



Términos de Referencia

**Provisión del Servicio de Análisis de vulnerabilidades
(Ethical Hacking) para YPFB Transporte S.A.**

Gestión 2026

© 2026 YPFB Transporte S.A.

El contenido del documento es propiedad de YPFB Transporte S.A. y podrá ser utilizado exclusivamente para la elaboración y presentación de propuestas en el marco del presente proceso. Queda prohibida su reproducción, modificación o utilización con fines distintos a los establecidos en este Término de Referencia, sin autorización expresa de YPFB Transporte S.A.

INDICE DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETOS DEL REQUERIMIENTO	3
2.1 OBJETIVO GENERAL	3
2.2 OBJETIVOS ESPECIFICOS	3
3. ALCANCE	3
4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO	4
5. RECOMENDACIONES DE LAS HERRAMIENTAS A UTILIZAR	5
6. PERSONAL REQUERIDO PARA EL SERVICIO	5
7. INFRAESTRUCTURA TI PARA REALIZACION DEL ANALISIS DE VULNERABILIDADES	6
8. INFRAESTRUCTURA OT PARA REALIZACION DEL ANALISIS DE VULNERABILIDAD	6
9. GARANTIA	7
10. LUGAR Y PLAZO DE ENTREGA	7
11. ENTREGABLES	7
12. PRESENTACION Y FORMATO DE PROPUESTAS	8
13. PAGOS	8
ANEXO 1	9

	TERMINOS DE REFERENCIA	Hojas: 3
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

1. INTRODUCCIÓN

YPFB TRANSPORTE S.A. invita a empresas legalmente establecidas en el Estado Plurinacional de Bolivia a presentar propuestas para la provisión del Servicio de Análisis de Vulnerabilidades (Ethical Hacking), orientado a evaluar el nivel de exposición al riesgo de seguridad de la información de las infraestructuras de Tecnologías de la Información (TI) y Tecnologías Operacionales (OT) de la empresa.

El servicio tiene como propósito identificar vulnerabilidades técnicas, operativas y de configuración susceptibles de ser explotadas por amenazas internas y externas, evaluar su potencial impacto sobre la confidencialidad, integridad, disponibilidad y continuidad operativa, así como verificar la efectividad de los controles de seguridad implementados.

2. OBJETOS DEL REQUERIMIENTO

2.1 OBJETIVO GENERAL

Contratar un servicio especializado orientado a evaluar y fortalecer los controles de seguridad de la información en las infraestructuras de Tecnologías de la Información (TI) y Tecnologías Operacionales (OT) de YPFB Transporte S.A., mediante la identificación, análisis y priorización de vulnerabilidades, contribuyendo a una gestión efectiva de riesgos y a la continuidad operativa, en cumplimiento de la normativa interna y los estándares internacionales vigentes.

2.2 OBJETIVOS ESPECIFICOS

El servicio busca satisfacer las siguientes necesidades:

- Identificar vulnerabilidades potencialmente explotables por atacantes externos y por usuarios internos.
- Evaluar el impacto de las vulnerabilidades encontradas a la infraestructura tecnológica de TI y OT de YPFB TRANSPORTE S.A.
- Evaluar la eficacia y efectividad real de los controles técnicos y organizativos de seguridad de la información implementados en las infraestructuras de Tecnologías de la Información (TI) y Tecnologías Operacionales (OT) de YPFB Transporte S.A.
- Verificar el cumplimiento de la normativa interna en seguridad de la información de YPFB TRANSPORTE S.A.
- Proporcionar controles y recomendaciones técnicas de remediación para las vulnerabilidades identificadas durante la ejecución del Servicio de Análisis de Vulnerabilidades (Ethical Hacking), debidamente priorizadas según su criticidad y nivel de riesgo, y alineadas a buenas prácticas y estándares internacionales de seguridad de la información.

3. ALCANCE

El Análisis de Vulnerabilidades (Ethical Hacking) comprende la ejecución planificada y controlada de pruebas internas y externas sobre los servicios publicados hacia Internet y la red interna, con el objetivo de determinar el nivel actual de protección de los activos de información. Como resultado

	TERMINOS DE REFERENCIA	Hojas: 4
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

del servicio, se elaborará un informe que detalle los hallazgos obtenidos durante las pruebas realizadas e incluya recomendaciones técnicas para la mitigación de las vulnerabilidades identificadas.

No se permitirá ninguna actividad que comprometa la continuidad operativa, la seguridad industrial o la integridad de procesos críticos, salvo autorización expresa y documentada.

- Análisis de vulnerabilidades de la infraestructura tecnológica de Tecnologías de la Información (TI) de YPFB TRANSPORTE S.A.
- Análisis de vulnerabilidades de las infraestructuras críticas de Tecnologías Operacionales (OT) de YPFB Transporte S.A., a realizarse en el sitio operativo de la Sitio operativo estación Terminal Santa Cruz.

4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

A continuación, se detallan las características técnicas del servicio:

- Para el análisis de vulnerabilidades se aplicará la metodología MITRE ATT&CK Enterprise para entornos de Tecnologías de la Información (TI) y MITRE ATT&CK for ICS para los entornos de Tecnologías de Operación (OT) e infraestructuras críticas, permitiendo identificar vectores de ataque relevantes y su impacto potencial sobre los activos evaluados.
- Las pruebas de aplicaciones web y entornos TI se realizarán bajo los enfoques de caja negra y caja blanca, conforme al alcance definido, utilizando información de infraestructura, diagramas, configuraciones y otros insumos cuando corresponda.
Las pruebas para entornos OT, se ejecutarán exclusivamente considerando las restricciones operativas, de seguridad industrial y de disponibilidad.
Las evaluaciones distinguirán entre entornos TI y OT, garantizando la operación segura de sistemas críticos y evitando impactos no autorizados sobre procesos productivos, sistemas SCADA, PLC u otros sistemas de control industrial.
- Para las pruebas en aplicaciones web, deberá realizarse aplicando la metodología OWASP (Open Web Applications Security Project) Top Ten en su versión vigente, enfocada en la identificación de fallas de configuración, errores de codificación y debilidades en el manejo de excepciones.
La severidad de las vulnerabilidades deberá clasificarse utilizando el CVSS en su versión vigente
- El servicio incluirá pruebas controladas de ingeniería social, orientadas a evaluar el factor humano como vector de riesgo, considerando simulaciones de campañas de phishing. Estas actividades deberán ejecutarse de forma ética, controlada y previamente autorizada, en cumplimiento de las políticas internas y la normativa legal vigente y los principios de confidencialidad.
- Elaboración de informes detallados que describan las vulnerabilidades identificadas, los riesgos asociados y las recomendaciones para su mitigación, considerando normas y estándares internacionales aplicables, tomando como referencia los controles establecidos en la ISO/IEC 27002 para entornos TI, así como buenas prácticas reconocidas de ciberseguridad industrial para entornos OT basadas en ISA99/IEC 62443.

	TERMINOS DE REFERENCIA	Hojas: 5
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

- f) Se debe garantizar la protección y privacidad de los datos recopilados producto de las pruebas realizadas, de acuerdo a normativa interna de YPFB TRANSPORTE S.A. (procedimiento de clasificación de la información).
- g) Todo trabajo a realizar, será previamente coordinado con el Especialista de Seguridad de la Información de YPFB TRANSPORTE S.A., esto para prever fechas y horarios en los que se realizaran las pruebas y no afectar a la continuidad de los servicios.
- h) La empresa proveedora del servicio, antes de comenzar el trabajo, deberá firmar un acuerdo de confidencialidad de la información (NDA). Así mismo, el personal asignado al servicio firmará el formulario FT.001 “Declaración de Seguridad y Confidencialidad en el Uso de Recursos de Tecnología de la Información”.

5. RECOMENDACIONES DE LAS HERRAMIENTAS A UTILIZAR

Características de las herramientas informáticas a utilizar para el análisis de vulnerabilidades:

- Uso de herramientas actualizadas a las últimas versiones y con los parches de seguridad correspondientes.
- Contar con una base de datos actualizada y completa de vulnerabilidades aceptadas por la industria (CERT, SANS) como el CVE (Common Vulnerabilities and Exposure) y las puntuaciones asociadas CVSS (Common Vulnerability Scoring System).
- Para realización de las pruebas se podrá utilizar software comercial (licenciado) y software libre será permitido únicamente como complemento, siempre que esté debidamente documentado, validado y aprobado, y no constituya la herramienta principal del análisis.
- Entre las herramientas sugeridas, pero no limitativas están las siguientes:
 - Tenable Nessus
 - Tenable.ot Nessus
 - Nexpose y Metasploit de Rapid7
 - WiFi Pineapple
 - Kali Linux
 - Framework OSINT

6. PERSONAL REQUERIDO PARA EL SERVICIO

La empresa contratada garantizará el personal mínimo requerido para la ejecución del servicio.

N°	Descripción	Cantidad	Descripción
1	Profesional senior en Ethical Hacking, con experiencia en análisis de vulnerabilidades en infraestructuras IT e infraestructura críticas OT.	1	▪ Certificado GIAC GICSP – Global Industrial Cyber Security Professional. ICS/SCADA (SANS Institute) *. ▪ Certificado CISSP (Certified Information Systems Security Professional) ▪ Curso de ISO/IEC ISO 27001. ▪ Curso de IEC 62443 o similares.
2	Profesional senior en Ethical Hacking (vulnerabilidades externas)	1	▪ Certificado OSCP – Offensive Security Certified Professional *. ▪ Certificado OSWE - Offensive Security Web Expert *.

	TERMINOS DE REFERENCIA	Hojas: 6
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

			▪ Certificado OPST (OSSTMM Professional Security Tester). *
3	Profesional senior en Ethical Hacking (vulnerabilidades internas)	1	▪ Certificado OSWP - Offensive Security Wireless Professional *. ▪ CEH Certified Ethical Hacker (EC-Council) ▪ eWPTxV2 (eLearnSecurity Web Penetration Tester eXtreme V2).

* Los certificados de los profesionales propuestos que realizarán el trabajo, serán validados. Se proporcionará los enlaces (links) de referencia de las certificaciones que cuenten con verificación en línea; para aquellas que no dispongan de dicho mecanismo, se aceptará copia del certificado y/o su código o ID de verificación.

7. INFRAESTRUCTURA TI PARA REALIZACION DEL ANALISIS DE VULNERABILIDADES

Nro.	Componente	Cantidad	Observaciones
1	Aplicaciones externas y servicios web publicados	7	Servicios expuestos a Internet: Aplicaciones externa que integra 3 módulos (SGTD Consiliacion, Inspección de Proveedores, Curruculum web), Gestión de Proveedores, GIS, Exchange, sitio web empresarial GTB y TR
2	Aplicaciones internas	2	
3	Servidores internos físicos y virtuales	40	Infraestructura on premise y virtualizada, TR, GTB, TS
4	Dispositivos de red y telecomunicaciones (firewall, switch, router, etc.)	10	Firewalls, Switches, VLAN de Servidores
5	Equipos cliente (PCs y portátiles)	12	Incluye laptops, escritorio, HMI y Workstation
6	Cámaras IP de videovigilancia	8	Sistema de control de acceso y CCTV
7	Ingeniería social (phishing controlado)	100	Envío de correos electrónicos a usuarios seleccionados

8. INFRAESTRUCTURA OT PARA REALIZACION DEL ANALISIS DE VULNERABILIDAD

Nro.	Componente	Cantidad	Observaciones
1	Sitios operativos	1	Sitio operativo de YPFB Transporte S.A.

	TERMINOS DE REFERENCIA	Hojas: 7
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

2	Zonas OT a evaluar SCADA (Router, HMI, PLC (Líquidos, Alivios, Procesos Líquidos, Computador de flujo, entre otros) en Sitio Operativo.	1	Sitio operativo estación Terminal Santa Cruz de YPFB Transporte S.A.
4	Dispositivos de red y telecomunicaciones en sitios operativos: switch (3), router (1), access point (2), teléfono IP (2)	8	Dirección de TI / Jefatura de Mantenimiento, Medición, Control, Comunicación y SCADA
5	Equipos finales (estaciones de ingeniería, mantenimiento y operadores)	2	Estación Terminal Santa Cruz

9. GARANTIA

El proveedor del servicio, deberá proporcionar un servicio de calidad en cuanto al análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A., manteniendo en todo momento la confidencialidad de la información que está siendo analizada y los resultados encontrados.

El proveedor del servicio deberá garantizar que las actividades de Análisis de Vulnerabilidades (Ethical Hacking), tanto internas como externas, ejecutadas sobre los distintos procesos, servicios y sistemas de Tecnologías de la Información (IT) y Tecnologías de Operación (OT), se realicen de manera controlada, preservando en todo momento la **disponibilidad, integridad y continuidad operativa** de los servicios, sistemas e información evaluados. Asimismo, deberá adoptar las precauciones y controles necesarios para evitar cualquier afectación, degradación o interrupción no autorizada de los entornos productivos durante la ejecución del servicio.

10. LUGAR Y PLAZO DE ENTREGA

El servicio será realizado **en instalaciones de YPFB TRANSPORTE S.A.**, doble vía la guardia Km 7 ½ , y en sitio operativo Estación Terminal Santa Cruz (17°52'57.6"S 63°11'55.0"W); así mismo, tomar en cuenta que: el transporte, la alimentación, viáticos y equipo de protección personal (EPP) para el personal de la empresa proveedora del servicio, estará a su cargo.

El plazo máximo para la entrega del informe final será de **45 días calendario**, computables a partir de la orden de servicio.

11. ENTREGABLES

Los entregables del servicio son:

- Resumen ejecutivo: Documento dirigido a la Alta Dirección que sintetiza los principales hallazgos, el nivel de riesgo identificado en las infraestructuras TI y OT, y las conclusiones relevantes del servicio.
- Informe final: Informe técnico detallado del trabajo realizado, que incluya los resultados del análisis de vulnerabilidades y pruebas de intrusión efectuadas, junto con las

	TERMINOS DE REFERENCIA	Hojas: 8
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

recomendaciones técnicas para la mitigación de las vulnerabilidades identificadas. El informe deberá contar con capítulos diferenciados para la infraestructura de Tecnologías de la Información (TI) y la infraestructura de Tecnologías Operacionales (OT).

- Listado de servicios y dispositivos analizados: Relación detallada de los sistemas, servicios, equipos y dispositivos analizados durante la ejecución del servicio, incluyendo su clasificación como activos TI u OT, así como el alcance de las pruebas realizadas sobre cada uno de ellos.
- Vulnerabilidades encontradas: Registro de las vulnerabilidades encontradas en los sistemas, servicios y dispositivos evaluados, indicando su nivel de gravedad, criticidad y el riesgo asociado, conforme a criterios y buenas prácticas de seguridad de la información.
- Intrusiones: Descripción de las intrusiones realizadas durante las pruebas, detallando las vulnerabilidades y los servicios con mayor probabilidad de explotación que fueron utilizados para comprometer o intentar comprometer los sistemas evaluados.

Tras la finalización del servicio y su correspondiente validación por parte de YPFB Transporte, el proveedor deberá confirmar la eliminación segura y definitiva de toda la información de la empresa obtenida, generada o procesada durante la prestación del servicio, incluyendo de manera enunciativa pero no limitativa: registros y archivos de logs, direcciones IP y datos de direccionamiento de red, resultados y reportes de escaneos, evidencias de vulnerabilidades, capturas de pantalla, credenciales o accesos obtenidos, configuraciones y cualquier otro dato técnico o sensible recopilado. Dicha eliminación deberá evitar su conservación, divulgación o uso no autorizado posterior, y ser respaldada mediante el documento de constancia de destrucción segura correspondiente.

12. PRESENTACION Y FORMATO DE PROPUESTAS

La propuesta técnica deberá incluir lo siguiente:

- Un plan del trabajo por el servicio, donde especifique un cronograma de actividades, el tiempo de duración y responsables asignados.
- Carta de aceptación, donde se manifieste la conformidad expresa con todas y cada una de las especificaciones del servicio descritas en los incisos 3, 4, 5, 6, 7, 8, 9, 10 y 11 del presente Terminó de Referencia.
- Identificación del responsable del servicio, indicando nombre completo, cargo, teléfono y correo electrónico. Esta persona será el **interlocutor válido** ante **YPFB TRANSPORTE S.A.** para todos los requerimientos comerciales y técnicos, durante la ejecución del servicio.
- La documentación referida a curriculum vitae, certificaciones y antecedentes deberá presentarse conforme a lo establecido en el ANEXO 1.

13. PAGOS

El pago se realizará una vez culminado las actividades de Análisis de Vulnerabilidades y a la entrega del informe final.

	TERMINOS DE REFERENCIA	Hojas: 9
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

N°	Descripción	Porcentaje de pago por el servicio	Entregable
1	Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	100%	Informe final de análisis de vulnerabilidades realizado a la infraestructura de TI y OT de YPFB TRANSPORTE S.A.

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
---	---

	TERMINOS DE REFERENCIA	Hojas: 10
	TITULO: Provisión del Servicio de Análisis de vulnerabilidades (Ethical Hacking) para YPFB TRANSPORTE S.A.	

ANEXO 1

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

1. La Empresa ofertante deberá presentar documentación donde demuestre y avale:
 - a. Experiencia comprobada mínima de tres (3) años en la prestación de servicios de Análisis de Vulnerabilidades y/o Ethical Hacking, preferentemente en empresas del sector petrolero y/o industrial.
 - b. Certificados de trabajos realizados, adjuntando al menos tres (3) certificaciones emitidas por empresas bolivianas donde se hayan ejecutado servicios de Análisis de Vulnerabilidades y/o Pruebas de Intrusión (Pentest).
 - c. Descripción de implementaciones similares realizadas en los últimos tres (3) años, indicando como mínimo: Año de ejecución, Nombre de la empresa, Persona de referencia (nombre y cargo).

2. La empresa ofertante deberá cumplir con los siguientes requisitos:
 - a. Designar un Administrador del Proyecto, responsable de la coordinación, seguimiento y comunicación durante la ejecución del servicio.
 - b. Contar con profesionales senior debidamente certificados en Ethical Hacking, quienes deberán cubrir, según su especialización, las siguientes responsabilidades:
 - i. Análisis de vulnerabilidades en infraestructuras de Tecnologías Operacionales (OT) e infraestructura crítica.
 - ii. Análisis de vulnerabilidades en infraestructuras de Tecnologías de la Información (TI), considerando vulnerabilidades internas y externas.
 - c. Presentar el Curriculum Vitae del personal técnico asignado, donde se evidencien: experiencia profesional, certificaciones requeridas conforme al punto **6. PERSONAL REQUERIDO PARA EL SERVICIO** del Termino de Referencia.
 - d. El Administrador del Proyecto, en el caso que sea profesional licenciado en ingeniería, sea boliviano o extranjero con residencia permanente en el país, deberá acreditar su Registro Nacional de Ingenieros de la Sociedad de Ingenieros de Bolivia (SIB), mediante copia a color del carnet correspondiente.