EnerGo

Análisis de vulnerabilidades y pruebas de penetración Monedero electrónico de combustibles

SENDERO FUEL S.A. DE C.V. / EnerGo

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

EnerGo

Índice

1. Objetivo y alcance
2. Marco documental y normativo
3. Activos considerados en el alcance
4. Metodología de análisis y pruebas
5. Herramientas utilizadas
6. Calendarización y ventanas de ejecución
7. Criterios de clasificación y SLA de remediación
8. Resumen ejecutivo de hallazgos
9. Matriz de hallazgos técnicos
10. Plan de remediación y seguimiento
11. Evidencia técnica de referencia
12. Validación de cierre
13. Anexos y referencias

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

EnerGo

1. Objetivo y alcance

El presente documento es un reporte integral correspondiente al análisis de vulnerabilidades y pruebas de penetración de los activos que soportan el monedero electrónico de combustibles de **SENDERO FUEL**. El reporte se estructura para evidenciar el cumplimiento documental del Punto 49 del Anexo 10 de la RMF 2026, incluyendo calendarización, protocolo de análisis, documentación de resultados, clasificación de vulnerabilidades, lineamiento de remediación y protocolo de pruebas de penetración para activos críticos.

El alcance técnico comprende los activos relacionados con las actividades del **monedero electrónico de combustibles**, equipos de red, servidores, servicios expuestos, ambientes de producción, QA/pruebas, desarrollo, sitio alterno DRP, oficina corporativa, canales conectados, estaciones de servicio afiliadas y equipos administrativos autorizados.

2. Marco documental y normativo

El Punto 49 requiere que la persona moral cuente con un procedimiento para gestionar vulnerabilidades técnicas de activos relacionados con el monedero electrónico, equipos de empleados y equipos de red. Para que el reporte sea auditable, cada hallazgo debe vincularse con evidencia técnica, clasificación de riesgo, responsable, acción correctiva, plazo de remediación y prueba de cierre.

El uso de herramientas de análisis de vulnerabilidades se vincula con el Punto 29, por lo que toda herramienta debe estar autorizada, registrada, acotada en alcance, ejecutada por personal autorizado y respaldada con evidencia de uso y cierre.

Documento / referencia	Uso dentro del reporte
PR-SF-014 Procedimiento para el uso de herramientas de análisis de vulnerabilidades	Controla autorización, registro independiente, vigencia, evidencia, cierre y controles compensatorios para herramientas como escáneres, utilerías administrativas y plataformas de monitoreo.
Documentación técnica integral del monedero electrónico de combustibles	Identifica arquitectura, stack tecnológico, servicios API, Portal Clientes, ERP, base de datos, CI/CD, seguridad técnica y trazabilidad de transacciones.
Anexo 10 RMF 2026, Punto 49	Base de cumplimiento para calendarización, análisis, resultados, clasificación, remediación y pentest de activos críticos.
ISO/IEC 27001:2022, control 8.8	Gestión de vulnerabilidades técnicas dentro del sistema de gestión de seguridad de la información.
OWASP WSTG / OWASP MASTG	Guías de referencia para pruebas de aplicaciones web, servicios API y aplicación móvil.
NIST SP 800-40 Rev. 4 / CIS Control 7	Buenas prácticas para gestión de parches, priorización, seguimiento y cierre de vulnerabilidades.

3. Activos considerados en el alcance

La matriz de activos se construye a partir de la arquitectura empresarial del monedero, la cual contempla centros de datos NGX y ASSETEL, producción activa, sitio alterno DRP/standby, oficina corporativa, VPN IPSEC, FortiGate, VMware, almacenamiento, plataforma del monedero y canales conectados.

Ubicación	Activo	Tipo	IP/FQDN	Función	Criticidad
NGX / Producción activa	FW-FTNET-NGX-01	FortiGate 200F	10.20.1.1	Perímetro y red	Crítico
NGX / Producción activa	SW-HP-NGX-01	HP FlexFabric 5700	10.20.1.2	Switch / red	Alto
NGX / Producción activa	HST-PRLN-01/02/03	Hosts VMware	10.20.1.4-10.20.1.6	Virtualización	Crítico
NGX / Producción activa	STR-MSA-01	Almacenamiento iSCSI	10.20.1.10	Almacenamiento	Crítico

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

Ubicación	Activo	Tipo	IP/FQDN	Función	Criticidad
NGX / Producción activa	VLT-SONCE-01	Respaldo inmutable	10.20.1.30	Backup	Crítico
NGX / Producción activa	SRV-NAS-APP	NAS / red	10.100.30.9	Repositorio / archivos	Alto
NGX / Producción activa	SRV-MON-DB-PR	Base de datos monedero	172.16.52.10	Base de datos	Crítico
NGX / Producción activa	SRV-MON-APP-PR	Aplicación monedero	172.16.52.11	Aplicación	Crítico
NGX / Producción activa	SRV-MON-SER-PR	Servicios web/backend	172.16.52.12	API / backend	Crítico
NGX / QA	SRV-MON-DB-QA	Base de datos QA	172.16.51.10	Pruebas	Alto
NGX / QA	SRV-MON-APP-QA	Aplicación QA	172.16.51.11	Pruebas	Alto
NGX / QA	SRV-MON-SER-QA	Servicios QA	172.16.51.12	Pruebas API	Alto
NGX / Desarrollo	SRV-MON-DB-DV	Base de datos desarrollo	172.16.50.10	Desarrollo	Medio
NGX / Desarrollo	SRV-MON-APP-DV	Aplicación desarrollo	172.16.50.11	Desarrollo	Medio
NGX / Desarrollo	SRV-MON-SER-DV	Servicios desarrollo	172.16.50.12	Desarrollo API	Medio
ASSETEL / DRP standby	FW-ASSETEL-NGX-01	FortiGate 300E	10.30.1.1	Perímetro DRP	Crítico
ASSETEL / DRP standby	HST-PRLN-04/05/06	Hosts VMware DRP	10.30.1.13-10.30.1.15	Virtualización DRP	Crítico
ASSETEL / DRP standby	STR-MSA-02 / VLT-SONCE-02	Almacenamiento y backup	10.30.1.18 / 10.30.1.9	Almacenamiento DRP	Alto
Oficina EnerGo	FW-FG200F-03	FortiGate 200E	10.100.0.1	Perímetro oficina	Alto
Oficina EnerGo	SW-ARUBA-2930	Switch Aruba 2930	10.100.0.14	Red oficina	Alto
Gestión y seguridad	SRV-GLPI	Tickets / soporte	10.255.248.26	Gestión TI	Medio
Canales conectados	Estaciones afiliadas	Equipos estación / dispensarios	192.168.2.x / 192.168.3.x / 192.168.x.x	Operación transaccional	Crítico
Canales conectados	Portal Clientes / API	Servicios web/API	FQDN interno/externo	Servicios expuestos	Crítico
Canales conectados	App móvil / operadores	Dispositivos móviles	N/A	Canal usuario	Alto

4. Metodología de análisis y pruebas

La metodología se organiza en fases controladas para evitar afectación a la disponibilidad, integridad o confidencialidad de la plataforma. Las actividades intrusivas quedan limitadas por reglas de enfrentamiento, ventanas autorizadas y criterios de suspensión.

Fase	Actividades	Evidencia
1. Preparación	Confirmar autorización, alcance, responsables, ventanas, cuentas de prueba y mecanismos de respaldo.	Solicitud autorizada, ticket GLPI, alcance firmado, lista de activos.
2. Descubrimiento	Identificar hosts, puertos, servicios, versiones, certificados, rutas web, endpoints y dependencias.	Reporte Nmap, inventario actualizado, mapa de servicios.
3. Análisis de vulnerabilidades	Ejecutar escaneo autenticado y no autenticado sobre red, servidores, web/API, código y dependencias.	Reportes Greenbone/OpenVAS, ZAP, Nuclei, Trivy, Dependency-Check, SonarQube.
4. Validación manual	Confirmar falsos positivos, revisar configuración y validar impacto sin explotación destructiva.	Hoja de validación, capturas controladas, evidencia de configuración.
5. Clasificación	Asignar severidad con CVSS, criticidad del activo, exposición, explotación conocida e impacto al negocio.	Matriz de clasificación y priorización.
6. Remediación	Asignar responsables, fechas compromiso, acciones correctivas, mitigaciones temporales y aceptación de riesgo residual.	Plan de remediación y tickets de seguimiento.
7. Reescaneo y cierre	Validar corrección mediante reescaneo, revisión de configuración y evidencia de cierre.	Reporte de validación, acta de cierre y actualización de matriz.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

EnerGo

5. Herramientas a utilizar

Herramienta	Propósito	Aplicación en SENDERO FUEL	Evidencia
Nmap	Descubrimiento de hosts, puertos y versiones.	Red, firewalls, servidores, estaciones, oficina.	Salida .nmap/.xml/.gnmap.
Greenbone Community Edition / OpenVAS	Escaneo de vulnerabilidades de infraestructura con pruebas autenticadas y no autenticadas.	Servidores, red, equipos de oficina, perímetro interno.	Reporte PDF/CSV con CVE, CVSS y evidencias.
OWASP ZAP	Pruebas DAST de aplicaciones web y API.	Portal Clientes, API monedero, endpoints de autenticación.	Reporte HTML/PDF de alertas.
Nuclei	Detección rápida con plantillas para tecnología web, exposición, CVE y configuraciones comunes.	Portal, API, GLPI, IIS, servicios internos.	Reporte JSON/Markdown.
Trivy	Análisis de dependencias, contenedores, sistemas de archivos, IaC y secretos.	Repositorios, contenedores, paquetes.	Reporte SARIF/JSON.
OWASP Dependency-Check	Identificación de dependencias vulnerables.	Backend .NET, frontend Angular, app móvil, ERP.	Reporte HTML/XML.
SonarQube Community Build	Análisis estático de calidad y seguridad del código.	Repositorios de API, Portal, App móvil y ERP.	Dashboard, issues y quality gate.
Gitleaks	Detección de secretos en repositorios.	GitHub/GitLab, carpetas de código, pipelines.	Reporte JSON/SARIF.

6. Calendarización y ventanas de ejecución

Tipo de actividad	Frecuencia recomendada	Alcance	Objetivo
Pre-operación	Quincenal o por cambio relevante	Todos los activos del alcance	Validar endurecimiento inicial antes de operar.
Operación normal	Mensual	Infraestructura, servidores, red y servicios internos	Detectar vulnerabilidades nuevas y desviaciones de configuración.
Perímetro y servicios expuestos	Trimestral	Portal, API, VPN, GLPI, servicios publicados	Evaluar exposición externa e interna con enfoque de ataque.
Código y dependencias	Cada liberación y mínimo mensual	Repositorios, pipelines, paquetes y contenedores	Evitar vulnerabilidades introducidas por cambios.
Prueba de penetración	Semestral y después de cambios mayores	Activos críticos: API, portal, app, VPN, producción, DRP	Validar controles de autenticación, sesión, autorización, exposición y segmentación.
Reescaneo de cierre	Después de cada remediación	Activos con hallazgos críticos, altos o medios	Comprobar efectividad de la corrección.

Durante la etapa previa al inicio de operaciones, las pruebas pueden ejecutarse en horario abierto. Al iniciar operación productiva, los análisis intrusivos y pruebas de penetración deberán programarse en fines de semana, preferentemente después de las 20:00 horas, con aviso previo a TI, proveedor de centro de datos, responsable del monedero y mesa de ayuda.

7. Criterios de clasificación y SLA de remediación

Severidad	Criterio	SLA / tratamiento
Crítica	CVSS 9.0-10.0 o impacto equivalente; explotación remota, compromiso de credenciales, ejecución de código, bypass de autenticación o afectación directa a producción.	Mitigación inmediata y remediación ≤ 72 horas. Escalamiento a Dirección si no puede cerrarse.
Alta	CVSS 7.0-8.9 o exposición importante; acceso no autorizado parcial, configuración insegura, componente vulnerable explotable o pérdida de trazabilidad.	Remediación ≤ 15 días naturales. Mitigación temporal obligatoria si el activo es crítico.
Media	CVSS 4.0-6.9; requiere condiciones adicionales, acceso interno o impacto limitado.	Remediación ≤ 30 días naturales o en siguiente ventana de mantenimiento aprobada.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

Severidad	Criterio	SLA / tratamiento
Baja	CVSS 0.1-3.9; bajo impacto o baja probabilidad de explotación.	Remediación ≤ 60-90 días o inclusión en hardening programado.
Informativa	No implica vulnerabilidad directa, pero mejora trazabilidad, seguridad o postura de cumplimiento.	Atención según plan de mejora continua.

La priorización no debe depender únicamente del puntaje CVSS. Se debe ajustar por criticidad del activo, exposición, existencia de explotación conocida, facilidad de remediación, impacto a confidencialidad de contribuyentes, continuidad del monedero y relación con puntos del Anexo 10.

8. Resumen ejecutivo de hallazgos

Severidad	Cantidad	Tema principal
Crítica	1	Interfaz administrativa de perímetro expuesta a red amplia sin endurecimiento suficiente.
Alta	6	Exposición de servicios sensibles, configuración débil en red/equipos, headers web faltantes, rate limit incompleto y permisos excesivos.
Media	4	Versionado visible, segregación mejorable, TLS/certificados y controles de bitácora incompletos.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

EnerGo

9. Matriz de hallazgos técnicos

ID	Activo	Categoría	Sev.	CVSS	Hallazgo	Riesgo	Recomendación
SF49-PT-001	FW-FG200F-03 / FW-FTNET-NGX-01	Perímetro / administración	Crítica	9.1	Interfaz administrativa accesible desde segmentos amplios de red interna/VPN, sin restricción granular por IP administrativa y sin evidencia de MFA obligatorio.	Posible toma de control de firewall, modificación de reglas, pérdida de disponibilidad o exposición de tráfico del monedero.	Limitar administración a red de gestión, activar MFA, restringir por ACL, deshabilitar administración por WAN/VPN general y registrar accesos.
SF49-PT-002	SRV-MON-APP-QA	Portal QA	Alta	8.2	Swagger/OpenAPI y paneles de diagnóstico accesibles en QA sin restricción suficiente.	Divulgación de rutas, modelos, parámetros y endpoints útiles para abuso de API.	Restringir por IP/VPN administrativa, requerir autenticación, desactivar en producción y limitar información de errores.
SF49-PT-003	SRV-MON-SER-QA / Portal Clientes	API / Web	Alta	8.0	Faltan headers de seguridad: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options o Referrer-Policy.	Aumenta riesgo de clickjacking, downgrade, fuga de referencia y ataques de navegador.	Configurar headers en IIS/reverse proxy, validar con ZAP/Nuclei y documentar baseline seguro.
SF49-PT-004	SW-ARUBA-2930 / SW-HP-NGX-01	Switches	Alta	7.5	SNMP v2c habilitado o comunidad débil en equipos de red.	Obtención de información de red, interfaces, rutas y configuración; posible abuso por actores internos.	Migrar a SNMPv3, cambiar comunidades, restringir por ACL y registrar consultas.
SF49-PT-005	SRV-NAS-APP	NAS / archivos	Alta	8.1	Compartidos SMB con permisos amplios y firma SMB no requerida.	Acceso no autorizado a paquetes, respaldos o archivos de aplicación; riesgo de alteración o ransomware.	Aplicar mínimo privilegio, grupos nominativos, SMB signing, auditoría de accesos y segregación de red.
SF49-PT-006	SRV-MON-DB-DV / SRV-MON-DB-QA	Bases de datos no productivas	Alta	8.3	Puertos de base de datos accesibles desde segmentos no administrativos y sin lista blanca estricta.	Riesgo de fuerza bruta, enumeración, extracción de datos de prueba y movimiento lateral.	Aplicar firewall local, ACL por host autorizado, cuentas de servicio con mínimos privilegios y monitoreo de intentos fallidos.
SF49-PT-007	Portal Clientes / API OTP	Autenticación	Alta	8.4	Rate limiting no uniforme en endpoints de login, recuperación y reenvío OTP.	Abuso de OTP, enumeración de usuarios o consumo de mensajería.	Aplicar límites por IP, usuario, dispositivo y ventana temporal; bloqueo progresivo y alertas.
SF49-PT-008	SRV-GLPI	Soporte / gestión	Media	6.8	Versionado visible de plataforma y servicios; banners técnicos expuestos.	Facilita selección de exploits contra GLPI, servidor web o componentes asociados.	Ocultar banners, actualizar GLPI, aplicar hardening y restringir acceso a red de gestión.
SF49-PT-009	SRV-MON-APP-DV / SRV-MON-SER-DV	Desarrollo	Media	6.5	Certificados autofirmados o TLS débil en servicios internos de desarrollo.	Riesgo de interceptación interna y falta de trazabilidad de certificados.	Emitir certificados internos confiables, deshabilitar TLS obsoleto y documentar política de certificados.
SF49-PT-010	HST-PRLN-01/02/03	VMware / gestión	Media	6.4	Interfaces de gestión de virtualización visibles desde segmentos operativos.	Aumenta superficie de ataque contra hipervisores y administración de máquinas virtuales.	Separar red de gestión, restringir por jump server, MFA y bitácora centralizada.
SF49-PT-011	Estaciones afiliadas / equipos de dispensario	Operación transaccional	Alta	8.6	Equipos de estación con credenciales por defecto o contraseñas compartidas en componentes auxiliares.	Riesgo de manipulación de autorización, tickets o comunicación con el backend del monedero.	Eliminar usuarios por defecto, credenciales únicas por estación, MFA donde aplique y revisión de configuración por proveedor.
SF49-PT-012	Repositorios / CI-CD	Código y pipelines	Media	6.7	Variables, tokens o cadenas de conexión sin rotación documentada; evidencia incompleta de escaneo de secretos.	Riesgo de fuga de credenciales y despliegues no autorizados.	Usar vault/secret manager, rotación programada, Gitleaks en pipeline y revisión trimestral de secretos.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

10. Plan de remediación y seguimiento

ID	Responsable	Acción correctiva	SLA	Evidencia de cierre	Estatus
SF49-PT-001	Seguridad / Infraestructura	Restringir administración de firewall a red de gestión, MFA, ACL y bitácoras.	72 horas	Captura de configuración, prueba de acceso denegado desde red no autorizada, log de MFA.	Abierto
SF49-PT-002	Desarrollo / TI	Deshabilitar o proteger Swagger/OpenAPI en QA y producción; limitar por IP/VPN.	15 días	Captura 401/403, regla en proxy/IIS, reescaneo ZAP/Nuclei sin alerta.	Abierto
SF49-PT-003	Desarrollo / Infraestructura	Aplicar headers de seguridad en IIS/reverse proxy y validar CSP/HSTS.	15 días	Reporte ZAP limpio o con riesgo aceptado; evidencia de web.config/proxy.	Abierto
SF49-PT-004	Redes	Migrar a SNMPv3, cambiar comunidades y restringir por ACL.	15 días	Configuración exportada, intento SNMPv2 fallido, logs de consulta autorizada.	Abierto
SF49-PT-005	Infraestructura	Revisar permisos SMB, aplicar grupos nominativos y activar firma SMB.	15 días	Listado de ACL, captura de política SMB, reescaneo de configuración.	Abierto
SF49-PT-006	DBA / Infraestructura	Cerrar puertos DB a segmentos no autorizados; whitelisting y reglas de host firewall.	15 días	Nmap posterior sin exposición no autorizada; matriz de reglas aprobada.	Abierto
SF49-PT-007	Desarrollo / Seguridad	Rate limit por IP/usuario/dispositivo en login, OTP, recuperación y reenvío.	15 días	Prueba controlada de bloqueo progresivo; logs de alerta.	Abierto
SF49-PT-008	TI / Soporte	Actualizar GLPI, ocultar banners y restringir acceso a red administrativa.	30 días	Versión actualizada, acceso denegado desde red no autorizada, ZAP/Nuclei actualizado.	Abierto
SF49-PT-009	Infraestructura / Desarrollo	Estandarizar certificados internos y deshabilitar TLS obsoleto.	30 días	Reporte SSL/TLS, captura de certificado válido y configuración de protocolos.	Abierto
SF49-PT-010	Infraestructura	Separar red de gestión VMware y obligar acceso mediante jump server con MFA.	30 días	Diagrama actualizado, ACL, bitácoras de acceso, prueba de segmentación.	Abierto
SF49-PT-011	Operaciones / Proveedor estación	Rotar credenciales, eliminar defaults y documentar configuración segura por estación.	15 días	Acta de proveedor, checklist de estación, evidencia de credenciales únicas.	Abierto
SF49-PT-012	DevOps / Seguridad	Implementar secret scanning, vault y rotación documentada de tokens.	30 días	Pipeline con Gitleaks, evidencia de rotación y reporte sin secretos.	Abierto

10.1 Lineamiento de aceptación de riesgo residual

Cuando una vulnerabilidad no pueda corregirse dentro del SLA por dependencia técnica, ventana operativa o tercero proveedor, el responsable del activo deberá documentar aceptación temporal de riesgo residual. La aceptación debe incluir justificación, controles compensatorios, fecha límite, responsable de seguimiento y aprobación de Seguridad de la Información y Dirección cuando la severidad sea crítica o alta.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

EnerGo

11. Evidencia técnica de referencia

Las siguientes salidas muestran el tipo de evidencia que deberá conservarse por herramienta. Los comandos deben ejecutarse únicamente dentro del alcance autorizado, con ventanas aprobadas y conforme al PR-SF-014.

Actividad	Comando / ejecución	Evidencia
Descubrimiento Nmap	nmap -Pn -sV --version-light --top-ports 1000 -oA SF49_NMAP_SCOPE_YYYYMMDD <rango_autorizado>	Inventario de hosts, puertos, protocolos y versiones.
Escaneo Greenbone/OpenVAS	Tarea autenticada/no autenticada por segmento: producción, QA, desarrollo, oficina y DRP.	Reporte de CVE, CVSS, evidencia de detección y recomendación.
Prueba web/API OWASP ZAP	zap-baseline.py -t <URL_autorizada> -r SF49_ZAP_PORTAL_YYYYMMDD.html	Alertas de headers, cookies, TLS, configuración y exposición web.
Nuclei	nuclei -u <URL_autorizada> -severity critical,high,medium -o SF49_NUCLEI.txt	Detección rápida de exposiciones, CVE y configuraciones conocidas.
Trivy / Dependency-Check	trivy fs --scanners vuln,secret,misconfig <repositorio> / dependency-check --scan <ruta>	Vulnerabilidades de dependencias, secretos, configuración insegura.
Gitleaks	gitleaks detect --source <repositorio> --report-format json	Secretos, tokens, credenciales y cadenas de conexión expuestas.

11.1 Extracto de resultados representativos

Herramienta	Activo	Resultado	Hallazgo relacionado
Nmap	SRV-MON-DB-QA 172.16.51.10	1433/tcp o 5432/tcp visible desde segmento no administrativo	SF49-PT-006
ZAP	Portal Clientes QA	Missing Content-Security-Policy / HSTS / X-Frame-Options	SF49-PT-003
Nuclei	SRV-MON-APP-QA	Swagger UI/OpenAPI expuesto	SF49-PT-002
OpenVAS	SW-ARUBA-2930	SNMP v2c o comunidad débil detectada	SF49-PT-004
OpenVAS	SRV-NAS-APP	SMB signing not required / shares enumerables	SF49-PT-005
Gitleaks	Repositorios CI/CD	Patrón de token o secreto pendiente de validación manual	SF49-PT-012

12. Validación de cierre

Cada hallazgo deberá cerrarse únicamente cuando exista evidencia verificable de remediación y revalidación.

Severidad	Criterio de cierre	Evidencia mínima
Crítica / Alta	Reescaneo obligatorio con herramienta original y validación manual.	Reporte comparativo, logs, ticket y aceptación de Seguridad.
Media	Reescaneo o revisión técnica de configuración, según naturaleza del hallazgo.	Captura, configuración exportada y resultado de prueba.

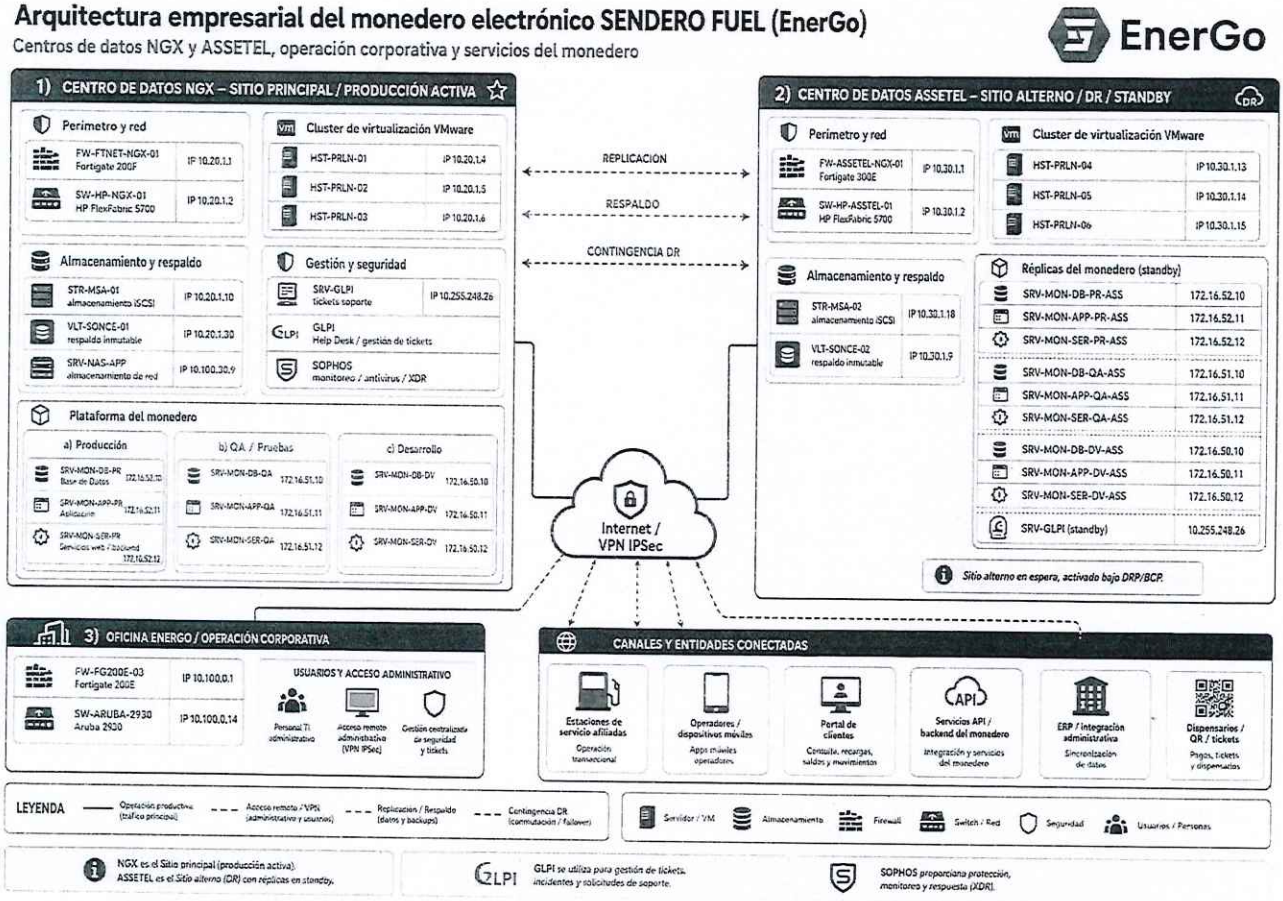
Cuando una remediación implique cambio en reglas de firewall, configuración de IIS, API, base de datos, credenciales, pipeline o infraestructura, deberá vincularse también al procedimiento de gestión de cambios, con respaldo previo, ventana de ejecución, validación posterior y plan de reversa.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

13. Anexos y referencias

13.1 Diagrama de arquitectura considerado



El diagrama identifica los centros de datos NGX y ASSETEL, producción activa, sitio alterno DRP/standby, plataforma del monedero, oficina corporativa, canales conectados, VPN IPSEC, FortiGate, VMware, almacenamiento, respaldos y servicios de gestión.

13.2 Referencias técnicas

- SAT, Resolución Miscelánea Fiscal 2026, Anexo 10, Punto 49.
- SENDERO FUEL, PR-SF-014 Procedimiento para el uso de herramientas de análisis de vulnerabilidades.
- SENDERO FUEL, Documentación técnica integral del monedero electrónico de combustibles.
- ISO/IEC 27001:2022, Anexo A, control 8.8 Gestión de vulnerabilidades técnicas.
- FIRST, Common Vulnerability Scoring System v4.0.
- NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning.
- OWASP Web Security Testing Guide y OWASP Mobile Application Security Testing Guide.
- CIS Critical Security Controls, Control 7 Continuous Vulnerability Management.

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido

13.3 Criterios de pruebas no destructivas

- No ejecutar pruebas de denegación de servicio, estrés o degradación intencional sin autorización separada.
- No modificar datos productivos, consumos, saldos, facturación ni registros fiscales.
- No extraer información sensible; cualquier evidencia deberá anonimizarse y limitarse al mínimo necesario.
- Suspender la prueba ante afectación operativa, alerta crítica o desviación respecto al alcance autorizado.
- Conservar bitácoras completas de inicio, ejecución, hallazgo, escalamiento y cierre.

APARTADO DE FIRMAS

Validación, aprobación y responsabilidad técnica del documento / ejecución de actividades relacionadas con el Punto 49 del Anexo 10.

VALIDÓ POR SENDERO FUEL	APROBÓ POR DIRECCIÓN	EJECUTÓ PRUEBAS TÉCNICAS
Axel Martínez Rentería Oficial de Seguridad de SENDERO FUEL Analista Administrativo / Seguridad de la Información	**Romina Monserrat Barbosa Apodaca** CEO / Gerente ENERGO Responsable de aprobación ejecutiva	**SMARTCONSULTING MÉXICO** Responsable de la ejecución del pentest Representada por Ing. Emanuel Andrés Parraga, CISSP No. 601993

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de carácter estrictamente confidencial. Este material deberá permanecer en todo momento en el ambiente interno de SENDERO FUEL S.A DE C.V.

SENDERO FUEL S.A DE C.V. podrá ejercer acción legal en contra de el o los individuos que hagan uso indebido de la información contenida en este documento, o que hayan facilitado dicho uso indebido