EnerGo

FO-SF-120

Calendario anual 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-120	**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

Objetivo del formato

Programar, controlar y evidenciar la ejecución periódica de análisis de vulnerabilidades sobre activos del monedero electrónico de combustibles, equipos de red, servidores, ambientes, estaciones conectadas y dispositivos autorizados.

Mes	Actividad	Alcance	Herramientas	Responsable	Ventana	Estatus	Observaciones
Julio 2026	Levantamiento base preoperativo	Todos los activos del alcance	Nmap, OpenVAS, ZAP, Nuclei, Trivy, Gitleaks	Seguridad / TI	Horario abierto	Programado	Primer baseline antes del inicio de operaciones.
Agosto 2026	Escaneo mensual de infraestructura	Producción, QA, desarrollo, oficina, DRP	OpenVAS autenticado/no autenticado, Nmap	Infraestructura	Horario abierto	Programado	Actualizar matriz y validar cierres.
Septiembre 2026	Prueba web/API trimestral	Portal Clientes, API, GLPI y servicios expuestos	OWASP ZAP, Nuclei	Desarrollo / Seguridad	Horario abierto o fin de semana 20:00	Programado	Revisar headers, rate limit, exposición de endpoints y diagnóstico.
Octubre 2026	Revisión de código y dependencias	API, Portal, App móvil, ERP, pipelines	SonarQube, Trivy, Dependency-Check, Gitleaks	DevOps / Desarrollo	Por liberación	Programado	Vincular con gestión de cambios.
Noviembre 2026	Escaneo mensual + red interna	Firewalls, switches, NAS, DB, VMware	OpenVAS, Nmap, revisión hardening	Infraestructura	Fin de semana 20:00	Programado	Validar segmentación, SNMP, SMB y administración.
Diciembre 2026	Prueba de penetración semestral	Activos críticos: API, portal, VPN, producción, DRP	ZAP, Nuclei, Nmap, pruebas manuales controladas	Seguridad / tercero autorizado	Fin de semana 20:00	Programado	Requiere autorización formal conforme PR-SF-014.
Enero 2027	Reescaneo de remediación	Activos con hallazgos abiertos	Herramienta original + validación manual	Responsables de activos	Según cambio	Programado	Cierre documental y evidencia comparativa.

FO-SF-120	Calendario anual de análisis de vulnerabilidades		EnerGo
Emisión: 29/06/2026	Versión: 1.0	Área: Seguridad de la Información / TI	Confidencial - uso interno

Mes	Actividad	Alcance	Herramientas	Responsable	Ventana	Estatus	Observaciones
Febrero 2027	Escaneo mensual y revisión de estaciones	Estaciones afiliadas y equipos auxiliares	Nmap controlado, checklist proveedor	Operaciones / proveedor	Ventana acordada	Programado	Credenciales, segmentación y acceso por VPN.
Marzo 2027	Prueba web/API trimestral	Portal, API, autenticación y OTP	ZAP, Nuclei, pruebas manuales	Desarrollo / Seguridad	Fin de semana 20:00	Programado	Validar abuso de OTP, login y endpoints.
Abril 2027	Revisión de código y secretos	Repositorios y CI/CD	SonarQube, Trivy, Gitleaks	DevOps	Por liberación	Programado	Rotación de secretos y calidad de código.
Mayo 2027	Escaneo mensual de infraestructura	Todos los segmentos autorizados	OpenVAS, Nmap	Infraestructura	Fin de semana 20:00	Programado	Vincular resultados a FO-SF-123/125.
Junio 2027	Revisión anual y actualización de plan	Todos los activos y formatos 120-128	Consolidación documental	Seguridad / Control Interno	Horario administrativo	Programado	Actualizar procedimiento y métricas.

Criterios de programación

- En etapa preoperativa, la ejecución puede realizarse en horario abierto con autorización vigente.
- Al iniciar operación productiva, las pruebas intrusivas se harán preferentemente fines de semana después de las 20:00 horas.
- Cada actividad debe generar solicitud/autorización de herramienta, reporte técnico, clasificación, plan de remediación y evidencia de cierre cuando aplique.
- Los reescaneos se programarán dentro de los SLA de remediación: crítica 72 horas, alta 15 días, media 30 días, baja 60-90 días.