CANAL DE PANAMÁ

ESTUDIO DE MERCADO PARA

SOLUCIÓN DE MONITOREO, OBSERVABILIDAD Y AIOPS

TABLA DE CONTENIDO

1. INFORMACIÓN GENERAL

El Centro de Monitoreo es responsable de la gestión de eventos de todos los servicios tecnológicos ofrecidos por la Vicepresidencia de Transformación Digital requeridos para la operación del Canal; incluyendo la infraestructura informática, aplicaciones, sistemas de telecomunicaciones y sistemas de electrónica. Centraliza el monitoreo para asegurar que se mantienen los niveles de servicio acordados y para la detección temprana de situaciones técnicas adversas y estados de operación anormales, con el fin de ayudar a mantener la operación correcta, eficiente e ininterrumpida de los servicios.

2. CONFIDENCIALIDAD

Todos los datos, información escrita/verbal/audiovisual u otra, y análisis e informes que el proponente confeccione y entregue a la ACP, o que la ACP entregue al proponente, constituyen propiedad exclusiva de la ACP, serán confidenciales y no podrán ser divulgados o de alguna forma utilizados por el proponente para otros asuntos diferentes a la ejecución de este estudio de mercado. El proponente 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.

3. ALCANCE Y OBJETIVOS

El propósito de este documento es realizar un Estudio de Mercado para recibir de las partes interesadas una propuesta de su solución y un precio de referencia. Esta propuesta debe cumplir con los requerimientos de una solución de observabilidad tipo “full-stack” para los sistemas y aplicaciones del Canal de Panamá, con funciones analíticas avanzadas, también conocido como “AIOps”, que permitan detectar condiciones anómalas de forma automática, con poca o sin intervención humana, ayude a identificar sus causas raíz y acciones de remediación.

Los objetivos son:

1. **Adquirir a través de una suscripción la Solución de Monitoreo, Observabilidad y AIOPS en un modelo de servicio SaaS (Software as a Service).**
2. **Contratar cien (100) horas de ”On-Boarding” y acompañamiento en la configuración y parametrización de la solución para monitorear los servicios, aplicaciones y dispositivos de acuerdo con las funcionalidades y requerimientos descritos en los puntos 5 y 6 de este documento. De las cien (100) horas contratadas se deben reservar veinticuatro (24) para realizar talleres de transferencia de conocimiento en el uso y aplicación de las herramientas de la solución.**
3. **Soporte y mantenimiento de la solución por doce (12) meses, extensibles mientras tengamos acceso a la solución.**

4. DEFINICIONES

- **AIOps (Artificial Intelligence for IT Operations):** término propuesto por Gartner que se refiere al uso de “big data” y apendizaje de máquina para automatizar procesos operacionales de IT, incluyendo correlación, detección de anomalías y determinación de causa raíz.

- **Alerta:** es el mecanismo de escalamiento, su propósito es asegurar que las personas con las habilidades apropiadas para enfrentar un evento sean notificadas.
- **Disponibilidad:** es el porcentaje del tiempo en que un sistema o servicio está brindando el servicio acordado con los clientes. La disponibilidad típicamente es una de las mediciones incluidas en los acuerdos de nivel de servicio, por lo que su medición es sumamente importante.
- **Monitoreo de la experiencia digital (DEM)**: técnicas de monitoreo que permiten medir el desempeño de una aplicación desde la perspectiva del usuario final.
- **Evento:** es cualquier suceso que representa algún tipo de cambio o condición fuera de lo normal que se pueda detectar en un componente de un sistema o aplicación y que potencialmente tenga relevancia en la entrega del servicio al usuario final.
- **Elemento de configuración (Configuration item o CI):** cualquier elemento ya sea de hardware, software o componente lógico que debe ser gestionado con el fin de entregar un servicio o aplicación. Entre los elementos de configuración se cuentan aplicaciones, servidores, conmutadores de red, balanceadores de carga, cuentas de aplicación, enlaces de Internet y sistemas de archivos.
- **Fabricante:** compañía que diseña y mantiene el producto o servicio que se desea adquirir.
- **Gestión de eventos:** El proceso de gestionar los eventos a lo largo de su ciclo de vida, desde que son detectados e interpretados, hasta la determinación de las acciones de control apropiadas.
- **Métricos:** son valores numéricos que representan mediciones específicas y que contienen información contextual para determinar su origen, fecha y hora de recolección, y relaciones con otros datos recolectados durante el monitoreo de un sistema de información.
- **Monitoreo:** para el propósito de este documento, es la recolección contínua de telemetría relevante a un componente de un sistema.
- **Proveedor:** distribuidor autorizado, revendedor, partner o equivalente que representa a un "fabricante" para la venta del producto o servicio en la República de Panamá. Será el responsable de cumplir a cabalidad con el contrato.
- **Observabilidad:** es la disciplina de recolectar simultáneamente y analizar en tiempo real múltiples fuentes de telemetría para un mismo sistema o aplicación, típicamente se abarca la recolección de por lo menos cuatro fuentes de datos, agrupados bajo el acrónimo "MELT", que significa métricos, eventos, bitácoras (logs) y trazas.
- **Observabilidad tipo "Full-stack":** se refiere a la habilidad de entender en cualquier momento lo que sucede a través de todas las capas o "technology stack" de un sistema informático complejo, que puede estar distribuido a través de múltiples servidores, contenedores, microservicios, aplicaciones desarrolladas en diversas tecnologías y servicios de nubes públicas.
- **Traza:** objeto que representan la travesía de una solicitud, transacción o acción de un usuario a través de los componentes de una aplicación o sistema. Recolecta información de rendimiento y errores de cada paso, junto con su relación con la secuencia de pasos que le precedieron y los que le siguieron, en la cadena de respuesta a la solicitud.
- **Umbral:** es una regla que se aplica a un métrico de monitoreo con el fin de generar eventos o alertas.

5. REQUERIMIENTOS EN BASE A LA ARQUITECTURA DE LOS SISTEMAS DEL CANAL DE PANAMÁ

5.1 Requerimientos funcionales

En esta sección se detallan los requerimientos funcionales del servicio o producto, de ahora en adelante denominada la "solución".

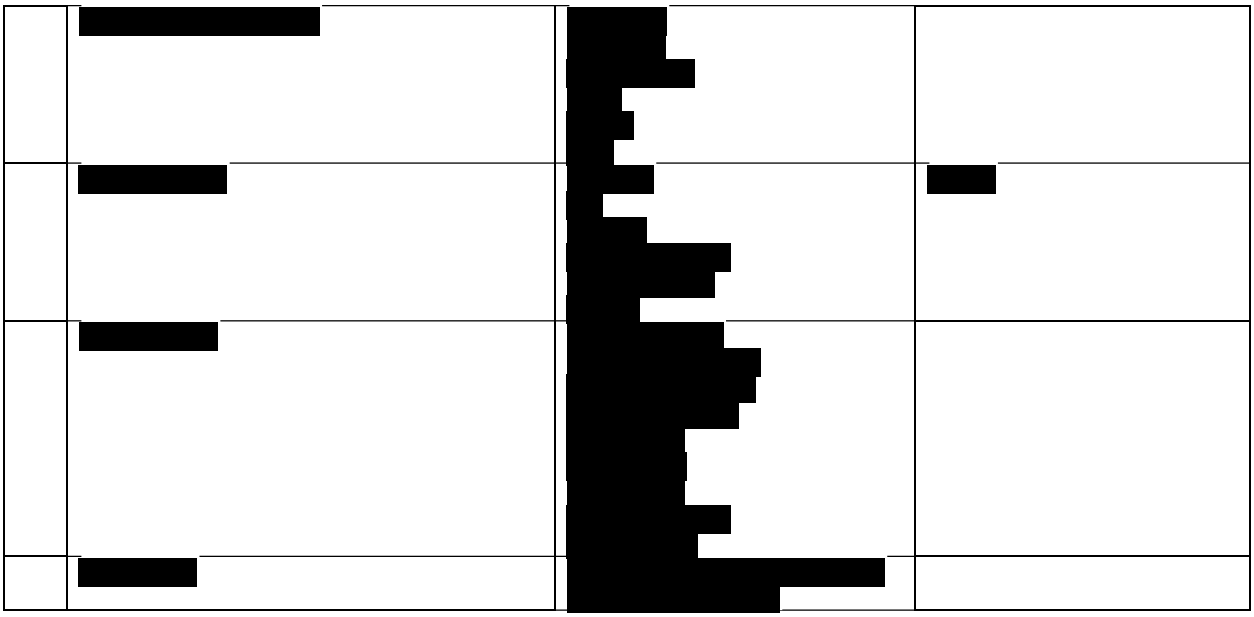
5.1.1 Recolección de métricos y bitácoras

Métricos y bitácoras son dos fuentes claves para comprender el comportamiento de sistemas informáticos.

La solución deberá proveer mecanismos, bajo soporte y mantenimiento del fabricante, que permitan interrogar y recolectar tanto métricos como bitácoras (logs) de forma continua, y para descubrir automáticamente nuevos objetos (p.ej., cuando se añada un nuevo disco lógico a un servidor monitoreado, o cuando se añada un nuevo manejado de WebLogic en un servidor monitoreado), en por lo menos las siguientes tecnologías en uso en el Canal de Panamá. Ver Tabla 1.

Tabla 1: Recolección de Métricos y Bitácoras

No.	TECNOLOGÍA	FAMILIAS DE MÉTRICOS	TIPOS DE BITÁCORAS
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	



La solución deberá permitir la configuración manual de umbrales para generación de alertas en todos los métricos recolectados.

La solución deberá tener sus propios mecanismos de extracción, categorización, valoración de criticidad y análisis para una amplia gama de tipos de bitácoras generadas por productos comúnmente usados en sistemas informáticos, incluyendo los listados en la Tabla 1: Recolección de Métricos y Bitácoras. También deberá contar con mecanismos que permitan al Canal de Panamá añadir bitácoras con formatos propios y para configurar reglas de extracción que permitan la captura de información relevante.

[redacted]

5.1.2 Monitoreo de rendimiento de aplicaciones (APM) y captura de trazas transaccionales (distributed tracing)

Monitoreo de rendimiento de aplicaciones (APM) son mecanismos de monitoreo que se integran con las aplicaciones, para permitir detectar y diagnosticar problemas de rendimiento y para asegurar que cumplen con las expectativas de rendimiento acordadas con los clientes. Típicamente incluye descubrimiento y generación automáticos de mapas de la aplicación y de sus componentes.

Seguimiento de trazas, conocido como “distributed tracing”, es la habilidad de recolectar información de rendimiento de cada componente o paso que atraviesa una solicitud de usuarios a través de una aplicación o sistema. Para cada aplicación se capturan una serie de trazas de ejecución, enlazadas y correlacionadas, que incluye información de latencia, errores y contextual que ayuda a determinar los cuellos de botella, latencias, errores y otras situaciones que afectan las transacciones de usuario.

La solución deberá incluir tanto mecanismos de APM, como de “distributed tracing”, para recolectar, visualizar y analizar el rendimiento de las aplicaciones, y deberá recolectar trazas de las transacciones de

usuario, con el fin de medir el rendimiento de: los servidores de aplicación, los “queries” a las bases de datos, microservicios, Web Services, servicios de cola de mensajería, servicos en la nube y otros componentes que participen en dar respuesta a la solicitud del usuario.

La solución deberá tener capacidad de recolectar 100% de las trazas de un sistema o aplicación y de mostrar cada paso atravesado por cada solicitud, incluyendo en componentes en premisa y en nubes, tales como servicios provistos por Microsoft Azure.

5.1.2.1 Auto - instrumentación

Instrumentación son los mecanismos a través de los cual se añaden la generación y captura de telemetría, es decir, métricos, bitácoras y de trazas, a una aplicación desarrollada con una tecnología específica.

La solución debe proveer mecanismos con soporte y mantenimiento del fabricante para instrumentar de forma automática (también conocido como “auto instrumentación”), es decir sin requerir modificaciones al código fuente de la aplicación o de requerir recompilarla, de por lo menos aplicaciones desarrolladas en los siguientes lenguajes y ejecutándose en los siguientes servidores de aplicación, para la captura de trazas transaccionales:

5.1.2.2 Instrumentación manual

La solución deberá permitir la instrumentación manual de aplicaciones utilizando por lo menos las herramienta, APIs, librerías y SDKs desarrollados para tal fin por OpenTelemetry (https://opentelemetry.io/).

La solución deberá poder recibir métricos, trazas y bitácoras en formato de OpenTelemetry e incorporarlas como parte del monitoreo, de manera similar a como lo haría con los recolectados con sus mecanismo propios.

5.1.2.3 Funciones de “Deep dive”, profiling, “code-level tracing”, o “stack tracing”

La solución deberá permitir identificar y visualizar el método o función dentro del código de una aplicación que contribuye a los problemas de rendimiento o errores identificados. El objetivo es proveer visibilidad a los desarrolladores de los elementos puntuales dentro del código que debieran analizar, porque están asociados a condiciones anómalas identificadas a través del monitoreo.

5.1.3 Monitoreo de la experiencia digital (DEM)

La solución deberá medir la experiencia del usuario final de aplicaciones para entornos web y aplicaciones para dispositivos móviles, tanto para aplicaciones publicadas al exterior de la red del Canal

de Panamá, como para aplicaciones que únicamente se pueden consumir estando dentro de la red de datos del Canal de Panamá.

La solución deberá permitir la identificación y recopilación de todas las acciones realizadas por el usuario en la página de la aplicación, como clics y llenado de campos de información, incluso si estas acciones no llaman a los servidores de la aplicación. Deberá permitir su análisis en el contexto del resto de la información recopilada por los otros mecanismos de monitoreo provistos por la solución, de forma que se puedan determinar las causas raíz de problemas de rendimiento y errores reportadas por los usuarios, en base a la visión global de la aplicación provista por todos los métodos de monitoreo y observabilidad que son parte de la solución.

Se deberá poder medir el rendimiento de las acciones del usuario. Para cada solicitud web, la satisfacción del usuario según el estándar APDEX o equivalente. Deberá mostrar los tiempos de carga de la página y los errores.

5.1.4 Monitoreo sintético

La solución deberá incluir un mecanismo para grabar y ejecutar regularmente transacciones sintéticas, es decir, realizadas por un robot de software sobre una aplicación real que simule las acciones que un usuario final haría sobre la aplicación.

Se deberá poder ejecutar transacciones sintéticas desde diversas redes externa e internas al Canal de Panamá, inclusive en aplicaciones que únicamente se pueden consumir estando dentro de la red de datos del Canal de Panamá.

5.1.5 Recepción y análisis de eventos

La solución deberá poder ingerir y analizar eventos recibidos de terceros; estos típicamente son alertas generadas por otros sistemas de monitoreo o por los mismos componentes de una aplicación o sistema, tales como servidores, equipos de red y bases de datos

La solución deberá proveer un API o mecanismo similar, incluyendo el correo electrónico (email), para la recepción de eventos significativos relacionados a los sistemas o aplicaciones monitoreadas.

5.1.6 Autodescubrimiento de elementos de un sistema y sus interrelaciones

La solución deberá incluir mecanismos automatizados para descubrir dinámicamente y mantener actualizado el inventario de componentes y sus interrelaciones, tanto de software como de infraestructura, que conforman el sistema o aplicación monitoreado. La intención es poblar continuamente la información topológica que se utiliza junto con los métricos, bitácoras, trazas, APM, experiencia de usuario y demás para predecir e identificar condiciones anormales, problemas de rendimiento o cualquiera otra condición adversa.

5.1.7 Creación flexible de “dashboards” (consolas de visualización)

La solución deberá permitir la creación y personalización de paneles, gráficos o mapas de visualización, con la posibilidad de seleccionar la inclusión o eliminación de información proporcionada por los

elementos de observabilidad de la solución. Cada usuario o grupos de usuarios deberán tener la flexibilidad de crear y administrar sus propios “dashboards”.

5.1.8 Mapas de servicio

La solución deberá generar y desplegar automáticamente mapas de servicio o aplicación, actualizados dinámicamente, que muestren los componentes que participan en la entrega al usuario final.

Los mapas deberán mostrar el análisis de desempeño de la aplicación, identificando los servicios e infraestructura utilizados por la misma, así como información sobre los accesos de origen de las transacciones, como navegador y vista geográfica de los accesos.

Los mapas podrán mostrar el volumen de ejecuciones y tiempos promedio de respuesta entre todos los componentes de la aplicación, de acuerdo con la escala y período de tiempo indicado.

5.1.9 Funciones analíticas y AIOps

La solución deberá utilizar mecanismos analíticos automáticos, apoyados con aprendizaje de máquina (AI/ML) y “big data”, para que sin intervención humana pueda correlacionar y fusionar todos los datos recolectados de un sistema o aplicación (métricos, bitácoras, trazas, APM, etc.), y aprender el comportamiento “normal” de la misma, para dar una visión integral de su salud y rendimiento, con el fin de predecir, detectar y diagnosticar condiciones anómalas en base al comportamiento histórico y a los objetivos de nivel de servicio.

La solución deberá contar con funciones de reducción de ruido para filtrar automáticamente información irrelevante o de poco valor al monitoreo de un sistema.

La solución deberá incorporar mecanismos que faciliten a los operadores dentro del Canal de Panamá indagar situaciones adversas con sus sistemas, interpretar los resultados del monitoreo, detectar tendencias e investigar las causas raíz de afectaciones o problemas de rendimiento.

5.1.10 Reportes y retención de datos

La solución deberá proveer un mecanismo para generar reportes según las necesidades del Canal de Panamá, utilizando datos recolectados en por lo menos los últimos 12 meses. Se deberá poder crear reportes de disponibilidad de los servicios o aplicaciones cubiertas con la solución.

La solución deberá proveer mecanismos propios para calcular objetivos de nivel de servicio (Service Level Objectives) por cada uno de los sistemas, aplicaciones o servicios del Canal de Panamá monitoreados con la solución.

5.1.11 Generación de alertas

La solución deberá permitir la creación de alertas para cualquier métrica individual o grupos de métricas configuradas en la solución. Se deberá poder emitir alertas a través de correo electrónico, webhooks, o a través de integraciones con otros servicios (ver Integraciones en el punto 5.1.12).

La solución deberá contar con un mecanismo de de-duplicación, consolidación o reducción inteligente de alertas.

5.1.12 Integraciones

La solución deberá permitir la integración con servicios externos, para:

- Notificación de alertas, incluyendo con [redacted]
- Generación de tiquetes de incidentes en servicios de Mesa de Servicio, tales como [redacted]
- Autenticación de los usuarios y asignación de grupos. La solución deberá permitir el uso de [redacted]
- Recolección de métricos, eventos, trazas y bitácoras de servicios de nube, incluyendo [redacted]

5.1.13 Configuración de horarios de mantenimiento

La solución deberá permitir la configuración de ventanas de mantenimiento, tanto recurrentes como en una hora y fecha específica, en las que no se debe alertar o recolectar información que pudiera modificar erróneamente los datos y tendencias.

5.1.14 Usuarios y roles

La solución deberá permitir la creación de grupos de usuarios o roles para segregar el acceso a la información recolectada. Por lo menos deberán existir grupos de: administradores de solución, con acceso total, incluyendo a funciones de configuración; operadores, con acceso a los datos recolectados y a tomar ciertas acciones no administrativas; usuarios de consulta, con acceso a la información del monitoreo de ciertos componentes o sistemas.

5.2 Requerimientos no funcionales

Deberá cumplir con estándares tales como el “Federal Risk and Authorization Management Program” (FedRAMP) de los Estados Unidos y el “General Data Protection Regulation” (GDPR) de la Unión Europea.

5.3 Requerimientos de la empresa y su personal técnico

5.3.1 Años de operación

La empresa debe tener por lo menos cinco (5) años operando.

5.3.2 Distribuidor Autorizado

La empresa debe ser un distribuidor autorizado del software y herramientas que forman parte de la solución.

5.3.3 Clientes

La empresa debe tener por lo menos dos (2) clientes en donde se haya implementado su Solución de Monitoreo, Observabilidad y AIOPS.

5.3.4 Personal Técnico

El personal técnico debe tener por lo menos dos (2) años de experiencia en la implementación, configuración y parametrización del software y herramientas de la Solución de Monitoreo, Observabilidad y AIOPS.

6. FUNCIONALDADES CLAVES DE LA SOLUCIÓN

La solución debe tener como mínimo las siguientes funcionalidades:

- **Automation:** The ability to onboard new applications and create useful analysis with minimal human intervention, with the extensibility to automate remediation for well-known processes.
- **Learning systems:** The AI engine is able to learn from the data being consumed by the AIOps tools and change behavior as it's exposed to more training data. Some tools are rules-based, whereas the true AI/ML systems are not. They may have some values that must be set, or information about what can be correlated, but the core engine is AI.
- **Dashboards and reports**: Dashboards are customizable, as is other reporting. Dashboards should be either shareable or exportable so users can have the same experience if that is what management expects. This is typically true for follow-the-sun models or multiple shifts of workers.
- **Data consumption:** The AIOps tool should consume inputs and correlate causation. It should be allowed either to make a change or notify humans and should grant a unique event channel in tools where the event can be managed.
- **Cross-cloud monitoring:** The ability to monitor across cloud providers using similar operational features and functions. The tool should also be able to consume feeds or pull cloud vendor APIs to get near-real-time metrics. Ideally, the tool would be able to correlate metrics from one cloud vendor to the corresponding metric from a different vendor.
- **Integration:** The AIOps tool can share data and services with other tools such as security and monitoring.
- **DevOps integration:** The AIOps tool can see the dev tool chain, including integration with traditional DevOps tooling. This includes the ability to see the outcomes of the continuous deployment process of a DevOps tool chain and correlate that with ITSM change requests validated by the CMDB.

7. METODOLOGÍA DE LA PROPUESTA

Desarrollar un plan y estrategia de abordaje a través de un Caso de Uso que permita aplicar todas las funcionalidades descritas en el punto "6. Funcinalidades claves de la solución" de este documento.

Es importante que el proponente explique lo siguiente:

1. Que los proveedores hagan separación del costo del monitoreo de infraestructura, monitoreo de base de datos y el costo de APM. Que el costo se presente por unidad (sea servidor, recursos u otro usada para la medición). El Canal de Panamá se reservaría el derecho de adquirir los componentes por separado y utilizarlos en base a demanda.

2. Que los proveedores expliquen si es posible mover el monitoreo a diferentes servidores, en base a demanda. El Canal de Panamá tiene una granja amplia de servidores y existe la posibilidad que se tenga que ir moviendo el monitoreo (infraestructura o APM) a diferentes recursos.

3. Que los proveedores expliquen, dado que se trata de servicios SaaS, como se puede limitar el costo del servicio, de forma que se tenga control de los costos.

4. Que los proveedores expliquen cómo se paga el servicio (modelo de costos).

8. CANTIDADES ESTIMADAS DE RECURSOS A MONITOREAR

8.1.1 Servidores

8.1.2 Aplicaciones

[redacted]

8.1.3 Servicios de nube

[redacted]

8.1.4 Transacciones de usuario

[redacted]

8.1.5 Bitácoras

[redacted]

8.1.6 Equipo de red

[redacted]

8.1.7 Componentes de software “legacy”

[redacted]

9. ENTREGABLES DEL RFI

Entregables
• Precio de referencia detallado de: 1. Adquirir a través de una suscripción la Solución de Monitoreo, Observabilidad y AIOPS en un modelo de servicio SaaS (Software as a Service). 2. Contratar cien (100) horas de ”On-Boarding” y acompañamiento en la configuración y parametrización de la solución para monitorear los servicios, aplicaciones y dispositivos de acuerdo con las

funcionalidades y requerimientos descritos en el punto 5 y 6 de este documento. De las cien (100) horas contratadas se deben reservar veinticuatro (24) para realizar talleres de transferencia de conocimiento en el uso y aplicación de las herramientas de la solución. 3. Soporte y mantenimiento de la solución por doce (12) meses, extensibles mientras tengamos acceso a la solución.
• Término y condiciones de su servicio y EULA (End User License Agreement). • Indicar explícitamente si existe una cláusula de "Límite de Responsabilidad del contratista, servicio o software".
• Metodología de la Propuesta (Punto 7).
• Requerimientos de la empresa. (Puntos 5.3.1 y 5.3.2)
• Lista de referencias de los clientes. (Punto 5.3.3)
• Perfiles de los consultores (seniors y asistentes) y conformación de los equipos. (Punto 5.3.4)

10. 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.

Debe enviar su propuesta al siguiente punto de contacto:

1. Punto de contacto
    a. Nombre: Diana Quintero
    b. Dirección:
        i. Autoridad del Canal
        ii. Edificio de La Administración – 101, Balboa – Ancón
        iii. Vicepresidencia de Transformación Digital
        iv. División de Digitalización de Procesos
    c. Teléfono: +507 272-1949
    d. Email: dcquintero@pancanal.com y acp-arquitectura@pancanal.com

2. Presentación de la propuesta

Si está interesado en participar de este estudio de mercado debe enviar cuanto antes la siguiente información al POC indicado arriba, (dcquintero@pancanal.com y acp-arquitectura@pancanal.com):

- Completar todos los artículos del acuerdo de confidencialidad (NDA) adjunto.
- Firmar el NDA.
- Fotocopia de cédula o pasaporte de la persona que firmó el NDA.
- Evidencia que el firmante es el representante legal o director de la empresa. Dicha evidencia puede ser el certificado de operación de la empresa emitido por una institución comercial, por ejemplo, el Ministerio de Comercio e Industrias del país en donde está registrada la empresa.

Una vez enviada y validada toda la documentación del acuerdo de confidencialidad (NDA) se le estará remitiendo el RFI completo y a partir de dicha fecha tiene 14 días calendario para enviar su propuesta.

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, si existiera. Cualquier desviación de los requisitos, o requisitos que el proveedor no pueda satisfacer, debe identificarse claramente.

Las respuestas deben incluir una declaración que indique que el proveedor comprende los requisitos de la RFI y acepta los términos y condiciones bajo los cuales se emitió la RFI al proveedor. La respuesta original debe estar firmada bajo el sello corporativo por un funcionario autorizado. El original, incluida toda la literatura complementaria, deben enviarse al punto de contacto identificado arriba (punto 10, sección #1) en formato electrónico, como por ejemplo uno o varios PDF.

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.

Este RFI sigue siendo propiedad de la ACP en todo momento y debe ser devuelta por el proveedor cuando se solicite. Los proveedores que no envíen una respuesta deben devolver inmediatamente toda la documentación impresa, gráfica y electrónica al punto de contacto.

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

Fin del Documento.

ACUERDO DE CONFIDENCIALIDAD
PARA ESTUDIO DE MERCADO

Por este medio yo _____, varón, _____, mayor de edad, con cédula/pasaporte _____, actuando en mi condición de Representante Legal de la sociedad _____, registrada bajo la identificación _____ de _____ (en adelante _____), debidamente facultado para este acto, por este medio declaro y comprometo a _____ en lo siguiente:

PRIMERO: Que por parte de la **AUTORIDAD DEL CANAL DE PANAMÁ**, entidad jurídica autónoma de Derecho Público creada mediante el Título XIV de la Constitución Política de la República de Panamá y organizada conforme a la Ley Nº19 de 11 de junio de 1997, (en adelante la **ACP**), se lleva a cabo un Estudio de Mercado para la adquisición de **Solución de Monitoreo, Observabilidad y AIOPS**. (en adelante el Estudio)

SEGUNDO: Que en virtud del Estudio, _____ tendrá acceso a "Información Confidencial" que será proporcionada por la **ACP**.

TERCERO: "Información Confidencial", tal y como se utiliza en el presente acuerdo, es toda información susceptible de ser revelada de palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, no pública proporcionada por o en nombre de la **ACP** a _____ durante el Estudio, incluyendo, sin limitación, información documental, electrónica y/o verbal que contenga aspectos de personal y/o recursos humanos, de mercado, de clientes y/o entidades bancarias con las cuales la **ACP** tenga relaciones comerciales, aspectos estratégicos, técnicos, de mercado, ambiental, operativos y jurídicos, las propuestas de ideas y la información personal al momento de la creación de los perfiles de cada empleado; y en general, toda información divulgada u obtenida a través de observación u otra percepción en cualesquiera de las instalaciones de la **ACP** que no sea pública y que, por tanto, no debe ser divulgada a terceras personas sin el consentimiento previo y por escrito de la **ACP**.

CUARTO: _____ reconoce la naturaleza confidencial de la Información antes descrita y que el hecho de que la **ACP** ponga a disposición dicha Información Confidencial a _____, no constituye un consentimiento expreso de su divulgación, ni la adquisición de derechos de propiedad intelectual, ni de licencia de uso, salvo lo estrictamente establecido en este documento. Asimismo, _____ reconoce que la Información Confidencial y todos los derechos de propiedad intelectual y otros relacionados pertenecen a la **ACP**, aun cuando se realicen sugerencias, comentarios y/o ideas por parte de trabajadores de la **ACP** durante la ejecución del Estudio.

QUINTO: _____ acepta y reconoce la naturaleza altamente confidencial de la información a la que tendrá acceso y por lo tanto se compromete a:

a. Mantener en secreto y estricta confidencialidad toda la "Información Confidencial" a que tenga acceso, ya sea en forma escrita, verbal o por cualquier otro medio por parte de la ACP.
b. Impedir el uso no autorizado o la reproducción de cualquier material que contenga "Información Confidencial".
c. Prohibir a cualquiera, cualquier copia o cualquier otra forma de reproducción de dichos materiales, salvo en la medida necesaria para proporcionar dicha información a los que tienen derecho a acceder a ella, según lo establezca la propia "Información Confidencial";
d. Asegurar que sus empleados, funcionarios, asesores, representantes (incluyendo abogados, personal técnico, etc.), y cualesquiera otros posibles participantes en la prueba de concepto, cumplan con los términos de este Acuerdo.
e. A comunicar a la ACP de toda filtración de información de la que tengan o lleguen a tener conocimiento producida por la infidelidad, imprudencia u otras omisiones de las personas que hayan accedido a la información confidencial.

f. No revelar la “Información Confidencial”, a ninguna persona sin la previa autorización escrita de la ACP. Esta prohibición es extensiva a representantes, empleados, contratistas y/o cualquier otro tercero vinculado a _____, todos los cuales deben ser conscientes del carácter confidencial de dicha información al realizar la prueba descrita en este documento.

En el evento que la información confidencial sea requerida a _____en virtud de una norma legal aplicable y por una autoridad competente, _____ deberá informar a la ACP de tal requerimiento, dentro de las veinticuatro (24) horas siguientes a la fecha en que reciba tal solicitud de información confidencial.

SEXTO: _____ acepta en proporcionar a la ACP, una lista con los nombres y direcciones de todas las personas, jurídicas o individuos que conocerán la “Información Confidencial” y se compromete a no utilizar dicha Información Confidencial para cualquier propósito que no sea con el fin de dar contestación a las solicitudes que haga la ACP durante el Estudio y conforme a los términos y condiciones de este, y no revelará la Información Confidencial a cualquier persona sin la previa autorización escrita de la ACP que no sean, en condiciones de confidencialidad y garantizará que sus representantes estén conscientes del carácter confidencial de dicha información y su uso exclusivo para cumplir con los propósitos del Estudio. Sin limitar la generalidad de lo anterior, en el caso de que _____ no brinde satisfactoriamente las consultas y requisitos que le haga la ACP; _____ ni sus trabajadores, sus representantes y/o cualquier otra persona vinculada a _____, podrán utilizar la Información Confidencial suministrada para otros propósitos distintos a los contemplados en este documento.

SÉPTIMO: _____ reconoce y acepta que el incumplimiento de los compromisos adquiridos en este acuerdo podrá dar lugar a que no se le siga tomando en cuenta para el Estudio, sin perjuicio de cualquier otra acción legal que diera lugar, según la normativa nacional vigente.

OCTAVO: _____ acepta y reconoce que todo intercambio de información confidencial, no supondrá, en ningún caso, la concesión de permiso o derecho expreso o implícito para el uso de patentes, licencias o derechos de autor o cualquier otro derecho de propiedad intelectual que sea de propiedad de la ACP que revele la información confidencial y reconoce que el presente documento, ni la entrega de la información confidencial o la realización del estudio constituyen un acuerdo con la ACP o el compromiso de la ACP, para entrar en una relación comercial.

NOVENO: Toda la Información Confidencial suministrada por la **ACP** a _____ en virtud de este acuerdo o generada durante la ejecución del Estudio, se emite bajo el concepto “como está”, sin garantía empresa o implícita, de que sea completa y/o precisa. La Información Confidencial se mantendrá y entenderá bajo la entera propiedad de la **ACP** y deberá ser devuelta, eliminada, borrada, o de cualquier otra forma destruida dentro de los diez (10) días calendarios siguientes a la terminación del Estudio o dentro de los cinco (5) días calendarios siguientes a la solicitud por escrito de la **ACP** a _____ para efectuar dichas acciones, lo que ocurra primero, entendiéndose con ello que _____ o sus representantes no podrán mantener copias, archivos o duplicados de dicha información, una vez la **ACP** haya realizado esta solicitud y/o haya terminado el contrato.

DECIMO: El presente Acuerdo se regirá e interpretará de conformidad con la normativa de la ACP y las leyes de la República de Panamá. Si alguna cláusula de este acuerdo es declarada nula o inaplicable por decisión de autoridad competente, esto no invalidará el resto del clausulado de este contrato, el cual será interpretado integralmente para lograr la debida confidencialidad que se pretende con este acuerdo. En caso de conflicto por la interpretación y/o cumplimiento de los términos de este acuerdo, el mismo será dirimido mediante Arbitraje en Derecho, en idioma español, ante el Centro de Conciliación y Arbitraje de Panamá (el Centro), ubicado en la Cámara de Comercio, Industrias y Agricultura de Panamá, ciudad y República de Panamá, bajo las reglas y procedimientos establecidos por el Centro.

UNDÉCIMO: _____ acepta y reconoce que el hecho de que la ACP suministre la información confidencial y realice este estudio, no dará lugar a que esta circunstancia se utilice, ya sea implícita o expresamente, para referencia de la calidad de _____, ni se autoriza bajo concepto alguno el uso del nombre de la ACP por parte de _____ como referencia con respecto a terceros.

Las provisiones del presente Acuerdo de Confidencialidad estarán vigentes por el término de hasta dos (2) años contados a partir de su firma.

EN FE DE LO CUAL, lo firmo a los_____ (__) días del mes de ____ de 20__.

_____ (_____)

Por:_____
Nombre:
Cargo:
Dirección