PARA: **OFERENTE**

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

ASUNTO: Sondeo de Mercado para la contratación cuyo objeto es *"*Adquirir una Herramienta Informática para gestión de permisos y seguimiento a los accesos de módulos, carpetas y archivos de datos no estructurados, compartidos en red*"*

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 "Adquirir una Herramienta Informática para gestión de permisos y seguimiento a los accesos de módulos, carpetas y archivos de datos no estructurados, compartidos en red."

Para tales efectos, le informo que la Entidad realizará una Audiencia Pública con todos los interesados en participar, el día martes diecisiete(17) de octubre del presente año a las 9:00 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 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 martes (17) de octubre del presente año, a los correos electrónicos juan.vila@anh.gov.coy carlos.bastidas@anh.gov.coa 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 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:	La ANH requiere adquirir una herramienta informática para gestión de permisos y seguimiento a los accesos de módulos, carpetas y archivos de datos no estructurados, compartidos en red, con el fin de poder adelantar la trazabilidad de los datos y archivos en sus almacenamiento NAS (Network Attached Storage) y de las carpetas competidas, con el fin de tener una visibilidad de seguridad y control de accesos a la información pública, semiprivada y privada con la que cuenta la Agencia, así como centralizar la gestión de permisos de los mismos, garantizando el adecuado acceso a la información misional, estratégica y de apoyo de la Entidad.
OBJETO A CONTRATAR:	Adquirir una Herramienta Informática para gestión de permisos y seguimiento a los accesos de módulos, carpetas y archivos de datos no estructurados, compartidos en red.
IDENTIFICACION DEL CONTRATO A CELEBRAR:	Compra / Venta

<table>
<tr>
<td>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:</td>
<td>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:

<table>
<tr><th>UNSPSC</th><th>CLASE</th></tr>
<tr><td>81112000</td><td>Servicios de datos.</td></tr>
<tr><td>43201800</td><td>Dispositivos de almacenamiento</td></tr>
<tr><td>43221700</td><td>Equipo fijo de red y componentes</td></tr>
<tr><td>43232300</td><td>Software de consultas y gestión de datos</td></tr>
<tr><td>81111700</td><td>Sistemas de manejo de información MIS</td></tr>
<tr><td>81111500</td><td>Ingeniería de software o hardware</td></tr>
<tr><td>43233500</td><td>Software de intercambio de información</td></tr>
</table>

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.</td>
</tr>
<tr>
<td>Plazo de Ejecución:</td>
<td>El plazo de ejecución del contrato es de VEINTE (20) DIAS SIN QUE EXCEDA EL 31 DE DICIEMBRE DE 2017 para la implementación del sistema, contadas a partir de la fecha del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento del contrato.

Periodo de Soporte y Mantenimiento: Doce (12) Meses</td>
</tr>
</table>

Modalidad de selección:	La Entidad acudirá a la modalidad de SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES POR SUBASTA INVERSA, prevista en el literal a) del numeral 2 del artículo 2 de la Ley 1150 de 2007 y el Capítulo II de la Sección I Modalidades de Selección, y lo dispuesto en el artículo 2.2.1.2.1.2.2 del Decreto 1082 de 2015. **La selección se efectuará bajo la ponderación de menor precio**, debido a que se trata de servicios con características técnicas uniformes y común utilización.

ESPECIFICACIONES TÉCNICAS DE LA HERRAMIENTAS DE SOFTWARE.

i.- HERRAMIENTA INFORMÁTICA PARA LA ANH	
1	**Características Generales.**
1.1	Solución integral de software para gobierno de datos no estructurados para la plataforma de servidores de ANH.
2	**Características Específicas.**
2.1	**Componentes.**
2.1.1	Software indicando tipo y versión (especificar)
2.1.2	La herramienta deberá realizar la Trazabildad de las actividades relacionadas de los siguientes productos y servicios Microsoft implementados en la infraestructura de ANH
2.1.3	**Active Directory 2008 y superiores**:
2.1.4	Describir el tipo de Directorio Activo
2.1.5	400 usuarios
2.1.6	**File Server con Windows 2008 y superiores**:
2.1.7	Describir el tipo de de File servers
2.1.8	400 usuarios
2.1.9	**Servidores de Clúster NAS**
2.1.10	**Describir el tipo de Cluster NAS**
2.1.11	**400 usuarios**
2.2.	**Escalabilidad.**
2.2.1	La herramienta debe permitir la expansión de la cantidad de licencias de usuarios en al menos en un 50% de lo solicitado en los puntos 2.1.5, 2.1.8 y 2.1.11 con la misma consola de administración y sin necesidad de una nueva instalación.

2.2.2	La herramienta debe permitir el incremento de usuarios concurrentes para la administración y operación de la solución con el mismo equipamiento provisto en al menos en un 50% de lo solicitado en el punto 2.2.1.
2.3	**Administración.**
2.3.1	La solución deberá permitir su gestión en forma centralizada. La provisión de dicha funcionalidad deberá suministrar la posibilidad de ser realizada mediante un canal seguro, local y remoto.
2.3.2	Debe permitir como mínimo 8 usuarios concurrentes para la administración y operación de la solución.
2.3.3	Debe suministrar identificación y autenticación simple de usuarios e integrable con Active Directory/ LDAP.
2.3.4	Debe facilitar la segregación de funciones entre los roles indicados permitiendo mínimamente el siguiente nivel de granularidad: capacidad de operar, consultar y administrar.
2.3.5	Debe suministrar un módulo de Trazabildad que registre y reporte la actividad realizada en la administración y uso de la misma, incluyendo mínimamente inicio y cierre de sesión y trazabilidad de las acciones de los usuarios de la solución, registro de eventos del ciclo de vida de los usuarios de la solución, registro de todos los eventos asociados a los usuarios de la solución y registro de eventos del ciclo de vida de las reglas de Trazabildad administradas por la solución.
2.3.6	Debe garantizar la operación normal de los sistemas bajo observación aún frente a fallas en el funcionamiento de la solución, sin afectar la operación de los sistemas monitoreados.
2.3.7	Si se requiere instalar un software del tipo agente, se deberá garantizar el mínimo impacto en el rendimiento de los equipos involucrados no incrementando el consumo de sus procesadores, uso de memoria y uso de servicios de red, en más de un 5% y no se deberá requerir el reinicio de dichos equipos para su instalación.
2.3.8	No deberá implementarse en función de los logs nativos de los componentes requeridos, y en caso de cortes de conexión la solución deberá contar con un buffer que le permita almacenar la información de eventos sin sobrescribirlos.
2.3.9	La herramienta debe permitir la visualización de los logs mediante una interfaz gráfica de administración y seguimiento detallado, y a su turno permitir la realización de análisis en tiempo real de los registros de eventos, brindando facilidades de explotación.
2.3.10	Los reportes programados deben poderse enviar mediante correo electrónico a diferentes destinatarios e incluir el adjunto en formatos como excel, pdf, como mínimo entre otros.
2.3.11	Debe permitir granularidad en la generación de reportes personalizados, a demanda y periódicos, que satisfaga una combinación de todas las variables y atributos que provea la solución y generación de reportes estadísticos. Estos deberán poder exportarse a formatos pdf,xls,html.
2.3.12	Debe permitir visibilidad gráfica de permisos por cada objeto, usuario o grupo de todas las carpetas donde el usuario o grupo tiene permiso de acceso.

2.3.13	Debe permitir una visibilidad gráfica de la configuración de permisos, incluyendo herencia on/off (protección), singularidad, y compartido/no compartido, de forma interactiva. Además de filtros para ver solo ciertos objetos, incluyendo carpetas protegidas o únicas.
2.3.14	La solución debe permitir en una sola interfaz gráfica para todas las plataformas, supervisar la visibilidad bi-direccional y multi-nivel de los directorios que pueden ser accedidos por los usuarios y en la dirección opuesta, mostrando todas las carpetas en las que tiene acceso el usuario y qué tipo de acceso (lectura, escritura, modificación).
2.3.15	La solución debe identicar los permisos excesivos basados en el análisis de los eventos de Trazabildad.
2.3.16	La herramienta debe permitir visibilidad completa de los permisos de usuarios, grupos y carpetas de los sistemas de archivos (carpetas de recursos compartidos).
2.3.17	Pista de trazabilidad detallada de cada evento de acceso, por usuario o por carpeta.
2.3.18	Alertar de puntos en donde los permisos excesivos pueden ser removidos y la habilidad de simulación de cambios sin afectar la producción.
2.3.19	La herramienta debe permitir gestión de usuarios y permisos a los datos y carpetas.
2.3.20	Identificar la propiedad de datos a través del análisis de la actividad del usuario.
2.3.21	La herramienta debe tener una arquitectura extensible para incluir otros metadatos, funcionalidades y plataformas.
2.3.22	Permitir a los usuarios y a los propietarios de los datos controlar el acceso a sus datos.
2.3.23	Identificar automáticamente a los propietarios de datos para incluirlos en procesos de gobierno de datos.
2.3.24	La herramienta debe permitir la administración del derecho y acceso de manera eficiente y efectiva.
2.3.25	La herramienta debe auditar el acceso a cada archivo y correo electrónico.
2.3.26	Identificar e incluir a los propietarios de datos.
2.3.27	Se requiere proveer inteligencia crítica para el personal de TI, acerca de quién puede y quién está teniendo acceso a los datos, quién es el propietario de los datos, y en qué lugar puede reducirse el acceso a los datos de manera fácil, sin afectar los procesos.
2.4	**Active Directory**. La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.4.1	Trazabilidad de la actividad total de usuarios y administradores y de cambios realizado en AD y GPO (Group Policies Object).
2.4.2.	Control de Cuentas de Usuarios: Bajas e Inhabilitaciones - Accesos No permitidos – Intentos de logueos fallidos – Identificar Cuentas Bloqueadas – Actividad de Usuarios
2.4.3	Identificación de patrones de actividad inusual en el Directorio Activo.
2.4.5	Proporcionar informes de inconsistentes SID en ACLs (Listas de Control de Acceso), y ACE de usuarios Individuales en ACL's (Listas de Control de Acceso).
2.4.6	Generar informes de datos inactivos o usuarios inactivos de una plataforma monitoreada.
2.4.7	Proporcionar informes de usuarios desabilitados que aún están en grupos de seguridad un dominio específico.

2.4.8	Uso del Active Directory como medio de autenticación y control de acceso de la Solución.
2.4.9	Deberá tener la capacidad de importar los diferentes datos adicionales del active directory en los reportes creados, como por ejemplo descripción, departamento,correo electrónico, OU entre otros.
2.4.10	Deberá contar con alertas en tiempo real sobre el bloqueo de cuentas en el active directory.
2.4.11	Deberá contar con alertas en tiempo real que identifiquen la eliminación de Políticas de grupo (GPO).
2.4.12	Deberá contar con alertas en tiempo real que identifiquen cuando un usuario está realizando eliminaciones de objetos en el directorio activo.
2.4.13	Deberá contar con la capacidad de identificar en tiempo real el bloqueo de cuentas de tipo (servicio, adminitradores).
2.5	**File Server**. La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.5.1	Trazabilidad de la actividad total de usuarios y de cambios realizados.
2.5.2	Control de permisos sobre usuarios y grupos.
2.5.3	Control de permisos sobre de archivos y carpetas.
2.5.4	Generación de reportes.
2.5.5	Permitir dar visualización bidireccional de permisos (usuario-carpeta, carpeta-usuario) de las asociaciones y privilegios de los usuarios y su alcance.
2.5.6	Permitir identificar patrones de actividad inusual en el acceso y uso de información en los File servers.
2.6	**Trazabildad.** La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.5.1	Grabar toda actividad de archivo y carpeta: abrir, crear, remover, modificar, mover, nombre de usuario, archivo impactado, ruta, nueva locación, hora de la actividad, número de veces de la actividad realizada entre otros.
2.5.2	Proporcionar una visibilidad gráfica de la actividad de acceso de los archivos y carpetas.
2.5.3	Proporcionar un filtro gráfico, para ordenar y agrupar los diferentes tipos de eventos y búsquedas.
2.5.4	Proporcionar informe de actividades de acceso de los archivos, carpetas, usuarios, grupos de seguridad.
2.5.5	No debe requerir Trazabildad nativa del sistema operativo para servidores de archivos windows.
2.5.6	Presentar normalización de datos.
2.5.7	Incluir información filtrada de clasificación de datos e identificación de datos críticos en modo gráfico identificando la actividad de acceso de archivos y carpetas con información confidencial.
2.5.8	Incluir información filtrada de clasificación de datos en informes sobre actividad de acceso de archivos y carpetas.

2.5.9	Proporcionar niveles altos, visibilidad de resumen gráfico de actividad auditada, incluyendo: vista de los usuarios mas y menos activos. vista de los directorios mas o menos activos. vista de directorios que un usuario o grupo accedido. vista de usuarios que han estado accesando un directorio.
2.5.10	Proporcionar informes personalizados, por demanda y programados con la capacidad de agregar filtros, condiciones, campos adicionales.
2.5.11	Proporcionar la identificación gráfica de niveles de actividad de acceso anormal a datos críticos, de acuerdo a niveles de clasificación configurados previamente.
2.5.12	Proporcionar informes de actividad de acceso anormal, identificando los diferentes tipos de eventos que están fuera del standard de uno o varios usuarios.
2.5.13	Proporcionar informe de administradores accesando datos del negocio, por demanda y programado con datos como fecha, número de veces, detalles del acceso (exitoso o fallido) entre otros.
2.6	**Remediación automatizada de control de acceso.** La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.6.1	Proporcionar recomendaciones gráficas sobre membresía de grupo excesivo basado en el análisis de actividad de acceso.
2.6.7	Proporcionar recomendaciones en formato de informe en diferentes esquemas.
2.6.8	Proporcionar utilidades gráficas para retroactivamente simular el efecto de cambios de permisos membresia de grupo basado en historia de eventos de acceso.
2.6.9	Capacidad de realizar simulaciones previas a un cambio de permisos sobre grupo de seguridad o usuarios conociendo el impacto de dicho cambio antes de aplicarlo.
2.6.10	Proporcionar informe incluyendo objetos de datos cuyos permisos están expuestos a "acceso global" grupos, everyone, usuarios de dominio, usuarios autenticados, y quién está usando activamente esos permisos para accesar a los datos.
2.6.11	Rectificar permisos y realizar cambios a grupos desde una interfaz gráfica.
2.6.12	Almacenar todos los cambios a permisos hechos dentro de la consola de administración y fuera de la consola (directamente en las plataformas monitoreadas).
2.6.13	Registrar todos los cambios de membresía de grupo hechos 'dentro de' y 'fuera de' la consola de gestión.
2.7	**Propiedad de datos**. La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.7.1	Proporcionar un método de asignar o asociar un usuario como un "propietario" de datos según el uso y cantidad de eventos.
2.7.2	Proporcionar informes en demanda y programados a propietarios asignados sobre sus objetos de datos y grupos, incluyendo permisos, actividad de acceso, estadísticas de acceso, y cambios en permisos.

2.7.3	Proporcionar un método para que los propietarios de datos reciban automáticamente informacion de recertificación de permisos/revocación/revisión de privilegios, incluyendo cambios recientes a permisos y membresía de grupos.
2.7.4	Proporcionar un método para que los propietarios de los datos efectúen cambios de permisos y grupos en sus objetos de datos sin elevar los privilegios del usuario.
2.7.5	Proporcionar un flujo de trabajo para datos y autorización de membresía de grupos.
2.8	**Eventos de Trazabildad.** La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.8.1	Proporcionar soporte para instalación remota de agentes de Trazabildad.
2.8.2	La recolección de eventos no debe almacenar archivos temporales en los sistemas monitoreados causando aumento en I/O y afectando el rendimiento de los sistemas.
2.8.3	El consumo de recursos en los sistemas monitoreados no debe afectar las diferentes aplicaciones y roles en ejecución en dicha plataforma.
2.9	**Gobierno de Informacion.** La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.9.1	Proporcionar una interfaz web que permita a los usuarios finales solicitar, aprobar y revisar el acceso a grupos y carpetas de Windows.
2.9.2	Permitir gestionar fechas de caducidad en las solicitudes y comentarios.
2.9.3	Confirmar los cambios automáticamente, sin intervención del usuario, cuando se aprueba una solicitud.
2.9.4	Proporcionar una forma de personalizar un flujo de trabajo de autorización para las solicitudes de acceso.
2.9.5	Proporcionar registros, permisos y estadísticas a los propietarios de carpetas a través de una interfaz web.
2.9.6	Habilitar a los administradores de TI para crear reglas de permisos forzados para bloquear ciertos grupos de usuarios para solicitar acceso a carpetas o grupos.
2.9.7	La herramienta debe eliminar el permiso automáticamente, siempre que un usuario intente agregar manualmente un permiso que no es compatible con la regla.
2.10	**Otras funcionalidades:** La solución a nivel funcional deberá cumplir con lo requerido en los siguientes puntos:
2.10.1	Deberá tener la capacidad de leer los diferentes permisos de una carpeta en sus máximos niveles y sub- niveles.
2.10.2	Deberá tener integración con sistemas de SIEM.
2.11.3	Deberá tener un dashboard con interface web para la gestión, monitoreo, de alertas personalizadas en tiempo real de acuerdo a parámetros definidos por la entidad.
2.11.4	Deberá contar con alertas en tiempo real identificando los accesos denegados sobre recursos específicos.
2.11.5	Deberá contar con la capacidad de generar alertas en el momento que se detecte un escalamiento de privilegios.

2.11.6	Deberá contar con alertas en tiempo real que identifiquen cuando uno usuario esta realizando eliminaciones de objetos en el directorio activo.
2.11.7	Deberá contar con alertas para identificación de comportamientos anómalos sobre datos confidenciales y de misión crítica en la entidad
2.11.8	Deberá contar con alertas para identificación en tiempo real de encripción de datos no estructurados
2.11.9	Deberá tener un motor de aprendizaje el cual identifica cuándo un comportamiento está fuera del umbral que se considere como normal.
2.11.10	Deberá contar con múltiples categorías de amenazas internas de fácil modificación y configuración.
2.11.11	Deberá contar con la visualización de gestión y análisis de comportamiento de usuarios en tiempo real de las plataformas monitoreadas.
2.11.12	Deberá tener normalización de datos de forma nativa y automatica en las diferentes bases de datos de la misma.
2.11.13	Deberá correlacionar todos los datos de usuarios inusuales o sospechosos y actividad de acceso de administradores.
2.11.14	Deberá tener la capacidad de crear alertas en tiempo real cuando se detecte que un usuario está abriendo data antigua u obsoleta.
2.11.15	Deberá tener una sola consola de gestión de todas las plataformas monitoreadas.
2.11.16	Deberá tener la capacidad de crear umbrales de alertas y tener la capacidad de definir diferentes criterios de búsqueda.
2.11.17	Deberá tener la capacidad de monitorear cuentas de usuarios locales.
2.11.18	Deberá tener diferentes categorías de alertas de acuerdo al nivel de impacto del evento realizado.
2.11.19	Deberá identificar los permisos NTFS y compartidos de forma gráfica y reportes (por demanda y programada).
3	**Hardware.**
3.1	Se deberá incluir la instalacion en el hardware (servidores) suministrado por la ANH, sobre la plataforma virytual OVM (Oracle Virtualization).
4	**Instalación.**
4.1	Se deberá realizar la instalación, configuración, ajuste, optimización, puesta en funcionamiento de todos los componentes requeridos.
4.2	Las fases de instalación, configuración básica y puesta en funcionamiento de los elementos suministrados, no deberán superar treinta (30) días.
5	**Capacitación.**
5.1	Se deberá proveer un plan de capacitación, que comprenda una descripción detallada de los cursos, contenidos, alcances, duración y demás condiciones del mismo.
5.2	Los cursos de capacitación deberán dictarse en idioma español o traducción simultánea, y debe ser presencial, dictado por personal del fabricante con amplio conocimiento de los productos incluidos en la propuesta.

6	**Soporte y Mantenimiento.**
6.1	Deberá proveerse un servicio de soporte, mantenimiento y suscripción con el fabricante que cubra a todos los componentes de la solución durante tres (3) años para la ANH.
6.2	El servicio deberá permitir a ANH acceder directamente y en forma inmediata a todas las actualizaciones, ajustes (parches/fixes) y nuevas versiones de los componentes de la toda la solución durante el período de vigencia de la garantía en un plazo no mayor de los 60 días hábiles a partir de la liberación al mercado local.
6.3	El servicio debe prestar soporte (proactivo y reactivo) y asistencia técnica vía telefónica, vía correo electrónico y on-site a los componentes licenciados a fin de solucionar problemas que surjan.
6.4	El servicio comprende la totalidad de los elementos y personal especializado, tanto para la resolución vía telefónica, vía correo electrónico y on-site, a fin de garantizar la correcta configuración y el óptimo funcionamiento de la solución.
6.5	Horario de cobertura de incidentes 5 días x 8 horas x 365 (año).

Nota: En caso de que la entidad lo requiera, la herramienta deberá permitir desarrollo a la medida por parte del fabricante a la Entidad

PROPUESTA ECONÓMICA:
"Adquirir una Herramienta Informática para gestión de permisos y seguimiento a los accesos de módulos, carpetas y archivos de datos no estructurados, compartidos en red"

tem	Descripción	Cantidad	Valor Unitario	SubTotal	IVA sobre el Total	Valor Total IVA incluido
1	Licenciamiento Plataforma	**1**	$	$	$	$
2	Licenciamiento para Usuarios	**400**	$	$	$	$
3	Instalación, soporte y Mantenimiento	**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 17 de octubre de 2017.