Términos de Referencia

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

Gestión 2023

INDICE DE CONTENIDO

1. INTRODUCCIÓN

YPFB TRANSPORTE S.A. invita a las empresas legalmente establecidas en Bolivia a presentar su propuesta para la provisión del Servicio de Análisis de Vulnerabilidades (Ethical Hacking), que comprende la evaluación de seguridad a la infraestructura tecnológica de TI e infraestructuras críticas OT (Operational Technology).

2. OBJETOS DEL REQUERIMIENTO

OBJETIVO GENERAL

Contratar un servicio para el análisis de vulnerabilidades a la infraestructura tecnológica de TI y OT de YPFB TRANSPORTE S.A. conforme a normativa interna y estándares internacionales.

OBJETIVOS ESPECIFICOS

El servicio busca satisfacer las siguientes necesidades:

- Identificar posibles vulnerabilidades que pueden ser explotadas tanto por atacantes (ciberdelincuentes) como 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 de los controles que actualmente se tienen implementados en la infraestructura tecnología de TI y OT de YPFB TRANSPORTE S.A.
- Verificar el cumplimiento de la normativa interna en seguridad de la información de YPFB TRANSPORTE S.A.
- Proporcionar los controles y las recomendaciones de remediación para las vulnerabilidades encontradas durante la ejecución del Servicio de Análisis de Vulnerabilidades (Ethical Hacking).

3. ALCANCE

El Análisis de Vulnerabilidades (Ethical Hacking) comprende la ejecución de pruebas (*test*) internas y externas, considerando los servicios publicados hacia internet y la red interna a fin de determinar el nivel de protección actual de los activos de información. Elaboración de un informe donde se detallen los resultados de las pruebas realizadas y presentación de recomendaciones para mitigar las vulnerabilidades encontradas.

- Análisis de vulnerabilidades a la infraestructura tecnologíca TI de YPFB TRANSPORTE S.A.

- Análisis de vulnerabilidades a las infraestructuras criticas OT de YPFB TRANSPORTE S.A.
  - Sitio operativo estación Terminal Santa Cruz
  - Sitio operativo estación Oleoductos Samaipata.

4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

A continuación, se detallan las características técnicas del servicio:

a) Para el análisis de vulnerabilidades se aplicará la metodología de Mitre ATT&CK, tanto para infraestructura de TI e infraestructuras criticas OT.

b) Se realizarán **test (pruebas) de caja blanca** (se proporciona información de aplicaciones, sistemas de información, diagramas de red, código fuente y toda información de la infraestructura tecnológica) y **test (pruebas) de caja negra** (no se tiene información previa sobre las políticas de seguridad, diagramas de red, código fuente, y demás información de infraestructura tecnológica).
c) Para el ***test*** de aplicaciones web se aplicará la metodología *Top Ten* de *OWASP* (Open Web Applications Security Project), que permite identificar: desde fallas de configuración segura de la plataforma, errores en su codificación y tratamiento de excepciones.
d) Realización de informes detallados sobre las vulnerabilidades encontradas, los riesgos asociados y las recomendaciones para su mitigación, conforme normas y estándares internacionales, tomando en cuenta controles de la norma ISO/IEC 27002 para IT e ISA99/IEC 62443 para OT.
e) 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).
f) 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.
g) 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. 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 criticas OT.	1	▪ Certificado GIAC GICSP – Global Industrial Cyber Security Professional. ICS/SCADA (SANS Institute) *. ▪ Curso certificado de ISO/IEC ISO 27001 e ISO/IEC 27002 *. ▪ Curso certificado de IEC 62443.

2	Profesional senior en Ethical Hacking (**vulnerabilidades externas)**	1	▪ Security Essentials - Network, Endpoint, and Cloud (SANS Institute) *. ▪ Certificado OSCP – Offensive Security Certified Professional *. ▪ Certificado OSWE - Offensive Security Web Expert *. ▪ Curso certificado de ISO/IEC ISO 27001 *.
3	Profesional en Ethical Hacking (**vulnerabilidades internas)**	1	▪ Certificado OSCP – Offensive Security Certified Professional *. ▪ Certificado OSWP - Offensive Security Wireless Professional *. ▪ Curso certificado de ISO/IEC ISO 27001 *.

*Los certificados de los profesionales propuestos que realizarán el trabajo, serán validados; esto para verificar la vigencia de los mismos. Se deberá proporcionar enlaces (links) de referencia donde se pueda constatar la veracidad y vigencia de las certificaciones presentadas.

7. INFRAESTRUCTURA TI PARA REALIZACION DEL ANÁLISIS DE VULNERABILIDADES

Nro.	Ítem	Cantidad	Observaciones
1	Aplicaciones y servicios web publicados	6	-
2	Servidores internos a testear (físicos y virtuales).	11	-
3	Dispositivos de red y telecomunicaciones (firewall, switch, router, etc)	10	-
4	Equipos clientes (PCs de escritorio, computadoras portátiles)	30	Dos segmentos de red
5	Cámaras de vigilancia IP	8	Corresponde al Sistema de Control de Acceso y Video vigilancia
6	Ingeniería Social (Phishing)	30	Envió de correos electrónicos

8. INFRAESTRUCTURA OT PARA REALIZACION DEL ANÁLISIS DE VULNERABILIDADES

Nro.	Ítem	Cantidad	Observaciones
1	Sitio operativo	2	En estaciones de YPFB TRANSPORTE S.A.

2	Zonas a testear (SCADA, SSP, SCP, F&G)	6	En estaciones de YPFB TRANSPORTE S.A.
3	Servidores internos a testear (físicos y virtuales)	3	Dentro de la infraestructura de TI
4	Dispositivos de red y telecomunicaciones en sitios operativos: switch (2), router(2), modem (2), aceleradores de tráfico (2).	8	Dirección de TI / Jefatura de mantenimiento medición, control, comunicación y SCADA.
5	Equipos finales a testear (estaciones de ingeniería, mantenimiento, operadores)	4	En estación Oleoductos Samaipata / Terminal Santa Cruz
6	PLCs / RTUs a testear	24	En estación Oleoductos Samaipata / 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.

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 sitios operativos Estación Terminal Santa Cruz (17°52'57.6"S 63°11'55.0"W) y Estación oleoducto Samaipata (18°09'54.0"S 63°48'34.6"W); así mismo, tomar en cuenta que: la alimentación, viáticos y equipo de protección personal (EPP) para el personal de la empresa proveedora del servicio, estará a su cargo.

El traslado a **sitios operativos** del personal de la empresa proveedora del servicio, estará a cargo de YPFB TRANSPORTE S.A., como actividad de seguimiento y supervisión del trabajo de Análisis de Vulnerabilidades a realizar.

Se deberá considerar un plazo máximo de **entrega de 45 días calendario**, computables a partir de la orden de servicio.

11.ENTREGABLES

Los entregables del servicio son:

- Resumen ejecutivo.

- Informe final del trabajo realizado, que contemple las recomendaciones para la mitigación de vulnerabilidades encontradas. El informe deberá contar con un acápite tanto para la infraestructura de IT e infraestructura OT.
- Listado de servicios y dispositivos analizados.
- Vulnerabilidades encontradas en los sistemas, servicios y dispositivos. Gravedad de cada una de las vulnerabilidades.
- Intrusiones realizadas en los sistemas. Vulnerabilidades y servicios con alta posibilidad de ser explotados para llevar a cabo la intrusión.

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 de todas y cada una de las especificaciones de servicio detalladas en los incisos 3, 4, 5, 6, 7, 8, 9, 10 y 11 del presente documento.
- Curriculum vitae del personal técnico que participará del servicio y la función de cada uno.
- El personal asignado al servicio, deberá contar con las certificaciones requeridas en el **punto 6. PERSONAL REQUERIDO PARA EL SERVICIO,** del presente documento.
- La empresa proveedora del servicio deberá adjuntar a la propuesta al menos 3 certificados de trabajo de Análisis de vulnerabilidades y/o PENTEST realizados en empresas bolivianas.

13.PAGOS

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

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.