Términos de Referencia

Servicio de Managed Detection and Response (MDR) /XDR

Gestión 2024

INDICE DE CONTENIDO

Contenido

1 INTRODUCCIÓN

YPFB TRANSPORTE S.A. en cumplimiento a su plan de adquisición de "Seguridad de la Información 2024", invita a las empresas legalmente establecidas en Bolivia a presentar su propuesta para la adquisición del servicio de administración gestionada de detección y respuesta o MDR (*Managed Detection and Response*).

Entiéndase por un servicio gestionado MDR (*Managed Detection and Response*) a un servicio que ofrece capacidades proactivas de búsqueda, monitorización y respuesta diseñadas específicamente para amenazas, respaldado por un equipo de técnicos avanzados en ciberseguridad que trabajan en conjunto con un análisis de datos correlacionados sólido.

2 ALCANCE DE LA PROVISIÓN DEL SERVICIO

El alcance de la provisión en lo que se refiere a equipos, hardware, software y materiales se describe en los siguientes ítems:

Importante. **-** El **Ítem 1** como **el Ítem 2**, podrán ser adjudicados en conjunto o por separado, es decir, pueden ser distintas empresas proveedoras.

ITEM 1. Servicio de implementación de MDR/XDR

Se requiere un servicio **llave en mano**, para la administración gestionada de detección y respuesta (MDR) a fin de detectar, analizar, investigar y responder activamente mediante la interrupción y contención de amenazas, proveyendo la tecnología necesaria para cubrir endpoints, servidores, HMI, firewall, AD entre otros.

CARACTERISTICAS DEL SERVICIO MDR		
N°	**Característica**	**Descripción**
1.1	Monitoreo	El servicio MDR debe ofrecer monitoreo constante de la red y los sistemas para identificar posibles amenazas en tiempo real.
1.2	Modalidad del servicio gestionado	Servicio gestionado 24x7 365 días del año, con un equipo de profesionales expertos en ciberseguridad (del fabricante) y respuesta a incidentes. Con respuesta en una hora para incidentes críticos
1.3	Cantidad de licencias	**1210** equipos
1.4	Tipo de licenciamiento	Suscripción por cinco (5) años
1.5	Consola de administración o plataforma de administración	Capacidad de correlación de millones de eventos/día.
		Inteligencia artificial para identificar cambios en las tácticas y estrategias adversarias
		Telemetría en todos los endpoints, activos de Tecnología de la Información (IT) y Tecnologia Operativa (OT).
		Acceso a la plataforma para distintos roles de usuario (ejemplo: Administrador total, Administrador, Analista de Seguridad, Analista de seguridad solo lectura, Dashboard, Investigador, Líder de seguridad y otros).

		La consola de administración de la solución propuesta debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.
		La consola de administración de la solución propuesta debe soportar 2FA (autenticación de dos factores) para autenticación de usuarios a la consola de gestión
		La solución propuesta podrá ser gestionada tanto en nube, on-premise o en una arquitectura hibrida, pudiendo conectarse a otros servicios en nube.
1.6	Detección avanzada de amenazas	Contar con capacidades avanzadas de detección de amenazas, utilizando tecnologías como análisis de comportamiento, inteligencia artificial, y aprendizaje automático para identificar actividades maliciosas.
1.7	Análisis de comportamiento	Debe tener la capacidad de analizar el comportamiento normal de la red y los sistemas para detectar anomalías que puedan indicar actividad maliciosa.
1.8	Investigación de amenazas	Contar con un equipo de expertos en ciberseguridad del fabricante que investiguen y analicen las amenazas detectadas para comprender su naturaleza y tomar medidas adecuadas para mitigarlas.
1.9	Respuesta rápida y efectiva a incidentes	Respuesta rápida y efectiva ante las amenazas detectadas, incluyendo la capacidad de contener y remediar rápidamente los incidentes de seguridad. Se requiere un SLA mínimamente de dos niveles de respuesta a incidentes de seguridad. Nivel 1 atención menor a dos horas como máximo luego de ocurrido el incidente de seguridad y Nivel 2 hasta 4 horas luego de ocurrido el incidente seguridad, según la criticidad.
1.10	Integración con herramientas de Seguridad Existentes	Debe integrarse fácilmente con las herramientas de seguridad existentes en la infraestructura de la organización para proporcionar una visión unificada de la postura de seguridad.
1.11	Informes y análisis de incidentes	Proporcionar informes detallados y análisis de los incidentes de seguridad detectados, así como recomendaciones para mejorar la postura de seguridad de la organización.
1.12	Cumplimiento normativo	Debe ayudar a la organización a cumplir con los requisitos de cumplimiento normativo relevantes, como GDPR, HIPAA, PCI-DSS, entre otros.
ESPECIFICACIONES TÉCNICAS DEL AGENTE		
1.13	Sistema Operativos soportados	La solución propuesta debe ser compatible con los siguientes sistemas operativos de usuario final: Windows (32-bit & 64-bit versiones) 7, 8, 8.1, 10 y 11
		La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, y 2022
		La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux , Suse Enterprise Linux 12 o superior

		La solución propuesta debe ser compatible con las siguientes tecnologías: Ambientes Virtual Desktop, Infraestructura (VDI) en VMware. VMware Horizon versión 7 y superior, VCenter y ESXI
1.14	Agente / Sensor	La solución propuesta en su conjunto deberá tener la capacidad de brindar el servicio mediante **un sólo agente**
		La solución propuesta debe soportar el despliegue masivo a través de herramientas, por ejemplo: MS System Center, Manage Engine EPC y otros.
		La solución propuesta debe tener la habilidad de actualizar el Endpoint sin interacción por parte del usuario y sin requerimiento de reinicio.
		La solución propuesta debe poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos.
		La desinstalación del agente puede realizarse de forma local desde el equipo o de forma remota desde la consola de administración.
		El agente podrá conectarse al Tenant (consola de administración), utilizando el protocolo TLS 1.2 y el puerto 443
		La solución debe funcionar en modalidad "offline" fuera de línea sin que el agente esté conectado a internet o no se encuentre conectado a la red empresarial
1.15	Instalación del agente/sensor en equipos HMI	Aparte de las características mencionadas en el punto 1.14, el agente instalado en equipos HMI de red OT de YPFB Transporte S.A. deberá trabajar detrás o a través de un **proxy o bróker, etc**. Ya que estos equipos por políticas de la empresa no pueden conectarse directamente a internet.
1.16	Instalación del agente/sensor en equipos con Sistemas Operativos Linux	Aparte de las características mencionadas en el punto 1.14, el agente instalado en servidores Linux deberá trabajar detrás o a través de un **proxy o bróker, etc.** (debe ser el mismo tipo de licenciamiento que para sistemas operativos Windows). Ya que estos servidores por políticas de la empresa no pueden conectarse a internet.
1.17	Visibilidad e inventario en tiempo real	Se requiere tener visibilidad de las computadores y aplicaciones en tiempo real.
1.18	Detección de Malware	La solución propuesta debe detectar, eliminar y volver a su valor inicial cambios realizados por procesos maliciosos en los equipos de usuarios finales, HMI, y Servidores que forman parte del servicio.
		La solución propuesta debe incorporar las técnicas de MITRE ATT&CK en el esquema de detección
		La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías (Ejemplo: Crítica, Alta, Media, Baja)
		La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos.
		La solución propuesta debe incorporar un motor de antivirus de última generación (NGAV).
		La solución propuesta debe tener capacidad de controlar dispositivos USB

1.19	Prevención de Malware	La solución propuesta debe bloquear tráfico malicioso de exfiltración de datos
		La solución propuesta debe bloquear tráfico malicioso de comunicación hacia C&C (Command & Control)
		La solución propuesta debe frenar brechas de seguridad e intentos de ransomware en tiempo real
		La solución propuesta debe evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos
1.20	Escenarios de ataque	La solución propuesta debe identificar y prevenir los intentos de escalación de privilegios
		La solución propuesta debe bloquear ataques de ransomware conocido
		La solución propuesta debe proteger contra Scripts de Powershell maliciosos
		La solución propuesta debe proteger contra Scripts de CScript maliciosos
		La solución propuesta debe proteger contra macros de MS Office maliciosos
		La solución propuesta debe tener control sobre dispositivos USB
		La solución propuesta debe tener la capacidad de detectar dispositivos IoT no administrados en la red
		La solución propuesta debe tener la capacidad de detectar dispositivos no administrados y protegidos por la solución con sistemas operativos macOS/Linux/Windows
1.21	Capacitación y Entrenamiento	Se deberá proporcionar entrenamiento del fabricante, al personal de la DTI (3 personas) de YPFB Transporte S.A en la administración, operación y uso de la consola, así como en el despliegue y operación del agente; esta capacitación tendrá una duración de 20 horas, distribuidos en 5 días en modalidad de aula o virtual. El entrenamiento debe incluir certificación oficial de la marca para cada participante.
CARACTERISTICA DE INTEGRACIÓN CON FUENTES DE DATOS		
1.22	Ingesta de datos de fuentes externas.	La solución propuesta debe permitir funciones de XDR (eXtended Detection and Response) que permite visibilidad entre múltiples sistemas de seguridad para detectar actividades maliciosas a través del uso de analítica y correlación de información de otras plataformas
		Firewall Fortigate, cantidad: 4 Firewall
		Identity (Cisco ISE), cantidad: 2
		Azure Active Directory, cantidad: 1 Tenant
		La solución deberá permitir la ingesta de datos de fuentes externas al menos de 30 GB/día

Las especificaciones descritas en la Tabla del **ITEM 1**. contemplan únicamente los principales componentes de la solución, es responsabilidad del proveedor la validación e inclusión de otros componentes que sean requeridos para el correcto funcionamiento de la solución.

El proveedor puede complementar o mejorar esta configuración en función a la validación que le proporcione el fabricante. Dichos componentes adicionales deberán detallarse en la oferta técnica y económica.

Se requiere que la Oferta Técnica y Económica del proveedor considere las siguientes condiciones:

- El proveedor deberá incluir en su oferta técnica un cronograma de trabajo para la instalación, configuración y pruebas de la solución. Dicho cronograma debe reflejar cual es el tiempo requerido para cada etapa del proyecto hasta la entrega final.
- El proveedor deberá entregar al inicio del proyecto un plan de las pruebas, que contemple mínimamente lo detallado en el punto 6. PRUEBAS DE ACEPTACIÓN del presente TDR, para corroborar la correcta instalación y funcionamiento de la solución. Dichas pruebas serán ejecutadas en coordinación con personal de YPFB TRANSPORTE S.A. previo a la aceptación conforme del servicio.
- Al menos una (1) persona de la empresa contratista trabajará en forma remota a lo largo del proyecto, incluyendo un máximo de 10 días en sitio a requerimiento de YPFB TRANSPORTE S.A. en caso de ser necesario durante la fase de instalación y configuración de los componentes, bajo la supervisión del encargado de proyecto por parte de YPFB TRANSPORTE S.A. Dicha persona podrá coordinar sesiones de soporte remoto con otros especialistas del fabricante si así fuera necesario.
- En el marco del desarrollo de este proyecto, el proveedor deberá designar un encargado de proyecto que trabajará en coordinación con el encargado de proyecto de YPFB TRANSPORTE S.A.
- El proveedor deberá entregar los instaladores, licencias y todo el software en las versiones actualizadas de toda la solución. Así mismo, se deberá contar con el servicio de afinamiento de reglas por parte del fabricante/proveedor, de acuerdo a buenas prácticas.
- Para el trabajo in situ, el/los técnicos acreditados trabajarán en oficinas de YPFB TRANSPORTE S.A. ubicadas en la Doble Vía a la Guardia KM 7 ½, de lunes a viernes en horario de 8:00 a 16:00 y los sábados de 08:00 a 12:00 bajo la supervisión del encargado del proyecto y será imprescindible que porten un documento de identidad, previo al ingreso a las oficinas. Si el realizar alguna actividad de instalación o configuración implica un riesgo que pueda afectar o interrumpir las operaciones de YPFB TRANSPORTE S.A., se deberá programar el cambio en horarios fuera de oficina, incluyendo fin de semana, sin que esto represente un costo adicional para YPFB TRANSPORTE S.A.
- El proveedor deberá notificar con 24 horas de anticipación las ausencias por vacaciones o faltas circunstanciales/permisos que deba tomar el personal involucrado en este proyecto.
- El proveedor deberá entregar al finalizar el proyecto toda la documentación incluyendo mínimamente y no limitado a toda la documentación requerida en el punto 9 del presente TDR.

ITEM 2. PLATAFORMA PARA CLIENTE DE CONEXIONES REMOTAS DE CONFIANZA CERO

ITEM 2:	Plataforma para cliente de conexiones remotas de confianza cero

2.1	Hardware/Software	Software / Plataforma
2.2	Marca	Fortinet
2.3	Modelo	FortiClient ZTNA
2.4	Cantidad	366 usuarios
2.5	Vigencia	5 años

Requerimientos		
#	**Característica**	**Descripción**
2.6	Plataforma de administración centralizada	La solución deberá contar con una interfaz simple y de facil utilización.
		Deberá permitir el deployment del cliente de manera remota.
		Deberá soportar la orquestación de etiquetas de confianza cero.
		Deberá contar con un dashboard con información en tiempo real de los clientes.
		Deberá soportar la integración con Active Directory.
		Deberá permitir la asignación de grupos de manera dinámica.
		La plataforma propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, y 2022
2.7	Cliente para dispositivos finales	El cliente para dispositivos finales deberá soportar acceso universal a la red de confianza cero.
		Deberá permitir que las sesiones se inicien de manera automática, con túneles encriptados a equipos FortiGates como pasarela de aplicaciones.
		Deberá soportar la verificación de postura de dispositivos y usuarios.
		Deberá permitir el acceso remoto con políticas contextuales para acceso controlado a las aplicaciones.
		Deberá permitir el filtrado web con seguridad para sitios web y filtrado de contenido.
		Deberá soportar la asignación de etiquetas confianza cero en base a la postura del dispositivo.
		El cliente para dispositivos deberá ser compatible con los siguientes sistemas operativos: Windows 7 (32-bit & 64-bit versiones), 8 (32-bit & 64-bit versiones), 8.1 (32-bit & 64-bit versiones), 10 y 11
2.8	Integraciones de la solución	El cliente y la plataforma de gestión deberá integrarse de manera nativa con los firewalls fortigates con los que cuenta YPFB Transporte S.A.. Para funciones de telemetría, acceso dinámico y refuerzo de cumplimiento de políticas, cuarentena de dispositivos finales y controles de navegación web.
2.9	Licenciamiento y garantía técnica	La plataforma ofertada deberá incluir Garantía y Soporte de fabricante 24x7 con respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para problemas no críticos. por el periodo de 5 años.
2.10	Instalación	La oferta debe incluir la instalación y configuración completa de la solución en coordinación con la unidad solicitante.
2.11	Certificación	4 certificaciones para personal de YPFB TRANSPORTE S.A. con número de parte **NSE-EX-FTE2**

3 MODIFICACIÓN DE ESPECIFICACIONES

Las modificaciones para reemplazo o mejoras a cualquier punto de este Pliego deberán ser consultadas y aprobadas por el equipo evaluador de YPFB TRANSPORTE S.A. durante el periodo de consultas, para ello se deberá utilizar el siguiente formato:

Ítem	Numero de parte a reemplazar	Numero de parte Propuesto	Descripción del Componente propuesto	Motivo del Cambio

Se aclara que cualquier modificación que no esté consensuada con YPFB TRANSPORTE S.A. será considerada como incumplimiento y descalificación.

4 ALCANCE

La solución y todos sus componentes deberá implementarse en un máximo de 90 días calendario en coordinación con personal de la Dirección de Tecnologías de la Información de YPFB TRANSPORTE S.A. en dispositivos finales, escritorios virtuales (VDI), HMI y servidores con su respectiva configuración de acuerdo a buenas prácticas para un correcto funcionamiento.

5 PROVISIÓN

A continuación, se especifican las condiciones requeridas:

5.1 PROCEDIMIENTO DE COMUNICACIÓN/ATENCIÓN

La empresa ofertante deberá designar un encargado de proyecto que trabajará bajo la supervisión del encargado de proyecto de YPFB TRANSPORTE S.A., Especialista de Seguridad de la Información, para aplicación del soporte de garantía y consultas cuando sea solicitado.

5.2 GARANTÍA

Toda la solución ofertada que requiera suscripción deberá contar con suscripción vigente de acuerdo al periodo especificado en el detalle del **inciso 1.4 para el ítem 1** y del **inciso 2.5 para el ítem 2**. Con la finalidad de garantizar la continuidad de los servicios.

5.3 PROVISIÓN DEL SERVICIO

Todas las características técnicas del servicio listados en la tabla de especificaciones tanto del ítem 1 como del ítem 2 de este documento, así como otros que no formen parte de la solución, deberán ser incluidos en la cotización y podrán ser entregados como elementos independientes.

En caso del licenciamiento y otros intangibles, de ser requerido por el encargado de proyecto de YPFB TRANSPORTE S.A. estos deberán ser entregados en cuanto el fabricante procese la activación de los mismos.

5.4 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

La empresa proveedora del servicio, antes de comenzar el trabajo, deberá firmar un acuerdo de confidencialidad y no divulgación de la información (NDA), conforme a los ítems a los que aplico.

6 PRUEBAS DE ACEPTACIÓN

El proponente deberá junto a su propuesta, entregar un listado de las pruebas de aceptación que planea realizar, las que serán consensuadas con YPFB TRANSPORTE S.A. posterior a la adjudicación. Estas pruebas servirán para garantizar la correcta instalación, configuración y operación del servicio MDR. Las siguientes son pruebas requeridas:

- Health Check “estado de salud” ejecutado por el fabricante de acuerdo a las buenas practicas.
- Pruebas de instalación y desinstalación del agente, desde la consola de administración y desde el equipo local.
- Pruebas de rendimiento en equipos de IT y OT
- Pruebas de rendimiento en servidores (Windows, Linux)

7 PLAZOS Y CONDICIONES DE ENTREGA

Se deberán considerar los siguientes plazos y condiciones de entrega:

Para el ítem 1:

- Puesta en marcha (llave en mano) del servicio de administración gestionada de detección y respuesta (MDR - *Manage Detection and Response*) hasta noventa (90) días calendario, luego de recibida la orden de proceder; implica la configuración del servicio e instalación de agentes o sensores en equipos finales, escritorios virtuales (VDI), servidores y HMI. La ejecución del servicio MDR de seguridad y protección de equipos finales, escritorios virtuales (VDI), servidores y HMI; monitoreo proactivo de amenazas y remediación de incidentes de seguridad por un periodo de cinco (5) años en modalidad 24x7x365 realizado por el fabricante para YPFB Transporte S.A.

Para el ítem 2:

- Entrega de la plataforma para cliente de conexiones remotas de confianza cero hasta noventa (90) días calendario luego de recibida la orden de proceder. Licenciamiento y garantía técnica más soporte en la solución por cinco (5) años.

8 PAGOS

El pago se realizará por hitos contra entrega de informes:

ITEM 1: SERVICIO DE IMPLEMENTACIÓN DE MDR/XDR

HITO	Descripción de avance del servicio	Porcentaje de pago por el servicio	Entregable
1	Implementación de la solución MDR/XDR, en equipos finales, VDI de YPFB TRANSPORTE S.A., de acuerdo a buenas prácticas	50%	▪ Primer informe de avance
2	Implementación de la solución MDR/XDR, en equipos HMI y Servidores de YPFB TRANSPORTE S.A., de acuerdo a buenas prácticas	50%	▪ Contra entrega de informes finales de funcionamiento correcto del servicio MDR, (informes aprobados).

ITEM 2: PLATAFORMA PARA CLIENTE DE CONEXIONES REMOTAS DE CONFIANZA CERO

N°	Descripción de avance del servicio	Porcentaje de pago por el servicio	Entregable
1	Implementación en la cantidad de equipos y características descritas en el ítem 2.	100%	▪ Contra entrega de informes finales de funcionamiento correcto de la plataforma para cliente de conexiones remotas de confianza cero

9 ENTRENAMIENTO EN SOFTWARE (SOLUCIONES DE SEGURIDAD)

Para el **ítem 1**, la propuesta deberá incluir cupos de entrenamiento del fabricante que permita al personal de YPFB TRANSPORTE S.A. adquirir conocimiento en administración, configuración y optimización de la tecnología ofertada en relación MDR/XDR, la cual deberá cumplir con las siguientes condiciones:

a) Podrá ser utilizado en cualquier momento mientras esté vigente el soporte de los equipos y software incluidos en este pliego.
b) Deberá ser impartido mediante seminario y/o conferencia internacional en la locación principal del fabricante. El proponente deberá adjuntar un documento o carta de compromiso especificando el nombre y lugar del seminario y/conferencia.

c) Deberá contemplar la participación de al menos dos (2) personas a los seminarios descritos en el anterior inciso.
d) El proponente deberá proveer toda la logística y gastos necesarios (transporte, alimentación, alojamiento y otros) para la asistencia a los seminarios mencionados en el inciso b).

La selección de asistentes, fechas y logística de asistencia será coordinada con el encargado de proyecto de YPFB TRANSPORTE S.A. y podrá ser ejecutada en cualquier momento después de la adjudicación dentro del plazo de garantía del servicio.

Para el **ítem 2**, la empresa proponente deberá incluir en su oferta al menos cuatro (4) voucher de certificación oficial en la plataforma base de FortiOS – NSE4.

La propuesta de los ofertantes deberá incluir la aceptación de estos puntos, la ausencia de estos será considerada como incumplimiento y descalificación.

ANEXO 1

A continuación, se detalla la información a ser entregada con la propuesta técnica, la misma deberá estar correctamente ordenada y enumerada según el siguiente listado.

1. Es un requisito indispensable para los proveedores que participen de esta licitación que todas las cartas y/o certificaciones solicitadas en este pliego sean emitidas y/o firmadas por representantes del fabricante que estén designados para territorio de Bolivia.

2. La Empresa ofertante deberá presentar certificados donde demuestre y avale:

    a. Condición de canal autorizado (partner) para el territorio de Bolivia, incluyendo la antigüedad como canal, mínimamente de un (1) año. La documentación proporcionada por el fabricante de la marca, no deberá ser modificada o alterada bajo ninguna circunstancia.
    b. Documentación que acredite la ejecución de la implementación a través de los servicios profesionales propios del fabricante, para asegurar que el proyecto será correctamente implementado y el servicio sea ejecutado por el personal idóneo. La documentación proporcionada por el fabricante de la marca, no deberá ser modificada o alterada bajo ninguna circunstancia.

3. La empresa ofertante deberá cumplir con los siguientes requisitos:

    a. La garantía y condición del servicio MDR (*Managed Detection and Response*) (aplica para el ítem 1).
    b. Certificado emitido por el fabricante, acreditando la autorización para comercializar en Bolivia las licencias del software requerido para la implementación de la solución.
    c. Contar con al menos una (1) persona en Bolivia que posea certificación técnica vigente, misma que puede ser personal propio de la empresa ofertante o personal del fabricante de la marca relacionada al servicio ofertado, de acuerdo a los ítems del presente TDR y que el ofertante aplique, se aclara que no se tomará en consideración las certificaciones de ventas o 'pre-sales'.
    d. Contar con un (1) especialista del fabricante de la marca ofertada para el startup y configuración inicial del software ofertado.
    e. En referencia al punto anterior. El Ofertante deberá presentar:
        - Curriculum Vitae del personal que realizará la implementación el servicio, donde se demuestre las certificaciones del fabricante en los ítems que implementará.
        - Organigrama y Cargo dentro del marco de ejecución del proyecto.
        - Se deberá contar con personal de planta que tenga una antigüedad de por lo menos 6 meses en la empresa a cargo del proyecto.

    f. Todo profesional licenciado en ingeniería que sea boliviano o extranjero con residencia permanente en el país, para participar dentro de un proceso de contratación o se requiera su contratación de manera directa, deberá estar inscrito en el Registro nacional de Ingenieros de la Sociedad de Ingenieros de Bolivia (SIB); para lo cual, deberá imprescindiblemente acreditar lo referido a través de la presentación de una fotocopia a color carnet vigente emitido por la citada entidad.

4. La empresa ofertante deberá tener una antigüedad en el rubro tecnológico mínimamente de cinco (5) años comercializando en el territorio de Bolivia. Deberá presentar su matrícula de comercio adjunto.

5. Descripción de trabajos donde cumplan con implementaciones similares a la ofertada no mayor a 2 años:
   a. Por lo menos una (1) implementación de productos similares
   b. Antigüedad de la implementación (cuando se realizó).
   c. Referencia de la empresa donde se realizó la implementación (nombre, cargo, teléfono y/o correo electrónico).

6. Documentación técnica del software ofertado.

7. Nombre y teléfono de contacto de la persona a cargo del proyecto como interlocutor válido para YPFB TRANSPORTE S.A. para todos los requerimientos comerciales y técnicos, esta persona deberá tener un celular con disponibilidad 24x7 (horas x días a la semana). Esta persona será también el encargado de atender cualquier reclamo asociado a la provisión del software y/o los servicios asociados.

Nombre: Renán Luis Layme Yucra **Cargo:** Especialista de Seguridad de la Información	**Nombre: Rafael Barrios** **Cargo:** Analista de Soporte Técnico