Al contestar cite Radicado 20191500101623 Id: 393524
Folios: 38 Fecha: 2019-05-08 12:35:48
Anexos: 0
Remitente: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA
Destinatario: VICEPRESIDENCIA ADMINISTRATIVA Y FINANCIERA

PARA: **COTIZANTE**

ASUNTO: *"Contratar la Implementación del Sistema de Gestión de Seguridad de la Información SGSI, la adquisición de una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, fortalecimiento de controles de seguridad física y el apoyo especializado en seguridad informática y forense, alineada a la Estrategia de Gobierno Digital, conforme a las necesidades de la ANH y a las buenas prácticas vigentes"*

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 "*Contratar la Implementación del Sistema de Gestión de Seguridad de la Información SGSI, la adquisición de una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, fortalecimiento de controles de seguridad física y el apoyo especializado en seguridad informática y forense, alineada a la Estrategia de Gobierno Digital, conforme a las necesidades de la ANH y a las buenas prácticas vigentes*."

Para tales efectos, le informo que la Entidad realizará sondeo de mercado y recibirá las cotizaciones hasta el día **8 de mayo de 2019** al correo electrónico german.suarez@anh.gov.co, 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 aclarar 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,

Sandra Milena Rodriguez Ramirez
Vicepresidencia Administrativa y Financiera (E)
Agencia Nacional de Hidrocarburos – ANH

Aprobó: Germán Augusto Suarez – Jefe Oficina de Tecnologías de la Información (E) / Componente Técnico Proyectó: Edwin Mauricio Gonzalez Hernandez – Contratista / Componente Técnico

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:	Contar con un Sistema de Gestión de Seguridad de la Información -SGSI documentado, sistemático, estructurado y alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI), que cumpla con los requisitos de Gobierno Digital, la Norma NTC ISO/IEC 27001:2013, legislación vigente sobre protección y tratamiento de datos personales, lineamientos gubernamentales en gestión de riesgos de seguridad digital y de la AGENCIA NACIONAL DE HIDROCARBUROS - ANH, con el fin de ser identificados, asumidos, gestionados y/o minimizados por la Entidad de una forma continua, repetible, eficiente y adaptada a los cambios que se produzcan; así como, adquirir una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, fortalecer los controles de

	seguridad física y el apoyo especializado en seguridad informática y forense, para generar valor público en un entorno de confianza digital.
OBJETO A CONTRATAR:	*Contratar la Implementación del Sistema de Gestión de Seguridad de la Información SGSI, la adquisición de una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, fortalecimiento de controles de seguridad física y el apoyo especializado en seguridad informática y forense, alineada a la Estrategia de Gobierno Digital, conforme a las necesidades de la ANH y a las buenas prácticas vigentes*
ALCANCE DEL OBJETO:	• Implementar y apropiar el Sistema de Gestión de Seguridad de la Información en la ANH conforme a lineamientos y características detalladas en el anexo técnico. • Implementar los controles necesarios para disminuir el nivel de riesgo al nivel aceptado por la Entidad conforme a las especificaciones del anexo técnico. • Elaborar y actualizar los procesos, políticas, procedimientos, guías, instructivos y manuales necesarios para cumplir con los requisitos del modelo de Seguridad y Privacidad de la Información MSPI en el marco del SGSI mediante la implementación y gestión del cambio de los mismos, en toda la Entidad. • Identificar y actualizar los activos de información de la ANH conforme a los lineamientos de Seguridad y privacidad de la información, así como su criticidad para la Entidad. • Identificar, analizar, evaluar tratar, controlar y hacer seguimiento a la gestión de riesgos de seguridad digital de la ANH conforme a los lineamientos y metodologías gubernamentales y buenas prácticas que apliquen. (Metodología gestión de riesgos de seguridad digital - MINTIC, Guía de Gestión de riesgos - MSPI, Guía administración de riesgos seguridad digital - Función Pública entre otras). • Suministrar una solución tecnológica (Software), para la

	gestión del Sistema de Gestión de Seguridad de la Información (SGSI). El software debe ser de uso específico para la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información, permitiendo la gestión de activos de información, gestión y tratamiento de riesgos de Seguridad digital, normograma, instrumentos y procedimientos, incidentes de seguridad de la información, indicadores, auditorias, reportes y mejora continua. • Implementar los controles de seguridad física requeridos por la norma NTC ISO/IEC 27001:2013 para mitigar los riesgos identificados, que contemplen control de acceso y fortalecimiento de controles de protección de la información conforme especificaciones técnicas detalladas más adelante. • Capacitar a los servidores públicos y colaboradores de ANH según plan de concienciación y apropiación del SGSI que se defina según condiciones exigidas por ANH • Proveer el servicio profesional especializado en materia de seguridad informática, forense y ciberseguridad que ejecute, supervise y establezca los procedimientos para la identificación, preservación y análisis de la evidencia digital en los procesos de investigaciones forenses, así como la implementación de la estrategia de ciberseguridad de la entidad, incluyendo documentación y técnicas de Étical Hacking • Capacitar y certificar personal de ANH como Auditor, Líder Auditor, Implementador en ISO/IEC 27001:2013 y Lead Cybersecurity Manager ISO/IEC 27032 incluyendo exámenes de certificación internacional, conforme especificaciones técnicas. • Realizar el cronograma, plan de trabajo, ejecución y presentación de resultados y recomendaciones de una preauditoria de cumplimiento ante certificación NTC-ISO/IEC 27001:2013 garantizando el ajuste de las no conformidades, así como la estimación de costos y demás preparación para la certificación.

	El detalle de cada ítem se explica en el apartado especificaciones técnicas El lugar de ejecución del contrato será en las instalaciones de la ANH en Bogotá D.C. Av. Calle 26 No. 59 - 65 Piso 2 -Edif. Cámara Colombiana de Infraestructura, con una población estimada de seiscientos (600) servidores públicos, contratistas y colaboradores.
IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:	El contrato que se pretende celebrar mediante el presente proceso de selección es de Consultoría, en virtud de lo establecido en el inciso segundo del numeral 2 del artículo 32 de la ley 80 de 1993 Para la selección del proponente idóneo para ejecutar el contrato por celebrar, corresponde la modalidad de selección conocida como Concurso de méritos. "***Concurso de méritos*** *(numeral 3 del artículo 2 de la Ley 1150 de 2007 modificado por el artículo 219 del Decreto 19 de 2012): Corresponde a la modalidad prevista para la selección de* consultores *o proyectos, en la que se podrán utilizar sistemas de concurso abierto o de precalificación. En este último caso, la conformación de la lista de precalificados se hará mediante convocatoria pública, permitiéndose establecer listas limitadas de oferentes mediante resolución motivada, que se entenderá notificada en estrados a los interesados, en la audiencia pública de conformación de la lista, utilizando para el efecto, entre otros, criterios de experiencia, capacidad intelectual y de organización de los proponentes, según sea el caso"*.
CÓDIGO UNSPSC (The United Nations Standard Products and Services Code® - UNSPSC, Código Estándar de Productos y Servicios de	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 los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC):

Naciones Unidas), correspondiente al bien, obra o servicios a contratar:

SEGMENTO	FAMILIA	CLASE	PRODUCTO	NOMBRE
80	8010	801015	80101500	Servicios de Gestion, Servicios Profesionales de Empresa y servicios administrativos / Servicios de Asesoría de Gestion / Servicios de Consultoría de Negocios y administración corporativa
80	8010	801016	80101600	Gerencia de proyectos.

y en **por lo menos uno** de los siguientes Códigos Estándar de Productos y Servicios de Naciones Unidas (UNSPSC):

SEGMENTO	FAMILIA	CLASE	PRODUCTO	NOMBRE
81	8111	811122	81112200	Mantenimiento y soporte de software
81	8111	811118	81111800	Servicios de sistemas y administración de componentes de sistemas
81	8116	811615	81161500	Servicios de administración de acceso
81	8111	811119	81111900	Sistemas de recuperación de información

En el caso de propuestas presentadas por consorcios, uniones temporales o promesas de sociedad futura, **cada uno de los integrantes** debe encontrarse inscrito, clasificado y calificado **en los códigos solicitados como exigibles y por lo menos uno** de los códigos anteriormente mencionados; en todo caso, el consorcio, la unión temporal o la promesa de sociedad futura deberá acreditar, en conjunto, todos los códigos exigidos.

ASPECTOS TÉCNICOS:

ESPECIFICACIONES TÉCNICAS

1. Definir un Plan de trabajo, especificando etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir la metodología, las técnicas y herramientas que utilizará en la ejecución del contrato, previa aprobación del supervisor del

contrato en la Agencia Nacional de Hidrocarburos. El plan de trabajo debe considerar el cumplimiento de los lineamientos fijados por las normas legales descritas anteriormente y estándares aplicables a la Gestión de la Seguridad de la Información que sean necesarias para la Agencia Nacional de Hidrocarburos y las que surgieren en el desarrollo del contrato.

Durante la ejecución del contrato el Contratista participará y dispondrá las sesiones que requiera el supervisor del contrato (mínimo una sesión mensual) para dar cuenta de los avances de la implementación, resultados y demás informes de la ejecución contractual.

2. Mantener actualizada la estrategia de seguridad de la información de la Agencia Nacional de Hidrocarburos, ejecutando e integrando los proyectos necesarios para garantizar la confidencialidad, integridad, disponibilidad, no repudio y privacidad de la información de la ANH, conforme lineamientos de MINTIC como el Modelo de Seguridad y Privacidad de la Información, sus guías y Gobierno Digital armonizados con temas como Arquitectura Empresarial, Modelo de Gestión IT4+, normatividad vigente en materia de Teletrabajo, Delitos Informáticos, Conpes 3854 Política Nacional de Seguridad Digital, protección de datos personales, habeas data, propiedad intelectual y derechos de autor así como la norma NTC-ISO/IEC 27001:2013.

3. Implementar los controles de seguridad requeridos por la norma NTC ISO/IEC 27001:2013 para mitigar los riesgos identificados, que contemplen acceso físico y fortalecimiento de controles de protección de la información, que incluya como mínimo:

    - Sistema de etiquetado y alarma antihurto: tres (3) **antenas de techo lectoras de RFID** (1 master y dos esclavas) que serán ubicadas en una salida principal y dos salidas alternas de la Entidad, con su

ASPECTOS TÉCNICOS:	respectiva controladora y alarma (sonora, visual y digital) así como su software de administración licenciado a perpetuidad con garantía y soporte de mínimo de tres (3) años, deben detectar los artículos etiquetados que pasan por debajo de la antena en el rango de la salida a cubrir y comprobar si estos artículos han sido autorizados o no para su salida o movimiento, según previa configuración en el software de administración respectivo, generando la alarma respectiva; dos mil (2000) **etiquetas RFID** adhesivas compatibles y con la frecuencia requerida para ser leídas plenamente por la antena, para la protección de equipos tecnológicos que la ANH defina. El contratista deberá instalar las etiquetas que la ANH indique y entregar las sobrantes, todas las antenas y demás elementos de la solución, dejar funcionando todo el sistema y capacitar a los involucrados en la gestión. La ANH suministrará el equipo de cómputo para la instalación del software de administración, previa presentación de requisitos mínimos de recursos por parte del contratista. El contratista deberá suministrar todo el material, la mano de obra y demás requisitos para la instalación eléctrica y de datos que se requieran, para lo cual realizará el levantamiento de requisitos al inicio del contrato; así mismo, deberá garantizar que las instalaciones físicas de ANH impactadas con este proceso, queden en iguales condiciones a las previas a su intervención, sin afectar la infraestructura de la Entidad y/o el edificio. Todo el trabajo deberá cumplir las condiciones de seguridad y salud en el trabajo y otra normatividad relacionada y deberá ceñirse a los horarios y protocolos que la ANH defina para realizar esta labor, sin que genere costos adicionales para la Entidad. • Controles antihurto y privacidad: ciento cincuenta (150) **Protectores de cámara web** (anti-camfecting) con sistema de apertura y cierre, dimensiones

	mínimas 3, 7 cm x 1,3 cm, ciento veinte (120) protectores o filtros de privacidad (visión lateral oscurecida, frontal nítida) "**anti espías**", que eviten que la información sea visible a partir de un ángulo de visión de 30º (50 para computadores de escritorio, 30 para portátiles y 40 para pantallas Wyse modelo W11B); ciento veinte (120) **guayas** con clave (50 para computadores de escritorio, 30 para portátiles y 40 para pantallas Wyse modelo W11B). Las dimensiones de los elementos a instalar (cuando aplique) corresponderán a las de los dispositivos que se definan en el levantamiento y análisis de criticidad de los mismos que el contratista deberá realizar como parte de sus actividades, así como la respectiva instalación de cada elemento. • Dispositivos de almacenamiento seguro: veinte (20) **USB** 3.1 Gen 1 (USB 3.0) de 64 GB compatible con 2.0, con cifrado completo de datos de disco AES de 256 basado en hardware, teclado alfanumérico para bloqueo de la unidad, velocidad 135MB/s de lectura, 40MB/s de escritura, PIN del Administrador, opción de partición de solo lectura, compatible con Windows, Linux y Mac, cuerpo del producto metálico y duradero, con llavero, a prueba de agua y polvo (certificado IP57) y certificación FIPS 197, temperatura de funcionamiento de 0°C a 40°C y de almacenamiento de -20°C a 60°C y tres (3) años de garantía con soporte técnico gratuito. No debe requerir software para su administración. El contratista deberá entregar funcionando los dispositivos y realizar la transferencia de conocimiento en cuanto a su uso a mínimo cinco (5) servidores públicos o contratistas que la ANH defina. • Dispositivos de almacenamiento seguro: Tres (3) **discos duros externos** de 2TB USB 3.0 y 2.0 compatible, cifrado basado en Hardware – Dos

motores de encriptado AES dual de 256 bits, operando en modos XTS y CBC, cumplimiento de estándares TAA, RoHS, FCC, CE y certificados FIPS 197 (Cert # 250) y FIPS 140-2 cripto chip validado (Cert # 1472), compatible con Windows, Linux y Mac y dos (2) años de garantía. No debe requerir software para su administración. El contratista deberá entregar funcionando los dispositivos y realizar la transferencia de conocimiento en cuanto a su uso a mínimo cinco (5) servidores públicos o contratistas que la ANH defina.

- Custodia de información clasificada: una (1) **Caja de seguridad** para guardado seguro de documentos y dispositivos con información confidencial como UBS's, DD, etc., en acero solido extra grueso, montaje en el piso, instrucciones de uso, doble puerta, cerradura electrónica programable y opción de reseteo, apertura con código secreto PIN y llaves incluidas (mínimo 4 llaves), indicador y batería incluida, dimensiones mínimo 60 centímetros de alto, 30 centímetros de fondo y 40 centímetros de ancho. El contratista deberá entregar funcionando el dispositivo y realizar la transferencia de conocimiento en cuanto a su uso a mínimo cinco (5) servidores públicos o contratistas que la ANH defina.

4. Adoptar, alinear, apropiar e implementar el Modelo de Gestion de Riesgos de Seguridad Digital en la ANH, así como las guías de orientación que apliquen.
5. Desde el enfoque del SGSI, realizar la identificación, análisis, evaluación, tratamiento del riesgo y definir en conjunto con las diferentes áreas los planes de tratamiento de riesgos y el apoyo a la implementación de los controles necesarios para disminuir el riesgo hasta llevarlos a un nivel aceptable en todos los veinte (20) procesos de la ANH conforme lineamientos gubernamentales y de la ANH. Los

	procesos se encuentran disponibles para consulta en la sección de transparencia de la página web de la ANH. Se debe incluir como mínimo: los procesos, los activos, las personas, la tecnología, las amenazas con mayor probabilidad de ocurrencia, las vulnerabilidades con mayor probabilidad de presencia, posteriormente el monitoreo de la efectividad de los controles implementados y la mejora continua. El contratista deberá socializar a los interesados que ANH defina, el resultado de este punto. 6. Ejecutar las actividades relacionadas con la implementación y mejoramiento del Sistema de Gestión de Seguridad de la Información NTC ISO/IEC 27001:2013, incluyendo los dieciocho (18) dominios de seguridad definidos en el anexo A de dicha norma (Dominios - Objetivos de Control y controles), con el fin de cumplir con los requisitos de la norma y la implementación de los controles, evaluar las prácticas de gestión de la seguridad y privacidad de la información conforme lineamientos y legislación vigente. La estrategia a utilizar debe considerar por los menos lo siguiente: revisión y/o actualización de la documentación y controles establecidos en el proceso de implementación del SGSI, sesiones de trabajo, análisis de información recopilada y valoración de cumplimiento, documentación, recomendaciones y generación de planes de remediación. 7. Apoyar la integración de los requisitos de la Norma NTC ISO/IEC 27001:2013 respecto a otros estándares implementados en la Agencia Nacional de Hidrocarburos (ejemplo: NTC ISO 9001:2008 u Otros). Deberá incluir como mínimo alineación entre normas implementadas y la NTC ISO/IEC 27001:2013, recomendaciones y aspectos de mejora; para lo cual el proveedor participará activamente en las sesiones de trabajo que la Entidad lleva a cabo en el Sistema Integrado de Gestion y Control. 8. Actualizar y apoyar la implementación de procedimientos, normas e instructivos de seguridad de la información conforme a la normatividad vigente, los requisitos del Sistema de Gestión de seguridad de la información (SGSI),

	el Modelo de Seguridad y Privacidad de la Información (MSPI), directrices en materia de privacidad y tratamiento de datos personales, alineado al sistema de gestión de calidad de la Entidad; así como, el acompañamiento y generación de documentación que se presente durante la vigencia del contrato solicitada por entes de control u otras entidades gubernamentales, en este mismo contexto. 9. Elaborar y ejecutar el plan de concienciación y apropiación del Sistema de Gestión de Seguridad de la Información, dirigido a todos los Servidores Públicos y colaboradores de la ANH. Se deben realizar como mínimo las siguientes sesiones de transferencia de conocimiento presenciales así: • Una (1) sesión Magistral inicial para todo el personal de ANH como línea base e introducción al SGSI. Mínimo dos (2) horas de duración. Una vez avanzada la implementación del SGSI y antes de finalizar contrato, sesiones tipo Taller con el uso de recursos didácticos: • Una (1) sesión dirigida a Directivos. Mínimo dos (2) horas de duración. • Sesiones para abarcar todo el personal de ANH finalizando contrato, socializando el SGSI implementado y políticas más relevantes. Deberán participar como mínimo tres (3) personas designadas para cada uno de los veinte (20) procesos del Mapa de Procesos de la ANH, en grupos no mayor a veinte (20) personas por sesión. • Una (1) sesión Magistral finalizando contrato para todo el personal de ANH con el resumen de la implementación, aspectos más relevantes del SGSI y requisitos a tener en cuenta para la certificación

	ISO 27001:2013. Mínimo dos (2) horas de duración. Incluye entrega de material (folletos, material POP, etc.) que promuevan la apropiación del SGSI, a todos los asistentes. • Realizar como mínimo, durante la ejecución del contrato tres (3) ejercicios lúdico-prácticos de apropiación asociados a la seguridad y privacidad de la información, los cuales se realizarán en las instalaciones de la ANH. Cada ejercicio deberá concientizar sobre un tema específico y deberán ser acordado, programado y aprobado por el supervisor del contrato previas propuestas presentadas por el contratista. Los ejercicios podrán ejecutarse mediante recreadores o tratarse de ejercicios de ingeniería social o similares, teniendo como característica destacada la retroalimentación al usuario de buenas prácticas en seguridad y privacidad de la información y el uso de estrategias pedagógicas adecuadas al público. • El contratista deberá entrega dos (2) videos con narración en audio y subtítulos para apoyar la apropiación del SGSI así: o Uno (1) con conceptos básicos del SGSI. Mínimo tres (3) minutos de duración o Uno (1) con el resumen de la implementación del SGSI en la ANH (políticas, controles, y procedimientos más relevantes). Mínimo tres (3) minutos de duración Los videos deben ser originales, adaptados para la ANH, los contenidos deben respetar los derechos de autor y propiedad intelectual, cediendo los derechos de uso y patrimoniales a la ANH, para lo cual el contratista deberá presentar por escrito carta donde exime a la ANH de responsabilidades en este sentido y garantizando el cumplimiento de los

requisitos.

El personal de ANH, incluye quienes prestan los servicios generales y de vigilancia.

Con una anticipación previa de por lo menos quince (15) días a la ejecución prevista de las sesiones, el contratista debe presentar para aprobación del equipo de trabajo de seguridad de la Información de ANH y del supervisor del contrato, el plan de cada sesión especificando objetivo, contenido programático, metodología, didáctica a utilizar y demás aspectos logísticos, los cuales corren por cuenta del Contratista incluyendo el suministro de refrigerio para los asistentes (1 bebida y 1 snack como mínimo) en todas las sesiones. Para las sesiones generales a todo el personal, se tendrá como promedio ciento cincuenta (150) personas para contabilización de la logística asociada. El material que se utilice para las sesiones será entregado a la ANH para posteriores usos en la apropiación del SGSI. La ANH dispondrá el Auditorio para su realización, lo que requiere programación previa.

Para la planeación y ejecución de las sesiones de transferencia de conocimiento y ejercicios se deberá incluir un facilitador con capacidad y experiencia en transmitir el conocimiento, proactivo, con iniciativa, buenas relaciones interpersonales y dispuesto a atender inquietudes. El facilitador debe demostrar experiencia como docente o facilitador en eventos similares. La descripción mínima se encuentra detallada en el apartado EQUIPO DE TRABAJO.

10. Proponer las actualizaciones y recomendaciones que apliquen a la documentación y estrategia actual de Continuidad del negocio de la ANH y Programa Integral de Gestión de Datos Personales de la ANH en alineación con las políticas de seguridad de la información, las buenas prácticas y lineamientos gubernamentales, en cumplimiento de la normatividad vigente. Deberá incluir la

alineación entre los temas mencionados y la norma NTC ISO/IEC 27001:2013, recomendaciones y aspectos de mejora; para lo cual el proveedor participará activamente en las sesiones de trabajo que la Entidad lleva a cabo para estos temas.

11. Establecer el nivel de madurez del SGSI y de la privacidad de la información de la ANH como línea base de la implementación y al finalizarla, realizar preauditoria conforme a la norma NTC ISO/IEC 27001:2013 para validar tanto el incremento del nivel de madurez como el cumplimiento de los requisitos de la norma mencionada a fin de certificar la Entidad bajo estas buenas prácticas.

12. Implementar una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, debidamente licenciada On Premise o como servicio (SaaS), con soporte y garantía mínimo por dos (2) años. Para la opción On Premise, la ANH suministrará el equipo de cómputo para la instalación del software, previa presentación de requisitos mínimos de recursos por parte del contratista. La solución debe cumplir la norma NTC ISO/IEC 27001:2013 y los siguientes requerimientos como mínimo:

Comentario [GASV1]: Si es un SaaS, ¿Aplicaría esto?

Comentario [SMRF2R1]: Se agrega la aclaración

	FUNCIONALIDAD
ADMINISTRACIÓN	Alcance a todos los niveles de la organización y configuración para múltiples áreas, dependencias, sedes, etc.
	Permitir la parametrización, adición, activación /inactivación, eliminación de campos según requerimientos de la ANH
	Debe establecer controles de ingreso y perfil por usuario a través del directorio activo de la entidad.
	Debe permitir el control de la documentación evitando el Ctrl - V, Ctrl - P, Ctrl - C, evitando imprimir información

		restringida, además debe permitir generar perfiles de acceso para impresión.
		Debe facilitar el cargue de tablas básicas prediligenciadas como áreas, procesos, cargos y en general los datos que la entidad requiera para parametrizar adecuadamente la aplicación. Así mismo, durante la operación, debe permitir el cargue masivo de información en los diferentes campos.
		Fácil consulta a través de filtros con combinación de criterios
		Debe tener control y auditoria para identificar la trazabilidad de los registros y acciones de los usuarios
		Utilizar seguridad basada en Roles de Usuarios según perfiles determinados por el área de seguridad de la información
		Permitir la parametrización y gestión de diferentes flujos de aprobación
	SISTEMA DE NOTIFICACIONES	La herramienta debe contar con un motor de tareas pendientes o un tablero de tareas en donde por perfiles de usuario se identifiquen las actividades pendientes del sistema de gestión de seguridad de la información, con semáforos de vencimiento parametrizables por la Entidad
		Permitir parametrización de diferentes tipos de notificaciones y alertas electrónicas
		Que permita configurar los tiempos de gestión de dichas tareas según lo disponga la Entidad.
		Debe a partir de estas tareas permitir anexar archivos de evidencia o consulta
		Debe estar integrado con el correo electrónico para su asignación en tiempo real, generar alarmas y monitoreo
		Debe tener la opción de establecer fechas

		propuestas de terminación y su responsable de las tareas
		Debe administrar la asignación de tareas para gestionar las actividades propias al sistema, tales como asignación de no conformidades y actividades asociadas, asignación de acciones preventivas, entre otras que el equipo de seguridad de la información considere necesarias para sus actividades.
		Debe permitir identificar los estados de las tareas de los servidores públicos, contratistas o colaboradores frente al sistema de gestión de seguridad de la información, es decir tareas abiertas, cerradas, atrasadas, por tipo de tarea identificando el estado general del sistema de gestión.
	GESTION DOCUMENTAL	Debe permitir cargar todos los tipos de documentos que se requieren manejar en el sistema, tales como Guías, Manuales, Protocolos, Instructivos, normativa, procedimientos etc.
		Los documentos se deben catalogar según su clasificación y etiquetado y sobre ellos garantizar permisos de consulta. El proponente debe garantizar que el software permita crear y visualizar la caracterización del proceso de seguridad de la información de manera simple y dinámica.
		El glosario de términos debe ser completamente parametrizable, el cual permite la sensibilización fácil del uso adecuado del lenguaje y terminología

		propia del Sistema de Gestión de Seguridad de la Información.
		Debe permitir construir un banco de conocimiento de la documentación vigente del sistema de gestión de seguridad de la información, normatividad asociada, etc. (Listado Maestro de Documentos) en donde se permita tener un motor de búsqueda robusto sobre los documentos, clasificando por proceso, por tipo de documento y que permita buscar hasta dentro del contenido de los documentos. Permitiendo según esta búsqueda crear una interface exportable a Excel con la información de dichas consultas.
	INDICADORES DE GESTION	Es necesario tener la definición de los posibles indicadores del sistema de gestión de seguridad de la información y su respectiva ficha técnica para su respectiva medición, seguimiento y control.
		La ficha técnica del indicador debe tener un control de versión identificando el cambio y mejora de la definición de cada Indicador. Conservando la trazabilidad de los cambios.
		Debe permitir parametrizar la herramienta de tal forma que levante hallazgos de manera automática cuando el incumplimiento de un indicador se dé.
		Debe brindar la posibilidad de generar hallazgos a partir de los resultados de los indicadores y análisis de datos con el fin de generar mejora continua en el sistema de gestión de seguridad de la información. Debe permitir anexar un archivo en el momento de la medición del indicador como

		evidencia. Mínimo debe soportar archivos PDF, Excel, Word y Power Point.
		Debe permitir filtrar la información de los indicadores según campos disponibles
		El módulo de indicadores debe generar reportes estadísticos, gráficos y poseer elementos que permitan hacer un mejor seguimiento, análisis y mejora a la Entidad, los cuales deben ser parametrizables según necesidades de la ANH. Mínimo contemplar gráficas tipo radial o radar, barras, circulares y lineales.
		Debe permitir establecer una meta final y metas intermedias de acuerdo con la periodicidad de medición para un seguimiento más eficaz, igualmente la definición de rangos superiores e inferiores.
		Deberá permitir vía correo-electrónico u otro mecanismo automático de alarma sobre el estado de los indicadores, notificando la fecha de su medición y el incumplimiento cuando esto ocurra.
		De manera automática el sistema debe crear hallazgos por incumplimiento a indicadores según los rangos de tolerancias definidas en la planeación.
		El módulo debe permitir realizar comparaciones de mediciones actuales con mediciones de vigencias anteriores.
	GESTION DE ACTIVOS	La solución debe estar en la capacidad de realizar la gestión de activos: identificación, registro, clasificación, criticidad y valoración entre otras, permitiendo el cargue masivo de archivos.
		Debe permitir filtros de los activos por diferentes campos. Mínimo por proceso, área, tipo de activo, fechas de registro,

		responsable.
		Los tipos, número y descripción de los campos asociados a la gestión de activos deben ser parametrizables acorde a las necesidades de ANH. El identificador o ID del activo debe generarse de forma automática y tener una traza
		Debe permitir validaciones de los campos y evitar el uso de campos que se inactiven en los flujos de trabajo
		Debe permitir el cargue masivo de información previa, mínimo en formato Excel.
		Generar reportes estadísticos, gráficos y poseer elementos que permitan llevar control y detalle de la gestión de activos de información, los cuales deben ser parametrizables según necesidades de la ANH. Mínimo contemplar gráficas tipo radial o radar, barras, circulares y lineales.
	GESTION DE RIESGOS	La solución debe estar en la capacidad de realizar la gestión de riesgos: identificación, tipificación, análisis, tratamiento entre otros permitiendo el cargue masivo de archivos, mínimo en Excel
		En la identificación de Riesgos debe permitir enlazar el inventario de activos.
		Parametrización de probabilidad e impacto, valoración de riesgos, análisis de costos, amenazas por activos y ser configurables.
		Definición de riesgo aceptable, niveles de riesgo aceptable, listado de riesgos, mapa de riesgos, mapa de calor, riesgos simultáneos o dependientes. Debe permitir la comparación de los mapas antes y después de valoración de riesgos.

		Catálogo de controles asociados a los riesgos y los activos, configurables y resumen de los mismos, parametrización de la gestión, reevaluación del riesgo, cuestionarios parametrizables.
	GESTION DE AUDITORIA	El módulo debe permitir administrar y gestionar de manera integral todo el proceso de auditorías internas de seguridad de la información de la entidad en cada una de sus fases.
		El módulo debe permitir crear el programa o cronograma de las auditorias por año, el plan a seguir de cada auditoría, la relación de los criterios a verificar y las creación de las listas de chequeo.
		La herramienta debe permitir la creación automática del informe por cada auditoría realizada y el cargue de archivos, mínimo en formatos PDF, Excel, Word y Power Point.
		Debe poder levantar hallazgos y no conformidades frente al incumplimiento de una política, lineamiento o control desde cada documento del sistema de gestión, como por Ejemplo Acciones Correctivas, Acciones Preventivas. Debe permitir gestionar su tratamiento.
		Debe tener la posibilidad de enviar el informe a aprobación antes de levantar los hallazgos.
		Debe permitir registrar los hallazgos de auditoria directamente en la herramienta.
		Debe permitir cargar evidencias cuando sean requeridas y en las subsanaciones o acciones en las diferentes fases, mínimo en formatos PDF, Excel, Word y Power Point.

	GESTION DE INCIDENTES	Registrar el incidente, asignándole un identificador o ID de manera automática, las actividades realizadas para diagnosticar, analizar, contener, erradicar y recuperarse de un incidente.
		Debe permitir asignar responsable(s) del incidente, tipificarlo y establecer tiempos de respuesta. Permitir escalamiento, notificaciones enlazado con el correo electrónico y la traza de reporte a entidades externas.
		Obtener reportes gráficos para descubrir tendencias, según activos de información, procesos, áreas, riesgos identificados a fin de establecer el comportamiento de la gestión de incidentes y aprender de ellos. Mínimo contemplar filtros por campos disponibles, gráficas tipo radial o radar, barras, circulares y lineales.
		Debe permitir la traza del registro de los incidentes, custodia, filtrado según campos disponibles, cargue de archivos mínimo en formatos PDF, .png, .jpg, .jpeg, Excel, Word y Power Point.
		Mantener un histórico centralizado de los incidentes ocurridos, para poder consultarlos en cualquier momento que se requiera y reportar las actividades realizadas en una investigación.
	MEJORAMIENTO CONTINUO	Levar a cabo todas las acciones encaminadas a la mejora continua según dominio de la norma NTC ISO/IEC 27001.
		Articular este módulo con el resultado de auditorías internas y externas, indicadores, resultados del seguimiento y demás fuentes generadoras de acciones

		El módulo debe permitir registrar las correcciones inmediatas a las no conformidades detectadas y acciones de mejora.
		Debe monitorear, medir la mejora continua y la eficacia del sistema de gestión de seguridad de la información, haciendo seguimiento y control de todas las acciones correctivas, preventivas y de mejora para la entidad.
	REVISIÓN POR LA DIRECCIÓN	Debe generar de forma automática la información requerida para el proceso de revisión por la dirección, con el estado del sistema de gestión de seguridad de la información en tiempo real.
		El informe de la revisión por la dirección debe tener la información y los campos requeridos de manera precisa por la norma NTC ISO/IEC 27001:2013
	SEGURIDAD DE LA INFORMACIÓN ISO 27001	Integración con todos los módulos
		Declaración de Aplicabilidad (controles implementados, justificación, flujos de aprobación, versionamiento)
	OTRAS GENERALIDADES	Debe ser una herramienta diseñada específicamente para la gestión de Sistemas de Gestion de Seguridad de la información y contemplar todos los dominios, objetivos de control y controles que la norma NTC ISO 27001:2013 exige.
		Debe contar con una cartelera virtual de comunicaciones para dar a conocer a los usuarios los avances del sistema de gestión de seguridad de la información.
		La navegación debe ser intuitiva, es decir permitir el uso fácil y amigable de la aplicación.
		Implementar seguridad de acceso sobre las

	paginas (Utilizar tiempos de inoperancia de las páginas, evitando que la sesión de la página quede abierta)
	El software se debe ejecutar en ambiente WEB a través de un Browser
	El software debe ser arquitectura escalable
	Se debe entregar licencia, manual de usuario, manual técnico, Modelo Entidad Relación y demás información técnica, los cuales deben estar escritos en español.
	Debe contar con Menú de Ayuda
	El software debe operar bajo el sistema operativo WINDOWS SERVER
	El proveedor se compromete a entregar sin costo adicional todas las actualizaciones del Software que se desarrollen durante la vigencia de la garantía, sin costo adicional, y a suministrar acompañamiento técnico y soporte cuando se instalen las actualizaciones
	El proponente deberá especificar los planes de mantenimiento correctivo y preventivo que prestará durante el término de garantía del software.

13. Proveer en sitio de manera permanente y presencial durante la ejecución del contrato, el servicio profesional experto en seguridad informática, informática forense y ciberseguridad que ejecute, supervise y establezca los procedimientos para la identificación, preservación y análisis de la evidencia digital, así como, la implementación de la estrategia de ciberseguridad de la entidad incluyendo documentación, ejecución de las actividades de remediación de vulnerabilidades y aplicación de buenas prácticas optimizando los recursos en materia de seguridad informática de los cuales dispone la Entidad.

    El propósito de este servicio es apoyar, generar y fortalecer

capacidades al interior de la entidad en materia de seguridad informática, informática forense y ciberseguridad, por lo cual el servicio del profesional experto se seguirá prestando como soporte técnico por demanda por un término de seis (6) meses posteriores a la finalización del contrato con una disponibilidad de horario de 8:00 a.m. a 5:00 p.m. de lunes a viernes, para lo cual el Contratista debe proporcionar al menos tres (3) canales de comunicación para la solicitud del servicio (Telefónico, Correo, Web) y deberá garantizar su contacto inicial en un término no mayor a una (1) hora y su atención/resolución máximo según criticidad así:

- Evento menor -afecta un usuario/herramienta tecnológica no crítica-: un (1) día
- Incidente moderado -afecta más de un usuario/herramienta tecnológica hasta un 30% de la entidad-: cinco (5) horas
- Incidente mayor -afecta más de un usuario/herramienta tecnológica hasta un 60% de la entidad-: cuatro (4) horas
- Incidente crítico -afecta más de un usuario/herramienta tecnológica hasta un 90% o más de la entidad-: tres (3) horas

El perfil del profesional a cumplir se encuentra descrito en el apartado “Equipo de Trabajo” y realizará las siguientes actividades durante la ejecución del contrato, sin que genere algún tipo de relación contractual o laboral directa con la ANH:

- Realización de diagnósticos y análisis de riesgos, vulnerabilidades, amenazas (incluyendo amenazas persistentes avanzadas, potenciales ataques a infraestructuras críticas) a las que se pueda ver expuesta la ANH. El contratista deberá proveer las herramientas requeridas para estas labores.
- Asesoría en el análisis e inteligencia de amenazas,

capacidades prospectivas y de pronóstico en materia de ciberseguridad

- Afinar y colaborar en la administración de las plataformas y soluciones de seguridad informática de la ANH entre otras: Plataforma Fortinet (FortiWeb, Forti Analizer, FortiSandBox, FortiSIEM, FortiDB, FortiADC, FortiDDOS) y CarbonBlack.
- Participar en la definición, implementación y aseguramiento de la estrategia de ciberseguridad de la entidad
- Gestionar la identificación, actualización, tratamiento y monitoreo de los riesgos de seguridad informática, seguridad digital y ciberseguridad, así como, su relación con el plan de continuidad y recuperación ante desastres
- Implementar los controles en materia de seguridad informática y ciberseguridad que sean requeridos
- Definir los requisitos de seguridad mínimos a cumplir por los sistemas de información a desarrollar, actualizar o adquirir por la ANH
- Generar conceptos técnicos e informes en materia de seguridad informática, seguridad digital y ciberseguridad
- Establecer y gestionar el programa de gestión de incidentes de seguridad informática y ciberseguridad
- Definir, ejecutar, supervisar y gestionar los procedimientos y procesos de investigaciones forenses digitales
- Establecer el procedimiento aprobado e implementado para la identificación, preservación y análisis de la evidencia digital.

Así mismo, en los seis (6) meses posteriores a la finalización del contrato (Soporte técnico) realizará las siguientes actividades por demanda en las instalaciones de ANH, salvo casos excepcionales que no requieran su presencia física en las instalaciones y siempre y cuando se pueda dar atención

efectiva al requerimiento; sin que genere algún tipo de relación contractual o laboral directa con la ANH.

- Identificación, diagnóstico, análisis, remediación y seguimiento de eventos e incidentes de seguridad de la información que cubra las fases de identificación, detección, respuesta, recuperación y protección de los activos de información en materia de ciberseguridad.
- Apoyo en actividades relacionadas con seguridad informática, informática forense o ciberseguridad según requerimientos específicos de la Entidad.
- Documentación de los eventos e incidentes de seguridad reportados y atendidos conforme a los procedimientos establecidos por la ANH.
- Generación de recomendaciones post materialización de Eventos e incidentes de seguridad informática, informática forense o ciberseguridad.

El profesional experto que preste este servicio, deberá firmar el respectivo acuerdo de confidencialidad de manera individual el cual estará vigente durante todo el contrato y su posterior soporte técnico.

14. Capacitar y certificar a los servidores públicos y/o colaboradores que la ANH defina, así:

- ✓ Curso Auditor Interno ISO/IEC 27001:2013 incluyendo examen de certificación internacional para tres (3) personas de ANH
- ✓ Curso Auditor Líder ISO/IEC 27001:2013 para incluyendo examen de certificación internacional para dos (2) personas de ANH
- ✓ Curso Implementador ISO/IEC 27001:2013 para incluyendo examen de certificación internacional para dos (2) personas de ANH
- ✓ Curso Lead Cybersecurity Manager ISO/IEC 27032 incluyendo examen de certificación internacional para dos (2) personas de ANH

Las propuestas de los cursos (contenido, horario, material, etc.) deberán ponerse a disposición del supervisor del contrato para su aprobación. Los cursos serán dictados y certificados por una entidad avalada para ofrecerlos y reconocida, incluir material y se deberán cursar fuera de las instalaciones de ANH sin ningún costo adicional para la Agencia, así como serán dirigidos con prioridad a las personas de Planta, previa autorización de los jefes respectivos y el supervisor del contrato. Todos los gastos asociados corren por cuenta del Contratista.

ENTREGABLES

1. Cronograma, Plan de trabajo e implementación y, Metodología conforme NTC-ISO/IEC-27001:2013 según los requerimientos del ítem 1 especificaciones técnicas, actas de reunión, listados de asistencia, informes.

2. Documentos elaborados y/o actualizados relacionados con la estrategia de seguridad de la información de la Agencia Nacional de Hidrocarburos conforme a los requerimientos del ítem 2 de las especificaciones técnicas, previo plan de actualización aprobado por el supervisor del contrato.

   Como mínimo:

   - GAP del estado actual de la Entidad en la Implementación de la NTC-ISO/IEC-27001:2013
   - GAP de Cumplimiento de la Normativa de Gobierno Digital (antes Gobierno en Línea) en el contexto del Modelo de Seguridad y Privacidad de la Información (MSPI)
   - GAP del estado actual de la Entidad frente al cumplimiento de la normatividad vigente en privacidad y tratamiento de datos personales, habeas data, propiedad intelectual y derechos de autor

- GAP del estado actual de la Entidad frente al cumplimiento del Conpes 3854
- Documento de ajustes y recomendaciones para reducir las brechas identificadas y plan de implementación de estas
- Plan Estratégico de Seguridad de la Información actualizado
- Plan de Gestión de Incidentes
- Recomendaciones sobre perfiles, roles y responsabilidades para el SGSI en la ANH
- Procedimiento de gestión para toda la documentación del SGSI.
- Propuesta de elaboración y actualización de documentación necesarios para la seguridad de la información

3. Dispositivos mencionados en el ítem 3 de las especificaciones técnicas, debidamente instalados y funcionando. Actas de entrega, licencias y certificados que apliquen, levantamiento y análisis de criticidad, listados de asistencia a reuniones y capacitaciones, instrucciones de uso, material y documentación técnica.
4. Procedimiento, matrices, glosario, instructivo y guías asociadas para la gestión de riesgos de acuerdo con el Modelo de Riesgos de Seguridad Digital aplicable en la Agencia Nacional de Hidrocarburos alineado con las metodologías de gobierno vigentes que correspondan.
5. Matriz de riesgos aplicada a los veinte (20) procesos de la ANH actualizada con la identificación, análisis y evaluación de riesgos conforme lo estipulado en el ítem 5 de Especificaciones técnicas y el Plan actual de tratamiento de los riesgos de la ANH, así como el nuevo Plan de tratamiento, evidencias de la implementación y seguimiento, actas de reunión, listados de asistencia y capacitaciones.
6. Declaración de aplicabilidad (SOA-Statement of Applicability-) conforme a la norma NTC ISO/IEC

	27001:2013 basados en cada una de las actividades y acciones descritas en el ítem 6 de Especificaciones técnicas, actas de reunión, listados de asistencias, documentación y planes asociados. 7. Documento que contenga la integración de los requisitos de la Norma NTC ISO/IEC 27001:2013 respecto a otros estándares implementados en la Agencia Nacional de Hidrocarburos (ejemplo: NTC ISO 9001:2008 u Otros), recomendaciones, actas de reunión, listados de asistencia. 8. Políticas, procedimientos, guías e instructivos de seguridad de la información mencionados en el ítem 8 de las especificaciones Técnicas elaborados y/o actualizados, conforme a lista aprobada por supervisor del contrato. Como mínimo: • Normograma actualizado de Seguridad y Privacidad de la Información, alineado con legislación aplicable del sector al que pertenece la Entidad y teniendo en cuenta la reglamentación interna de ANH. • Políticas actualizadas de seguridad y privacidad de la información conforme lineamientos gubernamentales y la norma NTC-ISO/IEC 27001:2013 • Inventario actualizado de Activos de Información que abarque todos los procesos de ANH • Clasificación de activos de la Información, criticidad, tipología según triada de seguridad de la información y privacidad incluyendo tratamiento de datos personales • Manual de Operación del SGSI • Procedimiento de Gestión de Incidentes • Plan Integral de Datos Personales • Demas documentos (elaborados y/o actualizados) requeridos para la implementación adecuada y completa de la seguridad y privacidad de la información conforme lineamientos de MINTIC como el Modelo de Seguridad y Privacidad de la Información, sus guías y Gobierno Digital, armonizados en lo referente los temas que apliquen de Arquitectura Empresarial, Modelo de

	Gestión IT+4, normatividad vigente en materia de Teletrabajo, Delitos Informáticos, Conpes 3854 Política Nacional de Seguridad Digital, protección de datos personales, habeas data, propiedad intelectual y derechos de autor así como la norma NTC-ISO/IEC 27001:2013. 9. Plan de concienciación y apropiación del Sistema de Gestión de Seguridad de la Información, cronograma, documentos asociados, evidencias de la realización de las sesiones, evaluación de las sesiones, material utilizado, videos, actas de reunión, listados de asistencia. 10. Documentos independientes que contengan actualizaciones y recomendaciones que apliquen a la estrategia actual de Continuidad del negocio de ANH y al Programa Integral de Gestión de Datos Personales de la ANH en alineación con las políticas de seguridad de la información y las buenas prácticas y lineamientos gubernamentales, en cumplimiento de la normatividad vigente. 11. Diagnóstico del nivel de madurez del SGSI y de la privacidad de la información de la ANH conforme a la norma NTC ISO/IEC 27001:2013, Plan de preauditoria como preparación para la certificación, informe de resultados de preauditoria, con el plan de cumplimiento de las no conformidades detectadas y evidencias de la subsanación de los hallazgos, documento con la estimación de costos de preparación y el aprovisionamiento necesario para aspirar a la certificación NTC-ISO/IEC 27001:2013. 12. Solución tecnológica instalada, parametrizada e implementada que cumpla los requerimientos técnicos mencionados en el apartado especificaciones técnicas, licenciamiento, soporte y garantía. 13. Plan de trabajo e informes mensuales de ejecución de las actividades asociadas a la identificación de riesgos, infraestructura, vulnerabilidades, amenazas, brecha, tratamiento, controles, documentación, gestión de incidentes y demás implementaciones y acompañamiento

	en materia de seguridad informática, hacking ético (direccionamiento público y privado), evidencia digital, técnicas forenses y ciberseguridad. 14. Listados de asistencia, memorias, material y certificaciones obtenidas por el personal de ANH capacitado
Equipo de Trabajo	**EQUIPO DE TRABAJO** El contratista deberá contemplar como mínimo los recursos de personas que se encuentran definidos en la tabla personal mínimo requerido. La experiencia profesional se computará conforme lo señalado en el artículo 229 del Decreto Ley 019 de 2012, siempre y cuando se tenga certeza mediante certificado de la fecha de terminación y aprobación del pensum académico de educación superior (pregrado). De lo contrario y en los demás casos, se computará a partir de la fecha de grado. No se tendrá en cuenta experiencia simultánea o certificaciones sin el lleno de requisitos. Así mismo, todas las profesiones que requieran Tarjeta profesional deberán acreditarla desde el momento de la propuesta. 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 o superior que el presentado en la propuesta. Cuando el personal asignado por el Contratista requiera contactarse con personal de otros grupos o dependencias, deberá estar acompañado por algún representante del Equipo de trabajo de Seguridad de la información de ANH o en su defecto, del Jefe de la Oficina de Tecnologías de la Información.

PERSONAL MÍNIMO REQUERIDO				
Rol	**Perfil**	**Experiencia específica mínima**	**Certificaciones estándares**	**Dedicación**
Gerencia de	Debe contar con título	Acreditar como mínimo	• PMP Vigente	50%

		Proyecto	profesional en Ing. de Sistemas, Eléctrico o Electrónico, Industrial o Administrador de Empresas. Debe contar con una especialización en áreas administrativas o de gestión de proyectos	cinco (5) años de experiencia profesional como director o Gerente de Proyecto en Implementaciones del SGSI. Mínimo dos (2) certificaciones de experiencia en Proyectos en Implementaciones del SGSI en diferentes entidades del estado a nivel nacional.	• ISO 27001 Auditor Lider o Interno.	
		Consultor Senior de Seguridad de la Información	Profesional Titulado en Ing. de Sistemas, Eléctrica, Telemática, Ing. Electrónico, Telecomunicaciones o afines. Debe contar con una especialización o maestría en seguridad de la información o seguridad informática	Acreditar como mínimo cinco (5) años de experiencia profesional en Proyectos de Implementaciones del SGSI como consultor senior en seguridad de la información. Tres (3) Certificaciones de Proyectos de diseño y/o desarrollo y/o implementación de Sistemas de Gestión de Seguridad de la Información como Líder de Seguridad de la Información. Al menos dos (2) de las certificaciones de experiencia deber ser en entidades del estado a nivel nacional.	• Auditor Líder ISO 27001:2013 o Implementador ISO 27001:2013	50%
		Implementador Solución Tecnológica	Profesional Titulado en Ing. de Sistemas, Eléctrica, Telemática, Ing. Electrónico, Telecomunicaciones o afines	Acreditar como mínimo dos (2) años de experiencia profesional en Implementaciones y/o soporte y/o mantenimiento de la solución tecnológica ofrecida a implementar.		100% durante implementación de la solución tecnológica
		Consultor Seguridad de la Información II	Profesional Titulado en Ingeniera de Sistemas o telemática o Electrónica o Telecomunicaciones o Administrador de Sistemas de Información Especialización o Maestría en Seguridad de la Información o seguridad informática	Acreditar como mínimo cinco (5) años de experiencia como consultor en Seguridad de la Información y experiencia específica en al menos dos (2) proyectos de implementación de SGSI en el rol propuesto. Al menos uno (1) de los proyectos en una (1) entidad del estado.	Auditor Líder o Implementador ISO 27001	100%
		Documentador	Profesional titulado en Ingeniería de Sistemas o Ingeniera de Telecomunicaciones o Ingeniería Telemática o Industrial	Acreditar como mínimo dos (2) años de experiencia en generación de manuales y documentación técnica	N.A.	100%
		Experto Seguridad Informática, informática forense o ciberseguridad	Profesional Titulado en Ingeniera de Sistemas o telemática o Electrónica o Telecomunicaciones Especialista o Magíster en Seguridad Informática o ciberseguridad	Acreditar como mínimo cinco (5) años de experiencia profesional en Proyectos de Implementaciones del SGSI y/o como experto en seguridad informática, informática forense o ciberseguridad	Contar con mínimo dos (2) de las siguientes certificaciones: CIFI- Certified Information Forensics Investigator CEG- Certified Ethical Hacker CISA - Certified Information	100% durante el contrato y disponibilidad en soporte técnico los siguientes seis (6) meses a la finalización del contrato

			Dos (2) Certificaciones de Proyectos de diseño y/o desarrollo y/o implementación de Sistemas de Gestión de Seguridad de la Información como Líder de Seguridad Informática, experto en seguridad informática, en informática forense o en ciberseguridad. Al menos una (1) de las certificaciones de experiencia en una (1) entidad del estado a nivel nacional.	System Auditor CSX - Cybersecurity Nexus Lead Cibersecurity Manager ISO/IEC 27032 Certified Ethical Hacker (CEH) CISM – Chief Information Security Managment CISSP - Certified Information Systems Security Professional	
Facilitador transferencia de Conocimiento	Profesional o licenciado titulado en áreas relacionadas con el objeto contractual, docencia o pedagogía	Acreditar como mínimo cinco (5) años de experiencia profesional como docente o facilitador en Proyectos de Implementaciones del SGSI o temáticas asociadas a la Tecnología.		100% en la planeación y ejecución y entrega de resultados de las sesiones y ejercicios de apropiación	

PLAZO:	El plazo de ejecución del contrato a celebrar será hasta el 31 de Diciembre de 2019 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. Con posterioridad a la finalización del contrato, se continuará prestando el servicio de soporte técnico del profesional especializado en materia de seguridad informática, informática forense y ciberseguridad, por un término de seis (6) meses, conforme especificaciones técnicas indicadas.
LUGAR DE EJECUCIÓN:	Para todos los efectos el domicilio contractual será la ciudad de Bogotá D.C.
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

Contratar la Implementación del Sistema de Gestión de Seguridad de la Información SGSI, la adquisición de una solución tecnológica para la administración, evaluación, gestión de riesgos y las etapas del ciclo de vida del SGSI, fortalecimiento de controles de seguridad física y el apoyo especializado en seguridad informática y forense, alineada a la Estrategia de Gobierno Digital, conforme a las necesidades de la ANH y a las buenas prácticas vigentes

Ítem	Descripción	Cantidad	Valor (COP)	IVA (19%)	Total (COP)
1	Gerente de Proyecto para el desarrollo de todas las actividades hasta 31 de Diciembre de 2019 según disponibilidad solicitada.	1	$	$	$
2	Consultor Senior de Seguridad de la Información para el desarrollo de todas las actividades hasta 31 de Diciembre de 2019 según disponibilidad solicitada.	1	$	$	$
3	Implementador solución tecnológica para el desarrollo las actividades asociadas según disponibilidad solicitada.	1	$	$	$
4	Consultor Seguridad de la Información II para el desarrollo de todas las actividades hasta 31 de Diciembre de 2019 según disponibilidad solicitada.	1	$	$	$
5	Documentador para el desarrollo de todas las actividades hasta 31 de Diciembre de 2019 según disponibilidad solicitada.	1	$	$	$
6	Experto en seguridad informática, forense o ciberseguridad para el desarrollo de todas las actividades hasta 31 de Diciembre de 2019 y seis (6) meses más por demanda.	1	$	$	$
8	Facilitador para el desarrollo de todas las actividades asociadas, según disponibilidad solicitada.	1	$	$	$
9	Proveer un Software especializado, para la Gestion del SGSI y el seguimientos a	1	$	$	$

	los riesgos.				
10	Sistema de etiquetado y alarma antihurto (antenas y software)	Según especificaciones	$	$	$
11	Controles antihurto y privacidad (protectores cámara, anti-espías y guayas)	Según especificaciones	$	$	$
12	Dispositivos de almacenamiento seguro (USB´s)	Según especificaciones	$	$	$
13	Dispositivos de almacenamiento seguro (DD)	Según especificaciones	$	$	$
14	Caja de seguridad	Según especificaciones	$	$	$
15	Cursos, certificaciones, transferencia de conocimiento y preauditoria				
VALOR TOTAL			**$**	**$**	**$**

Comentario [GASV3]: ¿No entiendo, están cobrando por aparte la consultoría?
¿No estaría incluido en el personal que estamos sondeando?

Comentario [SMRF4R3]: Se elimina consultoría
Se agrega los cursos certificables ya que no estaban incluidos

Por favor abstenerse de modificar la propuesta económica.

Nombre y Firma Represéntate Legal:
_____

Nombre Empresa:
_____

NIT:
_____

Página
Web:_____

Correo:
_____

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: german.suarez@anh.gov.co antes del día **8 de mayo de 2019**, 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.