SONDEO DE MERCADO PARA "Adquirir el licenciamiento de plataforma de seguridad de usuario final con servicio de soporte, para la infraestructura tecnológica y parque computacional de la Agencia Nacional de Hidrocarburos.".

TABLA DE CONTENIDO

1 SONDEO DE MERCADO.

1.1 Objeto

Adquirir el licenciamiento de plataforma de seguridad de usuario final con servicio de soporte, para la infraestructura tecnológica y parque computacional de la Agencia Nacional de Hidrocarburos

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 Incio hasta el 20 de Diciembre de 2015.

1.4 Duracion del Contrato

El licenciamiento y soporte deberá ser suministrado por un periodo de 3 años. Dentro de este periodo se dispondrán 15 días, para la implementación y despliegue de la solución.

1.5 Especificaciones Técnicas Equipos

1.5..1 Componente de Protección de Información de Punto Final

Requerimientos Generales:

La solución deberá brindar protección para servidores, equipos portátiles y estaciones de trabajo sobre deberá estar soportado para instalarse en: Sistemas operativos Windows: Windows XP (32 bits, SP3 o posterior; 64 bits), Windows XP Embedded (SP3 o posterior), Windows Vista (32 o 64 bits), Windows 7 (32 o 64 bits), Windows 7 Embedded, Windows 8 (32 o 64 bits), Windows 8 Embedded, Windows 8.1 ,Windows 10, Windows Server 2003 (32 bits, 64 bits, R2, SP1 o posterior), Mac OS X 10.6.8, 10.7 (32 bits, 64 bits); 10.8 (64 bits), Mac OS X Server 10.6.8, 10.7 (32 bit o 64 bits); 10.8 (64-bit).

Deberá ser capaz de proveer funcionalidad de protección con las siguientes tecnologías:

- Antivirus basado en firmas y definiciones
- Motor reputacional alimentado por mecanismos globales de inteligencia
- Antispyware
- Firewall de punto final
- IDS/IPS de punto final
- Motor de detección y prevención contra intrusos
- Control de aplicaciones

- Control de dispositivos
- Control de Integridad
- Motor heurístico basado en comportamiento
- Capacidad de Listas Blancas y negras para control de aplicaciones
- Monitoreo de comportamiento de aplicaciones
- Control físico de dispositivos
- Compatibilidad con Network Access Control
- Reportes avanzados.
- Borrado seguro de malware residente en memoria difíciles de erradicar, para evitar el reinicio de servidores críticos.

- La solución deberá permitir que el uso e integración de las tecnologías de protección sea a través de políticas configurables y flexibles en un esquema jerárquico (dominios, sitios, grupos, subgrupo, cliente, usuario, localidades, etc) para aplicar a perfiles de usuario o equipos en base a los criterios definidos y deberán asignarse desde la consola de administración de la solución.

- La solución de protección deberá ser configurable para definir de forma flexible diferentes niveles de interacción con el usuario final, es decir permitir al usuario realizar algunas o varias funciones o restringirlas por completo.

- La solución de protección deberá permitir que las actualizaciones llámese versiones, parches, adecuaciones o modificaciones propias de la solución de protección puedan realizarse de forma automatizada con escasa o nula interacción administrativa teniendo en cuenta un parque de equipos protegidos de la ANH es de al menos 550 unidades.

- La solución deberá ser capaz de prevenir la desinstalación sin autorización de la herramienta e incluso poder utilizar una contraseña.

- La solución deberá ser capaz de evitar que los procesos correspondientes que proveen la protección sean manipulados, deshabilitados o comprometidos en forma mal intencionada o sin autorización.

- La solución deberá ser capaz de enviar en forma automática al fabricante los riesgos de seguridad detectados para su revisión y valoración.

- La solución deberá poder desinstalar la solución de antivirus existente antes de hacer la instalación del nuevo antivirus.

- La solución deberá permitir la configuración flexible de acciones a tomar ante la detección de riesgos de seguridad.

- La solución deberá ser capaz de configurar notificaciones sobre la detección de riesgos en base a roles o perfiles de responsabilidad definidos por la entidad
- La solución deberá ser capaz de soportar esquemas de replicación, balanceo de cargas en las consolas de administración centralizadas para estar abiertos a la implementación de planes de recuperación de desastres y disponibilidad de servicio.

- La solución deberá ser capaz de integrarse al directorio activo para importar y configurar estructuras organizacionales (usuarios y equipos) para ser cubiertos con la protección de seguridad.

- La solución debe ser capaz de manejar diferentes formas de instalación en los equipos de los usuarios finales (por ejemplo interactiva, silenciosa, reiniciar equipo o no)

- La solución deberá contar con el respaldo de una base de datos de conocimientos, descargas, actualizaciones, documentación, soporte, seguimientos de casos de escalación, despliegue de información provista y mantenida directamente por el fabricante.

- La solución deberá ser capaz de manejar un esquema que incluya cuarentena centralizada de los riesgos de seguridad detectados.

- La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales administrados centralmente como a usuarios finales que descentralizados.

- La solución deberá de ser capaz de proveer protección de seguridad tanto a usuarios finales como a servidores de propósito específico.

- La solución deberá de ser capaz de poder remover antivirus de diversos fabricantes antes de poderse instalar el cliente.

- La solución deberá ser capaz de soportar la administración centralizada de un ambiente de mínimo 550 usuarios finales.

- La solución deberá ser capaz de soportar el uso de BDs externas (no propietarias de la solución) por ejemplo SQL server.

- La tecnología de protección provista por la solución deberá ser altamente efectiva para la detección y remoción de riesgos de seguridad en la categoría de rootkits.
- La instalación del agente de protección deberá poder realizarse de al menos los siguientes métodos: local utilizando la media de instalación, remotamente desde la consola, por medio de un servidor de Intranet o utilizando herramientas de distribución de terceros.

- La comunicación del agente con la consola de administración deberá poder realizarse por medio de los protocolos http y https para facilitar la inspección de tráfico y evitar la apertura de puertos en firewalls y otros dispositivos de red.

- La solución deberá actualizar su contenido (firmas de detección de virus, firmas de detección de intrusos, listado de aplicaciones) desde la consola de administración, desde Internet, desde un equipo definido para la actualización local, inclusive en forma manual.

- La solución de protección deberá incluir tecnología de antivirus y antispyware que detecte intentos de infección desde unidades de disco, unidades removibles, unidades compartidas, así como memoria.

- La solución de protección podrá ser configurada para que al intentar abrir la interface del usuario solicite una contraseña, en caso de no conocer la contraseña, el usuario no podrá abrir la interface.

- Las políticas para la solución de protección deberán poderse aplicar por computadora o por usuario, deberán poderse aplicar por grupo, subgrupo o a todo el universo de equipos.

- La solución de protección deberá tener capacidad para identificar el tipo de red al cual se está conectando para adecuar las políticas de protección de antivirus y antispyware, Firewall, IPS, control de Dispositivos, así como de políticas de actualización. La detección de la ubicación deberá poder realizarse por al menos las siguientes variables: rango de dirección IP, dirección IP/nombre del servidor de nombres DNS, dirección IP/nombre del servidor de WINS, default Gateway.

1.5.1.1 Administración

- Deberá contar con una consola de administración centralizada, desde la cual se pueda monitorear el estado de la seguridad en los equipos de cómputo de la ANH.

- La consola deberá tener la capacidad de ser accedida desde cualquier punto de la red utilizando un navegador de páginas de Internet como Internet Explorer o Mozilla Firefox.

- La consola deberá indicar por medio de una representación gráfica el estado actual de la seguridad en los equipos de la ANH, los niveles de seguridad deberán poder ser definidos por el personal de la Entidad.

- La consola de administración deberá mostrar en una gráfica el estado de la actualización de los patrones de detección en los agentes. En una tabla de mayor detalle deberá indicar el nombre del equipo, su dirección IP, el usuario que se firmó en el equipo y el sistema operativo.

- La consola de administración deberá mostrar en una gráfica los intentos de infección más recientes, así como los equipos que presentaron dichos intentos de infección indicando además la acción tomada por el agente de protección.

- La consola de administración deberá mostrar un indicativo del estado de la seguridad en Internet, este estado deberá permitir al administrador de la solución identificar los niveles de riesgo del exterior para poder realizar ajustes en las políticas de protección.

- La consola de administración deberá funcionar como un repositorio central de políticas para las tecnologías de Antivirus, firewall personal, detección y prevención de intrusos así como de protección al sistema operativo y control de dispositivos.

- La consola de administración deberá contar con un esquema de autenticación local, con enlace al directorio activo o con un enlace por medio de RSA para autenticación fuerte.

- La consola de administración deberá permitir la creación de administración por roles, para permitir a los administradores contar con una segregación de funciones.

- La consola de administración deberá permitir la generación de reportes gráficos que permitan identificar: los intentos de infección más repetidos en los equipos, también los equipos con mayor número intentos de infección, versión del agente de protección instalado en los equipos y un reporte de los equipos con las firmas de contenido.
- La consola de administración deberá integrar una función que permita reconocer equipos que no tengan el agente de protección instalado. Para posteriormente enviárselo a través de la consola.

- La consola de administración deberá permitir la instalación remota del agente de protección en los equipos que no cuenten con dicho software. La instalación deberá poderse realizar dando el nombre del equipo, su dirección IP o una lista combinando ambas opciones.

- La consola de administración deberá permitir la creación de roles para definir diferentes niveles de administración.

- La herramienta debe poder aplicar diferentes políticas a los equipos clientes, de acuerdo a la ubicación de los mismos. Esta ubicación se podrá definir de acuerdo al tipo de conexión (ethernet, ethernet, vpn, dial-up), rango de IP, DNS, entre otros.

1.5.1.2. Características de la tecnología antivirus

- La tecnología de antivirus deberá contar con certificación AV-Test Corporativa más actual y deberá contactar con la certificación AAA de Dennis technology labs.

- La tecnología de antivirus de la solución deberá ser capaz de detectar y eliminar spyware.

- La tecnología de antivirus de la solución deberá ser capaz de analizar los mensajes de correo electrónico recibidos en los protocolos SMTP (Simple Mail Transfer Protocol) y POP3 (Post Office Protocol).

- La tecnología antivirus de la solución deberá poder actualizar sus definiciones de virus desde Internet, el servidor central y desde un repositorio local (será decisión de la Entidad determinar el método más adecuado teniendo en cuenta diversos factores), la actualización de definiciones deberá poderse programar para realizarse en un horario que no provoque afectación a la red.

- La tecnología antivirus de la solución deberá ser capaz de realizar las actualizaciones de forma óptima, firmas de virus así como el motor de búsqueda (por ejemplo utilizando actualizaciones diferenciales y métodos de distribución).

- La tecnología antivirus de la solución deberá ser capaz de analizar archivos comprimidos en al menos los siguientes formatos: ZIP, RAR, y TAR con capacidad de analizar hasta 10 niveles de compresión.

- La tecnología de antivirus de la solución deberá ser capaz de definir exclusiones por tipo de archivo, directorios y tipo de amenaza.

- La tecnología de antivirus deberá realizar escaneos de los equipos de manera eficiente, excluyendo todos aquellos archivos que basados en reputación por parte del fabricante, no representen un riesgo, al contar con una buena reputación.

- Las políticas de antivirus de la solución deberán poderse adaptar de acuerdo al reconocimiento de la red a la cual se está conectando.

- El fabricante de la solución deberá tener su propio centro de investigación y respuesta de virus, además debe poder generar actualización a contenidos para las tecnologías de antivirus, el firewall personal y detección y prevención de intrusos.

- La tecnología de antivirus deberá contar con tecnología de reputación, es decir que valide si un archivo goza de mala reputación para que este sea bloqueado, o si goza de buena reputación para que este sea excluido.

- El agente deberá ofrecer protección al descargar archivos desde internet, al validar que el archivo descargado tenga una reputación aceptable, o en términos de distribución y antigüedad del mismo a nivel mundial.

- La solución deberá contar con herramientas con permitan escáner máquinas virtuales off-line.

- La solución deberá contar con la capacidad de excluir en las máquinas virtuales, todos aquellos archivos que ya hayan sido escaneados de una imagen base, con la finalidad de reducir el consumo de recursos.

Características de la tecnología de firewall personal y prevención de intrusos

- La tecnología de firewall personal de la solución deberá ser de tipo stateful inspection capaz de analizar el tráfico en paquetes de tipo TCP, UDP, IP y en flujo de datos.

- La tecnología de firewall de la solución deberá permitir la definición de reglas por aplicación, por protocolo, por horario, por dirección IP y por tipo de tarjeta de red.

- La tecnología de firewall de la solución deberá integrar un módulo de detección y prevención de intrusos, deberá contener firmas de ataques, estas firmas deberán ser actualizadas desde Internet o desde el servidor central.

- La tecnología de firewall de la solución deberá ser capaz de detectar y deshabilitar controladores de programas como WinPcap y VMware de considerarse riesgosos para la organización.

- La tecnología de firewall de la solución deberá contener un módulo que permita el reconocimiento de explotación de vulnerabilidades no importando el método de explotación que se esté utilizando.

- La tecnología de firewall de la solución deberá tener un módulo de inspección profunda para los protocolos DHCP, DNS y WINS.

- La tecnología de firewall de la solución deberá ser capaz de configurar el navegador en modo seguro de tal manera que no publique la versión del navegador ni la dirección IP con la que sale a Internet.

- La tecnología de firewall de la solución deberá ser capaz de detectar y bloquear ataques de OS fingerprint y de generación de secuencias de TCP.

- La tecnología de detección de intrusos de la solución deberá incluir ataques en diferentes categorías, las categorías incluidas deberán ser: ataques de buffer overflow, puertas traseras, ataques de negación de servicios, puertas traseras, programas de P2P, mensajeros y propagación de amenazas.

- La tecnología de antivirus deberá contar un módulo de evaluación de posturas de seguridad, considerando al menos búsqueda de llaves de registro, estado de antivirus, la presencia de un archivo e inclusive ejecutar scripts y contar con una serie de respuestas en caso de ser necesario, desde el mismo software de antivirus, sin instalar un software adicional en los clientes o consola de administración adicional.

- La tecnología de detección de intrusos también se deberá integrar al navegador de internet, para brindar protección a los usuarios finales.

1.5.1.3. Características de control de integridad

- La tecnología de análisis de integridad deberá poder identificar parches de sistema operativo instalados, software de terceros de seguridad instalados tales como Antivirus y Firewalls personales.

- La tecnología de análisis de integridad podrá aplicar acciones correctivas cuando detecte que existe una faltante dentro del sistema.

- La tecnología de análisis de integridad podrá aplicar acciones tales como descargar software, enviar a ejecutar aplicaciones, modificar llaves de registro, entre otros.

- La tecnología de análisis de integridad deberá poder ejecutar scripts creados por el administrador en los equipos.

1.5.1.4. Características de control de aplicaciones para protección de sistema Operativo

- La tecnología de protección de la solución al sistema operativo debe incluir mecanismos que eviten la ejecución de procesos maliciosos, estos procesos deberán poder ser definidos a través de políticas.

- La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, lectura o modificación de archivos o directorios. Estos deberán poderse definir a través de políticas.
- La tecnología de protección de la solución al sistema operativo deberá incluir mecanismos que eviten la escritura, modificación o eliminación de llaves de registro. Las llaves de registro a proteger deberán definirse por medio de políticas.

1.5.1.5. Características de bloqueo de dispositivos

- La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de los siguientes dispositivos: USB, bluetooth, PCMCIA, SCSI. Tarjetas inalámbricas, además deberá permitir la definición de nuevos dispositivos por medio del Class ID y Device ID.

- La tecnología de bloqueo de dispositivos de la solución deberá permitir la creación de exclusiones para permitir el bloqueo de USB pero no del teclado y el Mouse por ejemplo.

- La tecnología de bloqueo de dispositivos de la solución deberá permitir el bloqueo de ejecución de programas desde dispositivos removibles.

- La tecnología de bloqueo de dispositivos de la solución deberá permitir utilizar los dispositivos removibles como solo lectura.

1.5.2. Componente de Prevención contra Fuga de Información

1.5.2.1 Definición de Políticas

- La solución debe tener la capacidad de usar una sola política para explorar los datos en cualquier medio donde se almacenen o se utilicen, ya sea en la red y en los equipos de los usuarios

- Debe ser posible configurar dentro de las políticas, los mecanismos de respuesta automática que efectúen una acción cuando una amenaza sea detectada.

- La solución debe tener una SOLA consola basada en web para TODOS los aspectos relacionados con la edición y administración de políticas, a través de todos los módulos de detección (a través del monitoreo y la prevención y a través de la red y de puntos finales).

- La solución debe tener la capacidad para definir las políticas por cualquiera de los siguientes criterios: contenido, remitente/receptor, características de archivo, y protocolo de comunicaciones
- La solución debe permitir el registro configurable en las políticas de la severidad del incidente basado en:

o Cantidad de registros de datos expuestos en un incidente

- Remitente o receptor específico
- Protocolo de red utilizado
- Registros específicos que fueron expuestos
- Documentos específicos que fueron expuestos

• La solución debe soportar reglas de inclusión y de exclusión basadas en directorio de datos corporativos para reforzar las políticas basándose en cualquier atributo del remitente o del receptor de la información tales como unidad de negocio, departamento, nivel de responsabilidad, situación del empleado, nivel de acceso del usuario, ubicación geográfica, o empleado especifico o usuario externo.

• La solución debe incluir una biblioteca de plantillas de políticas predefinidas de detección orientadas al cumplimiento con regulaciones como HIPAA, así como mejores prácticas, incluyendo reglas que contengan léxicos pre-definidos para las regulaciones comúnmente requeridas

1.5.2.2. Detección - General

• Debe tener la posibilidad de extraer y examinar el contenido del texto de los archivos y de anexos con información confidencial que sean detectados

• Las capacidades de la detección y de indexación deben poder ser aplicadas para contenido de lenguaje de Europa Occidental y Asia (Japonés, Chino tradicional, Chino simplificado, y Coreano)

• La solución debe poder examinar recursivamente el contenido de los archivos tipo ZIP y TAR e identificarlos a través de la firma digital, aun cuando esté integrado en varios niveles de compresión.

• La solución debe permitir manejar archivos y anexos de correo muy grandes (20MB y más) durante el proceso de detección del contenido

• La solución debe contar con referencias de clientes que puedan proveer de testimonio sobre la exactitud de su solución.

1.5.2.3. Detección – Firma Digital de los datos (Data fingerprinting)

• La solución debe proporcionar un método de detección eficaz basado en Firma Digital de los Datos (Data Fingerprinting) para cualquier tipo de dato, tales como expedientes del cliente

• La solución debe proteger sobre una sola política por lo menos 10 millones de filas de contenido específico de información sensitiva de una Base de Datos (tal como datos del cliente o del empleado) sin el uso de palabras clave, passwords o patrones

• El método de detección de datos debe especificar qué columnas de una base de datos constituyen un elemento a proteger dentro de una o varias políticas específicas.

- El método de detección de firmas digitales de los datos debe distinguir entre campos información que pertenecen al mismo registro o fila de una base de datos contra diversas filas de la misma base de datos.

- El método de detección basado en la firma digital de los datos debe obtener coincidencias con solo el nombre y el apellido de las personas registradas en una base de datos de migrantes o empleados, sin la necesidad de un contar con un número, identificador o patrón (ej., RFC, Número de Pasaporte, etc.)

- La solución debe distinguir entre diversos tipos de números aunque estos tengan la misma cantidad de dígitos sin la necesidad de que exista una palabra clave como “Pasaporte”. Por ejemplo, distinguir un número de pasaporte de nueve dígitos que pertenece a un migrante de un número de teléfono de nueve dígitos sin la presencia de una palabra clave (ej., “SSN")

- La solución debe definir una política con datos muy específicos que pueda ser comparada contra un conjunto de datos dado, (ej., cualesquiera 3 de 5 campos de una Base de Datos que en sus combinaciones particulares no constituyan una violación)

- Debe poder normalizar en la detección cualquier variante de presentación de la información a proteger.
- La solución debe permitir especificar el grado de proximidad como una condición de una coincidencia para un incidente.

- La solución debe detectar la información sin importar que el orden de los datos haya sido alterado

- La solución debe permitir indexar 500 millones de filas datos fuente y detectar contra este índice con la misma velocidad que para una fuente de datos con 100 filas.

Detección – Firma Digital en Documentos (Document Fingerprinting)

- La solución debe permitir la aplicación de un método de detección generando una Firma Digital a partir de un documento tales como dibujos de CAD, archivos en PDF, DOC, XLS, PPT, etc.

- La solución debe tener la capacidad para proteger al menos 100.000 documentos específicos con contenido sensible (tal como propiedad intelectual, código fuente, documentos financieros, etc.) sin la dependencia de palabras claves o patrones

- El método de detección basado en Firma Digital de Documentos debe soportar la detección del contenido si este es idéntico o en porciones de contenido o en diversos formatos de archivo. Por ejemplo, si un documento está en el formato de Microsoft Word, la solución detectará una violación aunque el mismo texto se ha cortado y pegado en un email directamente o se ha convertido a formato PDF

- La solución debe soportar la detección de coincidencias en un contenido con exactitud del 100% para documentos específicos tales como código fuente, párrafos específicos, documentos de diseño, documentos de comercialización, financieros, etc.

- La solución debe soportar la detección coincidencias de derivados o de versiones de cortado y pegado del contenido de documentos específicos tales como código fuente, párrafos específicos, documentos de diseño, documentos de comercialización o financieros.

- Debe ser posible definir un umbral o porcentaje mínimo requerido de coincidencia de un documento para considerar que existe una violación a la política configurada (ej., se registra una violación a la política si y solamente si el 50% o más de un documento es encontrado). Esta función debe ser configurable por cada política.
- Debe ser posible definir "listas blancas" sobre la información y contenidos protegidos por una política para evitar que sean detectados y se generen eventos “falsos-positivos”.

1.5.2.4. Detección – Descripción de Contenidos

- La solución debe soportar la detección vía descripción de contenidos usando reglas completamente adaptables con palabras y frases claves no solo como palabras independientes sino también como palabras dentro de frases completas u otras palabras.

- Debe ser posible configurar dentro de las políticas listas de palabras clave o diccionarios para la detección por lo menos de 10.000 entradas sin la degradación del rendimiento en la detección

- Debe soportar la detección basada en expresiones regulares completamente adaptable

- Debe soportar la detección de eventos combinando la coincidencia con patrones de datos y validaciones específicas del contenido que desea ser detectado. Por ejemplo, puede detectar patrones comunes de un dato estructurado combinado con validaciones de digito verificador para asegurar que sea un dato válido.

- Debe poder detectar la presencia o transmisión de archivos cifrados.

- Debe permitir incluir coincidencias de datos dentro de ciertos rangos definidos por el usuario sin tener que escribir una expresión regular. Por ejemplo, puede detectar datos estructurados solamente identificando una parte de la cadena de dígitos que represente números específicos de identificación del país emisor de un pasaporte

- Debe soportar la detección basada en un tipo de documento particular, incluso si el remitente o usuario ha cambiado la extensión o el nombre del archivo

1.5.2.5. Respuestas a Incidentes automatizada y obligatoria

La respuesta a incidentes de fuga de información deberá:

- Enviar las alarmas de incidencia vía email

- Notificar automáticamente a remitentes o a los jefes inmediatos cuando un usuario ha violado una política.

- Proporcionar notificaciones en pantalla a los usuarios administradores de la consola sobre violaciones en "puntos finales". Los usuarios infractores deben poder proporcionar una justificación de su conducta, misma que será adjuntada al incidente en cuestión

- Ejecutar diferentes acciones de respuesta para diversos casos dentro de una misma política dependiendo de diversos parámetros, tales como la política violada, la severidad del incidente, el número de coincidencias encontradas, el protocolo de comunicaciones usado, el estado de conexión del "punto final", y el método de detección utilizado

- Permitir el registro y modificación del flujo de trabajo para el seguimiento y la remediación de un incidente (ej., códigos de estado, atributos, asignación de colas, severidad etc.)

1.5.2.6. Flujo de seguimiento para la respuesta a incidentes

- Los incidentes registrados deben ser visibles vía "web" en un formato útil para los usuarios de negocio.

- Los incidentes registrados deben incluir una indicación clara de cómo la transmisión de información o el archivo especifico violó la política en cuestión (en tiempo real, apenas la política fue violada), incluyendo la identificación clara del contenido identificado como coincidencia con la Política

- El Flujo de seguimiento para la respuesta a incidentes deberá:

- Mostrar claramente información de la identidad del remitente (tal como nombre completo, nombre del gerente, unidad de negocio, cuenta de correo)

- Permitir el abrir los anexos originales de la información confidencial anexada a un incidente directamente de la interfaz web de la consola de administración

- Permitir el definir diferentes niveles de acceso a los incidentes, de tal forma que la política pueda ser configurada para que solo ciertos usuarios puedan tener acceso y asignación para la remediación de cierto grupo de incidentes

- Permitir la definición y consulta directamente en la consola (no a través de un reporte) de un “caso” o un grupo de incidentes encontrados para ser relacionados en la ejecución de una investigación

- Permitir el exportar un grupo de incidentes fácilmente de la solución a un formato fácilmente legible por una persona sin acceso al sistema (ej., xls, txt)

- Por cada Política permitir la modificación de forma manual de la acción de respuesta del flujo de trabajo para la remediación de un incidente (ej., códigos de estado, atributos, asignación de colas, notificaciones, etc.)

- Permitir la creación de atributos especificados por el usuario sobre los incidentes que le permitan correlacionarlos al proceso de remediación existente

- Las políticas incluidas en las plantillas de políticas predefinidas de la solución deben contener también la configuración de respuestas recomendadas por las mejores prácticas de la industria para el cumplimiento de las normas.

1.5.3 Componente de Cifrado de Información

1.5.3.1 Requerimientos Generales

- Se requiere una herramienta para cifrar de manera completa los almacenamientos de los computadores portátiles y que también permita el intercambio de información cifrada.

- La solución se debe sincronizar con Directorio Activo, y debe soportar LDAP y OpenLDAP

- Deberá poderse integrar con soluciones DLP para prevención de fuga de información

- Deberá poder configurar políticas que fuercen el cifrado de archivos y carpetas que se almacenen en dispositivos de almacenamiento extraíble

- Deberá poder permitir la creación de usuarios que tengan privilegios de administración en la solución

- Deberá poder cumplir con los requisitos de contraseñas complejas para usuarios administradores definidos en la Entidad.

- Deberá permitir la creación de usuarios en la solución cuando esta esté sincronizada con el directorio activo.

- La consola de administración de la solución podrá accederse a través de un navegador de manera segura y cifrada

- Debe poder realizar un backup de la base de datos de una forma sencilla a través de la consola de administración y debe permitir que las copias de seguridad de configuración de la herramienta se guarden en un sitio via FTP o a través del protocolo seguro SCP.

- El Servidor de Gestión deberá permitir arquitecturas que aseguren la alta disponibilidad de la solución.

1.5.3.2. Gestión de la Solución

- Deberá generar reportes gerenciales, detallados de la solución

- Deberá generar logs o alertas por fallas en el cifrado de un disco y dispositivo de almacenamiento extraíble.

- Deberá cifrar las claves en la base de datos de la solución

Capacidades de los Agentes

- Los agentes de soportar los siguientes sistemas operativos: Windows XP, Windows 8, 8.1. y 10, MacOS X y Linux

- La herramienta permitirá el cifrado de discos duros internos (Ciframiento total del disco duro), ciframiento de archivos en general, ciframiento de carpetas, creación de archivos cifrados de manera segura (ZIP).

- Debe permitir la creación de carpetas y archivos cifrados y que puedan ser compartidos y accedidos por los usuarios autorizados.

- La solución permitirá la creación de discos duros virtuales cifrados que podrán montarse

- La solución de ciframiento permitirá la firma y el ciframiento de información a través de correo electrónico.

- Se podrá controlar la frecuencia que los agentes de la herramienta de cifrado renuevan sus políticas de cifrado con la consola de gestión.

- Debe controlar las opciones de cifrado inicial del disco cuando se presente interrupción en la alimentación de corriente eléctrica.

- Debe permitir la inscripción de usuarios del directorio activo y usuarios creados en la solución.

- Debe poder permitir restringir únicamente el cifrado de una partición en un disco duro, si esto es requerido.

- Debe controlar las opciones de cifrado inicial del disco cuando se presente interrupción en la alimentación.

- Debe permitir el acceso a usuarios del Directorio Activo previamente inscritos (enrolled)

- Debe permitir el acceso a varios usuarios del Directorio Activo a un mismo equipo cifrado (pre-boot)

- Debe permitir el cambio de contraseña cuando caduque en el Directorio Activo

- La solución no debe permitir la deshabilitación del pre-boot por parte de un usuario.

- La solución debe realizar el bloqueo del usuario por intentos fallidos al momento del inicio de la máquina (Booteo)

- La solución debe permitir la recuperación de contraseñas cuando el usuario tenga conectividad con el servidor.
- La solución debe permitir la recuperación de contraseñas cuando el usuario no tenga conectividad con el servidor.

- Debe permitir el acceso al disco encriptado con credenciales administrativas creadas en la solución.

- Debe permitir el cifrado completo de dispositivos de almacenamiento extraíble

- Debe permitir el cifrado de una partición en dispositivos de almacenamiento extraíble

- Debe permitir el cifrado de un archivo en dispositivos de almacenamiento extraíbles

- Debe generar archivos cifrados que puedan ser leídos por usuarios que no tengan instalado el cliente de cifrado.

- La solución debe integrarse con soluciones de autenticación de doble factor de autenticación.

- Debe generar logs y reportes sobre la actividad de cifrado en los clientes.

- Debe permitir varios mecanismos que permitan la ágil recuperación de claves

- Debe permitir el cifrado de una unidad externa o unidad mapeada

- Debe permitir el fraccionamiento de la llave de recuperación, para que esta sea custodiada por dos o más administradores

- Debe permitir el acceso remoto a un equipo que tenga cifrado de disco después del proceso de Pre-boot

1.6 Niveles de Servicio

Disponer de un modelo de servicio 5*8, es decir, 5 días a la semana, para dar asesoría que permita la solución de fallas técnicas o mejora en el desempeño de la solución. Este modelo de prestación de servicios incluye prestar el soporte en las diferentes actividades requeridas por la ANH.

1.7 Mantenimientos Preventivos y Correctivos

Durante el periodo de 3 años, contados a partir de la firma de acta de inicio del contrato, el servicio de mantenimiento preventivo deberá incluir como mínimo dos (2) visitas mensuales con un tiempo no inferior a cuatro (4) horas cada una (es decir ocho (8) horas de soporte al mes), para hacer seguimiento a las políticas de seguridad y al funcionamiento de la consola del Software Antivirus, así mismo verificar y aplicar las últimas actualizaciones de firmware y/o software existentes al momento del mantenimiento. El servicio no deberá significar costo alguno para la ANH.

Para el mantenimiento correctivo durante el período de soporte, éste deberá ser atendido en un tiempo máximo de 4 horas contadas a partir del requerimiento. El servicio requerido no deberá significar costo adicional alguno para la ANH.

En caso de presentarse una falla técnica que no pueda ser resuelta por vía telefónica, se debe asignar el recurso humano y técnico necesario para solucionar dicha falla técnica, el tiempo para estar en el sitio no debe ser mayor a cuatro (4) horas hábiles.

En caso de determinarse que el problema es de hardware y no puede ser resuelto dentro de las 8 horas siguientes, el contratista debe reinstalar la consola de antivirus con las configuraciones necesarias y subir la última copia de seguridad en un equipo suministrado por la ANH.

1.8 Actualizaciones de Software

El proponente deberá garantizar mediante certificación vigente emitida por el fabricante la actualización de firmware y/o software de tal forma que la entidad siempre tenga la última versión de la consola de antivirus; si es el caso durante el tiempo de ejecución del contrato, lo cual no deberá significar costo adicional alguno para la ANH.

1.9 Certificaciones

El Oferente debe proporcionar la certificación vigente del fabricante donde conste que es distribuidor autorizado para realizar la comercialización, el soporte y mantenimiento para la consola de antivirus suministrada.

1.10 Recurso Humano para el Soporte tecnico

Proveer el recurso humano necesario para la prestación del servicio, el cual estará bajo cuenta y riesgo del contratista, entendiéndose que no se genera relación laboral alguna ni con el contratista ni con el personal a su cargo, en consecuencia tampoco existirá pago de prestaciones sociales ni de ningún tipo de costos distintos al valor acordado, por parte de la ANH.

Para garantizar la calidad de los servicios de soporte, el oferente deberá disponer como mínimo de un (1) Ingeniero certificado vigente por el fabricante y con una experiencia mínima de dos (2) años en contratos de soporte relacionados con el objeto del contrato.

		CANT	PERFIL

ITEM	NIVEL EDUCATIVO		PROFESION	EXPERIENCIA
1.	INGENIERO	1	Ingeniero de sistemas o electrónico o comunicaciones o eléctrico, o redes	Experiencia profesional mínima de dos (2) años en contratos de soporte relacionados con el objeto del contrato y Certificación del Fabricante en los productos objeto del contrato.

1.11 Entrega de Información del Sondeo de Mercado

Las firmas interesadas deberán enviar una cotización antes de las 5:45 p.m. del día 8 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 ***1.5 Especificaciones Técnicas***
Formato de Propuesta Economica

ANH AGENCIA NACIONAL DE HIDROCARBUROS COLOMBIA

FORMATO DE PROPUESTA ECONOMICA

Objeto: Adquirir el licenciamiento de plataforma de seguridad de usuario final con servicio de soporte, para la infraestructura tecnológica y parque computacional de la Agencia Nacional de Hidrocarburos.

Item	Descripcion	Cantidad	Valor Unitario	Valor Total	IVA sobre el Total	Valor Total con IVA
1	Licenciamiento y Soporte de Sistema de Proteccion de Punto Final por 3 años(Antivirus, antispyware, Control de Aplicaciones. Anexo Tecnico Numeral 3.1)	500				
2	Licenciamiento y Soporte de Sistema DLP por 3 años (Anexo Tecnico Numeral 3.2)	400				
3	Licenciamiento y Soporte de Sistema de Cifrado de equipos de Computo (Anexo Tecnico Numeral 3.3)	20				
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 – Contratista