FO-SF-0054	SOLICITUD Y AUTORIZACIÓN DE USO DE HERRAMIENTA QUE PUEDE OMITIR CONTROLES DE SEGURIDAD		ENERGO SENDERO FUEL S.A. DE C.V. SENDERO FUEL
Emisión: 08/04/2026	Revisión: 29/06/2026	Versión: 1	Formato
Área: TI / SEGURIDAD DE LA INFORMACIÓN			

1. DATOS GENERALES DE LA SOLICITUD

Folio	SF-P49-HVA-2026-001
Fecha de solicitud	29/06/2026
Área solicitante	Seguridad de la Información / TI
Responsable técnico	Administrador de infraestructura y responsable de seguridad del monedero
Proveedor / tercero, si aplica	Proveedores de centro de datos, soporte de red, desarrollo y estaciones, conforme a permisos vigentes.
Ambiente	☒ Desarrollo ☒ Pruebas ☒ Producción ☒ Contingencia / DRP
Ventana solicitada	Etapa pre-operativa: horario abierto, con monitoreo y posibilidad de suspensión inmediata. En operación productiva: fines de semana después de las 20:00 h.
Prioridad	☒ Alta ☐ Media ☐ Baja

2. IDENTIFICACIÓN DE LA HERRAMIENTA

Nombre de la herramienta	Kit controlado de herramientas de análisis de vulnerabilidades y pruebas de penetración P49: Nmap, Greenbone/OpenVAS, OWASP ZAP, Nuclei, Trivy, OWASP Dependency-Check, Gitleaks y SonarQube Community Build.
Fabricante / desarrollador	Nmap Project; Greenbone Community; OWASP; ProjectDiscovery; Aqua Security; SonarSource / comunidad open source.
Versión	Última versión estable autorizada al momento de ejecución; cada herramienta se registra individualmente en FO-SF-0055.
Tipo de herramienta	☒ Vulnerabilidades ☒ Monitoreo ☒ Diagnóstico ☒ Administración ☐ Otra
Licenciamiento / procedencia	Gratuito, open source o edición community; descarga desde sitios oficiales o repositorios verificados.
Cuenta / usuario que la operará	Cuenta nominativa de Seguridad/TI; cuenta temporal de escaneo autenticado cuando aplique; sin cuentas compartidas.

3. ALCANCE, RIESGO Y CONTROLES

Objetivo de uso	Ejecutar análisis de vulnerabilidades técnicas, validación de exposición, descubrimiento de servicios, revisión de configuración web/API, revisión de dependencias, secretos y controles de hardening sobre los activos del monedero electrónico de combustibles, para dar cumplimiento al Punto 49 del Anexo 10.

Activos / sistemas objetivo	Todos los dispositivos del alcance del monedero de combustibles: FortiGate/perímetro, switches, VMware, almacenamiento, servidores de aplicación, API, Portal Clientes, ERP, bases de datos, GLPI/soporte, repositorios CI/CD, DRP, equipos administrativos autorizados, VPN IPSEC y estaciones afiliadas.
Controles que podría omitir o afectar	Puede detonar alertas de IDS/IPS, WAF, rate limiting, bitácoras, bloqueo de cuentas de prueba, monitoreo de firewall o controles antiescaneo. No se autoriza explotación destructiva, denegación de servicio, evasión deliberada de controles ni extracción de datos productivos.
Nivel de privilegio requerido	☐ Estándar ☒ Elevado ☒ Administrativo ☒ Temporal
Riesgos identificados	Incremento temporal de tráfico; falsos positivos; exposición de reportes sensibles; bloqueo de cuentas de prueba; saturación de servicios si se ejecuta fuera de límites; activación de alertas; riesgo sobre credenciales de escaneo autenticado.
Controles compensatorios	Autorización formal; alcance delimitado; IP origen controlada; cuentas nominativas; MFA donde aplique; monitoreo en tiempo real; respaldo previo cuando corresponda; límite de velocidad; evidencia de ejecución; bitácora FO-SF-0056; registro FO-SF-0055; suspensión inmediata ante afectación.
Fecha de inicio	29/06/2026
Fecha de término	31/07/2026 para la primera jornada de validación; registro de herramientas vigente hasta 31/12/2026, sujeto a revisión semestral.
Justificación del uso autorizado	La herramienta es necesaria para identificar, clasificar, priorizar y remediar vulnerabilidades técnicas de activos relacionados con el monedero electrónico de combustibles, previo al inicio de operaciones y posteriormente bajo calendario de revisión periódica.

4. VALIDACIONES Y AUTORIZACIONES

☒ Se evaluó el riesgo asociado al uso de la herramienta
☒ Se delimitó el alcance técnico y operativo autorizado
☒ La vigencia de la autorización quedó definida
☒ Se identificaron los activos / sistemas impactados
☒ Se definieron controles compensatorios aplicables
☒ La herramienta se integrará al registro independiente FO-SF-0055
☒ La ejecución deberá documentarse en la bitácora FO-SF-0056 y vincularse a los formatos FO-SF-0120 a FO-SF-0128 del Punto 49.

Seguridad de la Información / TI Nombre y firma	Infraestructura / Administrador de sistemas Nombre y firma	Responsable de Seguridad de la Información Nombre y firma	Dirección / Responsable del monedero Nombre y firma