

CIRCULAR NO.1 RESPUESTAS A CONSULTAS REALIZADAS PARA EL PROCESO DE LICITACIÓN PÚBLICA NACIONAL INDOTEL-CCC-LPN-2023-0009 (ADQUISICIÓN E IMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE INFORMACIÓN Y EVENTOS (SIEM)).

Pregunta 1.

¿Cuál es la cantidad de EPS diarios?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 2.

¿Cuál es la Cantidad de dispositivos?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 3.

¿Cuál es el tiempo de retención del log (días)?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 4.

¿Van a adquirir el almacenamiento de forma local o en nube?

Respuesta.

Hibrido. Favor apegarse al pliego de condiciones especificado, en la **2.7 Descripción de los Bienes y/o Especificaciones Técnicas:** del requerimiento No. **01.**

Pregunta 5.

¿Cuentan con disponibilidad para instalar un recolector dentro de su datacenter?

Respuesta.

Si. Favor apegarse al pliego de condiciones especificado, en la **2.7 Descripción de los Bienes y/o Especificaciones Técnicas:** del requerimiento No. **02.**

Pregunta 6.
¿Cuentan con un SIEM actualmente?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 7.
¿Necesitan Alta Disponibilidad?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 8.
¿Con relación al requerimiento 02 sobre “La solución debe permitir la ingesta de datos sin la necesidad de conectores de clientes o soporte de proveedores?” Favor establecer a que se refieren cuando dicen conectores de cliente (integración, agente instalado en servidores, o conector de pago adicional a la licencia base, etc.).?

Respuesta.

Favor apegarse al pliego de condiciones especificado, en la **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: del requerimiento No. 02.

Pregunta 9.
En el requerimiento de soporte 24/7, ¿Esperan soporte de configuraciones, ajustes de fuentes y casos de uso; o solo soporte del fabricante en caso de que pase un inconveniente con la plataforma?

Respuesta.

Si. como lo establece en el pliego de condiciones en el acápite **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: en los requerimientos **No. 58, 59, 60, 61,62 y 63.x|**

Pregunta 10.

¿Poseen un inventario de la cantidad de dispositivos y los fabricantes de las fuentes pertenecientes a la red de INDOTEL a integrar a la plataforma? ¿Favor indicar estimado de los equipos a integrar en cantidad y marca?

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 11.

¿Tienen un estimado de la cantidad los casos de uso que desean tener configurados en la plataforma?

Respuesta.

Si. como lo establece en el pliego de condiciones en el acápite **2.7 Descripción de los Bienes y/o Especificaciones Técnicas:** en los requerimientos No. 58, 59, 60, 61,62 y 63.

Pregunta 12.

¿Cuál sería el tiempo de retención que requieren de los datos que se almacenan en la nube?

Favor inquirir en la circular de enmienda No.02.

Pregunta 13.

Para la implementación e integración con la red de INDOTEL, detallar:

Para la integración de fuentes, indicar el detalle de las fuentes que estarán sujetas al alcance de su adición y configuración (Fuentes son: Servidores, DB, Firewall, SW, Monitoreo de Archivos, Monitoreo de directorios, etc).

- Cantidad
- Marca
- Modelo
- versión de firmware / Sistema Operativo

Para la configuración de alertas, detallar:

- Tipo de alerta
- Fuentes que enviaran eventos para la alerta

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 14.

Para los casos de uso deseados, detallar:

- Cantidad de casos de uso deseados
- Controles de correlación deseados para el caso de uso
- Indicar las fuentes asociadas que entregaran los eventos
- Cuentan con actividades en sus procesos para la validación de estos casos de uso desarrollados
- Identificar qué casos de uso apoyan a cumplimientos de estrategia y/o regulaciones

- Tomando en cuenta que los casos de uso contienen elementos adicionales a un panel (dashboards), los cuales son solicitados en la tabla de requerimientos en los numerales **58, 59, 60, 61, 62 y 63.**

Respuesta.

Favor apegarse al pliego de condiciones en el acápite **2.7 Descripción de los Bienes y/o Especificaciones Técnicas:** en los requerimientos No. **05, 07, 47, 58, 59, 60, 61,62 y 63.**

Pregunta 15.

Para las fuentes cloud que desean integrar:

- Indicar el licenciamiento de Office365

- Indicar si desean integrar otras fuentes de tipo SaaS, PaaS o IaaS adicional a Sophos Central y Office365. Esto porque en la tabla de requerimientos en el “Numeral 22 indica: La solución debe admitir de forma nativa la recopilación de todos los tipos de fuentes de datos multi-nube. Proveedores de nube comunes, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).”

- Indicar si INDOTEL cuenta con las suscripciones correspondientes por cada fuente para la obtención de eventos.

Respuesta.

Favor inquirir en la circular de enmienda No.02.

Pregunta 16.

Indicar si INDOTEL proveerá los recursos de servidores intermediarios para el desarrollo del API para obtener eventos de nube (si aplica) o Para el cumplimiento del numeral 64 de la tabla de requerimientos.

Respuesta:

Si, pudiéramos proveer recursos en la nube, Favor apegarse al pliego de condiciones en el acápite **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: en los requerimientos: 38, 45 y 46.

Pregunta 17.

INDOTEL, requiere que el proveedor entregue cualquier elemento como hardware, software que se necesite para la implementación del proyecto? ¿o INDOTEL proveerá recursos necesarios para la implementación del software necesario para la colección de bitácoras?

Respuesta:

Indotel pudiera proveer algún recurso esencial en la nube. Favor apegarse al pliego de condiciones en el acápite **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: en los requerimientos: 16 y 17.

Pregunta 18.

Para el cumplimiento del cronograma:

- INDOTEL, tiene un tiempo estipulado para la implementación posterior a la adjudicación del contrato tomando en cuenta que si es requerido solicitar hardware se contempla en los 4 meses del plazo indicado?
- INDOTEL, proveerá de un gestor de proyectos para el seguimiento y cumplimiento de las actividades?

Respuesta:

Favor apegarse al pliego de condiciones en el acápite, **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: del requerimiento **54 y 65, Resultados o Productos Esperados y EL Plazo de Ejecución.**

Pregunta 19.

19.1 ¿Si los 35Gb solicitado en el numeral 03 incluye los 90 días de retención o deben ser considerado por aparte?

Respuesta:

Favor apegarse al pliego de condiciones en el acápite, **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: del requerimiento **10**, y los **Objetivos Especificos de la Contratación**.

19.2 A que se refieren cuando dicen “conectores de clientes” (integración, agente instalado en servidores, o conector de pago adicional a la licencia base).

Respuesta:

SIN LA NECESIDAD DE CONECTORES DE CLIENTES O SOPORTE DE PROVEEDORES, Favor apegarse al pliego de condiciones especificado, en la **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: del requerimiento No. **02**.

19.3 No hay necesidad de utilizar ningún agente adicional de pago. En algunas ocasiones, puede que sea necesario instalar un agente gratuito en servidores/máquinas (Universal Forward) para ayudar a enviar datos a la plataforma.

Respuesta:

Favor apegarse al pliego de condiciones en el acápite, **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: de los requerimientos **no. 24 y 47**.

Pregunta 20.

¿Para el punto 36 de la matriz de requerimientos técnicos, INDOTEL permitirá que la herramienta cuente con funcionalidades de creación de filtros a través de “interesting Field” en lugar de arrastrar y soltar?

Respuesta:

La solución debe incluir una interfaz de usuario de arrastrar y soltar para permitir a los usuarios no técnicos crear informes complejos. Favor apegarse al pliego de condiciones en el acápite, **2.7 Descripción de los Bienes y/o Especificaciones Técnicas**: del requerimiento **no. 36**.