EnerGo

FO-SF-121

Protocolo de análisis de vulnerabilidades

Punto 49 del Anexo 10 RMF 2026 | Monedero electrónico de combustibles

Empresa	SENDERO FUEL S.A. DE C.V.	**Fecha**	29/06/2026
Área responsable	Seguridad de la Información / TI	**Versión**	1.0
Código	FO-SF-121	**Estatus**	Preoperativo / controlado
Elaboró	Seguridad de la Información	**Revisó**	TI / Control Interno
Referencia	PR-SF-014; documentación técnica integral del monedero; reporte SF-P49	**Producto**	Monedero electrónico de combustibles

1. Alcance autorizado

El análisis comprende todos los dispositivos y activos relacionados con el monedero electrónico de combustibles, incluyendo centros de datos NGX y ASSETEL, ambientes de producción, QA, desarrollo, DRP, red de oficina, equipos de red, servidores, servicios API, Portal Clientes, ERP, GLPI, estaciones afiliadas, dispositivos móviles y repositorios/pipelines asociados.

Elemento	Condición aprobada
Permiso de ejecución	Confirmado por SENDERO FUEL y proveedores involucrados.
Producto regulado	Monedero electrónico de combustibles.
Ventana preoperativa	Horario abierto por no existir operación productiva activa.
Ventana posterior a operación	Fines de semana, preferentemente después de las 20:00 horas.
Restricciones	No realizar pruebas destructivas, DoS/DDoS, extracción masiva de datos, persistencia no autorizada ni modificación de registros productivos.

2. Herramientas autorizadas

Herramienta	Uso previsto	Evidencia generada	Control PR-SF-014
Nmap	Descubrimiento de hosts, puertos y versiones.	Archivos .nmap, .xml, .gnmap y resumen de servicios.	Solicitud FO-SF-054 y bitácora FO-SF-056.
Greenbone/OpenVAS CE	Escaneo de infraestructura con pruebas autenticadas/no autenticadas.	Reporte PDF/CSV con CVE, CVSS, evidencia y recomendación.	Registro en padrón independiente FO-SF-055.
OWASP ZAP	Pruebas DAST de Portal/API.	Reporte HTML/PDF de alertas y evidencia.	Ventana controlada y revisión posterior.
Nuclei	Detección por plantillas de exposiciones, CVE y configuraciones.	Reporte TXT/JSON por severidad.	Alcance limitado a URLs/IPs autorizadas.
Trivy / Dependency-Check	Vulnerabilidades de dependencias y configuración.	Reporte JSON/HTML/SARIF.	Uso sobre repositorios autorizados.
Gitleaks	Detección de secretos en repositorios.	Reporte JSON/SARIF y evidencia de exclusiones.	Resguardo confidencial de hallazgos.

3. Secuencia de ejecución

Fase	Actividad	Salida esperada
Preparación	Validar autorización, alcance, responsables, ventana, respaldos y contactos de escalamiento.	Ticket/solicitud, matriz de activos, autorización de herramientas.
Descubrimiento	Identificar activos activos, puertos, servicios, versiones, certificados y rutas web.	Inventario técnico y mapa de superficie de ataque.
Análisis automatizado	Ejecutar herramientas por segmento y criticidad.	Reportes originales de herramienta.
Validación manual	Eliminar falsos positivos, validar impacto y confirmar criticidad.	Ficha de validación por hallazgo.
Clasificación	Asignar severidad CVSS ajustada por criticidad del activo y exposición.	Matriz FO-SF-124.
Remediación	Asignar responsable, SLA, acción correctiva y evidencia esperada.	Plan FO-SF-125 y tickets de seguimiento.
Reescaneo/cierre	Validar corrección y conservar evidencia antes/después.	Formato FO-SF-128 y reporte de revalidación.

4. Comandos y parámetros de referencia

Actividad	Comando / ejecución autorizada	Precauciones
Nmap descubrimiento	nmap -Pn -sV --version-light --top-ports 1000 -oA SF49_NMAP_<segmento>_<fecha> <rango_autorizado>	No usar scripts intrusivos ni pruebas de fuerza bruta sin autorización específica.
ZAP baseline	zap-baseline.py -t <URL_autorizada> -r SF49_ZAP_<activo>_<fecha>.html	Ejecutar contra QA o ventana aprobada; no modificar datos.
Nuclei	nuclei -u <URL_autorizada> -severity critical,high,medium -o SF49_NUCLEI_<activo>.txt	Usar plantillas no destructivas.
Trivy	trivy fs --scanners vuln,secret,misconfig <repositorio> --format json	Ejecutar sobre copia o repositorio autorizado.
Gitleaks	gitleaks detect --source <repositorio> --report-format json	Resguardar reportes como confidenciales.

5. Criterios de suspensión

- Afectación a disponibilidad, degradación perceptible o caída de servicio.
- Detección de modificación no prevista en configuraciones, datos o bitácoras.
- Hallazgo crítico que implique exposición activa de credenciales o datos.
- Ejecución fuera de alcance, ventana o cuenta autorizada.
- Solicitud expresa de TI, Seguridad, proveedor de centro de datos o responsable del activo.

6. Evidencia mínima

- Solicitud de autorización y registro de herramienta.
- Listado de activos incluidos y excluidos.
- Reportes originales de herramienta.
- Matriz de hallazgos y clasificación.
- Plan de remediación, tickets y responsables.
- Evidencia de reescaneo y cierre.