EnerGo

FO-SF-126

Protocolo de pruebas de penetración para activos críticos

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-126	**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. Objetivo

Validar de forma controlada la resistencia de los activos críticos del monedero electrónico de combustibles frente a escenarios razonables de ataque, sin afectar disponibilidad, integridad ni confidencialidad de la plataforma.

2. Activos críticos incluidos

Activo crítico	Motivo de criticidad	Pruebas permitidas
Portal Clientes / API	Canal de autenticación, consulta, administración y operación del monedero.	DAST, pruebas de autenticación, autorización, sesión, headers, rate limit y exposición de endpoints.
SRV-MON-APP-PR / SRV-MON-SER-PR	Aplicación y backend productivo del monedero.	Pruebas no destructivas, revisión de configuración, exposición y rutas públicas.
SRV-MON-DB-PR	Base de datos transaccional.	Validación de exposición, segmentación, cuentas de servicio y hardening; sin extracción masiva.
FortiGate NGX / Oficina / ASSETEL	Perímetro, VPN IPSEC y segmentación.	Revisión de superficie de administración, puertos, políticas, MFA y acceso por ACL.
DRP ASSETEL	Continuidad y recuperación.	Validación de exposición, replicación, segmentación y accesos administrativos.
Estaciones afiliadas	Canal de autorización de carga y comunicación con backend.	Pruebas de segmentación, credenciales, alcance VPN y checklist de configuración.

3. Reglas de enfrentamiento

- No realizar DoS, DDoS, estrés, fuzzing destructivo, borrado, alteración, persistencia ni exfiltración de datos.
- No ejecutar exploits destructivos ni pruebas de fuerza bruta sin autorización específica adicional.
- Usar cuentas nominativas, temporales y con alcance delimitado.
- Registrar hora de inicio, hora de cierre, responsable, IP de origen, herramienta y resultado.
- Suspender inmediatamente ante degradación de servicio o desviación del alcance.
- Coordinar con proveedores de centro de datos, estaciones y mesa de ayuda.

4. Casos de prueba autorizados

Caso	Descripción	Evidencia esperada
PT-01 Descubrimiento controlado	Identificación de puertos, servicios, versiones, certificados y cabeceras.	Nmap, ZAP, Nuclei, capturas y matriz de servicios.
PT-02 Autenticación y sesión	Validar login, OTP, expiración, bloqueo progresivo y protección de tokens.	Casos de prueba, logs y capturas de respuestas controladas.
PT-03 Autorización horizontal/vertical	Validar que usuarios no accedan a datos, tarjetas, consumos o reportes ajenos.	Pruebas con usuarios de bajo privilegio y respuestas 401/403.
PT-04 API y errores	Revisar exposición de Swagger, mensajes de error, métodos HTTP y validación de entrada.	Reporte ZAP/Nuclei y evidencia manual.
PT-05 Infraestructura y perímetro	Validar administración restringida, segmentación y servicios innecesarios.	Nmap/OpenVAS, configuración y pruebas de acceso denegado.
PT-06 Código y secretos	Detectar dependencias vulnerables, secretos, tokens o cadenas de conexión.	SonarQube, Trivy, Dependency-Check, Gitleaks.

5. Criterios de reporte

Cada hallazgo de pentest deberá reportarse con identificador, activo, vector, severidad, evidencia, impacto, prueba no destructiva realizada, recomendación, responsable de remediación, SLA y criterio de cierre.