Solicitud de Información

Solución de Gestión de Riesgos y Auditorías de Seguridad e Higiene Industrial

A. INFORMACIÓN GENERAL

Dentro de la hoja de ruta de la estrategia de transformación digital del Canal de Panamá presenta retos tecnológicos importantes para transformar temas claves de la organización como el modelo de negocios, la experiencia de usuario (integración de todos los canales) y la transformación de procesos (cómo se prepara a todo el personal y las capacidades), con el objetivo de posicionarnos como una organización ágil y flexible capaz de prosperar en un entorno disruptivo y cambiante.

Con el fin de lograr la agilidad empresarial y al mismo tiempo respaldar de manera confiable su operación actual, el Canal de Panamá está explorando el mercado para evaluar soluciones de gestión de auditorías y riesgos que apoyen al proceso de inspecciones de seguridad e higiene industrial que ejecuta el área de seguridad ocupacional del Canal de Panamá.

La iniciativa se enfoca en los siguientes objetivos:

- Facilitar la administración y cobertura completa de las inspecciones de seguridad e higiene industrial equipos/edificios de la ACP.
- Movilidad y conectividad para el registro de las inspecciones desde el campo.
- Visibilidad de los resultados de las inspecciones y hallazgos a los responsables de las áreas según su nivel de jerarquía.
- Participación de los especialistas y responsables de las áreas en el seguimiento de los hallazgos y las acciones correctivas.

B. CONFIDENCIALIDAD

Todos los datos, información escrita/verbal/audiovisual u otra, y análisis e informes que el Contratista confeccione y entregue a la ACP, o que la ACP entregue al Contratista, constituyen propiedad exclusiva de la ACP, serán confidenciales y no podrán ser divulgados o de alguna forma utilizados por el Contratista para otros asuntos diferentes a la ejecución de este estudio de mercado. El Contratista no podrá comercializar o disponer, a ningún título, de estos datos, información, análisis, ni informes, sin la autorización previa y por escrito de la ACP.

.

C. OBJETIVOS DEL ESTUDIO DE MERCADO

La Autoridad del Canal de Panamá desea recopilar información referente a las ofertas disponibles en el mercado de soluciones de gestión de auditorías y riesgos que apoyen al proceso de inspecciones de seguridad e higiene industrial que ejecuta el área de seguridad ocupacional del Canal de Panamá.

La exploración de posibles soluciones está basada en las siguientes premisas:

1. Servicio de aplicación tipo Software as a Service (SaaS) basado en las mejoras prácticas y estándares de auditorías, inspecciones y riesgos de Seguridad e Higiene Industrial
2. Cumplimiento de forma nativa con los requerimientos funcionales, sin la necesidad de esfuerzos adicionales por parte del fabricante o proveedor, para la adaptación o customización. Adicionalmente, que los requerimientos funcionales puedan ser ejecutados por un usuario administrador funcional.
3. Conocer la habilidad y experiencia de potenciales proveedores en el mercado en cuanto a su experiencia, conocimiento, certificaciones y alianzas.

D. REQUISITOS MÍNIMOS

A continuación, se presentan la tabla de requisitos mínimos a suministrar por el proponente:

Categoría	Requerimiento	Cumple/No Cumple	Comentarios
Requerimientos funcionales	Plantillas de inspecciones predefinidas derivadas de estándar internacional con opción para adecuarlas a las necesidades del usuario.		
	Crear nuevas plantillas de todo tipo de inspección/observación, configurar todo tipo de campo de respuestas.		
	Permitir crear plantillas desde formularios electrónicos existentes.		
	Manejo de tablas de referencia que permitan que, ante la escogencia del valor de un campo, otro campo traiga por defecto un valor asociado.		
	Mantenimiento de tablas de referencia (estarán relacionados a normas, hallazgos y sus atributos de riesgo correspondientes).		
	Mantenimiento de valores tipo catálogo / listas /opciones.		
	Manejar varios tipos de objetos de inspección (edificios/equipos) a los cuales se les asocian los hallazgos.		

	Contar con aplicación móvil, desde la cuál, por medio de dispositivos móviles tipo "*touch*", se pueda realizar el registro en campo de todos los siguientes elementos: 1. las inspecciones 2. las acciones correctivas que debe tomarse 3. seguimiento y cierre de las acciones correctivas.		
	Permitir registrar "*offline*", en la aplicación móvil, resultados de inspecciones y contar con la opción de sincronizar la información posteriormente cuando haya disponibilidad de red.		
	Guardar las inspecciones sin completar y retomarlas en otro momento.		
	Permitir la gestión de seguimiento y/o cierre de las acciones correctivas. La gestión incluye: 1. poder registrar comentarios de seguimiento 2. visibilidad de acciones que han vencido o sobrepasado el periodo de tiempo que se disponía para ser corregidas 3. cierre de las acciones que puede incluir fotos como evidencia de la corrección.		
	Permitir incluir documentos y archivos multimedia durante las inspecciones o en la corrección de los hallazgos. Permitir que se puedan añadir múltiples archivos multimedia por hallazgo o elemento del "*checklist*".		
	Generar informes de resultado de inspección, que NO incluyan los elementos que no fueron verificados en la inspección (es decir, los campos que fueron dejados en blanco).		
	Contar con la opción de compartir informes resultados de inspecciones por medio de correo electrónico.		
	Permitir que las áreas responsables de ejecutar las acciones correctivas identificadas en las inspecciones puedan dar "*feedback*" de las correcciones sin cerrar la acción correctiva, porque el cierre es responsabilidad del inspector.		
	Permitir hacer búsquedas de letras o palabras a nivel global dentro de una plantilla de inspección, las coincidencias de la búsqueda deben poder darse incluso hasta el nivel de cada elemento del "*checklist*" de la plantilla.		
	Manejar estados de acciones correctivas.		

	Visibilidad de los resultados de las inspecciones y acciones correctivas a las áreas responsables.		
	En la pantalla de consulta de las inspecciones realizadas, permitir: 1. agregar atributos en el despliegue de los datos de las inspecciones 2. criterios de búsqueda/filtrado que incluyan campos creados/incluidos en la plantilla de inspección realizada por el por el usuario funcional administrador.		
	En la pantalla de consulta/resumen de las acciones correctivas creadas, permitir: 1. agregar atributos en el despliegue de los datos de las acciones 2. criterios de búsqueda/filtrado que incluyan campos creados/incluidos en la plantilla de inspección realizada por el por el usuario funcional administrador.		
	Que cada usuario inspector pueda tener visibilidad de la cobertura de áreas de responsabilidad que ha cubierto en un periodo de tiempo y cuánto le hace falta por cubrir		
	Permitir programar inspecciones para fechas específicas, periodos de frecuencia (diario, semanal, mensual, anual) o personalizado.		
	Permitir firma de responsable a través del dispositivo móvil.		
	Contar con gráficas sencillas de estadísticas para facilitar visualmente seguimiento de pendientes.		
	Gestionar periodo de vencimientos de inspecciones (considerando la fecha de la última inspección que se realiza y el parámetro de vigencia) La herramienta debe permitir que el parámetro de vigencia de la inspección se pueda modificar a nivel del administrador funcional de la solución.		
	Configuración de notificaciones a nivel de administrador funcional.		
	Gestión de grupos, roles y permisos a nivel de administrador funcional.		
	Mostrar historial de respuestas en inspecciones previas, relacionadas a los elementos del "*checklist*" para el objeto inspeccionado. Que visualmente, mientras se realiza una inspección a un objeto (edificio/equipo), permita identificar en cuales elementos del "*checklist*" de inspección hubo algún hallazgo en alguna inspección previa.		

	Permitir acceder a informes de inspecciones previas desde: 1. una acción correctiva 2. un historial de no cumplimientos		
	La aplicación puede ser utilizada sin la necesidad de esfuerzos adicionales por parte del fabricante o proveedor, para la adaptación o customización.		
Integración	Lista de valores que puedan ser cargadas de archivos CSV.		
	API o integración con servicios web para actualizar listas de valores o datos de inspecciones.		
	API que permita extracción de datos de inspecciones, incluyendo las imágenes asociadas a las inspecciones.		
	Invocación de servicios web para el envío de información hacia sistemas externos.		
Seguridad	**Cifrado de datos** 1. La información en tránsito debe estar cifrada en todo momento utilizando protocolos seguros y aceptados en la transmisión de datos. Por ejemplo: TLS 1.2, certificados SHA256. 2. La información en reposo también debe estar cifrada.		
	Cumplimiento estricto de controles de seguridad informática - Se requiere que el Centro de Datos de la solución ofrecida cumpla con la certificación ANSI/TIA 942 Rating 3 o mejor; o en su defecto el proveedor brinde evidencia de su resiliencia operativa contra ataques cibernéticos, tomando en cuenta factores como disponibilidad, escalabilidad, seguridad, manejabilidad y desempeño tal como lo indican otras normas y estándares de seguridad de Centro de Datos. - El proponente debe cumplir con SOC 2 Type 2 o en su lugar, se requiere que el proveedor de servicios en la nube garantice que cuenta con procesos formales de seguridad y audito; que cuenta con sistemas y controles que mitigan el riesgo cibernético para protección de los datos del cliente (disponibilidad, confidencialidad, integridad). -Se requiere que proveedor cumpla con Cloud Security Management System START certification GOLD LEVEL o con el estándar ISO 27001.		
	Auditorías Los informes de auditoría o las cartas de los auditores externos deben estar a disposición de la		

	ACP bajo demanda (on demand). El proveedor debe ser capaz de demostrar que es auditado anualmente.		
	Portabilidad El proveedor debe proporcionar las facilidades/garantías de que la data e información de la ACP pueda ser exportada/descargada en casos de finalización de contrato/migración a otro proveedor/fin de vida del proveedor o producto.		
	Manejo de Identidad El proveedor de nube debe ser capaz de utilizar, a través de federación, las identidades de los usuarios de ACP, que residen en el Directorio Activo (AD) de la organización. El proveedor de servicio deberá ofrecer la capacidad de utilizar múltiples factores de autenticación (MFA) o doble factor de autenticación (2FA) para los usuarios de la plataforma.		
	Control de acceso El servicio de nube debe poder proveer niveles de acceso granulares con roles/responsabilidades documentadas y debe permitir la creación de roles personalizadas (RBAC).		
	Bitácoras El proveedor de servicio de nube debe generar y proveer las bitácoras de actividad detalladas con los requisitos que solicite la ACP para el control de acceso a aplicaciones (SaaS) o infraestructura (IaaS o PaaS). Dichas bitácoras deberán poder integrarse con el sistema de gestión de incidentes (SIEM) de la ACP y deberán estar disponibles en formato SPLUNK o similar (universal). Las bitácoras podrán ser solicitadas en cualquier momento por la ACP y deben estar disponibles y almacenadas, mínimo, por un año.		
	Funcionalidad de legal hold sobre documentos El proveedor del servicio deberá contar con la opción de la funcionalidad de retención legal (legal hold) sobre documentos y/o archivos. En caso contrario, deberá enviar justificación a la ACP para su evaluación y aprobación.		
	Actualizaciones de seguridad (parchado) de sistemas El proveedor del servicio en la nube deberá realizar las actualizaciones de seguridad, de todos los parches disponibles y versiones más recientes en todos los componentes relacionados con servicios brindados en modalidad SaaS (Software como Servicio) o PaaS (Plataforma como Servicio),		

	tanto a nivel de hardware como de software que se requieran. En caso de IaaS, el proveedor del servicio de nube deberá proveer los mecanismos para que la ACP realice las actualizaciones de todos los componentes de la infraestructura, tales como firmware, sistemas operativos utilizados en modalidad IaaS (Infraestructura como Servicio). El proveedor del servicio en la nube deberá brindar información acerca del manejo de vulnerabilidades, especialmente si afectan el servicio.		
	Protección contra código malicioso (antimalware) La plataforma debe contar con una solución antimalware reconocida que ejecute rastreos en tiempo real, de todos los archivos entrantes y salientes, actualización automática de firmas, capacidad de detección de código malicioso no basado en firmas (heurística, machine learning) y debe ser capaz de alertar seguridad que impacte el sistema utilizado por ACP en un tiempo no mayor a 24 horas de la detección. Deberá indicar punto de contacto en caso de incidentes de ciberseguridad. sobre detecciones de código malicioso. Excepción: En caso de que el proveedor no cuente con soluciones antimalware, deben informar y enviar documentación técnica de los mecanismos que utilizan para proveer un aseguramiento similar a la solución antimalware.		
	Respuesta a incidentes de seguridad El proveedor del servicio debe contar con un proceso de gestión de incidentes de ciberseguridad y equipo de Respuesta a Incidentes de Seguridad y notificar a la ACP sobre cualquier incidente de seguridad que impacte el sistema utilizado por ACP en un tiempo no mayor a 24 horas de la detección. Deberá indicar punto de contacto en caso de incidentes de ciberseguridad.		
	Respaldos Para los servicios tipo SaaS, el proveedor del servicio en la nube deberá contar con capacidad de respaldo para ejecutar actividades de recuperación de desastre. El tiempo de retención de los respaldos deberá ser mínimo un año. El proveedor deberá entregar documentación sobre la metodología de respaldo utilizada. El proveedor de servicios en la nube deberá proveer los		

	registros que la ACP le solicite que evidencie que los respaldos se están ejecutando y funciona. Para los casos de IaaS, el proveedor de servicio de nube deberá proveer la capacidad de configurar dichos servicios, por parte de la ACP. El proveedor del servicio de la nube deberá indicar la ubicación de sus sitios de respaldo y los acuerdos de confidencialidad que mantiene con el subcontratista en caso de ser un tercero. El proveedor de servicio que tercerice deberá indicar a la ACP toda la información correspondiente a ese tercero.		
	Recuperación de desastres El proveedor de servicio deberá contar con planes de recuperación de desastre; también se requiere que pueda demostrar el cumplimiento con dichos planes de recuperación de desastres mediante certificaciones de terceros (auditorias) que incluyan pruebas de estos planes. Estos planes deben incluir sitio de recuperación o sitio alterno, tiempo de recuperación según las necesidades de la ACP, punto de contacto por parte del proveedor del servicio.		
	Redundancia El proveedor de servicios en la nube deberá proporcionar información sobre sitios de redundancias y locación de los Centros de Datos.		
	Política de privacidad El proveedor de servicio deberá contar con una política de privacidad de datos del cliente, donde ser describa los siguientes puntos: • Uso de datos personales • Uso de sub-procesadores (terceros) • Descripción de autoridades regulatorias y metodología de revelación de información cuando sea requerida por entes reguladores • Descripción del método de resolución de disputas • Acuerdos de Confidencialidad con la ACP y con terceros • Acuerdos de Confidencialidad con sus colaboradores que participan en el proceso		
	Pruebas de Intrusión El proveedor de servicio deberá realizar pruebas de intrusión sobre su propia infraestructura de manera periódica mínimo 2 veces al año; y deberá demostrar la ejecución de estas mediante informes técnicos y/o certificaciones realizadas		

	por terceros independientes (que no tenga relación con el proveedor).		
	Sobre terminación de la suscripción (Exit) En caso de terminación de la suscripción, no debe haber ningún costo adicional asociado con el proceso de salida. El proveedor del servicio de nube debe ser responsable de eliminar los datos de propiedad de la ACP de todos los dispositivos, y en caso de ser necesario apoyar a la ACP en la extracción y borrado de los datos proporcionando una documentación clara y concisa. Los datos e información pertenecientes a la ACP se deben mantener en acuerdo a los requerimientos funcionales especificados y luego deben ser eliminados por completo. Esto debe brindar a la ACP, tiempo suficiente para encontrar un nuevo proveedor y continuar recibiendo el servicio del proveedor actual de forma provisional durante la transición. La documentación pertinente a este tema debe establecerse en un anexo legal.		
	Sitio de almacenamiento de la información Con el propósito que la información esté protegida y resguardada, se requiere que el posible proveedor indique el país y sitio en donde se almacena y se replica la data en producción en caso se activen sus planes de recuperación.		
	Código seguro En caso de servicios SaaS, el proveedor del servicio de nube deberá contar con certificación de código seguro de su servicio como OWASP.		
Auditoría	El sistema debe generar entradas/registros de auditoría para las operaciones realizadas por el administrador del sistema u operadores en la aplicación, sin importar si acciones de varios administradores se solapan ("*overlap*"). Esto incluye acciones de administración de cuentas de usuarios, leer los datos de algún usuario y habilitar o deshabilitar la función de auditoría.		
Licenciamiento	Las licencias de la herramienta deberán ser otorgadas por concurrencia, por usuario o por roles.		
Capacitación	Proveer entrenamiento basado en web /e-learning para ser consultado cada vez que sea requerido por los usuarios		
	Proveer técnicos certificados con disponibilidad para ser contactados vía email, videollamadas, teléfono.		

Soporte Técnico	El proveedor deberá brindar soporte con garantía mientras dure el contrato.		
	Los técnicos certificados deberán brindar un tiempo de respuesta ante los problemas del producto, en un periodo no mayor a 8 horas.		
	El proveedor deberá contar con un plan anual de mantenimiento correctivo del software.		
	El proveedor debe contar con un plan anual de mantenimientos y actualizaciones de la solución.		
	El proveedor del servicio debe contar con un proceso de gestión de incidentes de ciberseguridad y equipo de Respuesta a Incidentes de Seguridad y notificar a la ACP sobre cualquier incidente de seguridad que impacte el sistema utilizado por ACP en un tiempo no mayor a 24 horas de la detección. Deberá indicar punto de contacto en caso de incidentes de ciberseguridad.		

E. ENTREGABLES DEL RFI

Se deberá entregar para aprobación de la ACP, la siguiente información:

Entregables
1. Precio de referencia de licenciamiento por un (1) año para 25 usuarios
2. Término y condiciones de su servicio
3. Tabla de Requisitos Mínimos completada; Sección E., punto #1
4. Disposición del proveedor de participar en Licitaciones Públicas de la ACP
5. Tiempo de presencia en el mercado, ubicación de sus oficinas principales y regionales, si es proveedor directo o un tercero.
6. Referencias de clientes y puntos de contacto, número de empleados de cada uno y proyectos ejecutados
7. Potenciales servicios complementarios ofrecidos por el proponente

Se deberá entregar en formato electrónico su respuesta y cualquier otra información generada durante la realización del estudio que ACP solicite explícitamente. Todos los documentos deben ser preparados y entregados en formato PDF. Toda la comunicación (reuniones, entrevistas, talleres e informes) deberá ser en los idiomas español y/o inglés.

F. INSTRUCCIONES A LOS PROPONENTES

Esta es una Solicitud de información (RFI), no una orden. No se puede cargar ningún costo a la ACP por ningún motivo.

Este documento no se interpretará como una solicitud o autorización para realizar un trabajo por cuenta de la ACP. Cualquier trabajo realizado por un proveedor será a su propia discreción y gasto. Este RFI no representa un compromiso de compra o arrendamiento. La presentación de una respuesta constituye el reconocimiento de que el proveedor ha leído y acepta estar sujeto a dichos términos.

La ACP tiene la intención de presentar una Solicitud de Propuesta (RFP) formal para los servicios descritos en este documento antes del final de 30-diciembre-2021. No hay garantía de que la ACP presente una RFP o, si se envía una RFP, que ocurrirá en el marco de tiempo descrito en esta RFI. Si se envía, la RFP lo publicará a través de los mecanismos oficiales de la Oficina de Contratos a través de una licitación pública y los proponentes deberán cumplir con todos los requisitos para que sus respectivas propuestas sean aceptadas y evaluadas. La información contenida en este RFI es precisa según el mejor conocimiento del autor, pero no se garantiza que sea correcta.

1. Punto de contacto
    a. Nombre: Lorena Rebollo
    b. Dirección:
        i. Canal de Panamá
        ii. Vicepresidencia de Transformación Digital
        iii. División de Digitalización de Procesos
    c. Email: lirebollo@pancanal.com
2. Presentación de Respuesta

    La fecha para recibir una respuesta fue establecida para el 10-noviembre-2021. **Sin embargo, se ha considerado una extensión hasta el 19-noviembre-2021. No se garantizan más extensiones a esta fecha.**

    Las respuestas deben enviarse completas y por escrito. Todas las solicitudes de información en todas las secciones de este documento deben responderse de la manera más concisa posible y, al mismo tiempo, proporcionar toda la información necesaria para comprender el proceso de subcontratación propuesto. Cualquier desviación de los requisitos, o requisitos que el proveedor no pueda satisfacer, debe identificarse claramente.

    Se considera que, al enviar la respuesta a este RFI, el proponente comprende los requisitos de la RFI y acepta los términos y condiciones bajo los cuales se emitió el RFI.

    Cualquier información de naturaleza confidencial o patentada contenida en la respuesta de un proveedor debe estar claramente marcada como "PROPIEDAD" o "CONFIDENCIAL" por elemento o en la parte superior de cada página. Se tomarán precauciones razonables

para salvaguardar cualquier parte de la respuesta identificada por un proveedor como confidencial o patentada.

Todas las respuestas, una vez entregadas, pasan a ser propiedad de la ACP.

De forma opcional, los interesados pueden coordinar una demostración con el Canal de Panamá durante el periodo de solicitud de información.

Fin del documento.