EnerGo

FO-SF-125

Plan de remediación y seguimiento

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-125	**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

Plan de remediación

ID	Sev.	Responsable	Acción correctiva	SLA	Fecha compromiso	Evidencia de cierre	Estatus
SF49-PT-001	Crítica	Seguridad / Infraestructura	Restringir administración de firewall a red de gestión, MFA, ACL y bitácoras.	72 horas	02/07/2026	Captura de configuración, prueba de acceso denegado desde red no autorizada, log de MFA.	Abierto
SF49-PT-002	Alta	Desarrollo / TI	Deshabilitar o proteger Swagger/OpenAPI en QA y producción; limitar por IP/VPN.	15 días	14/07/2026	Captura 401/403, regla en proxy/IIS, reescaneo ZAP/Nuclei sin alerta.	Abierto
SF49-PT-003	Alta	Desarrollo / Infraestructura	Aplicar headers de seguridad en IIS/reverse proxy y validar CSP/HSTS.	15 días	14/07/2026	Reporte ZAP limpio o con riesgo aceptado; evidencia de web.config/proxy.	Abierto
SF49-PT-004	Alta	Redes	Migrar a SNMPv3, cambiar comunidades y restringir por ACL.	15 días	14/07/2026	Configuración exportada, intento SNMPv2 fallido, logs de consulta autorizada.	Abierto
SF49-PT-005	Alta	Infraestructura	Revisar permisos SMB, aplicar grupos nominativos y activar firma SMB.	15 días	14/07/2026	Listado de ACL, captura de política SMB, reescaneo de configuración.	Abierto
SF49-PT-006	Alta	DBA / Infraestructura	Cerrar puertos DB a segmentos no autorizados; whitelisting y reglas de host firewall.	15 días	14/07/2026	Nmap posterior sin exposición no autorizada; matriz de reglas aprobada.	Abierto
SF49-PT-007	Alta	Desarrollo / Seguridad	Rate limit por IP/usuario/dispositivo en login, OTP, recuperación y reenvío.	15 días	14/07/2026	Prueba controlada de bloqueo progresivo; logs de alerta.	Abierto
SF49-PT-008	Media	TI / Soporte	Actualizar GLPI, ocultar banners y restringir acceso a red administrativa.	30 días	29/07/2026	Versión actualizada, acceso denegado desde red no autorizada, ZAP/Nuclei actualizado.	Abierto
SF49-PT-009	Media	Infraestructura / Desarrollo	Estandarizar certificados internos y deshabilitar TLS obsoleto.	30 días	29/07/2026	Reporte SSL/TLS, captura de certificado válido y configuración de protocolos.	Abierto

ID	Sev.	Responsable	Acción correctiva	SLA	Fecha compromiso	Evidencia de cierre	Estatus
SF49-PT-010	Media	Infraestructura	Separar red de gestión VMware y obligar acceso mediante jump server con MFA.	30 días	29/07/2026	Diagrama actualizado, ACL, bitácoras de acceso, prueba de segmentación.	Abierto
SF49-PT-011	Alta	Operaciones / Proveedor estación	Rotar credenciales, eliminar defaults y documentar configuración segura por estación.	15 días	14/07/2026	Acta de proveedor, checklist de estación, evidencia de credenciales únicas.	Abierto
SF49-PT-012	Media	DevOps / Seguridad	Implementar secret scanning, vault y rotación documentada de tokens.	30 días	29/07/2026	Pipeline con Gitleaks, evidencia de rotación y reporte sin secretos.	Abierto

Lineamientos de seguimiento

- Los hallazgos críticos se revisarán diariamente hasta su mitigación.
- Los hallazgos altos se revisarán al menos dos veces por semana hasta cierre.
- Todo cierre requiere evidencia técnica, ticket y revalidación por Seguridad de la Información.
- Si no es posible remediar dentro del SLA, se documentará aceptación temporal de riesgo residual con controles compensatorios y fecha límite.