzadas y ataques de día cero del tipo BDS (Breach Detection System)”.

- Será responsabilidad del Contratista, realizar el acompañamiento debido en la implementación de medidas de remediación de vulnerabilidades que se deriven de eventos de seguridad detectados por el proveedor, acorde al modelo operativo definido en el presente documento.

- Sera responsabilidad del proveedor realizar la respuesta y seguimiento correspondiente ante un incidente o evento de seguridad que se presente en los equipos incluidos en el servicio.

- El prestador del servicio en conjunto con la entidad (en la fase de implementación del servicio) se acordarán las clasificaciones de eventos e incidentes de seguridad para la definición de los incidentes Nivel 1, 2 y 3 acorde la matriz de clasificación de activos de información de la entidad y la criticidad de los servicios.

- El proponente debe entregar informes extraordinarios originados por los incidentes de seguridad informática de categoría crítica y realizar la respectiva gestión de remediación y/o recomendaciones acordes al modelo operativo definido en el presente documento.

- Para todos los equipos requeridos para la prestación del servicio, deberá asegurarse por parte del Contratista, que estos cuentan con el debido mantenimiento, soporte y garantía en caso de fallas, con lo cual se asegura su reemplazo inmediato.

- El proponente deberá realizar todas las conexiones físicas entre los dispositivos que soportan el servicio y los elementos activos de red, garantizando los elementos y accesorios necesarios para realizar las mismas, sin que esto genere costos adicionales para la entidad.

- A fin de asegurar la calidad de los servicios prestados a la entidad, El proponente deberá presentar certificacion de ser partner, de los Fabricantes de las plataformas con los cuales soportará los servicios de NOC/SOC, el servicio de protección y monitoreo de las aplicaciones web de la entidad, el servicio de monitoreo y detección de amenazas avanzadas y ataques de día cero del tipo BDS (Breach Detection System), servicio de monitoreo de integridad de archivos y servicio de análisis de desviación de línea base.

ESPECIFICACIONES TÉCNICAS DEL SERVICIO.

SERVICIO DE MONITOREO DE SEGURIDAD, DISPONIBILIDAD Y DESEMPEÑO – SOC.

Este servicio contempla el monitoreo a nivel de seguridad, disponibilidad y desempeño de 400 dispositivos definidos por la entidad, dicho **servicio deberá ser prestado teniendo en cuenta las siguientes características:**

- Se requiere que el servicio sea prestado con una plataforma SIEM que sea del tipo Security Information and Event Manager que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura IT de la entidad.
- Adjuntar junto con la oferta, las fichas técnicas de las plataformas que soportarán el servicio, en las cuales evidencien el cumplimiento de las características solicitadas.
- Recolectar los eventos de seguridad de múltiples marcas para lo cual se deberá incluir el licenciamiento necesario para esto.
- Monitorear los cambios en los archivos de configuración de los servidores que la entidad defina.
- Aprovisionar con una plataforma del tipo Virtual Appliance con el fin de que la entidad pueda asignar recursos virtuales a la misma a medida que se requieran, por lo tanto, dicha plataforma SIEM deberá se instalada en el datacenter de la entidad.
- Por temas de Confidencialidad e Integridad de la información de la entidad, La colección de bitácoras de los dispositivos para este servicio deberá ser de forma local por tal razón no se acepta la colección de bitácoras de forma remota.

- Aprovisionado con una plataforma dedicada para la entidad, para tal fin el licenciamiento de dicha plataforma deberá estar a nombre de la entidad.
- Almacenar las bitácoras en información generada por el mismo en un sistema de bases de datos hibrida, lo que quiere decir que esté basado en NoSQL y SQL, no se acepta que el almacenamiento de bitácoras e información se base únicamente en motores de bases de datos del tipo SQL, esto con el fin que en el servicio se soporten grandes volúmenes de datos sin afectar la estabilidad del mismo.
- Contemplar la actualización constante de la base de datos de contextos, configuraciones, software instalado y servicios corriendo de los dispositivos monitoreados.
- Realizar un análisis constante el desempeño de las aplicaciones lo cual permita realizar un triage de la seguridad.
- Contemplar un Visor personalizado de log de tráfico y se deberá dar acceso de consulta a la entidad con el fin de que personal designado pueda acceder a esta información.
- Contemplar una Herramienta de búsqueda sobre los logs de tráfico y se deberá dar acceso de consulta a la entidad con el fin de que personal designado pueda acceder a esta información.
- Contemplar para el monitoreo de 300 dispositivos y 3000 Eventos por Segundo.
- No se acepta que el servicio sea prestado con soluciones de Código Abierto (Open Source).
- La plataforma que soporte el servicio deberá permitir ser desplegado en VMWare ESXi o Hyper-V, KVM o OVM.
- Monitorear de aplicaciones via JMX, WMI y PowerShell.
- Contar con la característica de Monitoreo de Hipervisores tales como VMWARE, Hype-V y OVM.
- Monitorear plataformas de almacenamiento tales como EMC, ORACLE, HP, Nimble, etc a nivel de desempeño y uso de almacenamiento.
- Monitorear de sistemas del tipo Directorio Activo y Exchange basado en WMI y PowerShell.
- Se deberá Monitorear los motores de Bases de datos SQL Server, Oracle, MySQL entre otras via JDBC.
- Monitorear la Infraestructura VoIP via IPSLA, SNMP, CDR y CMR.
- Permitir realizar Análisis del desempeño y flujo de las aplicaciones vía NetFlow, Sflow, Cisco AVC y NBAR, en caso que la entidad lo requiera, sin que esto genere costos adicionales para la entidad.
- Permitir la Capacidad de definir métricas ajustadas en caso de que la entidad lo requiera.

- Permitir la Capacidad de monitorear dispositivos del entorno tales como Liebert UPS, HVAC, FPC y APC, en caso de que la entidad lo requiera, sin que esto genere costos adicionales para la entidad.
- Monitorear las caídas e inicios de los sistemas vía Ping, SNMP, WMI, así como análisis del inicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage.
- Permitir la capacidad de hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos, en caso de que la entidad lo requiera.
- El servicio deberá estar aprovisionado por una solución que soporte de forma nativa el monitoreo de las plataformas definidas por la entidad, en caso de que no esté soportado dicho monitoreo el oferente deberá contemplar el desarrollo de conectores personalizados para la misma.
- Colectar logs por cualquiera de los siguientes métodos:

- Web – HTTP/HTTPS
- DNS
- FTP/SCP
- Generic TCP/UDP
- ICMP
- IMAP4
- JDBC
- LDAP
- POP3
- POP3S
- SMTP
- SOAP
- SSH
- Telnet/SSH
- SNMP
- WMI
- JMX

- Realizar la Correlación y Correlación Cruzada de Eventos de múltiples fuentes, tales como Firewalls, Switches, Consolas Antivirus, Servidores, estaciones de trabajo entre otros.

- El servicio deberá realizar monitoreo de inteligencia por medio de la Integración por API's con fuentes de información externa sobre amenazas, tales como Dominios de Malware, IPs, URLs, Hash y Nodos de Tor, en caso de que la entidad lo requiera.
- Deberá tener la capacidad de modificar los normalizadores (parsers) por medio de interface gráfica, sin que esta modificación afecte la colección de logs o genere caídas en los servicios de la solución.
- La plataforma con la que se arquitecta el servicio deberá tener la capacidad de ejecutar scripts de remediación cuando un incidente ocurra.
- Contar con un sistema de tickets, con el cual se escalen de manera automática los incidentes que se detecten en el monitoreo.
- Tener la capacidad de integrarse con sistemas de tickets externos en caso que la ANH lo requiera, dicha integración deberá ser por API.
- Aprovisionar el servicio con una solución que soporte la detección de incidentes, el cual deberá ser en tiempo real anterior al almacenamiento del evento, utilizando técnicas del tipo "Correlación Distribuida".
- Deberá contar con una consola de visualización de logs y eventos correlacionados la cual cuente con un sistema para el filtrado de los mismos por medio de condiciones Lógicas.
- Generar un reporte de incidentes el cual deberá poder ser priorizado por los servicios críticos, dicho informe deberá ser entregado de forma mensual a la entidad.
- Entregar un informe mensual de las actividades realizadas en aras de mejorar el servicio de monitoreo.
- Entregar un informe semanal de incidentes de seguridad que hayan sido detectados.
- Entregar un informe semanal de incidentes de disponibilidad que hayan sido detectados.
- Entregar un informe semanal de incidentes de Rendimiento que hayan sido detectados.
- Contar con una consola del tipo dashboard en la cual se pueda personalizar varios tipos de gráficas y tablas, lo cual permita tener una visión global de los incidentes de seguridad.
- La plataforma que soporta el servicio deberá tener un gran número de reportes predefinidos y deberá permitir crear reportes Parametrizables (custom).

SERVICIO DE MONITOREO DE INTEGRIDAD DE ARCHIVOS.

La entidad requiere el servicio de monitoreo de un grupo de 100 Equipos definidos por la entidad, el cual permita detectar posibles alteraciones que puedan sufrir archivos contenidos en dichos activos de información, este servicio deberá cumplir con las siguientes características:

- monitorear los cambios en los archivos de configuración de los servidores que la entidad defina.
- Deberá contar con la característica de detección automática en cambios en archivos y carpetas, de las plataformas Windows y Linux monitoreadas, donde se detalle el “Quien” y el “Que”.
- El servicio deberá hacer Monitoreo de la Integridad de Archivos o FIM basada en agente tanto para Windows como Linux.
- El servicio deberá contar con un módulo para la administración de los agentes Windows FIM.
- Deberá contar con la característica de detección automática basada en agente, de cambios en el registro de los sistemas Windows monitoreados.
- generar un informe mensual de los incidentes detectados a nivel de alteraciones sospechosas que se hayan podido presentar en los activos de información monitoreados

SERVICIO DE DETECCION DE DESVIACIONES EN LA LINEA BASE TI.

La entidad requiere un servicio de monitoreo que permita detectar cambios que se puedan presentar en los 400 dispositivos de la infraestructura monitoreada en el servicio “SERVICIO DE MONITOREO DE SEGURIDAD, DISPONIBILIDAD Y DESEMPEÑO - SIEM”, así como alertar posibles desviaciones relevantes que se puedan presentar en las configuraciones de las plataformas tecnológicas de la entidad, por otro lado, darle a la entidad una base de información de las plataformas tecnológicas monitoreadas, dichos servicio deberá cumplir con las siguientes características:

- El servicio deberá tener un componente del tipo CMDB (Configuration Management DataBase), el cual permita tener una base de las configuraciones de las plataformas monitoreadas.
- El servicio deberá contar con un módulo de administración para la característica de CMDB (Configuration Management Database).
- El servicio deberá monitorear los cambios en los archivos de configuración de los servidores que la entidad defina.
- El servicio deberá colectar archivos de configuración de los dispositivos de red monitoreados que defina la entidad, almacenada en un repositorio de versiones.
- El servicio deberá realizar la detección automática de los cambios en la configuración de las plataformas de red monitoreadas.

AGENTES DE SEGURIDAD DE PUNTO FINAL PARA MITIGACION DE AMENAZAS AVANZADAS.

Se deberá proveer un servicio de detección, protección y análisis de los ataques orientados a afectar las estaciones de trabajo de la entidad, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan en el presente anexo. Este servicio deberá ser puesto en funcionamiento en las instalaciones de la entidad, por lo cual el prestador del servicio deberá suplir totalmente la instalación de dichos agentes con el debido licenciamiento y soporte de fabricante:

- Se requiere el servicio de 600 agentes de punto final.
- La solución que soporte el servicio debe ser compatible para ser integrada de forma nativa con la actual solución de sandbox de la entidad.
- Debe contar con Agentes de seguridad de “Punto Final” para servidores y estaciones de trabajo.
- Estos agentes deberán integrarse con la solución de Deteccion de Brechas de Seguridad, de tal forma que se le envíen los archivos sospechosos.
- La solución que soporte el servicio debe capturar y grabar comportamientos anómalos en tiempo real, detectar amenazas, detenerlas y remediarlas, dicho evento debe ser centralizado para que los ingenieros de monitoreo de forma inmediata tomen acciones de corrección.
- La solución que soporte el servicio debe ser implementada en modo On premise sobre la infraestructura de la Agencia Nacional de Hidrocarburos.

- A nivel Administración, almacenamiento y control centralizado, la solución que soporte el servicio debe realizar búsqueda de comportamientos sospechosos, filtrado de actividad, investigación profunda, descubrimiento de actividad maliciosa, evaluación de alcance de la amenaza, remediación, actualización de las bases de conocimiento.

- La solución que soporte el servicio debe permitir como mínimo:

- Hacer detección y grabacion de ataques en tiempo real
- Validación y clasificación de alertas de seguridad.
- Aislar ataques de seguridad.
- Hacer caza de amenazas que burlan la capa de seguridad perimetral de la entidad.
- Hacer remediación.

- Visualizar la cadena de ataque.
- Registro continuo de la actividad del punto final
- Mitigación de ataques futuros
- Integración nativa de doble chequeo con soluciones de mitigación de amenazas avanzadas de red
- Realizar inventario de archivos del Entorno
- Protección Man-in-the-middle a través de la autenticación SSL bidireccional con el servidor
- Visualización de la cadena del ataque de seguridad: Debe permitir ver la trazabilidad del ataque, lo que se afectó y lo que se debe reparar.
- Caza de amenazas en tiempo real: Debe permitir visibilidad de lo que pasa en el servidor en tiempo real (Zero-gap) para encontrar amenazas o comportamientos anómalos antes de que un ataque se lleve a cabo.
- Respuesta y remediación: Debe manejar una única consola para el manejo de detección y remediación de un ataque. Una vez el mismo es detectado, se debe poder aislar y acceder de forma remota al servidor para realizar remediación.
- Debe soportar sistemas operativos:

- Windows.
- Apple.
- Linux Read Hat.
- Linux CentOS

- El Software de punto final o agente utilizado para la prestación de este servicio no debe consumir más de:

- 1% del CPU.
- 20 MB de RAM.
- 50 bytes del ancho de banda de la conexión a red.

- La garantía y los servicios de soporte post venta deben ser directos del fabricante por Tres (3) años de suscripción de software en un esquema de Soporte 24x7.

- La solución propuesta para soportar el servicio debe ser de tecnología actual por parte del fabricante por lo cual no se aceptarán propuestas que incluyan tecnologías que hayan sido descontinuadas por su fabricante.

Con el fin de que la entidad como se está prestando este servicio y el alcance del mismo, se debe incluir una capacitación en línea en la solución ofertada para mínimo una persona. La capacitación debe incluir la administración y operación de la herramienta.

SERVICIO DE DETECCION DE BRECHAS DE SEGURIDAD

La entidad requiere un servicio en aras de detectar, proteger y mitigar amenazas avanzadas que permita la utilización de mecanismos combinados para la detección de virus, virus polimórficos y otras amenazas avanzadas y de día cero. Este servicio deberá ser puesto en funcionamiento en las instalaciones de la entidad con equipos totalmente nuevos y con el debido licenciamiento y soporte de fabricante, las características de dicho servicio son como se enuncian a continuación:

- Dicho servicio deberá integrarse con la actual plataforma de seguridad perimetral con la que cuenta la entidad y con la solución de agentes avanzados de seguridad para punto final que se oferte con el presente proceso, de tal manera de que esta le envíe archivos para el análisis y revisión de los mismos.
- El servicio deberá contemplar un escaneo de todos los recursos compartidos de la entidad vía (CIFS/SMB) en busca de amenazas de dia-zero que ya se encuentren residentes en dichos repositorios.
- El servicio de detección de brechas de seguridad deberá realizarse en varios ámbitos:
  - Información en movimiento a través de los end points que le envían archivos sospechosos para análisis en sandbox
  - Información en movimiento a través de hacer snnifing de red conectado al switch de core
  - Informacion en reposo con el análisis proactivo de los repositorios de archivos compartidos.
  - Información por demanda a través de permitir el posting de información desde una interface web

- El servicio deberá contemplar el análisis de tráfico por medio de un Port Span de los segmentos que la entidad defina, en busca de brechas de seguridad, botnets o amenazas que a se encuentren residentes en la entidad, dicho análisis deberá contemplar como mínimo los protocolos, HTTP, SMTP, POP3, IMAP, FTP, SMB.

- El servicio deberá soportar una capacidad de mínimo Capacidad de análisis de archivos para detección de amenazas de día cero de mínimo Quinientos (500) archivos por hora.
- El servicio deberá aprovisionarse con una solución que cuente con mínimo 2 interfaces SFP+ (10 Gbps) y 2 GE.
- El servicio deberá estar en la capacidad de detectar amenazas avanzadas en sistemas operativos Windows 7, Windows 8.1, Windows 10 y Android, mediante el uso de mínimo veinticuatro (24) máquinas virtuales concurrentes.
- El servicio deberá se ofrecido con una solución tipo appliance, de propósito específico. No se aceptarán solución de tipo Opensource.
- El servicio deberá poder detectar mínimo los siguientes tipos de amenazas:
- La solución debe estar en la capacidad de detectar los siguientes tipos de infección y ataques:

  - 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 esconder 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.
  - Greyware: Archivos con comportamiento similar al de virus.

- La ejecución del servicio 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, para lo cual semanal mente se deberá presentar un informe a la entidad con el detalle de los archivos analizados, el cual para el caso de los archivos sospechosos deberá tener como mínimo:
  - Descarga de Virus.

- Modificación de registro.
- Conexiones externas a IPs maliciosas.
- Infección de procesos.

- Debe ser posible habilitar el envío de notificaciones cada vez que el análisis detecte Malware.
- El servicio debe entregar información específica de los análisis realizados, esto debe ser sobre una interfaz gráfica con filtros predeterminados como eventos, malware, entre otros.
- El servicio deberá poder analizar los tipos de Archivos: exe, dll, PDF y Javascript. En modo integrado debe poder analizar tar, gz, tar.gz, zip, bz2, tar.bz2, bz, tar.
- Debe presentarse información completa del análisis de amenazas del ambiente virtual incluyendo Actividades del sistema, acción del exploit, trafico web, intentos de comunicación entre otros.

SERVICIO DE BALANCEO DE DATACENTER, APLICACIONES Y ENLACES.

La entidad requiere un servicio de balanceo de datacenter, aplicaciones y enlaces el cual deberá estar prestado en modalidad dedicada en las instalaciones de la Agencia Nacional de Hidrocarburos, con plataformas en formato appliance de propósito específico que cumplan con las características que se enuncian a continuación:

- El servicio debe ser prestado con una 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.
- La solución debe ser desarrollada por el fabricante y no debe incluir desarrollos de terceros

El equipo que soporte el servicio deberá cumplir con las siguientes características de desempeño y conectividad ya activas y funcionales:

- Rendimiento Capa 4 y 7: 15 Gbps
- Rendimiento Compresión: 8Gbps
- Transacciones por Segundo SSL: 12.000

- Conexiones por Segundo Capa 4: 300.000
- Dominios Virtuales: 5
- 4 puertos de 10Gbps SPF+.
- 4 puertos de 1Gbps SPF.
- 4 puertos de 1Gbps RJ45.

El equipo que soporte el servicio debe cumplir con las siguientes características y funcionalidades las cuales podrán ser solicitadas por la entidad en cualquier momento, sin que esto genere costos adicionales al servicio:

- La solución debe estar diseñada para proveer aceleración en Layer-4 y Layer-7.
- La solución debe ser capaz de balancear trafico ICMP,UDP,TCP y poseer entendimiento de protocolos como HTTP/s, FTP y RADIUS.
- La solución debe ser capaz de balancear carga de manera transparente o utilizando NAT basándose en información obtenida de Layer-7 como URL, Cookie, SSL ID, etc.
- La solución debe poseer distintos métodos de balance como round robin, weighted round robin, least connection y shortest response.
- La solución debe ser capaz de hacer routing/switching inteligente de contenido en Layer-7 basándose en la información enviada por el cliente (URL, HTTP header, cookie, URL, etc).
- La solución debe proveer persistencia en Layer-4 basándose en la dirección IP de origen y puerto. Adicionalmente la persistencia en Layer-7 debe poder ser configurada basándose en la información del cliente como URI, HTTP headers, hostname, SSL session ID y Cookies.
- La solución debe ser capaz de hacer SSL Offloading
- La solución debe ser capaz de realizar balance entre datacenters (GSLB)
- La solución debe poseer la capacidad de proteger aplicaciones y servidores de ataques SYN-Flood y cantidad de conexiones. Además, debe ser capaz de integrar tabla de conexiones statefull para IPv4 e IPv6.
- La solución debe poder ser administrada vía interfaz gráfica (GUI) e interfaz de línea de comandos (CLI).
- La Solución propuesta deberá proveer alta disponibilidad, failover transparente y escalabilidad para las aplicaciones.
- La solución propuesta deberá contar con un servicio de protocolo virtual de para los siguientes protocolos HTTP, HTTPS, TCP, TCPS, FTP, FTPS, UDP, DNS, SIP UDP, SIP TCP, RTSP, RDP, IP, L2IP, este servicio virtual también deberá funcionar en modo proxy reverso, proxy transparente y proxy en modo de triangulación.

- La solución propuesta deberá reenviar los paquetes IP a diferentes destinos MAC para distribuir la carga a nivel de capa 2 puerto físico, a nivel de capa 3 dirección IP y rango de puertos TCP/UDP.
- La solución propuesta deberá ofrecer un sistema de almacenamiento de contenido Web completamente integrado con funcionalidades de HTTP/HTTPS, compresión y funciones de administración de tráfico para almacenar y enviar objetos validando las peticiones de los clientes sin tener que consultar a los servidores reales acelerando la respuesta de las aplicaciones, reduciendo el ancho de banda y la carga de los servidores.
- Deberá proveer estadísticas detalladas del acceso al cache basándose en IP o en http hosts como mínimo, las coincidencias de los objetos almacenados podrán estar basadas en URL parciales.
- Deberá tener reglas configurables para tamaño máximo de objetos, TTL y la forma de acceso, soporte del set de caracteres extendidos.
- La solución propuesta deberá tener un sistema de compresión dinámico en línea basado en hardware, en donde de forma automática deberá comprimir archivos de texto, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT y XLS, también deberá contemplar reglas para no comprimir URL seleccionados que contengan RegEx y objetos web seleccionados para el servicio virtual seleccionado y proporcionar estadísticas detalladas de la compresión.
- La solución propuesta deberá tener un sistema de aceleración de SSL basado en hardware soportando HTTPS, NNTPS, SMTPS, POPS, IMAPS y LDAPS. Soporte de SSLv3 y TLSv1 con un cifrado máximo de 2048-bits, redirección automática de HTTP a HTTPS, deberá poder actuar como servidor de SSL o como cliente de SSL al mismo tiempo, hasta 64 servicios virtuales podrán utilizar el mismo certificado.

MODELO OPERATIVO DEL SERVICIO

El servicio requerido deberá prestarse acorde a las mejores prácticas de gestión de servicios de TI enmarcadas por ITIL. Así mismo deberá contar con las mejores prácticas y contar con un gerente de proyecto con dedicación compartida acorde a los perfiles definidos en el presente documento.

El prestador del servicio deberá tener como mínimo una mesa de ayuda (para la gestión de incidentes) basada en una plataforma licenciada, la cual cumpla como mínimo 13 procesos certificados de ITIL. Esta plataforma permitiría hacer toda la gestión e interface del servicio contra el prestador

El prestador de servicio deberá considerar un modelo operativo con los perfiles, dedicaciones, experiencias y certificaciones a continuación descritas (para lo cual deberán adjuntar las hojas de vida,

con una carta de compromiso de participación en la prestación del servicio en caso de ser contratado con el oferente.

EQUIPO DE TRABAJO MINIMO

El proveedor deberá contemplar como mínimo los recursos de personas que se encuentran definidos en la tabla personal mínimo requerido.

El personal presentado en la propuesta debe ser el mismo que realiza el desarrollo del contrato no obstant,e Si durante la ejecución del contrato la ANH considera necesario, podrá solicitar cambios de personal del equipo de trabajo del Contratista por otro con el mismo perfil que el presentado en la propuesta.

Cuando el personal asignado por el proveedor requiera contactarse con personal de otros grupos o dependencias, deberá estar acompañado por algún representante del Grupo de Seguridad Informática o de seguridad de la información

GERENTE DE SERVICIO

Integrante Equipo	**Formación Profesional**		**Experiencia Profesional Específica y Funciones Requeridas**
	Pregrado	**Posgrado/Certificaciones /Cursos**	
Un (1) Profesional Ubicación: en las instalaciones de la entidad en la modalidad bajo demanda.	Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones, o afines.	**Certificación:** ITIL SOA y OSA.	Cinco (5) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. Experiencia especifica de tres (3) años como Gerente y/o Líder de Servicio.

50% de Dedicación.			

NIVEL 1

Integrante Equipo	**Formación Profesional**		**Experiencia Profesional Específica y Funciones Requeridas**
	Pregrado	**Posgrado/Certificaciones /Cursos**	
Un (1) Profesional Ubicación: en las instalaciones del Proveedor del Servicio 100% de Dedicación.	Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones, o afines.	**Certificación:** ISO/27001:2013 **Cursos:** Diplomado o Especialización en Gestión de TI	Cinco (5) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. Experiencia especifica de cinco (5) años como líder técnico de proyectos de Infraestructura y/o seguridad de información.

NIVEL 2

Integrante Equipo	**Formación Profesional**		**Experiencia Profesional Específica y Funciones Requeridas**
	Pregrado	**Posgrado/Certificaciones /Cursos**	

Un (1) Analista Ubicación: Remota Dedicación 100%	Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones.	**Certificación:** NTC-ISO/IEC 27001:2013 – 27002:2015 **Cursos:** Gestión del Riesgo Operativo y Continuidad del Negocio.	Tres (3) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. Experiencia especifica de tres (3) años como operador o analista de redes y/o seguridad.

NIVEL 2

Integrante Equipo	**Formación Profesional**		**Experiencia Profesional Específica y Funciones Requeridas**
	Pregrado	**Posgrado/Certificaciones /Cursos**	
Un (1) Analista Ubicación: Remota Dedicación 100%	Título como Técnico Profesional o Tecnólogo Profesional en electrónica o informática o telecomunicaciones o sistemas o cursando últimos semestres del ciclo profesional.	**Certificación:** Certificación en Mesa de Servicios.	Dos (2) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. En caso de estar finalizando estudios del ciclo profesional, se debe adjuntar acta de vigente emitida por la universidad en la cual realiza sus estudios.

			Experiencia especifica de dos (2) años como operador o analista de redes y/o seguridad.

NIVEL 3

Integrante Equipo	**Formación Profesional**		**Experiencia Profesional Específica y Funciones Requeridas**
	Pregrado	**Posgrado/Certificaciones /Cursos**	
Un (1) Profesional / Experto Ubicación: Remota y en las Instalaciones del cliente con dedicación al 50% bajo el esquema bajo demanda.	Título en Ingeniería de Sistemas, Ingeniería electrónico, Ingeniería de telecomunicaciones.	**Certificación:** ISO/27001:2013	Dos (2) años de experiencia a partir de la expedición de la tarjeta profesional. Debe incluirse certificación de vigencia. Experiencia especifica: de cinco (5) años como Ingeniero Líder de Redes / Seguridad de Información y SOC.

Informes de actividades:

El contratista deberá generar y entregar un informe de las actividades realizadas de cada mes durante el periodo de ejecución del contrato, discriminando mantenimiento, soporte y hallazgos encontrados por las herramientas.

Nivel de acuerdo de servicios ANS (Tiempos de Respuesta):

El oferente deberá cumplir los siguientes niveles de acuerdo de servicios:

MATRIZ PRIORIDADES	ALTO IMPACTO	MEDIO IMPACTO	BAJO IMPACTO	NULO IMPACTO
ALTA URGENCIA	Prioridad 1	Prioridad 2		
MEDIA URGENCIA	Prioridad 2	Prioridad 2	Prioridad 3	
BAJA URGENCIA	Prioridad 3	Prioridad 3	Prioridad 4	Prioridad 4
NULA URGENCIA			Prioridad 4	Prioridad 5

PRIORIDAD	TIEMPO DE RESPUESTA INICIAL
1	2 HORAS
2	6 HORAS
3	2 DÍAS HABILES SIGUIENTES
4	4 DÍA HABILES SIGUIENTES
5	5 DÍAS HABILES SIGUIENTES

Apertura de tickets y soporte

La atención a los servicios de soporte y apertura de tickets se debe dar por el oferente en horario 7x24 según lo adquirido. Los tickets deben poderse abrir vía correo eléctrico, teléfono y vía página web.

PROPUESTA ECONÓMICA
"Contratar los servicios de NOC - SOC para la infraestructura actual y así como los sistemas de detección, protección y contención de las amenazas avanzadas, para complementar la plataforma actual de seguridad informática de la ANH"

tem	**Descripción**	**Cantidad**	**Valor Unitario**	**SubTotal**	**IVA sobre el Total**	**Valor Total IVA Incluido**
1	Servicio de monitoreo de seguridad, disponibilidad y desempeño – SOC.	**1**	$	$	$	$
2	Servicio de monitoreo de integridad de archivos.	**1**	$	$	$	$
3	Servicio de detección de desviaciones en la línea base ti.	**1**	$	$	$	$
4	Agentes de seguridad de punto final para mitigación de amenazas avanzadas	**1**	$	$	$	$
5	Servicio de balanceo de datacenter, aplicaciones y enlaces.	**1**	$	$	$	$
VALOR TOTAL				**$**	**$**	**$**

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

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

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

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

Nit de la Persona Jurídica:

Nombre de la Empresa:

Teléfono:

Dirección Sitio Web:

Email de contacto:

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

Firma Representante Legal: _____

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

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