R3DkODE-39

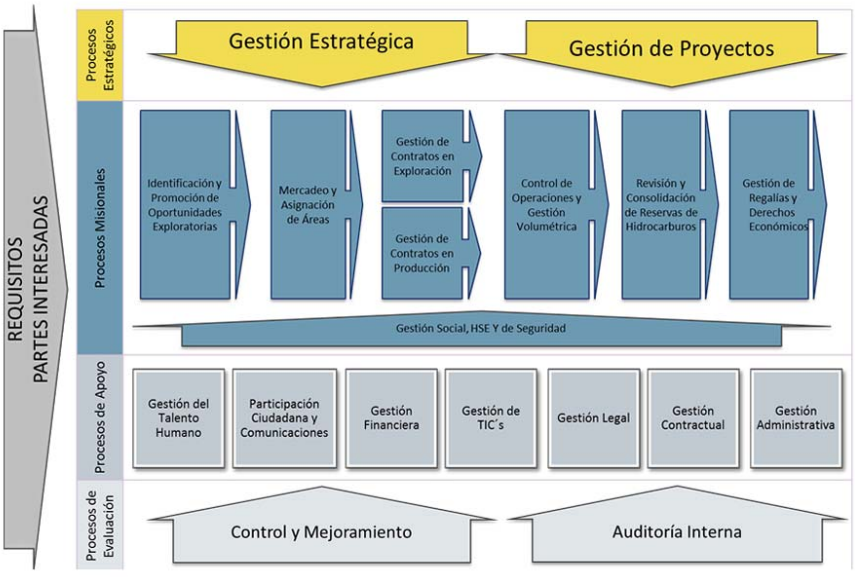
R4D1C4D0

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, teniendo en cuenta que no se está formulando invitación para participar en un concurso o proceso selectivo. - Se reitera, que 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.*

<table>
<tr><td>DESCRIPCIÓN DE LA NECESIDAD:</td><td>Conocer los riesgos de la seguridad de la información de la AGENCIA NACIONAL DE HIDROCARBUROS para que sean asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías; en el marco del modelo de Seguridad y Privacidad de la Información del Ministerio de las Tecnologías y Comunicaciones, dentro de los lineamientos en Línea vigentes.</td></tr>
<tr><td>OBJETO A CONTRATAR:</td><td>Consultoría para la implementación del Sistema de Gestión de Seguridad de la Información</td></tr>
<tr><td>ALCANCE DEL OBJETO:</td><td>.</td></tr>
<tr><td>IDENTIFICACION DEL CONTRATO A CELEBRAR:</td><td>PRESTACIÓN DE SERVICIOS POR CONCURSO DE MERITOS</td></tr>
<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>Identifique el o los Códigos UNSPSC:
<table><tr><td>SEGMENTO</td><td>FAMILIA</td><td>CLASE</td><td>PRODUCTO</td><td>NOMBRE</td></tr><tr><td>80</td><td>8010</td><td>801015</td><td>80101507</td><td>Servicios de asesoramiento sobre tecnologías de la información</td></tr></table></td></tr>
</table>

ASPECTOS TÉCNICOS:	**ACTIVIDADES A DESARROLLAR** 1. Definir un Plan de trabajo, especificando fases, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir las técnicas y herramientas que utilizará en la ejecución del contrato, previa aprobación de la Agencia Nacional de Hidrocarburos. El plan de trabajo debe considerar el cumplimiento de los lineamientos fijados por las normas legales vigentes aplicables a la Entidad y estándares aplicables a la Gestión de la Seguridad de la Información como ISO 27001:2013, COBIT 5, ISO 20000-1:2011, NIST, que sean necesarias para la Agencia Nacional de Hidrocarburos y las que surgieren en el desarrollo del contrato. 2. Realizar pruebas de Vulnerabilidad externas sobre máximo 50 direcciones IP y pruebas internas sobre máximo 100 direcciones IP. Se deben realizar pruebas de ingeniería social sobre un máximo de 15 personas, aplicando diferentes técnicas para obtener información sensible. 3. Mantener actualizada la estrategia de seguridad de la Agencia Nacional de Hidrocarburos, involucrando los proyectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información. 4. Realizar la identificación y clasificación de los activos de información de los procesos misionales y de Tecnología, lo cual se desarrollará en conjunto con los responsables de dichos procesos de la siguiente cadena de valor. 

ASPECTOS TÉCNICOS:	5. Proponer y apoyar la definición e integración de una metodología de gestión de riesgos a implementar en la Agencia Nacional de Hidrocarburos, para realizar el levantamiento de riesgos de Seguridad y privacidad de la Información teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad de la información. 6. 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 los siguientes procesos y su relación con el contexto: • Procesos Misionales: 7 • Procesos de Tecnología y Plataforma que soporta la Infraestructura TI. 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, y posteriormente el monitoreo de controles implementados. 7. Apoyar la gestión de actividades relacionadas con la implementación y mejoramiento del Sistema de Gestión de Seguridad de la Información ISO 27001:2013, incluyendo los dieciocho (18) dominios de seguridad definidos en el anexo de dicha norma A la cual forma parte del mismo estándar (NTC ISO 27001:2013 – Anexo A -> 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 actuales en la Entidad. La metodología a utilizar debe considerar por los menos lo siguiente: Revisión y/o actualización de la documentación y controles establecidos en el proceso de implantación del SGSI, sesiones de trabajo, análisis de información recopilada y valoración de cumplimiento, documentación, recomendaciones y generación de planes de remediación. 8. Apoyar la integración de los requisitos de la Norma ISO 27001:2013 respecto a otros estándares implementados en la Agencia Nacional De Hidrocarburos (ejemplo: NTC ISO 9001:2008 u Otros). 9. 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) y alineado al sistema de gestión de calidad si existe, los resultados de la gestión de riesgos y el monitoreo de las políticas de seguridad de la información de la Entidad y cualquier observación que se presente durante la vigencia del contrato dada por los entes de control.

ASPECTOS TÉCNICOS:	10. Elaborar y ejecutar el plan Anual de sensibilización del Sistema de Gestión de Seguridad de la Información, dirigido a los usuarios de la red corporativa y terceros, incluidos los diferentes usuarios a nivel nacional. El plan debe considerar actividades mensuales de sensibilización durante la vigencia del contrato. La definición del plan está a cargo del proponente y debe ser acordado con el personal del Grupo conformado por el área de Seguridad Informática y seguridad de la Información de ANH. 11. Ejecutar mensualmente durante la ejecución del contrato, en conjunto con el grupo de monitoreo de la Agencia Nacional De Hidrocarburos, revisiones a cada uno de los requisitos de seguridad del estándar y las que surjan aplicables a la ANH, para validar permanentemente su cumplimiento y la debida actualización de los soportes. 12. Apoyar la documentación de la estrategia de Continuidad del Negocio, todos los procedimientos para la administración, operación, mantenimiento del Plan de Recuperación de Desastres y el seguimiento a la ejecución de las pruebas (Escritorio, planeadas y totales) necesarias para garantizar la operación del DRP, igualmente, apoyo y acompañamiento en caso de requerir su activación o creación. Se deben ejecutar las siguientes acciones: a. Realizar el análisis de impacto en el negocio (BIA) para los procesos que hacen parte del alcance del SGSI b. Realizar un análisis de escenarios de falla y estrategias de recuperación actualmente implementadas por la Entidad. c. Generar Planes de recuperación específicos para los procesos incluidos dentro del alcance del SGSI 13. El personal en sitio, que está conformado por el equipo consultor (Equipo de trabajo) durante la ejecución del contrato, debe apoyar la revisión de las respuestas a los requerimientos sobre seguridad de la información que efectúen los entes de control internos y externos. 14. Monitorear durante la ejecución del contrato, el SGSI de la Agencia Nacional De Hidrocarburos frente al cumplimiento de la normatividad vigente y a la ISO 27001:2013 y evaluar el nivel de madurez del SGSI y de la privacidad de la información de la ANH. 15. Desarrollar estándares o plantillas de seguridad para las siguientes plataformas tecnológicas: a. Windows Server 2012 b. SQL Server 2012 c. Firewall y Telecomunicaciones

ASPECTOS TÉCNICOS:	d. Aplicaciones web 16. El proveedor deberá contemplar como mínimo los recursos de personal que se encuentran definidos en el Requerimientos de Personal. 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 o mejor perfil solicitado en la invitación. 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. 17. Gap Análisis del estado actual de la Entidad en la Implementación de la NTC-ISO-27001 18. Matriz detallada con los resultados del análisis GAP, situación actual, principales hallazgos y oportunidades de mejora identificadas. 19. Gap Análisis de Cumplimiento de la Normativa de Gobierno en Línea en el contexto del Modelo de Seguridad y Privacidad de la Información. 20. Informe técnico de las pruebas de vulnerabilidad externas. 21. Informe técnico de las pruebas de vulnerabilidad internas. 22. Informe ejecutivo de las pruebas de vulnerabilidad internas y externas. 23. Plan de remediación de las vulnerabilidades identificadas con nivel de riesgo alto. 24. Informe de Pruebas de Ingeniera Social. 25. Matriz de Identificación y Clasificación de Activos de Información. 26. Procedimientos de clasificación, etiquetado y uso aceptable de activos de información. 27. Política de Seguridad General de la ANH. 28. Políticas Complementarias de Seguridad de la Información. 29. Metodología de tratamiento de Riesgos, acorde a la metodología que establezca la Oficina de Control Interno o la definida por el Departamento de la Función Pública del Estado Colombiano. 30. Nomograma de Seguridad y Privacidad de la Información en el cual está centrada la Entidad. 31. Alcance del SGSI. 32. Procedimiento de Control de Documentos y Registros. 33. Procedimiento de Auditorías Internas. 34. Procedimiento de Acciones Correctivas y de Mejora. 35. Procedimiento de Gestión de Incidentes de Seguridad. 36. Procedimiento de Gestión de medios removibles 37. Procedimiento de Eliminación segura de información 38. Procedimiento de Gestión de cuentas de usuario y contraseñas 39. Procedimiento de intercambio seguro de información

	40. Procedimiento de control de cambios de TI 41. Procedimiento de identificación de legislación aplicable y de los requisitos contractuales 42. Acuerdos de Confidencialidad definidos, para Contratistas, servidores públicos, empresas operadoras y entidades con las que se realice intercambio de información. 43. Plan de Tratamiento de Riesgos para todos los activos definidos en el alcance. 44. Inventario de Activos de Información de los procesos definidos en el alcance. 45. Clasificación de activos de la Información. 46. Definición por cada dominio, de un documento, detallando los controles, los activos y el cómo se ha operatividad este control, para mitigar los riesgos inherentes, así como el detalle de los riesgos residuales. Mejorar redacción. 47. Suministrar el Plan de comunicaciones del SGSI, con las herramientas que permitan la divulgación del mismo (Videos, fondos de Pantalla, Pendones, letreros, salvapantallas). 48. Matriz de Análisis de Impacto al Negocio (BIA). 49. Documento con el análisis de los escenarios de falla y Estrategias de recuperación actualizadas. 50. Planes de recuperación de los procesos incluidos dentro del alcance del proyecto. 51. Plan Maestro de Recuperación y manejo de crisis. 52. Plan (6 meses) de Pruebas del Plan de Continuidad del Negocio 53. Realizar 12 Capacitaciones de Concienciación en Seguridad de la Información. 54. Realizar 12 Capacitaciones en el SGSI. 55. Manual de Operación del SGSI: 56. Manual de Protección de Datos personales, donde se establezca, de la información que maneja la Entidad que datos son susceptibles de tratamiento. 57. Manual de Transparencia, donde se detalle que información es sujeta de cumplimiento del decreto 1712 de 2014. 58. Formatos para solicitud de Información Pública.
Herramienta de Seguimiento SGSI	**Se deberá entregar a la Entidad, implementada y en funcionamiento una herramienta licenciada por al menos (2) dos años para el seguimiento y control del SGSI con las siguientes características:** • gestión de la Implementación y el ciclo PHVA • gestión de arquitectura empresarial • gestión de activos de información • gestión de riesgos (identificación, valoración, evaluación y tratamiento) • gestión de incidentes de seguridad de la información • gestión de continuidad de seguridad de la información • gestión de roles de seguridad de la información • gestión documental • gestión de controles bajo 27001:2013

	• cumplimiento regulatorio • normas corporativas • indicadores y medición de seguridad de la información. • Se espera de esta herramienta, poder sistematizar de manera óptima, el seguimiento y control del SGSI de la entidad.
Equipo de Trabajo	**EQUIPO DE TRABAJO** El proveedor deberá contemplar como mínimo los recursos de personas que se encuentran definidos en la tabla personal mínimo requerido. El personal presentado en la propuesta debe ser el mismo que realiza el desarrollo del contrato no 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 Indicar en las certificaciones estándares el conector y .o texto "Contar con las siguientes certificaciones" Con una dedicación del 50%del personal es suficiente para el proyecto. Incluir solo un senior en seguridad, recuerda que todo lo que coloques aquí incrementa los costos del proyecto.

PERSONAL MINIMO REQUERIDO				
Rol	Perfil	Experiencia específica mínima	Certificaciones estándares	Dedicación
Gerente de Proyecto	Profesional universitario en ingeniería electrónica, sistemas o telecomunicaciones, Administración de empresas o afines.	El profesional deberá contar mínimo con seis (6) años de experiencia, en gerencia de Proyectos de tecnología de los cuales 3 deben ser liderando proyectos de implementación del sistema de gestión de seguridad de la información.	Contar con las siguientes certificaciones Magister en Gestión de Proyectos Certificado PMP V5 Certificado ITIL V3 Foundation	50%

		Auditor Líder ISO 27001	Profesional universitario en ingeniería electrónica, sistemas o telecomunicaciones, Administración de empresas o afines.	Debe haber participado en el diseño, e implementación en sistemas de gestión de seguridad de la información, mínimo dos (2) proyectos cuyo objetivo sea la implementación de un Sistema de Gestión de Seguridad de la Información, estándar ISO 27001. Debe contar con una experiencia no inferior a seis (6) años en proyectos de seguridad de la información. Debe tener conocimiento en gestión de riesgos	Contar con las siguientes certificaciones Certificado Auditor Líder ISO 27001 Certificado Lead Risk Manager bajo ISO31000:2009 Certificado Auditor Interno ISO 22301 Certificado Auditor Interno ISO 20000 Certificado Auditor Interno ISO 9000 Certificado ITIL V3 Foundation Certificado COBIT 5 Foundations Certificado CISM	50%
		Profesional Sénior en Seguridad de la Información (2)	Profesional universitario en ingeniería electrónica, de sistemas o de telecomunicaciones.	Debe contar con una experiencia no inferior a seis (6) años en proyectos de tecnología y/o seguridad informática y/o administración de herramientas de seguridad y aseguramiento de sistemas	Contar con las siguientes certificaciones Certificado Auditor líder ISO27001 Certificado Auditor Interno ISO 22301 Certificado Lead Risk Manager bajo ISO31000:2009 Certificado COBIT 5 Foundations	100%

	<table><tr><td>Experto en Hacking Ético</td><td>Profesional universitario en ingeniería electrónica, de sistemas o de telecomunicaciones.</td><td>Debe contar con una experiencia no inferior a seis (6) años en proyectos de tecnología y/o seguridad informática y/o administración de herramientas de seguridad y aseguramiento de sistemas</td><td>Contar con las siguientes certificaciones Certificado CEH Certificado Auditor líder ISO27001 Certificado Auditor Interno ISO 22301 Certificado Lead Risk Manager bajo ISO31000:2009 Certificado COBIT 5 Foundations</td><td>50%</td></tr></table> Nota: Aquellas profesiones que les sea aplicable la ley 842 de 2003 en cuanto al cómputo de la experiencia profesional, deberá regirse por lo establecido en el artículo 12 de la mencionada ley.
PLAZO:	El plazo de ejecución del contrato a celebrar será hasta el 31 de diciembre de 2.016, 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 D.C.
PROPUESTA ECONÓMICA:	Incluir el formato económico diseñado por la ANH, el cual incluye los costos e impuestos que apliquen.

PROPUESTA ECONOMICA

PROPUESTA ECONÓMICA:

"Consultoría para la implementación del Sistema de Gestión de Seguridad de la Información"

Ítem	Descripción	Cantidad	Valor Unitario	Valor Total	IVA sobre el Total	Valor Total con IVA
1	Gerente de Proyecto	1				
2	Auditor Líder ISO 27001	1				
3	Profesional Sénior en Seguridad de la Información	2				
4	Experto en Hacking Ético	1				
5	Herramienta de Seguimiento SGSI	1				
Valor Total				**$**	**$**	**$**

Por favor abstenerse de modificar la propuesta económica.

Nombre y Firma Representante Legal:_____

Nombre Empresa:_____

NIT :

Validez de la Oferta 120 días

Nota: La propuesta no podrá sobrepasar el presupuesto oficial estimado, so pena de incurrir en causal de rechazo.

_____
Firma del Representante Legal

ENTREGA DE INFORMACIÓN DEL SONDEO DE MERCADO: Las firmas invitadas deberán entregar la información solicitada en el presente sondeo de mercado al correo electrónico: carlos.bastidas@anh.gov.co Eric.vargas@anh.gov.co antes del día 29 de Julio de 2016.

ORLANDO VELANDIA SEPÚLVEDA
Vicepresidente Administrativo y Financiero

Aprobó: Juan Carlos Vila Franco – Jefe Oficina de Tecnologías de la Información.
Proyectó Carlos Abel Bastidas Cubides – Experto Grado 7 G3 - Componente Técnico