



## **Términos de Referencia**

Servicio de Implementación del Sistema de Gestión  
de Seguridad de la Información (SGSI) – Fase II  
(Diagnostico de situación actual de YPFB  
TRANSPORTE S.A. en Seguridad de la Información  
respecto a la norma ISO/IEC 27001:2022)

Gestión 2024

### 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

<b>1. INTRODUCCIÓN</b>	<b>3</b>
<b>2. OBJETOS DEL REQUERIMIENTO</b>	<b>3</b>
OBJETO GENERAL	3
OBJETIVOS ESPECIFICOS	3
<b>3. ALCANCE</b>	<b>3</b>
<b>4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO</b>	<b>4</b>
<b>5. CALIDAD EN EL SERVICIO</b>	<b>5</b>
<b>6. Lugar y PLAZO DE ENTREGA</b>	<b>5</b>
<b>7. ENTREGABLES</b>	<b>6</b>
<b>8. PRESENTACION Y FORMATO DE PROPUESTAS</b>	<b>6</b>
<b>9. PAGOS</b>	<b>7</b>

## 1. INTRODUCCIÓN

YPFB TRANSPORTE S.A. invita a las empresas legalmente establecidas en Bolivia a presentar su propuesta para la provisión del Servicio de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) - Fase II (Diagnostico de situación actual de YPFB TRANSPORTE S.A. en Seguridad de la Información respecto a la norma ISO/IEC 27001:2022), que comprende el diagnóstico en seguridad de la información y el análisis de riesgos, priorizando procesos críticos del negocio.

## 2. OBJETOS DEL REQUERIMIENTO

### OBJETO GENERAL

Contratar un servicio para la implementación del **Sistema de Gestión de Seguridad de la Información (SGSI) - Fase II** (Diagnóstico de situación actual de YPFB TRANSPORTE S.A. en Seguridad de la Información respecto a la norma ISO/IEC 27001:2022).

### OBJETIVOS ESPECIFICOS

La implementación del servicio busca satisfacer las siguientes necesidades:

- Determinar la brecha respecto a Seguridad de la Información en YPFB TRANSPORTE S.A. en función a requisitos de las normas: ISO/IEC 27001:2022 y ISO/IEC 27002:2022.
- Realizar el análisis de riesgos en seguridad de la información, priorizando los procesos de: Operaciones GAS, Operaciones Líquidos, Transporte por Poliductos, Proyectos y Construcciones, Control del Sistema, Mantenimiento, Planificación, Comercial, Gestión de CSSM y RSE, Regulaciones, Administración y Finanzas, Contrataciones, Talento Humano, Legal y Tecnologías de la Información.
- Identificar controles de seguridad de la información actualmente implementados en YPFB TRANSPORTE S.A. para la protección de los activos de información, tomando en cuenta procesos críticos del negocio y verificar si estos controles son los adecuados.
- Elaborar un plan de acción para la implementación de controles de seguridad de la información, que cierren las brechas identificadas, de acuerdo a una alternativa adecuada especificando un presupuesto tentativo para su ejecución en una siguiente fase.
- Generar cultura de seguridad de la información en YPFB TRANSPORTE S.A.

## 3. ALCANCE

El alcance está determinado a realizar el diagnostico de situación actual en seguridad de la información respecto de la norma ISO/IEC 27001:2022, la gestión de riesgos en seguridad de la información en base a la metodología de gerenciamiento de riesgos y oportunidades de YPFB TRANSPORTE S.A., identificación de controles de seguridad de la información actualmente implementados en YPFB TRANSPORTE S.A. para la protección de los activos de información y si estos son los adecuados; además de la elaboración de un plan de acción para la posible implementación de controles de seguridad de la información faltantes de acuerdo a una alternativa adecuada con un presupuesto tentativo.

A continuación, se detallan los procesos que forman parte del alcance del Sistema de Gestión de Seguridad de la Información SGSI – FASE II de YPFB TRANSPORTE S.A.

- Operaciones GAS
- Operaciones Líquidos
- Transporte por Poliductos
- Proyectos y Construcciones
- Control del Sistema
- Mantenimiento
- Gestión de calidad, Salud, Seguridad, Medio ambiente y RSE
- Planificación
- Comercial
- Regulaciones
- Administración y Finanzas
- Contrataciones
- Talento Humano
- Legal
- Tecnología de la Información

#### 4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

A continuación, se detallan las características técnicas del servicio:

- a) Para el diagnóstico de situación actual en Seguridad de la Información de YPFB TRANSPORTE S.A. aplicar las normas NB/ISO 19011:2018 y la norma ISO/IEC 27001:2022
- b) Se debe tomar en cuenta la primera fase del Sistema de Gestión de Seguridad de la Información (SGSI), que **corresponde a la clasificación de activos de información**, como insumo para la ejecución de la segunda fase del SGSI.
- c) Para el análisis de riesgo, la norma base es NB/ISO 31000, conforme se tiene establecido en la normativa interna de gerenciamiento de riesgos y oportunidades de YPFB TRANSPORTE S.A.
- d) Proponer mejoras al procedimiento de gestión de riesgos, específicamente para: la identificación, análisis y tratamiento de los riesgos de seguridad de la información.
- e) Para la elaboración del plan de acción, realizar la identificación de controles de Seguridad de la información faltantes basado en la norma ISO/IEC 27002:2022
- f) Realizar cursos de concienciación en seguridad de la información dirigido al personal (punto focal) que forma parte de alcance del SGSI - Fase II, para explicar el cómo y por qué se está realizando el trabajo de diagnóstico de brecha de seguridad de la información.
- g) Presentación de informes de avance del servicio según cronograma establecido.
- h) La empresa proveedora del servicio, antes de comenzar el trabajo, deberá firmar un acuerdo de confidencialidad de la información (NDA).
- i) La empresa contratada garantizará el personal mínimo requerido (3 personas), para la ejecución del servicio, de acuerdo al siguiente detalle:

N°	Descripción	Cantidad	Descripción
1	Auditor líder en Sistemas de Gestión Seguridad de la Información (7 años de experiencia comprobable).	1	<ul style="list-style-type: none"> <li>▪ Experiencia en auditorías de Sistemas de Gestión de Seguridad de la Información bajo las normas ISO 19011 y ISO/IEC 27001.</li> <li>▪ Experiencia en la Implementación de Sistemas de Gestión de Seguridad de la Información bajo norma ISO/IEC 27001 y ISO/IEC 27002.</li> </ul>

			<ul style="list-style-type: none"> <li>Experiencia en gestión de riesgos de Seguridad de la Información, bajo la norma ISO 31000.</li> <li>Experiencia en la implementación de controles de seguridad de la información.</li> <li><b>Coordinará todo el trabajo a realizar respecto a la Implementación del SGSI – FASE II.</b></li> </ul>
2	Implementador de Sistemas de Gestión de Seguridad de la Información (3 años de experiencia comprobable)	1	<ul style="list-style-type: none"> <li>Experiencia en la Implementación de Sistemas de Gestión de Seguridad de la Información mediante normas ISO/IEC 27001 e ISO/IEC 27002.</li> <li>Experiencia en auditorías de Sistemas de Gestión de seguridad de la información.</li> <li>Experiencia en el análisis de riesgos de seguridad de la información.</li> </ul>
3	Profesional técnico en Sistemas SCADA (2 años de experiencia comprobable).	1	<ul style="list-style-type: none"> <li>Experiencia en el manejo de sistemas SCADA.</li> <li>Experiencia en la Implementación de Sistemas de Gestión de Seguridad de la Información mediante normas ISO/IEC 27001 y ISO/IEC 27002.</li> <li>Certificado de cursos realizados referente al estándar ISA99/IEC-62443.</li> </ul>
<p>***Se considera que el personal asignado al servicio debe trabajar in situ (en oficina) al menos el 40% del tiempo destinado al servicio, esto para garantizar que se realice un diagnóstico más preciso de situación actual en seguridad de la información; se entiende que el tiempo restante es de trabajo en Gabinete</p>			

## 5. CALIDAD EN EL SERVICIO

El proveedor del servicio, deberá proporcionar a YPFB TRANSPORTE S.A. un servicio de calidad en el trabajo de **diagnóstico de situación actual de YPFB TRANSPORTE S.A. en Seguridad de la Información** y las actividades relacionadas a este trabajo, segunda fase de la Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para YPFB TRANSPORTE S.A.

## 6. LUGAR Y PLAZO DE ENTREGA

El servicio será realizado **en instalaciones de YPFB TRANSPORTE S.A.** (oficina central Santa Cruz de la Sierra); así mismo, tomar en cuenta que: el traslado, alimentación para el personal de la empresa proveedora del servicio, estará a cargo de la misma.

Se deberá considerar un plazo máximo de entrega del servicio **de ochenta (80) días calendario**, este periodo de tiempo incluye la entrega de informes finales, computables a partir de la orden de servicio.

En el plan de trabajo especificado en el **punto 8** del presente documento, tomar en cuenta, el trabajo a realizar, tanto in situ, es decir, en instalaciones de YPFB TRANSPORTE S.A., como en gabinete (ejemplo: elaboración de informes).

## 7. ENTREGABLES

Los entregables del servicio de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) – Fase II Diagnostico de situación actual de YPFB TRANSPORTE S.A. en Seguridad de la Información respecto a la norma ISO/IEC 27001:2022, son los siguientes:

1. **Informe de hallazgos de la brecha de seguridad:** documento que detalla los resultados del análisis de brechas, identificando la brecha entre las prácticas actuales de seguridad de la información y los requisitos establecidos por la norma ISO/IEC 27001:2022.
2. **Matriz de brechas:** tabla que muestra de manera clara y concisa las brechas encontradas, indicando los requisitos específicos de la norma ISO/IEC 27001:2022, ISO/IEC 27002:2022 y cómo difieren de las prácticas actuales de seguridad de la información en YPFB TRANSPORTE S.A.
3. **Documentos del Sistema de Gestión Integrado (SGI) políticas, reglamentos y procedimientos actualizados:** documentos revisados y actualizados que reflejen los cambios necesarios para cumplir con los requisitos de seguridad de la información de la norma ISO/IEC 27001:2022.
4. **Registro de análisis de riesgos:** documento que registra los riesgos identificados durante el análisis de brechas y las medidas propuestas para mitigarlos.
5. **Plan de acción:** documento que describe las medidas específicas que se deben tomar para abordar cada brecha identificada, incluyendo plazos, responsables y recursos necesarios para implementar las correcciones (controles de seguridad de la información).
6. **Informe ejecutivo:** Resumen de alto nivel dirigido a la alta dirección, destacando las principales brechas de seguridad de la información encontradas y las acciones recomendadas para abordarlas.

## 8. PRESENTACION Y FORMATO DE PROPUESTAS

La propuesta técnica deberá incluir lo siguiente:

1. Un plan del trabajo por el servicio de diagnóstico de situación actual en seguridad de la información (determinación de la brecha de seguridad), donde se especificará un cronograma de actividades, el tiempo de duración y responsables asignados.
2. Carta de aceptación de todas y cada una de las especificaciones de servicio detalladas en los puntos 3, 4, 5, 6 y 7 del presente documento.
3. Curriculum vitae y organigrama del personal que participará del servicio y las funciones de cada uno.
4. El profesional auditor líder deberá demostrar conocimiento (mediante certificados de cursos o trabajos realizados con la norma ISO/IEC 19011) de la norma ISO/IEC 19011 Directrices para la auditoria de los sistemas de gestión.
5. Al menos dos (2) recursos humanos asignadas al servicio, deberán presentar el certificado del curso de Implementador de Sistemas de Gestión de Seguridad de la Información, basado en la norma ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información, certificado del curso de implementador de Sistemas de Gestión de Seguridad de la Información ISO/IEC 27001:2022; otorgado por una entidad competente.
6. Al menos un (1) recurso humano asignado al servicio, deberá demostrar conocimiento en la norma ISO 31000 Gestión del riesgo – Principios y Directrices.

7. Al menos un (1) recurso humano asignado al servicio, deberá demostrar conocimientos en infraestructuras críticas y sistemas SCADA. Adjuntar certificados de cursos en el estándar ISA99/IEC-62443.
8. La empresa proveedora del servicio deberá demostrar experiencia en trabajos similares o referidos a la implementación de Sistemas de Gestión de Seguridad de la Información, en empresas bolivianas o extranjeras adjuntando a la propuesta al menos 3 certificados de trabajo u otro documento que acredite los trabajos realizados. Se verificará la documentación presentada.

## 9. PAGOS

El pago se realizará por hitos contra entrega de informes, de acuerdo al siguiente detalle:

HITO	Descripción de avance del servicio	Porcentaje de pago por el servicio	Entregable
1	<b>Ejecución del servicio:</b> <b>determinación de brecha, riesgos, controles de seguridad de la información, de:</b> <ul style="list-style-type: none"> <li>- Operaciones GAS</li> <li>- Operaciones Líquidos</li> <li>- Transporte por Poliductos</li> <li>- Proyectos y Construcciones</li> <li>- Control del Sistema</li> <li>- Mantenimiento</li> <li>- Gestión de calidad, Salud, Seguridad, Medio ambiente y RSE</li> </ul>	50%	<ul style="list-style-type: none"> <li>▪ Primer informe de avance</li> </ul>
2	<b>Ejecución del servicio:</b> <b>determinación de brecha, riesgos, controles de seguridad de la información, de:</b> <ul style="list-style-type: none"> <li>- Planificación</li> <li>- Comercial</li> <li>- Regulaciones</li> <li>- Administración y Finanzas</li> <li>- Contrataciones</li> <li>- Talento Humano</li> <li>- Legal</li> <li>- Tecnología de la Información</li> </ul>	50%	<ul style="list-style-type: none"> <li>▪ Contra entrega de informes, enunciados en el punto de 7 del presente TDR (informes aprobados).</li> </ul>