

ANÁLISIS DE VULNERABILIDADES

INFORME TÉCNICO

Jean Carlos Iglesias Palma
Ingeniero consultor

Octubre 06 de 2025

CONFIDENCIALIDAD DEL DOCUMENTO

Toda la información contenida en el presente documento deberá mantenerse en forma estrictamente **confidencial**. Se prohíbe copiar y reproducir este documento o parte de este sin la debida autorización. El equipo de trabajo no asumirá responsabilidad ni obligación por cualquier pérdida sufrida, como resultado de la circulación, publicación, reproducción u otro uso de este reporte contrario a lo previsto en esta sección.

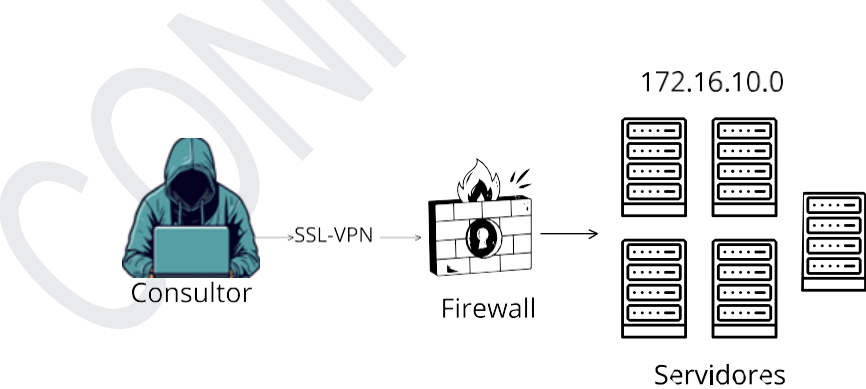
CONFIDENCIAL

1. ALCANCE

El alcance definido para estas pruebas de reevaluación está asociado con los sistemas de información evaluados en la prueba de septiembre del 2024 y cuyo objetivo de trabajo fue identificar y evidenciar las principales vulnerabilidades técnicas de las plataformas tecnológicas. El análisis realizado por la empresa TECSER & CLOUD, arrojo 7 hallazgos que fueron subsanados. Las pruebas realizadas pueden considerarse como una instantánea en el tiempo. Los hallazgos y recomendaciones reflejan la información recopilada durante la evaluación. Estas pruebas se planifican para un periodo mensual.

Alcance	
Tipo Pruebas	<div>✓ Análisis de vulnerabilidades semiautomatizado con supervisión de Ethical Hacker.</div> <div>✓ Caja negra: El equipo evaluador no tiene conocimiento de la infraestructura, no cuenta con usuarios por lo cual se realiza una revisión de seguridad enfocada en el análisis de las áreas accesibles de forma anónima. A excepción de la conexión provista para la VPN requerida para realizar el trabajo de forma remota.</div>
Fecha - Horarios	<div>3, 4 y 5 de Enero de 2025</div> <div>Sin restricción horaria 24/7 modalidad conexión VPN SLL</div>
Objetivos	<div>172.16.10.100</div> <div>172.16.10.110</div> <div>172.16.10.115</div> <div>172.16.10.120</div> <div>172.16.10.80</div>

Para realizar las pruebas se dispuso de una conexión VPN SSL entre el equipo del consultor y la infraestructura a analizar.

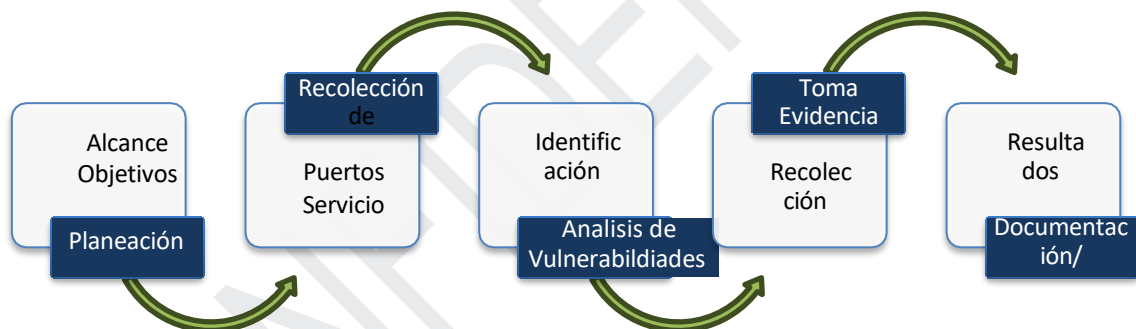


2. METODOLOGÍA

El análisis y el desarrollo de las pruebas se realizó tomando como referencia los siguientes estándares: OSSTMM (Open Standard Security Testing Methodology Manual), PTES (Penetration Testing Execution Standard), OWASP y Metodología de EC-Council. Para este alcance no se consideró explotación de las vulnerabilidades y se limitó a la reevaluación de las pruebas realizadas y sobre los hallazgos de la prueba del septiembre 2024 realizada por la empresa TECSER & CLOUD.

La metodología empleada permite:

- Proveer resultado bajo un esquema de administración del riesgo, relacionándolo con el esquema de seguridad existente.
- Comunicar los hallazgos encontrados que representan un mayor riesgo y/o exposición para la plataforma tecnológica.
- Identificar los sistemas relevantes y evaluar el riesgo relacionado con las vulnerabilidades detectadas.
- Desarrollar soluciones tecnológicas y/o estratégicas enfocadas a tratar los riesgos identificados.
- Generar una adecuada documentación de todas las etapas del trabajo.



Las pruebas de corrección se realizan sobre los hosts definidos en el alcance del proyecto y se comprueba el estado de corrección de las vulnerabilidades reportadas en el año 2023. Para ello se ejecutan las siguientes actividades:

- Análisis de vulnerabilidades con el software NESSUS SCANNER.
- Análisis de vulnerabilidades con el software INSIGHTVM.
- Análisis de puertos con el software nmap.
- Análisis de vulnerabilidades con el software BURPSUITE Professional.
- Comprobación manual por el ingeniero a cargo de la prueba.

3. RESULTADOS

Luego de la ejecución de las pruebas sobre los sistemas de información que hacen parte de esta prueba se tiene el siguiente resumen que se ilustra en la **tabla 1**.

#	Hallazgo	Criticidad	Estado	Razón
1	SSL No se puede confiar en el certificado.	Riesgo Medio	CORREGIDO	Se realiza bloque de puerto http// se admite https://
2	Detección de protocolo TLS versión 1.0	Riesgo Medio	CORREGIDO	Se realiza la habilitación de protocolos TLS 1.2 y 1.3 para los servidores 172.16.10.90, 172.16.10.115 y 172.16.10.120

De los 7 hallazgos reportados y corregidos en el informe del mes de septiembre realizado por la empresa TECSER & CLOUD, se evidencian nuevas correcciones para el sistema de bases de Datos SQL del servidor .80 y la recomendación para la adquisición de los certificados de seguridad SSL para los servidores de la aplicación Neotel

4. NUEVOS HALLAZGOS

Durante las pruebas realizadas se determinaron nuevos hallazgos, no obstante, se realizan actualizaciones de seguridad para el servidor de bases de datos y el versionamiento para Mysql Y SQL Server y la corrección de un hallazgo critico SSL con conjuntos de cifrado de potencia media compatibles con SWEET32 corregido.

CONCLUSIONES Y RECOMENDACIONES

- Basados en los resultados y en los análisis realizados se recomienda la adquisición y/o compra de certificados SSL para los servidores de la aplicación Neotel, 172.16.10.115/ y 172.16.10.120/

CONFIDENTIAL