



TÉRMINOS DE REFERENCIA

ACTUALIZACIÓN MANAGEENGINE ENDPOINT CENTRAL ENTERPRISE A SECURITY EDITION

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.

TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
ANTECEDENTES DEL PROYECTO	4
OBJETIVO	4
2. ALCANCE DEL SERVICIO	5
2.1. Licenciamiento	5
2.2. Alcance funcional mínimo	6
2.3. Alcance Implementación	7
2.4. Requisitos Funcionales Obligatorios, donde se exige explícitamente que la solución permita:.....	7
2.5. Consideraciones especiales para activos de control industrial (OT/HMIs).	8
3. PROVISIÓN E IMPLEMENTACIÓN	9
3.1. IMPLEMENTACIÓN.....	9
3.2. PROCEDIMIENTO DE COMUNICACIÓN	9
3.3. EQUIPO DE TRABAJO Y REQUISITOS DEL PERSONAL	9
3.4. PROVISIÓN DE LICENCIAS Y COMPONENTES	9
4. GARANTÍA Y SOPORTE TÉCNICO	10
4.1. Garantía de la Implementación.....	10
4.2. Soporte Técnico Post Implementación	10
4.3. Bolsa de Horas de Consultoría	11
5. PRUEBAS DE ACEPTACIÓN.....	12
5.1. Administración de Equipos	12
5.2. Gestión de Vulnerabilidades.....	12
5.3. OS Deployment.....	12
5.4. Application Control y Endpoint Privilege Management.....	12
5.5. Device Control	12
5.6. MDM	12
5.7. Patch Management.....	12
5.8. Failover	13
5.9. Integraciones	13
5.10. BitLocker Management.....	13
5.11. Reportes y Dashboard.....	13

6. DOCUMENTACIÓN DEL PROYECTO	13
6.1. DOCUMENTACIÓN PARA LA PROPUESTA	13
6.2. DOCUMENTACIÓN TÉCNICA FINAL DEL PROYECTO	14
6.3. ACCESO A MEJORES PRÁCTICAS	14
7. LUGAR DE ENTREGA	15
8. PLAZOS DE ENTREGA	15
9. PRESENTACIÓN DE PROPUESTAS.....	15
10. PAGOS.....	15

1. INTRODUCCIÓN

ANTECEDENTES DEL PROYECTO

YPFB TRANSPORTE S.A. (en adelante YPFBTR), en el marco de su estrategia de transformación digital y mejora continua de la gestión de activos tecnológicos, cuenta actualmente con herramientas destinadas a la administración de estaciones de trabajo y equipos portátiles corporativos.

Como parte de las iniciativas orientadas a fortalecer la ciberseguridad, la continuidad operativa, el cumplimiento normativo y la protección de la información corporativa, se ha identificado la necesidad de consolidar en una única plataforma especializada las capacidades de administración, automatización y gestión de los equipos clientes de la organización.

La creciente sofisticación de las amenazas informáticas, la necesidad de asegurar el cumplimiento de las políticas corporativas de seguridad, el control del cifrado de información, la gestión de privilegios locales y la automatización de despliegues operativos hacen necesaria la adopción de una solución integral que permita mejorar la visibilidad, gobernanza y protección de los endpoints corporativos y de control.

En este contexto, YPFBTR ha definido la implementación de la solución **ManageEngine Endpoint Central Security Edition**, con el propósito de fortalecer la gestión de equipos clientes mediante funcionalidades avanzadas de seguridad, control de configuraciones, administración del ciclo de vida de dispositivos, protección de datos y automatización operativa, en concordancia con las mejores prácticas internacionales de gestión de Tecnologías de Información y Seguridad de la Información.

OBJETIVO

Actualizar la versión **ManageEngine Endpoint Central Enterprise Edition** a la solución **ManageEngine Endpoint Central Security Edition** para optimizar la administración, seguridad y cumplimiento de los equipos clientes de YPFB Transporte S.A., permitiendo centralizar las capacidades de gestión, automatización y protección de estaciones de trabajo y equipos portátiles corporativos.

La implementación deberá permitir:

Objetivos específicos

1. Fortalecer la postura de seguridad de los equipos clientes mediante la gestión centralizada de vulnerabilidades y configuraciones de seguridad.
2. Implementar mecanismos de cifrado de discos utilizando BitLocker, incluyendo la administración centralizada de claves de recuperación y cumplimiento de políticas corporativas.

3. Automatizar el despliegue y recuperación de sistemas operativos mediante funcionalidades de OS Deployment para reducir tiempos de aprovisionamiento y recuperación ante incidentes.
4. Incrementar la visibilidad y trazabilidad de eventos relacionados con la seguridad y administración de los endpoints.
5. Fortalecer el cumplimiento de estándares corporativos mediante la aplicación automática de configuraciones seguras y remediación de desviaciones.
6. Optimizar la gestión del ciclo de vida de los equipos mediante procesos automatizados de configuración, actualización y mantenimiento.
7. Reducir los riesgos operativos asociados a software desactualizado, configuraciones inseguras y extravío de información corporativa.
8. Transferir el conocimiento al personal técnico de YPFBTR para la administración integral de la plataforma.

2. ALCANCE DEL SERVICIO

La propuesta deberá contemplar la provisión, implementación, configuración y puesta en producción de la solución ManageEngine Endpoint Central Security Edition para la administración y protección de equipos clientes corporativos.

2.1. Licenciamiento

La propuesta deberá incluir como mínimo:

Descripción	Cantidad
ManageEngine Endpoint Central Security Edition – Suscripción anual de 200 licencias adicionales para endpoints (Total 1000) endpoints, prorrateado hasta el 28 de junio 2028.	200
Upgrade ManageEngine Endpoint Central Enterprise a ManageEngine Security Edition – Suscripción anual para 1000 endpoints (Total 1000) endpoints, prorrateado hasta el 28 de junio 2028.	1000
Upgrade ManageEngine Endpoint Central de Endpoint a Security Edition – Suscripción anual para Servicio de Fail Over para 1000 endpoints (Parque total resultante:1000) endpoints, prorrateado hasta el 28 de junio 2028.	1000
Servicio profesional llave en mano para Instalación/Implementación, Configuración, Ajustes de optimización, Migración y Transferencia de conocimientos	1
40 horas de Soporte Técnico Especializado durante la vigencia de la licencia (Hasta 28 de junio 2028).	40 horas

2.2. Alcance funcional mínimo

La implementación deberá considerar la habilitación y configuración de los siguientes módulos:

- **Administración y Seguridad**
 - Patch Management.
 - Vulnerability Management.
 - Security Configuration Management.
 - Browser Security.
 - Compliance Management.
 - Elevación controlada de aplicaciones.
 - Auditoría de privilegios.
- **Protección de Información**
 - BitLocker Management.
 - Administración de claves de recuperación.
 - Monitoreo de cumplimiento de cifrado.
 - Reportes de estado de protección.
- **Control de Aplicaciones**
 - Application Control.
 - Lista blanca y lista negra de aplicaciones.
 - Control de software no autorizado.
 - Gestión de aplicaciones corporativas.
- **Control de Dispositivos**
 - Device Control.
 - Gestión de puertos USB.
 - Control de almacenamiento removable.
 - Políticas de acceso por grupos.
- **Gestión de Privilegios**
 - Endpoint Privilege Management.
 - Eliminación de privilegios administrativos permanentes.
- **Automatización y Despliegue**
 - OS Deployment.
 - Creación de imágenes corporativas.
 - Implementación masiva de sistemas operativos.
 - Recuperación de equipos.
 - Configuración automática post instalación.
- **MDM**
 - Gestión de dispositivos móviles.
 - Gestión de aplicaciones aprobadas.
- **DLP (Endpoint Data Loss Prevention)**
 - Identificar datos en todos los equipos.
 - Categorizar tipos de datos sensibles.
 - Controlar los métodos de transferencia de datos.
 - Configuración de alertas y opciones de corrección para falsos positivos.
- **Inventario y Cumplimiento**
 - Inventario de hardware.
 - Inventario de software.
 - Detección de software no autorizado.
 - Reportes ejecutivos y técnicos.

2.3. Alcance Implementación

La implementación deberá incluir:

- Servicio de Instalación y configuración de la plataforma.
- Actualización o migración necesarios para el (upgrade) del servicio incluyendo los respaldos necesarios.
- Habilitación y parametrización de los módulos de seguridad incorporados por la edición Security.
- Configuración de Alta Disponibilidad (Failover).
- Integración con Active Directory.
- Configuración de políticas de seguridad requeridas.
- Diseño e implementación de servidores de distribución por sitio remoto, con políticas de control de ancho de banda y ventanas de replicación
- Ajustes y optimización de la plataforma para el nuevo dimensionamiento (hasta 1.000 equipos).
- Validación funcional integral de la plataforma en su versión más actualizada.
- Pruebas de aceptación.
- Matriz de exclusiones y prueba de coexistencia con plataformas de antivirus/EDR.
- Transferencia de conocimiento con una duración mínima de 16 horas efectivas para 4 administradores designados por YPFBTR, debiendo cubrir:
 - Módulo 1. Arquitectura y Administración General
 - Arquitectura Endpoint Central, componentes, base de datos, Failover
 - Módulo 2. gestión de parches y vulnerabilidades
 - Introducción a Patch Management, Vulnerability Management, CVE, Compliance, automatización y Dashboards.
 - Módulo 3. Seguridad de Endpoints
 - Introducción a BitLocker Management, Device Control, Browser Security, Application Control y Endpoint Privilege Management.
 - Módulo 4. OS Deployment
 - Captura de imágenes, PXE, multicast, task sequences, drivers, recuperación
 - Módulo 5. Operación y Ssoporte
 - Troubleshooting, logs, recuperación, mantenimiento y upgrade de versión.

2.4. Requisitos Funcionales Obligatorios, donde se exige explícitamente que la solución permita:

- Gestión centralizada de BitLocker y recuperación de llaves.
- Vulnerability Assessment y remediación.
- OS Deployment para imágenes corporativas.
- Control de aplicaciones mediante listas blancas.
- Control de dispositivos USB.
- Gestión de privilegios locales.
- Integración con Microsoft Active Directory o Microsoft Entra ID.
- Soporte para Windows 10 y Windows 11.
- Dashboards ejecutivos de cumplimiento y postura de seguridad.

2.5. Consideraciones especiales para activos de control industrial (OT/HMIs).

Cuando el alcance del proyecto contemple la administración o monitoreo de equipos pertenecientes a entornos de control industrial, incluyendo, pero no limitado a, Estaciones HMI o cualquier otro activo OT vinculado a procesos operativos críticos, deberán aplicarse las siguientes condiciones obligatorias:

- Ninguna actividad de implementación, actualización, endurecimiento de seguridad, control de aplicaciones o gestión de privilegios deberá comprometer la disponibilidad de los sistemas de control industrial.
- Toda acción sobre activos OT deberá ser previamente validada y aprobada por las áreas responsables de Operaciones, Automatización Industrial y Tecnología de la Información.
- El proveedor deberá presentar un procedimiento de gestión de cambios específico para activos OT, incluyendo análisis de riesgos, plan de pruebas y procedimiento de reversión.

Gestión de Parches y Actualizaciones

- Queda prohibida la aplicación automática de parches, actualizaciones o remediaciones de vulnerabilidades sobre equipos OT.
- Toda actualización deberá ejecutarse únicamente mediante aprobación manual y documentada.
- Previamente a cualquier despliegue, deberá existir validación técnica del fabricante del sistema de control, integrador o proveedor responsable de la plataforma OT cuando corresponda.
- Las actividades de actualización deberán realizarse exclusivamente dentro de ventanas de mantenimiento previamente coordinadas con Operaciones.
- No se permitirá exposición directa a Internet desde la red OT.

Application Control y Endpoint Privilege Management (EPM)

- La funcionalidad de Application Control deberá operar en modo Auditoría durante un período mínimo de sesenta (60) días calendario antes de la activación de cualquier política de bloqueo.
- Ninguna restricción, eliminación de privilegios o política de elevación controlada podrá activarse sin aprobación formal de los responsables operativos.

La propuesta de la provisión de licencias, deberá ser presentada bajo la modalidad de servicio “llave en mano”, contemplando en forma detallada y por ítems los costos unitarios de todo lo requerido en cuanto a licencias, implementación, soporte, mantenimiento y servicios asociados necesarios para la correcta operación de la solución.

Cualquier costo asociado a la provisión de las horas de soporte y/o consultoría deberá estar incluido dentro de la oferta, formando parte de la propuesta económica.

El proveedor deberá asumir todos los costos relacionados al personal que brinde este servicio a YPFBTR, incluyendo alimentación, traslados, seguros y cualquier otro gasto asociado, sin costo adicional para la empresa.

Cualquier requerimiento de software base (motor de base de datos, sistema operativo, licencias de terceros) necesario para la arquitectura ofertada deberá ser declarado en la propuesta; su omisión no generará costo adicional para YPFBTR

3. PROVISIÓN E IMPLEMENTACIÓN

3.1. IMPLEMENTACIÓN

El proveedor deberá proporcionar a YPFBTR todo el apoyo requerido para la instalación, implementación, configuración y transferencia de conocimiento de la solución.

YPFBTR proporcionará el equipamiento y los recursos técnicos necesarios para la implementación de la solución.

3.2. PROCEDIMIENTO DE COMUNICACIÓN

El proveedor debe designar a un responsable del proyecto, para la coordinación directa con el encargado de proyecto de YPFBTR. Actuará como el único interlocutor válido para todos los requerimientos técnicos y/o comerciales y deberá contar con una línea telefónica corporativa de contacto permanente. Asimismo, será el encargado de gestionar y resolver cualquier reclamo vinculado a la provisión del servicio hasta la conclusión del proyecto.

Debe ser personal de planta que tenga una antigüedad de por lo menos 6 meses en la empresa.

El proveedor no podrá sustituir a los profesionales acreditados sin aprobación previa de YPFBTR, debiendo el reemplazo cumplir igual o mejor perfil

3.3. EQUIPO DE TRABAJO Y REQUISITOS DEL PERSONAL

Por lo menos uno de los integrantes del personal asignado a la ejecución del proyecto deberá contar con certificación oficial vigente emitida por el fabricante que acredite competencia técnica en la implementación, administración y soporte avanzado de la solución. Se deberá presentar copia de los certificados y hojas de vida actualizadas de cada integrante del equipo técnico.

3.4. PROVISIÓN DE LICENCIAS Y COMPONENTES

La vigencia de la suscripción se computa desde su activación por el fabricante y concluye el 28 de junio de 2028, independientemente de la fecha del Acta de Conformidad.

Los plazos de garantía de implementación y de la bolsa de horas se computan desde el Acta de Conformidad

Las licencias deben registrarse a nombre y bajo la cuenta corporativa de YPFB Transporte S.A., con acceso directo al portal de soporte del fabricante.

4. GARANTÍA Y SOPORTE TÉCNICO

4.1. Garantía de la Implementación

El proveedor deberá brindar soporte técnico presencial o remoto para garantizar la correcta instalación, configuración, integración y funcionamiento de la solución durante un período mínimo de tres (3) meses posteriores a la emisión del Acta de Conformidad Definitiva.

Durante este período, el proveedor deberá corregir sin costo adicional cualquier error o desviación atribuible al proceso de implementación.

La garantía deberá contemplar:

- Corrección de errores de configuración.
- Ajustes de parametrización de la plataforma.
- Soporte para incidentes relacionados con la implementación.
- Asistencia en la validación de políticas de seguridad implementadas.
- Acompañamiento en la estabilización de la solución.

Siendo este servicio de soporte independiente de la bolsa de horas mencionada en el alcance del servicio.

4.2. Soporte Técnico Post Implementación

El proveedor deberá brindar soporte técnico remoto y/o presencial según el caso durante la vigencia contractual para atender consultas, incidentes y requerimientos relacionados con la solución implementada.

El soporte deberá contemplar como mínimo:

Severidad	Descripción	Tiempo máximo de respuesta	Tiempo Resolución
Crítica	Interrupción total de la plataforma o imposibilidad de administración de endpoints. Aplicable en horario hábil.	30~45 minutos	2 ~ 4 horas
Alta	Funcionalidad crítica degradada sin solución alternativa.	2 ~ 4 horas	6 ~ 12 horas
Media	Incidencias operativas con impacto parcial.	6~10 horas	2 ~ 4 días
Baja	Consultas técnicas o requerimientos menores.	2 días	5 ~ 7 días

El proveedor deberá proporcionar:

- Correo electrónico de soporte.
- Línea telefónica de contacto.
- Chat en vivo
- Software de acceso remoto
- Esquema de soporte 8x5
- Escalamiento al fabricante cuando corresponda.
- Soporte remoto fabricante 24x7

4.3. Bolsa de Horas de Consultoría

La oferta deberá incluir una bolsa de cuarenta (40) horas de soporte técnico y consultoría especializada a ser utilizada durante la vigencia del licenciamiento.

Estas horas podrán destinarse a:

- Optimización de políticas de seguridad.
- Asistencia en OS Deployment.
- Configuraciones avanzadas de:
 - BitLocker.
 - Application Control.
 - Device Control.
 - DLP
 - Browser Security
 - Endpoint Privilege Management.
 - MDM
- Elaboración de reportes especializados.
- Optimización de configuraciones.
- Resolución de incidencias complejas.
- Asesoramiento en mejores prácticas.
- Soporte para la implementación de nuevas funcionalidades.

La bolsa de horas será independiente del soporte correctivo cubierto por la garantía.

El proveedor deberá llevar un control detallado de los tickets gestionados y de las horas consumidas de las bolsas contratadas, presentando reportes mensuales o trimestrales, según el nivel de uso registrado, que permitan verificar el cumplimiento, la trazabilidad y la correcta ejecución de los servicios.

Las actualizaciones de versión/build de la plataforma durante la vigencia contractual (mínimo dos por año) serán ejecutadas por el proveedor sin consumo de la bolsa de horas.

5. PRUEBAS DE ACEPTACIÓN

El proveedor deberá entregar un listado de las pruebas de aceptación a realizar, que permita verificar el correcto funcionamiento de la solución.

Estas pruebas servirán para garantizar la correcta instalación, configuración y alta disponibilidad de la solución, manteniendo sin afectación de las 20 licencias concurrentes para técnicos y el soporte Multilenguaje contemplados en la solución actual.

La conclusión del proyecto será formalizada mediante un Acta de Conformidad firmada por representantes autorizados del proveedor y de YPFBTR, la cual certificará el cumplimiento del alcance y la ejecución satisfactoria de las pruebas de aceptación.

Las pruebas deberán incluir como mínimo:

5.1. Administración de Equipos

- Enrolamiento exitoso de equipos clientes.
- Inventario de hardware y software.
- Comunicación con los agentes instalados.

5.2. Gestión de Vulnerabilidades

- Identificación de vulnerabilidades.
- Generación de reportes.
- Validación de remediaciones.

5.3. OS Deployment

- Captura de imagen maestra.
- Implementación automatizada.
- Validación de controladores y aplicaciones corporativas.

5.4. Application Control y Endpoint Privilege Management

- Bloqueo de aplicaciones no autorizadas.
- Ejecución de aplicaciones aprobadas.
- Elevación controlada de privilegios.
- Registro de auditoría.

5.5. Device Control

- Restricción de dispositivos USB.
- Aplicación de políticas diferenciadas.

5.6. MDM

- Gestión de dispositivos móviles.
- Gestión de aplicaciones aprobadas.

5.7. Patch Management

- Despliegue de parches con flujo de aprobación automáticas.
- Despliegue de parches con flujo de aprobación y prueba en grupo piloto.
- Exclusión de parcheo automático equipos OT (HMI's).

5.8. Failover

- Conmutación y retorno (failback) con medición de tiempo y validación de que no se pierden datos.
- Restauración de respaldo de la plataforma.

5.9. Integraciones

- Integración AD, administración basada en roles y doble factor en la consola.
- Coexistencia con antivirus/EDR y medición de impacto en rendimiento del equipo cliente.

5.10. BitLocker Management

- Migración o reactivación de cifrado en equipos con BitLocker.
- Recuperación de una clave desde la consola de Endpoint Central.
- Las claves residen exclusivamente en infraestructura de YPFBTR.
- Acceso bajo rol restringido con registro de auditoría
- Simulación de indisponibilidad de Endpoint Central y recuperación de la clave desde Windows AD o Microsoft Entra ID.
- Rotación de la clave y validación de actualización en el repositorio correspondiente.
- Recuperación y prohibición expresa de que el proveedor conserve copia o credenciales administrativas al cierre del proyecto.

5.11. Reportes y Dashboard

- Exportación de reportes y dashboard ejecutivos.
 - Vulnerabilidades por criticidad.
 - Cumplimiento de parches.
 - Estado de cifrado BitLocker.
 - Dispositivos bloqueados.
 - Aplicaciones restringidas.
 - Equipos fuera de cumplimiento.

La conclusión satisfactoria de las pruebas será requisito indispensable para la emisión del Acta de Aceptación del proyecto.

6. DOCUMENTACIÓN DEL PROYECTO

6.1. DOCUMENTACIÓN PARA LA PROPUESTA

El proveedor deberá incluir:

Carta de autorización vigente del fabricante: Carta o Certificado del fabricante, que acredite la autorización de ManageEngine para comercializar sus productos de software ofertado en Bolivia.

Documentación que acredite experiencia en proyectos similares: Documentación (contratos, órdenes de compra, actas de conformidad o referencias) que demuestre la ejecución de por lo menos un (1) proyecto similar al solicitado en el último año.

Empresas en Bolivia o países limítrofes donde hayan instalado los ítems ofertados.

Describir antigüedad y versión de la instalación (cuándo se realizó).

Cronograma de implementación: Plan detallado que incluya etapas e hitos temporales. Debe contemplar un listado de entregables, donde se incluya obligatoriamente un Informe Final en formato digital, que documente el alcance ejecutado, configuraciones aplicadas, topología, resultados de pruebas de aceptación y estado de cumplimiento.

Curriculum Vitae y Certificaciones Técnicas: El proveedor deberá adjuntar la documentación que acredite las certificaciones del equipo de trabajo, a fin de que YPFBTR pueda verificar la idoneidad técnica antes de la adjudicación. Cargo dentro del marco de ejecución del proyecto y experiencia detallada en el mismo cargo. Se deberán incluir las hojas de vida del personal propuesto, copias de certificaciones vigentes del fabricante, y cualquier otro certificado relevante que respalde la especialización técnica del equipo en la solución requerida.

Requerimientos mínimos de infraestructura: Especificaciones detalladas de la infraestructura base (software y hardware) necesaria para el correcto funcionamiento de la solución.

Fichas técnicas del software para el servicio ofertado: Manuales de instalación, configuración, operación y mantenimiento emitidos por el fabricante, incluyendo las URL oficiales de consulta técnica.

6.2. DOCUMENTACIÓN TÉCNICA FINAL DEL PROYECTO

Una vez concluido el proyecto el proveedor deberá entregar:

- Manual de instalación y configuración.
- Manual de operación, administración y mantenimiento.
- Procedimientos de respaldo y recuperación.
- Políticas de seguridad aplicadas.
- Inventario de licencias y/o suscripciones vinculadas a la cuenta de administración de YPFBTR.
- Informe final del proyecto detallando.
 - Topología física y lógica de la solución desplegada.
 - Configuraciones aplicadas
 - Políticas de seguridad y accesos aplicados
 - Rutas de Datos

La documentación deberá entregarse en formato PDF y editable.

6.3. ACCESO A MEJORES PRÁCTICAS

Durante la implementación, el proveedor deberá aplicar las mejores prácticas recomendadas por el fabricante, asegurando consistencia técnica, escalabilidad y facilidad de soporte a largo plazo.

Como parte de la transferencia de conocimiento, el proveedor deberá compartir con el equipo técnico de YPFBTR los recursos oficiales disponibles para la gestión y soporte de la solución, incluyendo:

- URL del portal de soporte del fabricante
- Acceso a foros técnicos
- Base de Conocimientos y Comunidad de Usuarios.

En caso de que el acceso a dichos recursos requiera credenciales o registro, el proveedor deberá facilitar los datos de acceso correspondientes.

7. LUGAR DE ENTREGA

La ejecución del servicio será principalmente remota, con ingresos puntuales en coordinación con el encargado de YPFBTR para actividades específicas de implementación y pruebas que no pudieran realizarse remotamente.

La ejecución del servicio objeto del presente TDR, se realizará en las oficinas de YPFB Transporte S.A. regional Santa Cruz.

La recepción del servicio se formalizará mediante la emisión de la correspondiente Orden de Servicio y la conformidad de los entregables establecidos en el cronograma de implementación.

8. PLAZOS DE ENTREGA

Se deberá considerar un plazo máximo de noventa (90) días calendario para la puesta en marcha de la solución, la cual incluye la ejecución del proyecto, habilitación de la plataforma, integración y enrolamiento de los equipos clientes.

9. PRESENTACIÓN DE PROPUESTAS

La oferta será evaluada en función del cumplimiento técnico y administrativo de los requisitos establecidos en el presente documento, la experiencia del proveedor y la oferta económica presentada.

10. PAGOS

El pago del servicio se efectuará por el cien por ciento (100%) del monto adjudicado, dentro de los veinte (20) días calendario posteriores a la recepción de la factura correspondiente, previa conformidad técnica y administrativa de YPFB Transporte S.A.

La conformidad estará sujeta a la entrega del licenciamiento, la implementación y puesta en producción de la solución, la aprobación de las pruebas de aceptación, la entrega de la documentación final y la suscripción del Acta de Conformidad del Proyecto.