Al contestar cite Radicado 20186010079123 Id: 271611
Folios: 9 Fecha: 2018-04-18 04:33:27
Anexos: 0
Remitente: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA
Destinatario: GESTION DOCUMENTAL

PARA: **COTIZANTE**

ASUNTO: Sondeo de Mercado para la contratación cuyo objeto es *"Realizar pruebas de Vulnerabilidad y ethical hacking a los sistemas 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 "*Realizar pruebas de Vulnerabilidad y ethical hacking a los sistemas de la ANH.".*

Para tales efectos, le informo que la Entidad realizará una Audiencia Pública con todos los interesados en participar, el día jueves (19) de Abril del presente año a las 11:00 a.m. en la Entidad – 2º piso, con la finalidad de exponer los aspectos técnicos del proyecto y resolver las observaciones e inquietudes de los participantes de la misma, de tal manera que la ANH realice el Análisis del Sector y establezca un valor estimado del proyecto que garantice, entre otros aspectos, un presupuesto acorde con los valores actuales del mercado y una participación plural de oferentes en el proceso de contratación.

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

Es de resaltar que los interesados en participar en el sondeo de mercado deberán enviar su cotización, a más tardar el día 23 de abril del presente año, a los correos electrónicos juan.vila@anh.gov.co y carlos.bastidas@anh.gov.co. A los 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 Administrativa y Financiera
Agencia Nacional de Hidrocarburos – ANH

Aprobó: Juan Carlos Vila Franco – Jefe Oficina de Tecnologías de la Información / Componente Técnico

Revisó: Carlos Abel Bastidas Cubillos -Experto G6 Grado 3 / Componente Técnico
Revisó:: Diana Constanza Rojas Rubio / Componente Financiero

Revisó:: Adriana Katherine Pena / Componente Jurídico
Proyectó: Nestor Geovanny Lopez Leguizamon / Componente Técnico / Cto 073 de 2018

SONDEO DE MERCADO

La AGENCIA NACIONAL DE HIDROCARBUROS 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 – AGENCIA NACIONAL DE HIDROCARBUROS, 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:	La AGENCIA NACIONAL DE HIDROCARBUROS necesita identificar la presencia de vulnerabilidades informáticas en un conjunto de equipos y aplicaciones de la Entidad. Así como analizar el tráfico de red en puntos estratégicos de la organización con el fin de determinar comportamiento anómalo desde el punto de vista de seguridad de la información. Identificar la presencia de posibles amenazas avanzadas persistentes. Nota: Teniendo en cuenta que esta contratación presenta concurrencia, entre un concurso de mérito y una mínima cuantía, según lo establecido con el numeral 3 del artículo 2 de la Ley 1150 de 2007 la modalidad de selección aplicable es la de mínima cuantía
OBJETO A CONTRATAR:	*Realizar pruebas de Vulnerabilidad y ethical hacking a los sistemas de la ANH.*
Línea en el PAA	555 de 2018
IDENTIFICACION DEL CONTRATO A CELEBRAR:	Consultoria
CÓDIGO UNSPSC (The United Nations Standard Products and Services Code® - 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:

Código Estándar de Productos y Servicios de Naciones Unidas), correspondiente al bien, obra o servicios a contratar:

CODIGO	DESCRIPCION
811111500	Ingenieria de Software o Hardware
81111900	Sistemas de Recuperación de Información
81111700	Sistemas de manejo de información MIS
81111800	Servicio de Sistemas y administración de componentes de sistemas

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.

ASPECTOS TÉCNICOS:

Requerimiento Técnico Mínimo

El servicio requerido está compuesto por tres actividades principales como se muestra a continuación:

Diagnóstico Actual de Vulnerabilidades
Búsqueda de Amenazas Avanzadas Persistentes
Análisis de Comportamiento de la Red.

Estas tres actividades están enfocadas a diagnosticar la seguridad de la red de datos y sistemas de comunicaciones de la organización, con el fin de determinar la presencia de vulnerabilidades conocidas en los principales sistemas de la organización, posibles fuentes de fuga de información, presencia de malware convencional o particularmente diseñado para la organización, o amenazas avanzadas persistentes.

Cada una de las actividades mencionadas es descrita de la siguiente forma:

1. **DIAGNÓSTICO DEL ESTADO ACTUAL DE LAS VULNERABILIDADES INFORMÁTICAS**

Se ejecutará un análisis de vulnerabilidades informáticas sobre un conjunto de 100 equipos muestra (entre internos y externos) con el fin de detectar la presencia de vulnerabilidades informáticas conocidas y la posible presencia de malware en los mismos.

Se debera generar un informe técnico y otro ejecutivo con los resultados obtenidos y un plan detallado de remediación.

Adicionalmente se ejecutará una prueba de retest para medir la eficiencia de las acciones de remediación ejecutadas por la entidad, esta prueba se realizará en un periodo posterior a su obtención sin que exceda el periodo del contrato

ASPECTOS TÉCNICOS:	**2. ANÁLISIS DEL COMPORTAMIENTO DE LA RED** Se analizará el tráfico de la red de la entidad en dos puntos críticos de la misma con el fin de detectar posibles comportamientos anómalos como: • Presencia de malware • Fuga de Información • Acceso a aplicaciones de alto riesgo • Amenazas de dispositivos móviles • Detección de equipos infectados perteneciendo a posibles botnets. **3. ANÁLISIS DE AMENAZAS PERSISTENTES AVANZADAS** Se realizará un análisis para determinar la presencia de posibles Amenazas Persistentes Avanzadas, y de las cuales, en caso de presentarse, se realizarán para estos dispositivos las siguientes fases: **a. EXTRACCIÓN DE IMÁGENES FORENSES** Esta actividad consiste en extraer una copia idéntica de la información digital contenida en cada uno de los medios de almacenamiento digital (PC, Smartphone), esto, para asegurar, identificar y posteriormente realizar actividades forenses que permitan determinar la existencia de algún software espía previamente instalado. La copia extraída es asegurada como evidencia digital bajo los lineamientos de la informática forense y de la cadena de custodia, para iniciar procesos legales, en caso de así requerirlo. Lo requerido de este procedimiento forense, es el aseguramiento de la evidencia digital desde el mismo momento de su recaudo, esto, mediante la identificación única a través de técnicas HASHING (cadena de 32 y/o 40 caracteres alfanuméricos que permita identificar de una manera única e inequívoca un archivo digital sin importar su extensión) y estampas de tiempo (Time Stamping), las cuales son registradas en la diligencia de inspección, así como en los formatos propios de cadena de custodia que deben ser diligenciados para este tipo de actividades. Para la intervención en campo, se tomarán como referentes las mejores prácticas en temas forenses, las cuales se encuentran referenciadas a través de la norma ISO/IEC 27037 del año 2012. Este requerimiento incluye: Recolección, embalaje, custodia, preservación y aseguramiento de evidencia digital bajo parámetros propios de cadena de custodia y con un tamaño máximo de 1TB de información en total.

Utilización de herramientas forenses en sitio, estas son: Bloqueadores, copiadores de discos, software de recolección de evidencias digitales, entre otros, los cuales permiten proteger la evidencia frente a cambios y/o modificaciones, y con ello, mantener su valor probatorio.

b. ANÁLISIS DE LA EVIDENCIA DIGITAL

Una vez extraídas las imágenes forenses, se debe realizar un proceso de recuperación de particiones eliminadas, ocultas, sobre escritas, así mismo, se procederá con la recuperación de información (datacarving), reconstrucción de archivos con estructuras complejas (File Mounter), ingeniería inversa, entre otros, culminando con búsqueda de información relacionada con posibles incidentes de seguridad ocurridos. Estas actividades se deben llevar a cabo en un laboratorio Forense dispuesto para tal fin.

Para la realización del análisis forense, se tendrán en cuanta todos los lineamientos de la norma ISO/IEC 27042 del año 2015.

Para este servicio se deben utilizar herramientas de software avaladas en todo el mundo y licenciadas -FTK (Forensics Tool Kit), así como equipos de hardware de última tecnología frente a temas de procesamiento.

c. ESCANEO DEL ESPECTRO RADIOELÉCTRICO

Se asignará un experto Forense, quien hará un escaneo al lugar determinado por el cliente, para lo cual deberá emplear una metodología de barrido, así como la utilización de equipos de hardware y/o software que permiten hallar frecuencias análogas y/o digitales emitidas por dispositivos electrónicos que pudieran haber sido instalados con fines de monitoreo.

4. EQUIPO MINIMO DE TRABAJO

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

El personal presentado en la propuesta debe ser el mismo que realiza el desarrollo del contrato, no obstante, 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 de la ANH.

PERFIL	CANT	DISPONIBILIDAD	PROFESION	EXPERIENCIA
Gerente de Proyecto	1	100%	Ingeniero Eléctrico, Electrónico o de Sistemas o carreras afines.	Experiencia Profesional de al menos diez (10) años y experiencia en implementación de al menos cinco (5) proyectos de seguridad de la Información.
Líder Técnico	1	70%	Ingeniero Eléctrico, Electrónico o de Sistemas o carreras afines	Experiencia Profesional de al menos diez (10) años y experiencia en al menos cinco (5) proyectos de seguridad de la Información. Al menos dos de las siguientes certificaciones Mínimas requeridas: Certified Information Security Manager de ISACA (CISM) Certified Information Systems Security Professional de ISC2 (CISSP) Auditor Líder de la norma ISO 27001:2013 Certified Ethical Hacker (CEH). Computer Hacking Forensic Investigator (CHFI), Certified Security Analyst, otorgadas por el E-Comerce Council (EC-Council®).
Consultor	1	70%	Ingeniero	

Senior			Eléctrico, Electrónico o de Sistemas o carreras afines	Experiencia Profesional de al menos diez (10) y Experiencia en al menos cinco (5) proyectos de seguridad de la Información como Perito de Delitos Informáticos y Computo forense.
Analista Senior	1	100%		Experiencia Profesional de al menos cinco (5) años y Experiencia en al menos cinco (5) proyectos de seguridad de la Información en aseguramiento, adquisición, recolección y análisis de evidencia digital como pruebas electrónicas, y de Delitos.

5. EJECUCIÓN BASADA EN PROYECTO

•Gerencia de Proyecto

El proponente deberá asignar un profesional con experiencia certificada en la gerencia de proyectos relacionado con el objeto de contrato como se establece en el equipo mínimo de trabajo.

En la fase inicial de la ejecución de la contratación como proyecto, el proponente deberá entregar la siguiente documentación.

- Plan de Proyecto
- Estructura de desglose de trabajo (EDT).
- Diccionario de EDT
- Cronograma
- Ruta Critica
- Líneas Bases
- Plan de Riesgos.

El proponente deberá entregar previo al inicio del proyecto, la Ingeniería de detalle, que tenga conexidad con los entregables propios del contrato, del plan de trabajo y que especifique en detalle, las ejecuciones técnicas

	a realizar. Se debe realizar reuniones mínimo cada 2 semanas para evaluar los avances de ejecución, del proyecto. Al finalizar el proyecto, el proponente deberá entregar el Asbuild donde se especifique en detalle, las actividades ejecutadas en su totalidad y se debe radicar como entregable obligatorio y previo a la radicación de la factura, en las instalaciones de la ANH, Calle 26 No. 59 – 65 Piso 1 Radicaciones.
PLAZO:	El plazo de ejecución del contrato a celebrar será hasta el 31 de diciembre de 2018 contados a partir de la suscripción del acta de inicio y de acuerdo con el cronograma acordado con el contratista, previos requisitos de perfeccionamiento y ejecución del contrato.
LUGAR DE EJECUCIÓN:	Para todos los efectos el domicilio contractual será la ciudad de Bogotá DC.
PROPUESTA ECONÓMICA:	Incluir el formato económico diseñado por el dueño del proceso el cual debe ser claro e incluir todos los costos e impuestos que apliquen.

PROPUESTA ECONÓMICA

"Realizar pruebas de Vulnerabilidad y ethical hacking a los sistemas de la ANH".

Ítem	Descripción	Valor (COP)	IVA (19%)	Total (COP)
1	Servicio de diagnóstico de seguridad informática Ethical Hacking, para las actividades anteriormente descritas.	$	$	$
VALOR TOTAL		**$**	**$**	**$**

Por favor abstenerse de modificar la propuesta económica.

Nombre y Firma Represéntate Legal: _____

Nombre Empresa: _____

NIT: _____

Validez de la Oferta 60 días.

Los valores deberán presentarse en Pesos Colombianos.

Adjuntar con la presente propuesta Económica, RUT.

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 23 de Abril de 2018, diligenciando la presente propuesta económica.

Nota: Se reitera que la presente consulta de precios no obliga ni compromete la responsabilidad de la Agencia Nacional de Hidrocarburos; más bien, se constituye en uno de los instrumentos para establecer el presupuesto oficial estimado del proyecto a contratar.