CIRCULAR N° 4

LICITACIÓN N° 5000005809
"ADQUISICIÓN DE PLATAFORMA DE MONITOREO, ANÁLISIS Y RESPUESTA DE SEGURIDAD DE LA INFORMACIÓN CON GESTIÓN OPERATIVA CONTÍNUA"

En atención a lo estipulado en la Cláusula **4 ACLARACIONES Y ENMIENDAS AL DOCUMENTO BASE DE CONTRATACIÓN**, mediante la presente procedemos a enmendar lo siguiente:

CONSULTAS

Infraestructura física requerida (punto 6.7 y punto 4.1 de las Especificaciones Técnicas)

1.- Las Especificaciones Técnicas (punto 6.7) exigen la provisión de servidores físicos dedicados on-premise. Sin embargo, existen soluciones 100% nativos de la nube (SaaS) y no requieren servidores locales para el análisis o almacenamiento principal. ¿YPFB aceptaría una arquitectura en la que los servidores físicos solicitados se utilicen únicamente como **colectores o forwarders** (por ejemplo, para logs Syslog, CEF o Windows Event Forwarding) que consoliden y remitan los eventos a la nube, sin que allí se realice la correlación o el almacenamiento de largo plazo? En caso afirmativo, ¿se mantendría el requisito de entregar servidores con las especificaciones de cómputo detalladas (alta capacidad de CPU, RAM, RAID) o podrían ser equipos de menores prestaciones para esa función de pasarela?

Respuesta. - No. La Circular N°1, Sección G pregunta 2, confirma explícitamente que "El oferente deberá provisionar e instalar infraestructura física (servidores y/o appliances) dedicada como parte de la solución llave en mano, conforme a las Especificaciones Técnicas, puntos 1, 4.1 y 6.4."

2.- ¿Se permite utilizar infraestructura de virtualización existente en YPFB (sin entrega de hardware nuevo) para alojar los componentes locales necesarios (por ejemplo, colectores, sensores)?

Respuesta. - No. Por favor remítase a la Circular N°1, Sección G pregunta 2.

3.- En el caso de una solución SaaS, los datos de seguridad residen en la nube del fabricante y no en servidores entregados a YPFB. Al final del contrato, si no se renueva la licencia, el acceso a los datos históricos se pierde. El punto 4.2.3 de las Especificaciones técnicas exige un plan de salida que garantice la portabilidad de los datos.
¿YPFB acepta que dicho plan de salida consista en la exportación masiva de todos los logs a un almacenamiento proporcionado por YPFB (blob storage on-premise o en la nube), sin que sea necesario que la plataforma original siga operativa?

Respuesta. - La pregunta no es procedente porque la arquitectura SaaS que la motiva no es compatible con la Especificaciones Técnicas. La Circular N°1, Sección P pregunta 2, confirma que "Los datos permanecerán alojados físicamente en infraestructura instalada en los centros de datos de YPFB Transporte S.A.".

4.- En el mismo punto, se requiere que la finalización del contrato no implique pérdida de información institucional. ¿Se permitiría que, durante la vigencia del contrato, se realice copias periódicas de sus datos (por ejemplo, exportaciones diarias o semanales) a un repositorio propio como medida de contingencia?

Respuesta. - La periodicidad que se indica, se determinara en la implementación con el proveedor adjudicado.

Protocolo de comunicación de incidentes (punto 4.3.1 de las Especificaciones Técnicas)

5.- El protocolo establece que para incidentes críticos (Sev 1) la notificación debe realizarse en **15 minutos** desde su clasificación. No obstante, si la clasificación la realiza un analista tras revisar la alerta, ese tiempo podría ser insuficiente. ¿YPFB aceptaría que el cronómetro de los 15 minutos comience desde que el analista confirma la criticidad del incidente (y no desde la generación automática de la alerta)? Y, alternativamente, ¿se aceptaría un plazo de **30 minutos** para la notificación inicial en caso de alertas críticas que requieran análisis humano?

Repuesta. - No se acepta el plazo de 30 minutos para Sev1: el documento de especificaciones técnicas punto 4.3.1 Protocolo de Comunicación de Incidentes por Área del Negocio, es explícito en ≤15 minutos.

6.- El protocolo señala que el canal primario de notificación será la llamada telefónica ¿YPFB acepta que el **canal principal sea el correo electrónico**, y que la llamada telefónica se utilice únicamente en casos de no respuesta al correo o cuando el incidente así lo requiera?

Respuesta. - Las Especificaciones Técnicas punto 4.3.1 incisos 1 y 2 establecen explícitamente que el canal primario es "llamada telefónica directa o medio síncrono equivalente" para Sev1 y Sev2. No se acepta el correo como canal primario.

7.- El protocolo exige enviar un informe preliminar dentro de los 30 minutos siguientes a la notificación, indicando la "próxima actualización programada". Dado que es imposible predecir con exactitud cuándo se obtendrá información relevante nueva, ¿YPFB acepta que en lugar de un plazo fijo se envíen actualizaciones **cada 1 hora** hasta la contención del evento, sin necesidad de anticipar la hora de la siguiente actualización, y que el contenido sea un mensaje ejecutivo en lugar de un informe formal?

Respuesta. - Por favor remítase a las Especificaciones Técnicas, punto 4.3.1: "…

Incidentes de Severidad Crítica (Sev 1) Cuando un incidente de seguridad afecte la disponibilidad, integridad o continuidad de un proceso crítico (por ejemplo, sistemas financieros, logísticos, operaciones - SCADA):

La notificación al área impactada deberá realizarse en un plazo máximo de 15 minutos desde su clasificación como crítico y/o tomar acción inmediata previa coordinación con YPFB TRANSPORTE S.A.

o El canal primario deberá ser llamada telefónica directa o medio síncrono equivalente.

o Deberá enviarse un informe preliminar por correo electrónico dentro de los 30 minutos siguientes, indicando:

- Descripción inicial del incidente
- Sistemas afectados
- Impacto estimado
- Acciones inmediatas en curso
- Próxima actualización programada

…. "

Definición de "informes a demanda" y "bajo demanda" (puntos 6.2 y 9 de las Especificaciones Técnicas)

8.- En el punto 6.2 se mencionan “informes formales de monitoreo de seguridad de manera: mensual, semestral, anual o **a demanda**”. ¿Podría YPFB especificar qué tipo de informes a demanda se requieren (ej. ¿para una investigación específica, para una auditoría, para un incidente particular?) y con qué frecuencia máxima espera poder solicitarlos (ej. hasta 2 por mes, etc.)?

Respuesta. - El contenido y frecuencia de los informes a demanda será establecido en coordinación con el proveedor adjudicado.

9.- En la tabla de SLA (punto 9), el Nivel 4 (Bajo) indica “bajo demanda” como frecuencia de actualización. ¿Podría aclararse qué significa “bajo demanda”? ¿Se refiere a que no hay un plazo predefinido y que YPFB puede solicitar una actualización cuando lo considere necesario, o a que el proveedor solo actualizará cuando haya algún cambio relevante?

Respuesta. - "Bajo demanda" significa que YPFB Transporte S.A. solicitará una actualización del estado del evento Nivel 4 cuando lo considere necesario. El proveedor deberá responder a dicho requerimiento en un tiempo razonable.

Certificaciones del personal (punto 8 de las Especificaciones Técnicas)

10.- El punto 8 requiere, para Nivel 2, certificaciones como CEH (Certified Ethical Hacker) o equivalentes. ¿YPFB aceptaría, en lugar de la certificación CEH, una **acreditación de conocimientos equivalentes**?

Respuesta. - No se acepta una acreditación de conocimientos. Es requerida una certificación válida como CEH (Certified Ethical Hacker) o equivalentes

11.- En el Nivel 3 se requiere CISSP, CISM u OSCP. ¿Se considera suficiente la OSCP para cumplir con el requisito de Nivel 3, sin necesidad de contar con CISSP o CISM adicionales?

Respuesta. - Sí, una sola de las certificaciones listadas en la Sección 8 de las Especificaciones Técnicas es suficiente para acreditar el Nivel 3, ya que las Especificaciones Técnicas las establece como opciones alternativas. Sin embargo, dado que las funciones del Nivel 3 incluyen gestión de incidentes críticos, análisis forense y coordinación de respuesta a nivel organizacional, se valorará positivamente que la certificación presentada demuestre competencias tanto técnicas como de gestión de seguridad.

Tamaño de la empresa (Anexo 1 de las Especificaciones Técnicas)

12.- El mismo Anexo 1 indica que la empresa debe tener “dotación superior a 1.000 empleados”. ¿Se trata de un requisito excluyente? En caso de que el proponente no tenga más de 1.000 empleados, pero el fabricante sí los tenga, ¿se consideraría cumplido el requisito mediante la carta del fabricante?

Respuesta. - No es un requisito excluyente. La mención de "dotación superior a 1.000 empleados" se encuentra en el punto 12 de la Especificaciones Técnicas. (Otras Buenas Prácticas), no en el Anexo 1. El punto 12 mencionado, es un contexto de referencia para las buenas prácticas recomendadas.

Pruebas de aceptación (punto 13.2 de las Especificaciones Técnicas)

13.- Las pruebas de aceptación funcional (UAT) incluyen simulación controlada de eventos de seguridad sobre sistemas críticos. ¿Estas pruebas serán ejecutadas por el proveedor o por un equipo auditor designado por YPFB? ¿El costo de dichas pruebas debe ser asumido por el proveedor o por YPFB?

Respuesta. - Remítase a la Circular N°1, Sección M preguntas 1 y 3, establece que el oferente presenta el listado de pruebas (punto 13.2 de las Especificaciones Técnicas) y que las UAT incluyen

simulaciones controladas bajo supervisión de YPFB Transporte S.A. Sobre el costo: la modalidad llave en mano DDP (Circular N°1, Sección O pregunta 3) establece que "los precios deben incluir todos los costos asociados."

Siendo esta toda la información, solicitamos tomar debida nota de la presente.

Santa Cruz, mayo de 2026.