



Especificaciones Técnicas

Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua

Gestión 2026

CONFIDENCIALIDAD


La información contenida en este documento es confidencial y propiedad de la Empresa YPFB TRANSPORTE S.A.
Queda prohibida su copia y/o distribución parcial o total sin el expreso consentimiento del propietario.

INDICE DE CONTENIDO

Contenido

1	INTRODUCCIÓN	1
2	OBJETIVO DEL PROYECTO	1
3	MODELO OPERATIVO DE SEGURIDAD	2
4	ALCANCE DE LA PROVISIÓN	2
4.1	Alcance General	2
4.2	Propiedad de los activos	3
4.3	Gobernanza y modelo de responsabilidades	4
5	CARACTERISTICAS DE LA PLATAFORMA	6
5.1	Inventario de Activos de Integrar y Monitorear	6
6	CARACTERISTICAS DE LA PLATAFORMA DE OPERACIÓN	6
6.1	Monitoreo Continuo	6
6.2	Modalidad de Acompañamiento Operativo	6
6.3	Plataforma Central de Gestión.....	7
6.4	Arquitectura de Recolección y Análisis On Premise	7
6.5	Disponibilidad y Continuidad Operativa de la Plataforma de Monitoreo	7
6.6	Características del agente o Collector.....	7
6.7	Infraestructura de Cómputo On-Premise para Plataforma de Monitoreo	9
7	DIMENSIONAMIENTO TÉCNICO REFERENCIAL	12
7.1	Supuestos Generales.....	12
7.2	Parámetros Técnicos de Referencia.....	12
7.3	Escalabilidad y Evolución	13
8	NIVELES DE ATENCIÓN y PERSONAL TÉCNICO CERTIFICADO	13
9	NIVEL DE SERVICIO (SLA)	15
9.1	Disponibilidad de la Plataforma	15
9.2	Personal de monitoreo, análisis y respuesta	16
10	AUTOMATIZACIÓN Y PROCEDIMIENTOS OPERATIVOS	16
10.1	Casos de usos mínimos de monitoreo, detección y respuesta	16
10.2	Procedimientos automatizados y orquestados de respuesta (Playbooks)	19

11	TRANSFERENCIA DE CONOCIMIENTO.....	21
11.1	Participación en eventos técnicos del fabricante	21
12	OTRAS BUENAS PRÁCTICAS	21
13	PLAZOS, ACEPTACIÓN Y PAGOS.....	22
13.1	Plazos y vigencia.....	22
13.2	Pruebas de aceptación.....	22
13.3	Pagos	23
ANEXO 1.	24

	ESPECIFICACIONES TÉCNICAS		Hojas: 1
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

1 INTRODUCCIÓN

YPFB Transporte S.A., en cumplimiento de su plan institucional de fortalecimiento de controles de ciberseguridad 2026, convoca a empresas legalmente establecidas en Bolivia a presentar propuestas para adquisición bajo modalidad llave en mano de una plataforma integral de monitoreo, análisis y respuesta a eventos e incidentes de seguridad de la información, basada en infraestructura tecnológica dedicada y software especializado.

La iniciativa tiene como finalidad dotar a la organización de una capacidad institucional permanente y centralizada para la vigilancia continua, investigación, gestión y respuesta ante incidentes de seguridad en entornos de Tecnología de la Información (IT) y Tecnología Operativa (OT), operando de forma ininterrumpida (24x7x365).

La contratación se estructura priorizando la provisión e implementación de activos tecnológicos institucionales, incluyendo servidores, appliances, licencias de software y componentes tecnológicos, los cuales serán instalados on premise en los centros de datos de YPFB Transporte S.A. y pasarán a ser de su propiedad, permitiendo el control directo de la plataforma, asegurando la continuidad operativa y habilitando su evolución y ampliación futura conforme a las necesidades de la organización.

De manera complementaria, se incluye acompañamiento operativo que tendrá carácter técnico-operativo y de soporte especializado, manteniéndose en todo momento la responsabilidad de gobierno, priorización de riesgos y toma de decisiones estratégicas en YPFB Transporte S.A., orientado a asegurar la operación continua de la plataforma, el cumplimiento de niveles de servicio, la atención oportuna de eventos e incidentes, el mantenimiento técnico de la solución y la transferencia progresiva de conocimiento al personal institucional.

2 OBJETIVO DEL PROYECTO

Implementar una capacidad institucional permanente de monitoreo, análisis, gestión y respuesta a eventos e incidentes de seguridad de la información, sustentada en infraestructura tecnológica dedicada y software especializado, instalada on premise, que permita a YPFB Transporte S.A.:

- Centralizar la recolección y análisis de eventos de seguridad provenientes de activos IT, OT y servicios en la nube.
- Operar un modelo continuo de vigilancia, investigación y respuesta 24x7x365.
- Gestionar incidentes de forma estructurada, trazable y basada en niveles de atención.
- Ejecutar acciones de contención, remediación y recuperación de manera manual y automatizada.
- Fortalecer progresivamente la madurez institucional en ciberseguridad.

	ESPECIFICACIONES TÉCNICAS		Hojas:2
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

La plataforma, sus componentes y licenciamiento asociado serán entregados bajo modalidad llave en mano y constituirán activos tecnológicos de propiedad de YPFB Transporte S.A., sobre los cuales se prestará un servicio de acompañamiento operativo especializado, sin transferencia de control ni custodia lógica de los activos durante el periodo contractual que incluya también actividades de actualización, soporte y mantenimiento de la mencionada plataforma.

3 MODELO OPERATIVO DE SEGURIDAD

La solución deberá habilitar un modelo operativo centralizado de seguridad, entendido como la integración coherente de:

- Tecnología: infraestructura, plataformas de análisis, automatización y visualización.
- Procesos: detección, clasificación, escalamiento, respuesta, recuperación y mejora continua.
- Personas: equipos especializados organizados por niveles de atención.

Este modelo actuará como un punto central de mando y control para la gestión de eventos e incidentes de seguridad, permitiendo una operación continua, coordinada, medible y alineada a las mejores prácticas de la industria.

El modelo operativo deberá contemplar mecanismos de revisión continua, periódica o bajo demanda, análisis de desempeño y mejora continua, alineados a buenas prácticas internacionales de gestión de incidentes.

4 ALCANCE DE LA PROVISIÓN

4.1 Alcance General

Implementación llave en mano de la plataforma de monitoreo y respuesta a incidentes de seguridad de la información, incluyendo como mínimo:

- Provisión e instalación de infraestructura física dedicada (servidores y/o appliances).
- Licencias de software necesarias para la operación integral de la plataforma por tres (3) años, considerando la ingesta diaria de logs entre 200 y 250 GB/día, componentes de recolección, análisis, correlación y soporte técnico del proveedor por una temporalidad igual a la duración de las licencias, que incluye:
 - Mantenimiento correctivo, preventivo y evolutivo de la plataforma.
 - Actualización y ajuste continuo de colectores, agentes y sensores.
- Integración con activos IT, OT y servicios en la nube definidos por YPFB Transporte S.A.

	ESPECIFICACIONES TÉCNICAS		Hojas:3
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- Acompañamiento operativo especializado 24x7x365 durante el periodo contractual de un (1) año, que se contabiliza a partir de la puesta en producción de la plataforma, que incluye principalmente los siguientes entre otros detallados en el presente documento:
 - Afinamiento permanente de reglas, casos de uso y procedimientos automatizados
 - Monitoreo y respuesta continua a alertas de seguridad.

YPFB TRANSPORTE S.A. contará con acceso y custodia compartida con el proveedor para el control administrativo de la plataforma, la cual permanecerá accesible y administrable por el personal designado de YPFB Transporte S.A.

4.2 Propiedad de los activos

Todos los equipos, appliances, licencias (licencias tipo suscripción), componentes de software y elementos tecnológicos provistos pasarán a ser propiedad exclusiva de YPFB Transporte S.A., debiendo ser inventariados como activos institucionales conforme a la normativa interna vigente.

4.2.1 Propiedad y custodia de la información

Toda la información generada, recolectada, procesada o almacenada por la plataforma —incluyendo logs, eventos, reglas de correlación, casos de uso, playbooks, configuraciones, reportes, indicadores y documentación técnica— será propiedad exclusiva de YPFB Transporte S.A.

Los datos permanecerán alojados físicamente en infraestructura instalada en los centros de datos de YPFB Transporte S.A., permitiendo realizar el análisis de metadatos en la nube.

El proveedor no podrá retener, replicar, utilizar ni almacenar información institucional fuera del entorno autorizado, salvo autorización expresa y documentada.


4.2.2 Continuidad Operativa y Garantía de Licenciamiento

El proveedor deberá garantizar la vigencia continua del licenciamiento durante todo el periodo contractual, incluyendo renovaciones oportunas, soporte del fabricante y actualizaciones, sin que exista interrupción del servicio.

Cualquier eventualidad relacionada con el fabricante o canal de distribución no eximirá al proveedor de su responsabilidad de mantener operativa la solución conforme a los niveles de servicio establecidos.

4.2.3 Plan de salida y transferencia

En caso de finalización o no renovación del contrato, el proveedor estará obligado a:

	ESPECIFICACIONES TÉCNICAS		Hojas:4
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

1. Entregar exportación íntegra y estructurada de todos los datos históricos.
2. Entregar configuraciones completas, reglas, casos de uso y playbooks.
3. Proporcionar documentación técnica actualizada.
4. Asistir técnicamente durante un periodo mínimo de transición de hasta 60 días.

La finalización del contrato no podrá implicar pérdida, bloqueo o inaccesibilidad de información institucional

4.3 Gobernanza y modelo de responsabilidades

YPFB Transporte S.A. define:

- Políticas de seguridad
- Niveles de severidad finales
- Criterios de escalamiento a Dirección / Legal / Operaciones

El proveedor:

- Ejecuta monitoreo, análisis y respuesta técnica
- Recomienda acciones
- Ejecuta acciones pre-autorizadas (playbooks)

4.3.1 Protocolo de Comunicación de Incidentes con Áreas del Negocio


La solución deberá contemplar un protocolo formal de comunicación de Incidentes de Seguridad que impacten procesos críticos de negocio, el cual deberá integrarse al modelo de gobernanza del servicio.

Este protocolo deberá definir como mínimo:

- Criterios para determinar cuándo un incidente de seguridad tiene impacto en procesos de negocio críticos.
- Clasificación de severidad alineada con el impacto operativo.
- Tiempos máximos de notificación a áreas de negocio.
- Canales formales de comunicación.
- Responsables de emisión y recepción de la comunicación.
- Contenido mínimo del reporte preliminar.

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):

	ESPECIFICACIONES TÉCNICAS		Hojas:5
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

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

2. Incidentes de Severidad Alta (Sev 2)

- Notificación a responsables del área en un plazo máximo de 60 minutos.
- El canal primario deberá ser llamada telefónica directa o medio síncrono equivalente y comunicación vía correo electrónico formal con copia a las partes definidas en la matriz de escalamiento.

3. Incidentes de Severidad Media/Baja (Sev 3)

- Notificación a responsables del área en un plazo máximo de 24 horas.
- Comunicación vía correo electrónico formal con copia a las partes definidas en la matriz de escalamiento.


4. Actualizaciones de Estado

- En incidentes críticos, deberán emitirse actualizaciones periódicas no mayores a 60 minutos, hasta la contención del evento.
- El cierre deberá incluir informe ejecutivo de impacto y lecciones aprendidas.

5. Matriz de Escalamiento

El proveedor deberá trabajar con la entidad contratante en la definición de una matriz de escalamiento que incluya:

- Dirección de TI
- Gerencia de Operaciones

	ESPECIFICACIONES TÉCNICAS		Hojas:6
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

5 CARACTERÍSTICAS DE LA PLATAFORMA

5.1 Inventario de Activos de Integrar y Monitorear

La plataforma deberá permitir la ingesta, normalización, correlación y análisis centralizado de eventos, logs y telemetría provenientes de los activos tecnológicos de YPFB Transporte S.A. detallados a continuación.

El presente listado constituye el alcance mínimo obligatorio de integración y monitoreo, sin perjuicio de que el proveedor deba incorporar otros activos que resulten necesarios para el correcto funcionamiento de la solución.

Adicionalmente, el proveedor deberá considerar dentro del alcance contractual la capacidad de integrar y monitorear una variación de hasta $\pm 10\%$ en la cantidad de activos detallados en la presente sección, sin que ello implique modificaciones contractuales, costos adicionales ni afectación a los niveles de servicio establecidos.

El detalle de los activos tecnológicos que deberán ser monitoreados por la plataforma se encuentra consignado en el **Anexo 2** del presente documento. Dicho anexo será proporcionado a los proponentes a través de canales autorizados, previa presentación de una nota de intención de participación y la suscripción de un Acuerdo de Confidencialidad y No Divulgación (NDA) con YPFB Transporte S.A.

6 CARACTERÍSTICAS DE LA PLATAFORMA DE OPERACIÓN

6.1 Monitoreo Continuo

Supervisión permanente (24x7x365) de redes, sistemas, endpoints y activos IT/OT para identificar, analizar, clasificar y responder ante eventos e incidentes de seguridad en tiempo real.

6.2 Modalidad de Acompañamiento Operativo

Acompañamiento operativo especializado sobre la plataforma instalada **on premise**, con equipos organizados en niveles de atención y tiempos de respuesta definidos por severidad, garantizando:

- Continuidad operativa de la plataforma.
- Cumplimiento de los niveles de servicio (SLA).
- Soporte técnico especializado.
- Mantenimiento y actualización continua de los componentes de la solución.
- Informes formales de monitoreo de seguridad de manera: mensual, semestral, anual o a demanda que incluyan la disponibilidad de la plataforma de seguridad y monitoreo.

	ESPECIFICACIONES TÉCNICAS		Hojas:7
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

En ningún caso este acompañamiento afectará la titularidad, control ni propiedad de los activos por parte de YPFB Transporte S.A.

El acompañamiento operativo no incluye actividades de rediseño de arquitectura, cambios estructurales en la infraestructura productiva, ni implementación de nuevos controles fuera del alcance acordado, salvo aprobación expresa mediante solicitud formal.

6.3 Plataforma Central de Gestión

La plataforma deberá permitir correlación avanzada de eventos, análisis de comportamiento, gestión estructurada de incidentes, ejecución de respuestas manuales y automatizadas, y visualización mediante dashboards operativos y ejecutivos.

6.4 Arquitectura de Recolección y Análisis On Premise

La solución deberá incluir un servidor físico o appliance dedicado, recolección local de telemetría con procesamiento, normalización y priorización, análisis centralizado, almacenamiento conforme a políticas de retención y comunicaciones seguras cifradas.

6.5 Disponibilidad y Continuidad Operativa de la Plataforma de Monitoreo

La plataforma de monitoreo, análisis y respuesta de seguridad de la información deberá garantizar un nivel mínimo de disponibilidad anual del 99,6%, aplicable a todos sus componentes, incluyendo, pero no limitándose a:


- Componentes de recolección e ingesta de eventos.
- Componentes de análisis, correlación y automatización.
- Consolas de administración y visualización.
- Integraciones con activos IT, OT y servicios en la nube.
- Mecanismos de respuesta manual y automatizada.

La arquitectura propuesta deberá contemplar mecanismos de **alta disponibilidad**, tolerancia a fallos y recuperación, de forma que la indisponibilidad de un componente no afecte la operación continua del servicio.

6.6 Características del agente o Collector


El Agente o Collector deberá ser compatible con Sistemas Operativos Windows y Linux descritos en el **Anexo 2**.

Agente liviano, diseñado para operar con un impacto mínimo en el rendimiento del sistema operativo donde sea instalado.

	ESPECIFICACIONES TÉCNICAS		Hojas:8
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- **Consumo de CPU:**
 - Consumo promedio no superior al 5% de CPU en condiciones normales de operación.
 - Consumo máximo no superior al 10% de CPU durante picos de recolección o eventos excepcionales.
- **Consumo de memoria RAM:**
 - Consumo promedio no superior a 300 MB de memoria RAM.
 - Capacidad de operación estable con asignación dinámica de memoria según la carga.
- **Uso de almacenamiento local:**
 - Requerimiento de espacio en disco no superior a 1 GB para instalación y operación con conectividad.
 - Capacidad de almacenamiento temporal (buffer) de eventos en disco para escenarios de pérdida de conectividad, con gestión automática de rotación y limpieza.
- **Recolección continua y en tiempo real** de eventos, logs y telemetría de seguridad provenientes del sistema operativo y aplicaciones soportadas.
- **Ejecución como servicio del sistema**, con inicio automático junto con el sistema operativo y operación desatendida.
- **Comunicación segura con la plataforma central**, mediante protocolos cifrados y autenticación mutua.
- **Gestión centralizada del agente o collector**, permitiendo:
 - Configuración remota de políticas de recolección.
 - Actualización remota del agente.
 - Monitoreo de estado, disponibilidad y versión.
 - Desinstalación remota
- **Tolerancia a fallos**, garantizando el reenvío automático de la información almacenada localmente una vez restablecida la conectividad.
- **Instalación y desinstalación no intrusiva**, sin requerir reinicio del sistema operativo.
- **Despliegue y administración masiva:** El Agente o Collector deberá permitir su despliegue masivo y automatizado en entornos Windows y Linux, mediante herramientas corporativas de administración y gestión de configuración, tales como sistemas de administración centralizada, políticas de dominio, herramientas de orquestación o mecanismos equivalentes.
- **Compatibilidad con entornos físicos, virtualizados y en la nube**, conforme al alcance del servicio descrito en el Anexo 2.
- **Registro de eventos operativos del agente**, incluyendo estado, errores y estadísticas básicas de funcionamiento.

Los valores indicados en los párrafos anteriores podrán variar razonablemente en función de la carga operativa y tipo de activo, debiendo el proveedor justificar técnicamente cualquier desviación.


	ESPECIFICACIONES TÉCNICAS		Hojas:9
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

6.7 Infraestructura de Cómputo On-Premise para Plataforma de Monitoreo

La solución deberá incluir la provisión e implementación de infraestructura física dedicada, instalada en el centro de datos de YPFB Transporte S.A., destinada a soportar la plataforma de monitoreo, análisis y respuesta de seguridad de la información.


La infraestructura propuesta deberá cumplir, como mínimo, con las siguientes características técnicas generales:

Características Generales	
Características	Requerimiento
Marca.	Indicar.
Modelo.	Indicar.
Factor de forma.	Mayor o igual a 1U Rackeable.
Puerto de administración.	Puerto de administración remoto con aprovisionamiento inteligente integrado. El puerto deberá contar con capacidad de administrar los componentes del servidor aun cuando esté apagado. Además, deberá proveer interfaz para asignar medios de almacenamiento como, USB, etc. también deberá almacenar un registro de fallas, enviar notificaciones y alertas de falla de componentes. Integración al directorio activo, y a sistemas SNMP y registro SYSLOG. Se deberá incluir servicio de monitoreo proactivo por el fabricante.
Ventiladores.	Enfriamiento por aire, utilizando ventiladoras de alto rendimiento en modo redundante.
Fuentes de energía.	Fuente de energía en modo redundante, las cuales deberán permitir el reemplazo en caliente (hot-plug).
Cables de energía.	Cables de energía C13 a C14 tipo PDU.
Mecanismos de seguridad	<ul style="list-style-type: none"> • Debe contar con las funcionalidades UEFI Secure Boot y Secure Start support, para así garantizar seguridad en el momento del encendido del equipo. • El chip integrado de seguridad debe de incluir un mecanismo de prevención de suplantación del firmware de la tarjeta principal del servidor como de la tarjetería adicional, además de que este mecanismo debe de ser protegido contra el ransomware (inmutable). El firmware debe de ser digitalmente firmado y verificado con una llave privada que prohíbe el que un firmware no autorizado se ejecute. • El servidor debe incluir la funcionalidad para reestablecer el firmware a una versión correcta conocida en caso de detección de un firmware comprometido. • Debe contar con soporte TPM (Trusted Platform Module) 2.0 resistente a la intromisión.
Integración	<p>El Oferente deberá garantizar la integración del equipamiento propuesto con la infraestructura de redes LAN existente en YPFB TRANSPORTE S.A.:</p> <ul style="list-style-type: none"> • LAN: Cisco NEXUS 9000 conectividad 8 puertos 10 Gbps.


	ESPECIFICACIONES TÉCNICAS		Hojas:10
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

Sistemas operativos soportados	<ul style="list-style-type: none"> • Proporcionar licenciamiento del sistema operativo y soporte, siendo este homologado para la solución propuesta
Garantía y soporte del fabricante.	<ul style="list-style-type: none"> • Garantía del fabricante con cobertura para reemplazo de partes, con duración de 3 años, bajo la modalidad 24x7. • La garantía del fabricante debe contemplar Soporte técnico incluyendo stock de partes en Bolivia, para el reemplazo de las mismas tras haber sido diagnosticada la falla completa del componente o equipo. • La marca ofertada deberá contar con al menos dos canales certificados con presencia en Santa Cruz. • La marca ofertada deberá contar con al menos dos técnicos certificados por fabricante. • El proponente deberá estar a cargo del mantenimiento preventivo y correctivo del equipamiento ofertado, durante la duración de garantía del fabricante, incluyendo la actualización, parches de seguridad del sistema operativo y firmware de todos componentes. • El proponente deberá incluir un cronograma donde se detalle el mantenimiento preventivo anual del equipo ofertado.
Servicios y soporte del fabricante	Servicio de Instalación y startup del equipamiento ofertado a cargo de personal especializado por parte del fabricante.
Documentación y entregables	<p>Diagramas de conexión a red LAN del equipamiento entregado. Diagrama del equipo a ser entregados (Front/Back). Diagrama de componentes internos del servidor o equipamiento solicitado. Diagrama lógico de configuración del servidor o equipamiento solicitado. Documentación técnica completa y manual de apertura de casos. Listado de licencias o suscripciones que deben estar asociadas a una cuenta de administración de YPFB TRANSPORTE S.A.</p>
Responsabilidad del proveedor	El proveedor debe de dimensionar, justificar y garantizar cumplimiento de desempeño, disponibilidad, retención y escalabilidad del equipamiento ofertado.

Características técnicas		
Descripción	Cantidad	Características
Procesador	Indicar	<ul style="list-style-type: none"> • Detallar marca, modelo y capacidad. • Capacidad para recolección, normalización y correlación sin degradación. • Crecimiento orgánico mínimo del 3% anual sin reemplazo del equipo.
Memoria RAM	Indicar	<ul style="list-style-type: none"> • Detallar marca, modelo y capacidad. • Los módulos deberán contar mecanismos de tolerancia rápida de fallas que permitan detectar y corregir errores de memoria antes que estos impacten en el sistema. • Memoria dimensionada para análisis en tiempo real y correlación de eventos.

	ESPECIFICACIONES TÉCNICAS		Hojas:11
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

		<ul style="list-style-type: none"> Capacidad ampliable según dimensionamiento del proveedor.
Network	Indicar	<ul style="list-style-type: none"> Detallar marca, modelo y capacidad. Se deberá incluir sus correspondientes trancivers SPF+ de tipo Short Range. Interfaces de red redundantes. Soporte para segmentación lógica y transmisión cifrada.
Storage	Indicar	<ul style="list-style-type: none"> Discos de tipo SSD mínimamente destinado para el Sistema Operativo del servidor. Detallar marca, modelo y capacidad. Discos de tipo Read Intensive Soporte para tolerancia a fallos y redundancia a nivel de discos. Capacidad dimensionada, considerando RAID 1 para discos de Sistema Operativo.
	Indicar	<ul style="list-style-type: none"> Discos de tipo 10K SAS mínimamente destinado para el almacenamiento de logs. Detallar marca, modelo y capacidad. Discos orientados a cargas intensivas de lectura/escritura de logs. Esquema recomendado: RAID 5 para almacenamiento de logs. Soporte para tolerancia a fallos y redundancia a nivel de discos. Capacidad dimensionada para retención mínimamente de seis (6) meses, en arreglo RAID 5 para almacenamiento de logs.
	1	<p>Controladora de Arreglo de Discos. Soportando discos rotacionales y discos de estado sólido.</p> <p>Con capacidad de crear arreglos tipo: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10.</p> <p>Deberá tener todas las funcionalidades habilitadas y/o licenciadas, incluyendo: Capacidad de Expansión en línea, Capacidad de Migración de arreglos en Línea, Utilización de discos de estado sólido como Cache, Creación de arreglos de discos RAID con discos rotacionales y discos de estado sólido, hot-spare global y dedicado a cada arreglo. Reconstrucción automática de arreglos.</p>
Puertos de Comunicación	Indicar	Puertos compatibles con estándar USB 3.0
Puerto de administración	1	Interfaz de red 100/1000 Base-T o Superior, dedicada exclusivamente a la administración remota del servidor. La cual deberá permitir Acceso mediante Interfaz web, incluyendo programación compatible con RESTful API.

	ESPECIFICACIONES TÉCNICAS		Hojas:12
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

Otros Componentes	1	Modulo Trusted Platform Module de Generación 2.0
	2	Cables de Energía Eléctrica de tipo C13 - C14, con capacidad de 250V 10Amp, de 3.0m de largo.
	1	Kit Para Rackeado del Servidor, en base a rieles deslizables con soporte de rodamientos.

7 DIMENSIONAMIENTO TÉCNICO REFERENCIAL

El presente dimensionamiento tiene carácter referencial y técnico, y tiene como objetivo establecer los parámetros mínimos que deberán ser considerados por los proponentes para el correcto diseño, provisión e implementación de la plataforma.

Los valores indicados no constituyen compromisos comerciales, sino lineamientos técnicos base, debiendo cada proveedor validar y ajustar su propuesta conforme a la arquitectura final propuesta.

7.1 Supuestos Generales

- La plataforma deberá operar en modalidad 24x7x365.
- El dimensionamiento deberá considerar eventos provenientes de entornos IT, OT y nube.
- Se deberá contemplar un crecimiento orgánico mínimo del 3% anual en volumen de eventos y activos monitoreados.
- La arquitectura deberá permitir escalabilidad horizontal y/o vertical, sin afectar la continuidad operativa ni la integridad de los datos.

7.2 Parámetros Técnicos de Referencia

Componente	Parámetro Técnico	Valor Referencial	Consideraciones Técnicas
Recolección de eventos	Eventos por segundo (EPS) sostenidos	≥ 10.000 EPS	Capacidad sostenida, no pico. Debe soportar ráfagas sin pérdida de eventos.
Recolección de eventos	Eventos por segundo (EPS) pico	≥ 20.000 EPS	Asociado a incidentes, escaneos o eventos masivos.
Volumen de logs	Ingesta diaria estimada	≥ 200 GB/día	Incluye red, seguridad, servidores, OT y nube.
Volumen de logs	Retención en línea	≥ 90 días	Almacenamiento activo para análisis e investigación.
Volumen de logs	Retención histórica	≥ 6 meses	Archivo para investigación forense y cumplimiento.
Activos monitoreados	Activos IT / OT / Nube	≥ 1.500 activos	Dispositivos de red, servidores, endpoints, OT y servicios cloud.

	ESPECIFICACIONES TÉCNICAS		Hojas:13
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

Componente	Parámetro Técnico	Valor Referencial	Consideraciones Técnicas
Endpoints	Equipos finales	≥ 1.200 endpoints	Cobertura actual con crecimiento anual.
Automatización	Procedimientos automatizados	≥ 10 flujos	Flujos operativos ampliables.
Disponibilidad	Plataforma central	≥ 99,6%	Alta disponibilidad lógica y de servicios.
Seguridad	Cifrado de comunicaciones	TLS 1.3 o superior	Entre todos los componentes de la arquitectura.

El volumen diario estimado de ingesta se sitúa en un rango de 200 a 250 GB/día, dependiendo del nivel de verbosidad, fuentes activas y casos de uso habilitados.

La retención histórica podrá implementarse en almacenamiento de menor costo (tiered storage), siempre que garantice integridad, trazabilidad y tiempos de recuperación aceptables para análisis forense en la Infraestructura de YPFB Transporte S.A.

7.3 Escalabilidad y Evolución

La solución deberá permitir:

- Incrementar la capacidad de procesamiento (EPS) sin reinstalaciones completas.
- Ampliar almacenamiento manteniendo integridad y trazabilidad de datos históricos.
- Incorporar nuevos tipos de activos, fuentes de eventos y casos de uso.
- Ajustar políticas de retención conforme a requerimientos regulatorios futuros.

8 NIVELES DE ATENCIÓN y PERSONAL TÉCNICO CERTIFICADO

El proveedor deberá garantizar que el personal asignado a cada nivel de atención cuente con formación, experiencia y/o certificaciones en ciberseguridad acordes a la complejidad de las funciones desempeñadas, conforme al siguiente esquema referencial:

- **Nivel 1: Monitoreo y primera respuesta.**

Funciones:

- Monitoreo continuo de eventos de seguridad
- Triage inicial de alertas

	ESPECIFICACIONES TÉCNICAS		Hojas:14
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- Clasificación y escalamiento

Certificaciones requeridas (Nivel Intermedio):

- Certificaciones de nivel intermedio en ciberseguridad, tales como:
 - CEH (Certified Ethical Hacker) o equivalentes
 - Certificaciones intermedias en seguridad de la información o redes
- Conocimiento en:
 - Análisis básico de logs
 - Identificación de eventos de seguridad
 - Procedimientos de escalamiento

• Nivel 2: Análisis y correlación avanzada.

Funciones:

- Investigación de eventos de seguridad
- Correlación de eventos
- Análisis técnico de incidentes


Certificaciones requeridas (Nivel Avanzado):

- Certificaciones de nivel avanzado en ciberseguridad, tales como:
 - CEH (nivel avanzado o especializado)
 - Certificaciones alineadas a ISO/IEC 27001 (es válido certificados de cursos de aprobación de IBNORCA) o Framework NIST
 - Certificaciones técnicas del fabricante de la solución (altamente valoradas)
- Conocimientos en:
 - Análisis de incidentes
 - Correlación de eventos complejos
 - Técnicas de respuesta a incidentes

• Nivel 3: Gestión de incidentes críticos, análisis forense y ciberinteligencia.

Funciones:

- Gestión de incidentes críticos
- Análisis forense digital
- Coordinación de respuesta a nivel organizacional

	ESPECIFICACIONES TÉCNICAS		Hojas:15
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- Toma de decisiones técnicas

Certificaciones requeridas (Nivel Experto):

- Certificaciones de nivel experto en ciberseguridad, tales como:
 - CISSP (Certified Information Systems Security Professional)
 - CISM (Certified Information Security Manager)
 - OSCP (Offensive Security Certified Professional) u otras equivalentes
- Experiencia comprobada en:
 - Gestión de incidentes complejos
 - Análisis forense
 - Coordinación con áreas técnicas y de negocio

9 NIVEL DE SERVICIO (SLA)


El servicio deberá cumplir como mínimo con los siguientes niveles de severidad y tiempos máximos, medidos desde la detección del evento:

Severidad	Descripción	Notificación Inicial	Actualización
Nivel 1 – Crítico	Compromiso activo, ransomware, exfiltración, impacto operacional	≤ 15 minutos	Cada 30 minutos
Nivel 2 – Alto	Amenaza activa sin impacto confirmado	≤ 30 minutos	Cada 1 hora
Nivel 3 – Medio	Actividad sospechosa validada	≤ 60 minutos	Cada 2 horas
Nivel 4 – Bajo	Eventos informativos	≤ 4 horas	Bajo demanda

Se deberán medir indicadores como MTTD y MTTR, siendo su cumplimiento obligatorio durante toda la vigencia contractual.

9.1 Disponibilidad de la Plataforma

El proveedor deberá garantizar un SLA mínimo de disponibilidad anual del 99,6 % para la plataforma en su conjunto y para cada uno de sus componentes críticos.

	ESPECIFICACIONES TÉCNICAS		Hojas:16
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

La disponibilidad será medida sobre una base anual, considerando la operación continua 24x7x365, y las ventanas de mantenimiento deberán ser previamente coordinadas y aprobadas por YPFB Transporte S.A.

Cualquier indisponibilidad que afecte la recolección, análisis, correlación, visualización o ejecución de respuestas deberá ser registrada, notificada y considerada para el cálculo del SLA correspondiente.

La suspensión o expiración del licenciamiento por causas atribuibles al proveedor será considerada incumplimiento grave contractual.

El incumplimiento del SLA de disponibilidad será considerado como incumplimiento de niveles de servicio, sujeto a las medidas contractuales que correspondan.

9.2 Personal de monitoreo, análisis y respuesta

El proveedor deberá garantizar que el personal asignado cuente con certificaciones vigentes y/o experiencia equivalente, alineadas al nivel de atención requerido (intermedio, avanzado y experto) del **punto 8** del presente documento, pudiendo presentar certificaciones equivalentes reconocidas en la industria.

10 AUTOMATIZACIÓN Y PROCEDIMIENTOS OPERATIVOS

La solución deberá soportar procedimientos operativos estandarizados de respuesta, ejecutables de forma automática o asistida, con capacidad de ampliación conforme a nuevas amenazas o necesidades operativas.

10.1 Casos de usos mínimos de monitoreo, detección y respuesta


La plataforma deberá implementar, como mínimo obligatorio, un conjunto de casos de uso funcionales que permitan detectar, analizar, responder y mejorar la postura de seguridad de YPFB Transporte S.A., considerando la criticidad de su infraestructura IT, OT y entornos híbridos.

Los casos de uso deberán operar de forma integrada, correlacionando eventos provenientes de múltiples fuentes, y deberán ser parametrizables, auditables y ampliables durante la vigencia contractual.

El proveedor deberá realizar revisiones periódicas de los casos de uso implementados, ajustando reglas para reducción de falsos positivos y mejora de precisión.

10.1.1 Casos de Uso sobre Perímetro y Red

1. Actividad y estado de accesos remotos (*Detect / Respond*)
 - Monitoreo de sesiones activas.
 - Análisis de geolocalización y patrones anómalos.

	ESPECIFICACIONES TÉCNICAS	Hojas:17
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026	
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua	

- Detección de fallos de conexión y autenticación.
- 2. Eficacia de controles perimetrales y políticas de seguridad (*Detect*)
 - Identificación de bloqueos por motores de seguridad.
 - Evaluación de la efectividad de reglas y políticas.
 - Detección de configuraciones ineficientes o permisivas.
- 3. Tráfico interno y movimiento lateral (*Detect*)
 - Análisis de tráfico este-oeste.
 - Detección de movimientos laterales y anomalías entre segmentos de red.

10.1.2 Casos de Uso sobre Aplicaciones y Servicios Expuestos


1. Superficie de ataque de aplicaciones web (*Detect / Respond*)
 - Detección de ataques alineados a OWASP Top 10.
 - Identificación y reducción de falsos positivos.
2. Eventos de denegación de servicio distribuida (DDoS) (*Respond*)
 - Monitoreo de volumetría de ataques.
 - Medición de tiempos de mitigación y efectividad de respuesta.

10.1.3 Casos de Uso sobre Endpoints

1. Visión global y estado de salud de endpoints (*Detect / Respond*)
 - Clasificación de endpoints por severidad.
 - Detección de comportamientos maliciosos.
 - Ejecución de acciones de aislamiento y contención.
2. Indicadores de ransomware y preparación para recuperación (*Respond / Recover*)
 - Identificación temprana de comportamientos asociados a ransomware.
 - Evaluación de la capacidad de recuperación ante incidentes.

10.1.4 Casos de Uso sobre Identidades y Directorios

1. Actividad de autenticación fallida (*Detect*)
 - Detección de intentos fallidos reiterados.
 - Identificación de origen y usuarios objetivo.
2. Uso de credenciales privilegiadas (*Detect / Respond*)
 - Detección de cambios de privilegios.
 - Identificación de accesos fuera de horario o patrón normal.
3. Abuso de replicación y servicios de directorio (*Detect*)

	ESPECIFICACIONES TÉCNICAS		Hojas:18
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- Detección de técnicas de replicación maliciosa.
- Identificación de modificaciones no autorizadas de políticas.

4. Identidades gestionadas y registros de sesión (*Detect / Respond*)

- Monitoreo de identidades administradas.
- Trazabilidad de sesiones y accesos.

10.1.5 Casos de Uso de Inteligencia de Amenazas

1. Indicadores de compromiso (IOC) y tiempo de bloqueo (*Detect / Improve*)

- Correlación de IOC internos y externos.
- Medición del tiempo desde detección hasta bloqueo efectivo.

10.1.6 Casos de Uso sobre Virtualización e Infraestructura

1. Eventos de seguridad y permisos en entornos de virtualización (*Detect*)

- Monitoreo de cambios de permisos y accesos.
- Detección de eventos críticos en plataformas de virtualización.

2. Operaciones sensibles en máquinas virtuales y almacenamiento (*Detect*)

- Detección de acciones críticas sobre datastores y VMs.

3. Salud de infraestructura de cómputo y red (*Detect*)

- Monitoreo de eventos críticos de servidores, red y plataformas base.

10.1.7 Casos de Uso sobre Tecnología Operativa (OT)

1. Anomalías de red OT y monitoreo de comandos industriales (*Detect*)

- Identificación de tráfico anómalo en redes OT.
- Monitoreo de comandos y operaciones críticas en equipos industriales.

10.1.8 Casos de Uso sobre Sistemas Operativos


1. Eventos de seguridad y cumplimiento de parches en sistemas Linux (*Protect / Detect*)

- Detección de eventos de seguridad relevantes.
- Verificación del cumplimiento de parches y configuraciones base.

10.1.9 Casos de Uso de Gestión y Mejora Continua

1. Indicadores de desempeño y ciclo de vida de incidentes (*Improve*)

- Medición de MTTD (Mean Time to Detect) y MTTR (Mean Time to Respond).
- Análisis del ciclo completo de los incidentes bajo el enfoque Detect–Respond–Recover.

	ESPECIFICACIONES TÉCNICAS		Hojas:19
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

2. Visión integral y amenazas ocultas (*Detect / Improve*)

- Correlación cruzada entre eventos de red, endpoints, identidades, aplicaciones y OT.
- Identificación de amenazas no evidentes en análisis aislados


10.2 Procedimientos automatizados y orquestados de respuesta (Playbooks)

La plataforma deberá contar con capacidades de automatización y orquestación de respuestas, permitiendo la ejecución de procedimientos estandarizados, tanto de forma automática como asistida, orientados a reducir los tiempos de detección, contención, erradicación y recuperación ante incidentes de seguridad.

Estos procedimientos, en adelante denominados Playbooks, deberán ser configurables, auditables, versionables y ampliables, y deberán integrarse con los distintos componentes tecnológicos de la organización, sin dependencia de marcas específicas.


El proveedor deberá implementar, como **mínimo obligatorio**, los siguientes **Playbooks de respuesta**:

1. Respuesta a Ransomware
 - Desconexión masiva de activos afectados.
 - Bloqueo de canales de comando y control (C2).
 - Acompañamiento y coordinación en la restauración desde respaldos seguros.
 - Análisis forense posterior al incidente.
2. Investigación de Alertas de Seguridad
 - Correlación automática de eventos.
 - Enriquecimiento con inteligencia de amenazas.
 - Clasificación y priorización por severidad.
3. Bloqueo de IP o Dominio Malicioso
 - Actualización automática de controles perimetrales.
 - Bloqueo en servicios de protección de aplicaciones y listas de denegación.
 - Registro y trazabilidad de la acción ejecutada.
4. Respuesta a Compromiso de Credenciales
 - Deshabilitación/Bloqueo inmediata de cuentas comprometidas.
 - Restablecimiento de factores de autenticación.
 - Revocación de tokens y cierre de sesiones activas.
5. Análisis de Archivos Sospechosos
 - Envío automatizado o asistido de archivos a entornos de análisis controlados (sandbox), ya sea mediante capacidades propias de la solución o integración con herramientas externas.
 - Ejecución de análisis estático y dinámico para la identificación de comportamiento malicioso.
 - Obtención de indicadores de compromiso (IOC) derivados del análisis realizado.
 - Correlación de resultados con eventos de seguridad existentes en la plataforma.

	ESPECIFICACIONES TÉCNICAS	Hojas:20
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026	
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua	

- Bloqueo, cuarentena o eliminación de artefactos maliciosos identificados, conforme a las políticas definidas.
- 6. Respuesta a Ataques de Denegación de Servicio (DDoS)
 - Activación de mecanismos de mitigación.
 - Aplicación de bloqueos geográficos o por dirección IP.
 - Monitoreo de la efectividad de la mitigación.
- 7. Investigación de URL Sospechosa
 - Expansión y detonación controlada de enlaces.
 - Verificación reputacional.
 - Bloqueo preventivo en servicios de navegación y acceso.
- 8. Respuesta a Alertas de Endpoint
 - Aislamiento del equipo afectado.
 - Remediación automática.
 - Validación de limpieza y cierre del incidente.
- 9. Explotación de Vulnerabilidad Crítica
 - Generación automática de ticket de incidente.
 - Coordinación para aplicación de medidas de mitigación o parches urgentes.
 - Confirmación de corrección.
- 10. Movimiento Lateral Detectado
 - Aislamiento del equipo afectado.
 - Cierre de puertos y servicios comprometidos a nivel de Firewalls.
 - Análisis de conexiones sospechosas.
- 11. Exfiltración de Datos
 - Cuarentena de transferencias.
 - Bloqueo de canales de salida no autorizados.
 - Notificación a las áreas de cumplimiento correspondientes.
- 12. Anomalías de Autenticación (Viajero Imposible)
 - Deshabilitación preventiva de cuentas.
 - Generación de alertas.
 - Correlación con otros eventos de seguridad.
- 13. Compromiso en Infraestructura OT / HMI
 - Aislamiento seguro de activos OT.
 - Análisis de comandos y operaciones ejecutadas.
 - Coordinación de restauración controlada de la operación.
- 14. Incidente en Infraestructura de Energía o UPS
 - Validación de continuidad operativa.
 - Registro y seguimiento del incidente.

La ejecución automática de playbooks que impliquen impacto operacional deberá contar con aprobación previa de YPFB Transporte S.A., salvo aquellos explícitamente definidos como de ejecución automática.”

	ESPECIFICACIONES TÉCNICAS		Hojas:21
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

11 TRANSFERENCIA DE CONOCIMIENTO

Se requerirá certificación para personal (3 personas) de YPFB Transporte S.A. La transferencia de conocimiento deberá incluir: Administración de la plataforma, creación/modificación de reglas de correlación, actualización de playbooks de automatización, resolución de problemas comunes entre otros.

La transferencia deberá garantizar que el personal YPFB Transporte S.A. pueda administrar la plataforma de manera autónoma al término del contrato.

11.1 Participación en eventos técnicos del fabricante

Con el objeto de facilitar la adecuada adopción, operación y optimización de la solución tecnológica ofertada, el proponente deberá incluir cupos de participación en eventos técnicos organizados por el fabricante de la tecnología propuesta, orientados a la transferencia de conocimiento sobre administración, configuración y mejores prácticas asociadas a la solución.

Esta participación tiene como finalidad facilitar la adopción de mejores prácticas del fabricante y optimizar la operación de la solución implementada, como parte del acompañamiento técnico asociado a la provisión de la tecnología.


Dicha participación deberá cumplir las siguientes condiciones:

- Los cupos podrán ser utilizados en cualquier momento mientras se encuentre vigente el soporte de los equipos y software incluidos en el presente proceso.
- La participación deberá realizarse en seminarios, foros técnicos, programas de actualización tecnológica o eventos equivalentes organizados directamente por el fabricante de la solución ofertada, en las ubicaciones que éste disponga.
- La propuesta deberá contemplar la participación de al menos dos (2) representantes de YPFB TRANSPORTE S.A. en el evento descrito en el inciso anterior.
- El proponente deberá cubrir todos los gastos asociados a la participación, incluyendo inscripción al evento, transporte, alojamiento, alimentación y cualquier otro gasto logístico necesario.

La designación de los participantes, definición de fechas y coordinación logística será realizada con el responsable del proyecto designado por YPFB TRANSPORTE S.A. y podrá ejecutarse en cualquier momento posterior a la adjudicación y durante la vigencia del soporte de la solución.

12 OTRAS BUENAS PRÁCTICAS

Además de los requisitos explícitos, el proveedor deberá aplicar otras buenas prácticas reconocidas de la industria, considerando la criticidad de la infraestructura, la operación continua, la cantidad de activos y una

	ESPECIFICACIONES TÉCNICAS		Hojas:22
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

dotación superior a 1.000 empleados, alineadas a ISO/IEC 27001, NIST CSF, MITRE ATT&CK, ITIL y prácticas empresariales consolidadas.

13 PLAZOS, ACEPTACIÓN Y PAGOS

13.1 Plazos y vigencia

Implementación completa bajo **modalidad llave en mano** en un máximo de ciento veinte (120) días calendario desde la orden de proceder, conforme el alcance descrito en el **punto 4. Alcance de la provisión** del presente documento.

A partir de la puesta en producción, **la gestión operativa continua** de la Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información de YPFB Transporte S.A. tendrá una vigencia de doce (12) meses por parte de la empresa proveedora de la mencionada plataforma.

13.2 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 validar instalación, configuración, operación y desempeño de la plataforma gestionada. Las siguientes son pruebas requeridas:


- Health Check “estado de salud” ejecutado por el fabricante de acuerdo a las buenas prácticas.
- Pruebas de instalación y desinstalación del agente colector, 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)

13.2.1 Pruebas de Aceptación Funcional (UAT)

Además de las pruebas técnicas de instalación, rendimiento y disponibilidad, el proveedor deberá ejecutar Pruebas de Aceptación Funcional (UAT) orientadas a validar el cumplimiento de los objetivos operativos y de negocio para los cuales fue implementada la plataforma.

Estas pruebas deberán realizarse bajo un enfoque de “**caja negra**”, verificando el comportamiento integral de la solución ante escenarios simulados de seguridad.

Las pruebas deberán contemplar como mínimo:

	ESPECIFICACIONES TÉCNICAS		Hojas:23
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

- Simulación controlada de eventos de seguridad sobre sistemas críticos definidos por la entidad.
Verificación de:
 - Generación correcta de alertas.
 - Visualización en el tablero de monitoreo.
 - Clasificación automática según severidad.
 - Activación de reglas de correlación.
 - Ejecución de playbooks o flujos de respuesta configurados.
 - Registro de evidencias y trazabilidad del evento.
- Validación de tiempos de detección y respuesta conforme a los SLA establecidos.
- Confirmación de que las notificaciones y mecanismos de escalamiento se ejecutan conforme al modelo de gobernanza definido.


La aceptación final de la plataforma estará condicionada al resultado satisfactorio de estas pruebas.

13.3 Pagos

Pago se realizará un solo pago de acuerdo al siguiente detalle:

Hito	Descripción de avance del servicio	Porcentaje de pago por el servicio	Entregable
1	Provisión e instalación de infraestructura física dedicada (servidores y/o appliances), licencias de software necesarias para la operación integral de la plataforma por tres (3) años, considerando la ingesta diaria de logs entre 200 y 250 GB/día y acompañamiento operativo especializado 24x7x365 durante el periodo contractual de un (1) año.	100%	<ul style="list-style-type: none"> ▪ Contra entrega de informe de implementación y funcionamiento correcto de la Plataforma con gestión operativa continua


Elaborado Por: Nombre: Renán Luis Layme Yucra Cargo: Especialista de Seguridad de la Información	Elaborado Por: Nombre: Edith Vera Cargo: Especialista de Seguridad de la Información
---	---

	ESPECIFICACIONES TÉCNICAS		Hojas:24
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

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 dos (2) años. 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 del fabricante o de partners certificados oficialmente por este, debidamente acreditados, 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 de gestión operativa continua de Plataforma de Seguridad y Monitoreo.
 - 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 documento 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 de la plataforma de monitoreo ofertada.
 - e. Contar con un (1) administrador del proyecto que acompañe toda la implementación de la plataforma de monitoreo hasta su puesta en producción.
 - f. En referencia al punto d). 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 antigüedad por lo menos de un (1) año en la empresa a cargo de proyectos de similar naturaleza.
 - g. 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

	ESPECIFICACIONES TÉCNICAS		Hojas:25
	PROYECTO: Implementación de controles de ciberseguridad 2025 - 2026		
	TITULO: Especificaciones Técnicas para Adquisición de Plataforma de Monitoreo, Análisis y Respuesta de Seguridad de la Información con Gestión Operativa Continua		

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 tres (3) 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 3 años:
 - a. Por lo menos dos (2) implementaciones 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 de la plataforma de monitoreo de seguridad ofertada.
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.