

TERMINOS DE REFERENCIA

Herramienta de Seguimiento SGSI

REQUERIMIENTOS MÍNIMOS EXCLUYENTES:

El oferente adjudicatario se obliga a cumplir con las siguientes especificaciones.

Funcionalidad de la herramienta

MÓDULOS DE LA HERRAMIENTA	FUNCIONALIDAD	DESCRIPCIÓN
ADMINISTRACIÓN	GESTIÓN DE SERVICIOS	<ul style="list-style-type: none"> - Permite la configuración de información, servicios contratados, usuarios y opciones específicas. - Permite la consulta del tipo de licencia y de los servicios contratados, siendo ambos conceptos independientes.
	GESTIÓN DE USUARIOS Y PERFILES	<ul style="list-style-type: none"> - En función del tipo de usuario se podrán crear y gestionar otros usuarios, o gestionar perfiles a medida. - La creación de perfiles permite la creación de roles con permisos especiales de acceso y modificación de la información - Permite la creación, modificación, supresión y configuración de usuarios. Dentro de configuración, se permite: modificar los datos de usuario, gestionar las notificaciones, gestionar usuario y contraseña, y elegir el huso horario en función del país en el que se encuentre. - Permite la configuración de notificaciones, a través de las cuales el usuario recibirá por correo electrónico información sobre el avance del proyecto, próximas tareas, tareas retrasadas, etc.
PROYECTOS	MODELOS	<ul style="list-style-type: none"> - Permite la creación de proyectos moldes que después pueden ser asignados a diferentes empresas. Se podrán definir los hitos y tareas genéricos comunes a cualquier proyecto de este tipo, así como las cargas.
	PROYECTOS	<ul style="list-style-type: none"> - Permite seleccionar un modelo de proyecto entre los que están previamente creados o crear un proyecto vacío. - Permite generar un proyecto asociado a la empresa, gestionando las cargas y tareas de los equipos de trabajo y asignar tareas a los miembros del equipo de trabajo. - Existen avisos mediante correo electrónico correspondientes a las tareas que se deben realizar, tareas retrasadas, hitos completados, entre otros, una vez cargado y configurado el proyecto. - Permite la configuración de estados para indicar el progreso o avance del proyecto. - Al finalizar hitos y tareas se podrán cerrar y traspasar a la barra de progreso, pasando a estado histórico una vez finalizado todo el proyecto. - Permite el seguimiento y coordinación del proyecto por tipo de rol a través de un calendario.
CONFIGURACIÓN	GENERAL	<ul style="list-style-type: none"> - Permite la configuración y edición de campos, valores así como diferentes visualizaciones de formularios. - El software proporciona numerosas opciones de configuración para adaptar la funcionalidad a las necesidades del cliente a través de la propia interfaz web de la herramienta.
	ALERTAS Y NOTIFICACIONES	<ul style="list-style-type: none"> - Incorpora notificaciones para facilitar la gestión global del sistema.
	METODOLOGÍAS	<ul style="list-style-type: none"> - Permite la configuración de la metodología para la evaluación de los riesgos. - Permite la definición de diferentes dimensiones, tanto cualitativas como cuantitativas, con diferentes niveles por cada dimensión. - Permite metodologías cuantitativas y cualitativas. - Permite la configuración de una metodología para la evaluación/calificación de controles. - Permite la definición de niveles por cada dimensión definida en la evaluación de controles.

		<ul style="list-style-type: none"> - Permite la evaluación de los riesgos considerando el resultado de la evaluación de los controles.
	CATÁLOGOS ANÁLISIS RIESGOS	<ul style="list-style-type: none"> - Dispone de un catálogo de amenazas y vulnerabilidades de seguridad de la información, de forma que puede ser utilizado en el análisis de riesgos de los activos. - Permite la modificación del catálogo de amenazas y vulnerabilidades para ajustarlo a las necesidades de la organización. - Permite la definición de amenazas en función de los Servicios, Procesos, Información, Hardware, Software, en la alineación con el Sistema de Gestión de Seguridad de la Información. - Permite la asignación de amenazas a cada categoría, así como establecer vulnerabilidades a cada amenaza. - Permite definir controles para cada amenaza. - Permite la exportación de catálogos ya creados e importar la información en otros catálogos nuevos.
	CATÁLOGO CUMPLIMIENTO / AUDITORÍA	<ul style="list-style-type: none"> - Dispone del catálogo de requisitos de la norma ISO 27001 vigente. - Permite la configuración propia de los catálogos. - Permite la configuración de ayudas a los catálogos. - Permite la configuración de niveles de madurez para la evaluación de los marcos definidos. - Permite el diseño de los niveles objetivos a conseguir.
	ENCUESTAS	<ul style="list-style-type: none"> - Permite la definición de modelos de encuestas para realizar la clasificación de los activos, el análisis de riesgos y la evaluación de los controles. - Permite definir las preguntas para generar el modelo de encuesta. - Permite publicar y distribuir las encuestas a los usuarios de la compañía que deben responder. - Permite el acceso a las encuestas publicadas sin necesidad de ingresar en la herramienta de gestión. - Permite la consolidación de la información recibida.
	INTEGRACIONES	<ul style="list-style-type: none"> - Permite la integración con otras fuentes de información de la organización, mediante diferentes mecanismos como Web Services, APIs, Import/Export de distintos tipos de archivos. - Permite la gestión desde una sola herramienta o entre módulos integrables. - Entre las herramientas y plataformas incluidas para la integración cabe destacar: herramientas de monitoreo, ticketing, CMDB e inventariado de activos, cuentas de correo electrónico o sincronización con el Directorio Activo.
OPCIONES COMUNES	GESTOR DOCUMENTAL	<ul style="list-style-type: none"> - Permite almacenar y controlar la documentación asociada al Sistema de Gestión, adaptándose a cada empresa puesto que dicha funcionalidad es completamente configurable. - Permite establecer la estructura de carpetas deseada para clasificar la documentación. - Permite almacenar las versiones obsoletas de cada documento gestionado. - Permite la creación y adaptación de flujos de revisión y aprobación de la documentación (workflow) para distintos tipos de documentos. - Permite la definición de los estados del flujo de aprobación así como roles o responsables de cada estado y de su paso al siguiente estado. - Permite definir criterios de cambio de estado según las especificaciones del workflow.
	INFORMES Y REPORTES	<ul style="list-style-type: none"> - Dispone de reportes genéricos que permiten visualizar la información relevante. - Dispone de interfaz para diseño de reportes a requerimientos del usuario. - Módulo de Generación de Informes. Permite la creación de informes personalizados sobre toda la información de la plataforma.
	OTRAS	<ul style="list-style-type: none"> - Actas de Reunión. Creación, modificación y gestión de actas de reunión que permitirán dejar constancia de las decisiones tomadas sobre el sistema de gestión. Además se podrán enviar por correo electrónico a los participantes de las mismas.

ESTRUCTURA ORGANIZATIVA		<ul style="list-style-type: none"> - Tareas Pendientes. A través de esta funcionalidad se puede crear un listado rápido de tareas por hacer en el Sistema de Gestión.
	CATÁLOGO DE SERVICIOS	<ul style="list-style-type: none"> - Permite definir los servicios y productos implicados en el alcance. Los servicios y productos que se definan en el catálogo, pasarán a formar parte del sistema (se convertirán en activos para su posterior análisis) y permitirán categorizar y tipificar todo el sistema capilarizando todo el sistema en estos servicios y productos.
	PROCESOS	<ul style="list-style-type: none"> - Permite la definición de los procesos de negocio que conforman la organización. - Permite establecer dependencias entre los diferentes procesos de negocio (macroprocesos, procesos principales, subprocesos, etc.). - Permite asociar los procesos de negocio a los servicios y productos de la organización.
	ESTRUCTURA ORGANIZATIVA	<ul style="list-style-type: none"> - Permite la definición de la estructura organizativa del cliente, es decir, los departamentos, áreas, gerencias, etc. en los que se estructura la organización. - Permite utilizar los elementos definidos en la estructura organizativa para asociar servicios, procesos, empleados, etc. a una estructura concreta.
	ALCANCE	<ul style="list-style-type: none"> - Permite definir el alcance del sistema de gestión de seguridad de la información, en base a los servicios y procesos definidos. - Permite definir información asociada al alcance, como por ejemplo el comité responsable, el responsable del sistema de gestión, los departamentos, la ubicación, entre otros. - Permite adjuntar documentos que describen el alcance con mayor detalle (diagramas, organigramas, etc.).
	OBJETIVOS	<ul style="list-style-type: none"> - Permite determinar los objetivos del sistema de seguridad de la información para un periodo determinado. - Permite asociar los objetivos a los servicios y productos definidos. - Permite definir objetivos específicos y establecer qué metas se propone la empresa para conseguir cada objetivo. - Permite la evaluación del cumplimiento de los objetivos.
	GESTIÓN DE ROLES	<ul style="list-style-type: none"> - Permite la asociación de roles a los empleados de la organización así como sus competencias, consiguiendo la trazabilidad entre los roles, los empleados, la capacitación de dichos empleados y las competencias de los puestos de trabajo.
	COMITÉS DE DECISIÓN	<ul style="list-style-type: none"> - Permite la definición de comités de la organización y los empleados que lo componen. - Permite el registro de las actas de reunión de cada uno de los comités.
	GAP ANALYSIS	<ul style="list-style-type: none"> - Permite la evaluación del estado de la organización respecto al cumplimiento de la norma ISO 27001 (u otra norma de seguridad de la información cargada en la herramienta) a través de un GAP Analysis o análisis de brecha. - Permite obtener gráficas que resumen el cumplimiento respecto al estándar evaluado.
	PLAN DE ADECUACIÓN	<ul style="list-style-type: none"> - Permite la generación de Planes de Adecuación para los GAP Analysis realizados. - Permite la planificación de las acciones a seguir para solventar los incumplimientos detectados. - Permite realizar el seguimiento de las acciones planificadas.
	GESTIÓN DE SLAs	<ul style="list-style-type: none"> - Permite definir los acuerdos de nivel de servicio y asociarlos al servicio o producto correspondiente del catálogo. - Permite añadir indicadores asociados a los Acuerdos de Nivel de Servicio (SLA) definidos. - Permite realizar la evaluación de los Acuerdos de Nivel de Servicio, generando conclusiones en función del resultado de la evaluación.
	PROVEEDORES	<ul style="list-style-type: none"> - Permite la definición de los proveedores/terceras partes, datos de contacto, contratos o incluso definir los SLAs además de evaluar el desempeño.


SEGURIDAD DE LA INFORMACIÓN (ISO 27001)		<ul style="list-style-type: none"> - La herramienta permite al usuario tener una base de datos de todos aquellos proveedores/terceras partes necesarios para la prestación de los servicios implicados en el alcance. - Permite subir cualquier archivo relacionado con la gestión de los suministradores (contratos, cláusulas de confidencialidad, etc.).
	INVENTARIO	<ul style="list-style-type: none"> - Permite la configuración de las categorías de elementos (servicios, procesos, personal, software, etc.) que se consideran en el inventario. - Permite la configuración de dimensiones cualitativas y cuantitativas para clasificar y valorar el elemento del inventario. - Permite calcular la Importancia de cada activo en función de la valoración realizada en las dimensiones definidas. - Dispone de un módulo de dependencias que permite asociar los elementos del inventario a los diferentes productos, servicios y procesos de negocio definidos, así como asociar los elementos entre sí. - Permite el levantamiento de información de elementos (identificación y clasificación) a través de encuestas. - Permite la importación de elementos en la herramienta, a partir de un archivo Excel.
	ANÁLISIS DE RIESGOS	<ul style="list-style-type: none"> - La herramienta dispone de un catálogo de seguridad de la información con amenazas, vulnerabilidades y controles predefinidos. - Permite la configuración de dimensiones y de metodologías para el cálculo de los riesgos. - El análisis de riesgos permite evaluar las amenazas que afectan a cada uno de los procesos y activos. - Permite analizar el coste que tienen los riesgos que se han identificado previamente en el inventario de elementos. - Permite realizar un análisis de coste-beneficio para determinar si compensa la implantación de un determinado control en función del coste del riesgo para la organización. - Permite asociar controles a los riesgos analizados para obtener el riesgo residual. - Actualización automática de los riesgos al modificar la valoración de los controles asociados. - Permite generar indicadores personalizados para el Análisis y Gestión de los Riesgos. - Permite asociar los indicadores de ScoreCard a cada uno de los riesgos valorados. - La herramienta ofrece la posibilidad de generar una amenaza específica que englobe varias amenazas definidas en el apartado de 'Análisis de Riesgos'. - Permite el levantamiento de información de las amenazas (identificación y evaluación) a través de encuestas.
	EVALUACIÓN DE RIESGOS	<ul style="list-style-type: none"> - Permite determinar el Nivel de Riesgo Aceptable global para todos los activos o particularizado para cada uno de ellos. - Permite visualizar de manera gráfica los resultados obtenidos tras la realización de los análisis de riesgos a través de un listado de riesgos, mapa de calor, gráfica de burbujas o el grafo dinámico de análisis repercutido.
	GESTIÓN DE RIESGOS	<ul style="list-style-type: none"> - Permite la posibilidad de realizar diferentes Planes de Tratamiento de Riesgos para los riesgos que se vayan a tratar, así como su seguimiento. - La herramienta permite realizar un seguimiento del grado de avance de implantación de los controles definidos. - Permite realizar proyecciones de riesgos para determinar que un Plan de Tratamiento de Riesgos es suficiente para conseguir los objetivos de la organización. - Permite realizar una proyección de los riesgos por costes, para analizar la inversión de la implementación de los controles frente a los impactos económicos que se producirían con la materialización de las amenazas. - Permite realizar la reevaluación de riesgos de forma automática a partir de las simulaciones realizadas.

	GESTIÓN DE CONTROLES	<ul style="list-style-type: none"> - Permite la configuración de dimensiones y de metodologías para la evaluación de controles. - Permite registrar todos los controles y medidas que la organización tiene implantado. - Permite el análisis de la eficacia de todos los controles registrados en esta opción, en función de la metodología definida para ello. - Permite asociar los controles a las amenazas/riesgos de forma que se pueda reflejar qué controles están relacionados con qué amenazas. - Permite el cálculo del riesgo residual en función de los controles implantados y su eficacia. - Permite la importación de controles y su valoración en la herramienta, a partir de un archivo Excel. - Permite el levantamiento de información de los controles (identificación y evaluación) a través de encuestas.
	HISTÓRICOS	<ul style="list-style-type: none"> - Permite la generación de históricos para comparar la evolución del análisis y gestión de riesgos a lo largo del tiempo. - La herramienta proporciona la opción de visualizar una gráfica de barras que muestra, separado por históricos, el número de amenazas por cada uno de los niveles de riesgos definidos. Esto permite ver la evolución de los distintos análisis realizados por parte de la organización y verificar gráficamente la tendencia que se pretende conseguir con la realización de los mismos.
	DECLARACIÓN DE APLICABILIDAD	<ul style="list-style-type: none"> - Permite definir la Declaración de Aplicabilidad de la norma ISO 27001 indicando la aplicabilidad y la justificación de cada uno de los controles de seguridad incluidos en la norma. - Permite el control y el seguimiento de la Declaración de Aplicabilidad a través de la asociación de documentación del gestor documental, la asociación de los controles a los riesgos y la asociación de no conformidades.
	ENCUESTAS	<ul style="list-style-type: none"> - Permite configurar encuestas relacionadas con activos, riesgos y/o controles, de forma que pueden ser utilizadas para realizar el levantamiento de la información del inventario de activos, el análisis de riesgos y los controles implantados de la organización. - Permite la publicación de encuestas de activos, riesgos y/o controles, de forma que los usuarios pueden completar la información requerida a través de un formulario Web accesible mediante un link, sin necesidad de acceder a la herramienta.
	PLANES DE FORMACIÓN	<ul style="list-style-type: none"> - Permite la gestión de formación o capacitación y la concienciación del personal. Desarrollo de planes que permitirán el seguimiento de la formación, análisis de resultados y posibles desviaciones
	AUDITORÍAS	<ul style="list-style-type: none"> - Permite establecer la programación de auditoría a realizar, todas aquellas que han sido llevadas a cabo, así como establecer todos aquellos puntos del proyecto que serán auditados y el informe generado de la auditoría. - Permite registrar y asociar los hallazgos detectados en la auditoría (no conformidades, acciones correctivas, mejoras...), pudiendo gestionar su resolución en la herramienta.
	INCIDENCIAS	<ul style="list-style-type: none"> - Permite la gestión de incidentes y problemas. Dispone de varios estados para los incidentes y problemas, permite asociarles categorías, servicios o priorizarlos. Además se podrá llevar un seguimiento pormenorizado de cada uno de ellos, enviar emails a los responsables y tomar decisiones. - Permite analizar las variaciones sobre el análisis de riesgos ante la ocurrencia de la incidencia. - Permite reevaluar los riesgos de forma automática a partir de la ocurrencia de la incidencia.
	PROCESOS DE GESTIÓN	<ul style="list-style-type: none"> - La herramienta proporciona la gestión integral de los empleados de la organización. Altas y bajas, roles y responsabilidades, y permisos de información. - Se podrán importar y exportar listados de empleados o sincronizar con sistemas de gestión de usuarios.

		<ul style="list-style-type: none"> - Permite la gestión de soportes, control de entradas y salidas y la asignación a empleados. - Se podrán crear, revisar y gestionar todas las no conformidades tanto derivadas de auditorías como de la propia mejora continua del sistema. Asociada a estas No Conformidades se podrán crear Acciones Correctivas, consiguiendo la trazabilidad necesaria. - Permite la gestión de Acciones Correctivas y Preventivas, su definición y relación con Incidencias, Problemas, Cambios y Entregas, No Conformidades, etc.
	INDICADORES	<ul style="list-style-type: none"> - Permite definir los indicadores necesarios para evaluar el desempeño del sistema. - El valor del indicador vendrá dado a través de una fórmula derivada de una o más métricas. - Los indicadores se pueden asociar a los riesgos identificados y analizados en las opciones de análisis de riesgos. - Visualización de gráficas de gestión de indicadores, a través de las cuáles se podrá ver el resultado de la fórmula anterior. - Permite descargar informes relativos a los indicadores.
	MÉTRICAS	<ul style="list-style-type: none"> - Permite la definición de métricas automáticas o manuales. - Catálogo de métricas automáticas relacionadas con otras opciones de la herramienta. - Visualización de gráficas de gestión de métricas dónde se mostrará el resultado obtenido. - Posibilidad de alertar al responsable de la métrica, mediante correo electrónico, para que registre la medición. - Permite descargar informes relativos a las métricas en distintos formatos.

Criterios técnicos de la herramienta:

Servicio	FUNCIONAL IDAD	DESCRIPCIÓN	CUMPLE		OBSERVA CIONES
			SI	NO	
CARACTERÍSTICAS TÉCNICAS		- Permite la integración de todos los sistemas en un solo entorno.			
		- Número ilimitado de usuarios a la herramienta.			
		- Conexión simultánea de usuarios.			
		- Permite la segregación de acceso para administradores, usuarios y operadores.			
		- Autenticación de los usuarios compatible con el directorio activo.			
		- Permite la gestión integrada de diferentes entidades de la misma organización.			
		- Idioma de la herramienta: español e inglés.			
		- Instalación en el Centro de Datos de la Organización adjudicadora (Modalidad insitu).			
		- Permite el cumplimiento íntegro de la norma ISO 27001, así como integrarlo con otras normas como ISO 9001, ISO 14001, ISO 22301, ISO 20000, ISO 31000, OHSAS, PIC y la propia Ley de Protección de Datos Personales con otros módulos.			

	<p align="center">AGENCIA NACIONAL DE HIDROCARBUROS FORMATO SONDEO DE MERCADO</p>	<p align="center">AGENCIA NACIONAL DE HIDROCARBUROS- GCO-FR- 17 01/03/2016 Versión N°01 Página 6 de 11</p>
---	--	--

	- La herramienta cuenta con esquema de Backup diario.			
LICENCIAMIENTO	- Permite el licenciamiento en SaaS o licenciamiento en sitio.			
DISTRIBUCIÓN	- Permite la distribución del software en SaaS o in situ en el cliente.			
CERTIFICACIONES	- La distribución SaaS está certificada en ISO 27001, ISO 20000 e ISO 22301			

