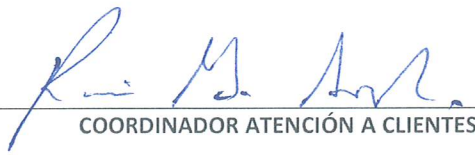
Revisado por:	Autorizado por:
	
COORDINADOR MMTO. Raúl Ernesto Galindo	**GERENTE ENERGO** Romina Monserrat Barbosa Apodaca
Revisado por:	**Autorizado por:**
	
COORDINADOR ATENCIÓN A CLIENTES Ramón Gabriel Salazar Rocha	**ANALISTA ADMINISTRATIVO** Axel Martínez Rentería
Representante Legal:	
	
REPRESENTANTE LEGAL David Orlando Navarro Santiesteban	

El contenido de este documento pertenece enteramente a SENDERO FUEL S.A DE C.V. y es de caracter 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.

Control de cambios

Capítulo/Apartado	Fecha	Descripción del Cambio	Editor	Versión
Todo el documento	29/6/2026	Creación del documento	Romina Monserrat Barbosa Apodaca	1

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

Contenido

1. DEFINICIÓN 1
2. OBJETIVO 1
3. ALCANCE 2
4. NORMATIVIDAD APLICABLE 2
5. FORMATOS RELACIONADOS 2
6. ROLES Y RESPONSABILIDADES 3
7. TIPOS DE ACTIVOS CUBIERTOS 4
8. LINEAMIENTOS GENERALES 4
9. PROCEDIMIENTO OPERATIVO 5
Identificación y actualización del inventario 5
Calendarización anual 5
Autorización de herramientas 6
Preparación de la ejecución 6
Ejecución del análisis de vulnerabilidades 6
Clasificación de vulnerabilidades 7
Registro de resultados 7
Plan de remediación y seguimiento 7
Validación de remediación y cierre 7
Aceptación de riesgo residual 8
Pruebas de penetración para activos críticos 8
Reporte ejecutivo y comunicación 8
10. CRITERIOS DE CLASIFICACIÓN Y TIEMPOS DE REMEDIACIÓN 8
11. INDICADORES DE CUMPLIMIENTO 9
12. INCUMPLIMIENTOS Y EXCEPCIONES 10
13. PERIODICIDAD DE REVISIÓN 10
14. GLOSARIO 12

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

1. DEFINICIÓN

Para **SENDERO FUEL**, la gestión de vulnerabilidades técnicas significa identificar, analizar, clasificar, priorizar, remediar y validar de manera formal las debilidades de seguridad que puedan afectar los activos tecnológicos relacionados con la operación del monedero electrónico de combustibles, incluyendo servidores, aplicaciones, bases de datos, equipos de red, infraestructura de comunicaciones, equipos de empleados, estaciones conectadas, ambientes de desarrollo, pruebas, producción y sitio alterno de recuperación.

Este procedimiento constituye el mecanismo formal mediante el cual la persona moral mantiene una vigilancia técnica continua sobre sus activos, documenta los resultados de análisis de vulnerabilidades y pruebas de penetración, asigna responsables de remediación, verifica la efectividad de las acciones correctivas y conserva evidencia suficiente para auditoría interna, revisión de seguridad y verificación tecnológica.

La gestión de vulnerabilidades no se limita a la ejecución de herramientas de escaneo. Comprende la actualización del inventario de activos, la autorización previa de herramientas, el control de ventanas de ejecución, la protección de información sensible, la coordinación con proveedores, el seguimiento de planes de remediación, la validación posterior mediante reescaneo y la aceptación formal de riesgos residuales cuando la corrección inmediata no sea técnica u operativamente viable.

2. OBJETIVO

Establecer el procedimiento mediante el cual SENDERO FUEL gestiona las vulnerabilidades técnicas de los activos relacionados con las actividades del monedero electrónico de combustibles, equipos de los empleados y equipos de red, asegurando que cada vulnerabilidad detectada sea registrada, clasificada, atendida, remediada, validada y cerrada con evidencia verificable.

El procedimiento tiene como objetivos específicos:

- Definir el ciclo de gestión de vulnerabilidades técnicas desde la identificación del activo hasta el cierre formal del hallazgo.
- Establecer responsabilidades claras para Seguridad de la Información, TI, proveedores, responsables de activos, desarrollo y usuarios custodios.
- Asegurar que las herramientas de análisis se utilicen bajo autorización, alcance y evidencia documental conforme al PR-SF-014.
- Definir criterios homogéneos de severidad, riesgo, SLA de atención y priorización de vulnerabilidades.
- Documentar los resultados de análisis de vulnerabilidades y pruebas de penetración en formatos controlados.
- Validar que las remediaciones implementadas reduzcan efectivamente el riesgo técnico identificado.
- Conservar evidencia suficiente para demostrar cumplimiento ante auditoría, revisión de seguridad y verificación tecnológica.

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

3. ALCANCE

Este procedimiento aplica a todos los activos tecnológicos que soportan, administran, protegen, transmiten, almacenan o permiten operar información del monedero electrónico de combustibles de **SENDERO FUEL**, incluyendo activos propios, administrados por proveedores o utilizados por terceros autorizados.

El alcance comprende, como mínimo:

- Aplicación móvil **SENDERO FUEL** y componentes asociados al canal de usuarios, conductores y administradores.
- Servicios API, Portal Clientes Monedero, ERP monedero, servicios web, endpoints, servicios de autenticación y componentes de integración.
- Bases de datos transaccionales, repositorios de información, respaldos, almacenamiento, documentación técnica y evidencias del monedero.
- Servidores de producción, desarrollo, pruebas/QA, sitio alterno DRP, hipervisores, máquinas virtuales, contenedores, runners de CI/CD y servicios de despliegue.
- Firewalls, VPN IPSEC, switches, routers, redes inalámbricas, enlaces, segmentos de gestión y componentes de seguridad perimetral.
- Equipos de empleados, laptops, estaciones de trabajo, dispositivos móviles, tokens, cuentas administrativas y equipos utilizados para soporte, operación, desarrollo, auditoría o seguridad.
- Equipos y componentes ubicados en oficinas, centros de datos, estaciones de servicio, sitios de proveedores, ambiente remoto y cualquier ubicación autorizada relacionada con el monedero electrónico.
- Herramientas de análisis de vulnerabilidades, escáneres, scripts, consolas y utilerías de diagnóstico utilizadas para evaluar los activos anteriores.

El alcance operativo será a todos los dispositivos relacionados con el monedero electrónico. Mientras **SENDERO FUEL** no haya iniciado operaciones productivas, las ventanas de análisis podrán ejecutarse en horario abierto, previa autorización interna. Una vez iniciada la operación, los análisis que puedan afectar disponibilidad deberán programarse preferentemente en fines de semana, después de las 20:00 horas, o en la ventana autorizada por el responsable del servicio.

4. NORMATIVIDAD APLICABLE

• Ley del Impuesto Sobre la Renta, Art. 27, Fracc. III

• Resolución Miscelánea Fiscal 2026, Anexo 10

• Resolución Miscelánea Fiscal 2026, Regla 3.3.1.8.

5. FORMATOS RELACIONADOS

• EV-SF-017 — DOC_SF_023 REPORTE PENTEST.pdf

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

- EV-SF-018 — ACTA_HECHOS_SMART.pdf
- FO-SF-120 — FO-SF-0120_Calendario_anual_analisis_vulnerabilidades_SENDERO_FUEL.docx
- FO-SF-121 — FO-SF-0121_Protocolo_analisis_vulnerabilidades_SENDERO_FUEL.docx
- FO-SF-122 — FO-SF-0122_Matriz_activos_sujetos_analisis_SENDERO_FUEL.docx
- FO-SF-123 — FO-SF-0123_Reporte_resultados_analisis_vulnerabilidades_SENDERO_FUEL.docx
- FO-SF-124 — FO-SF-0124_Clasificacion_vulnerabilidades_SENDERO_FUEL.docx
- FO-SF-125 — FO-SF-0125_Plan_remediacion_seguimiento_SENDERO_FUEL.docx
- FO-SF-126 — FO-SF-0126_Protocolo_pruebas_penetracion_activos_criticos_SENDERO_FUEL.docx
- FO-SF-127 — FO-SF-0127_Reporte_resultados_pruebas_penetracion_SENDERO_FUEL.docx
- FO-SF-128 — FO-SF-0128_Validacion_remediacion_cierre_SENDERO_FUEL.docx
- EV-SF-019 — FO-SF-0054_Solicitud_autorizacion_herramientas_P49_SENDERO_FUEL_LLENO.docx
- EV-SF-020 — FO-SF-0055_Registro_maestro_independiente_herramientas_P49_SENDERO_FUEL_LLENO.docx
- EV-SF-021 — FO-SF-0056_Bitacora_uso_cierre_herramientas_P49_SENDERO_FUEL_LLENO.docx

6. ROLES Y RESPONSABILIDADES

Rol / Puesto	Responsabilidades dentro del procedimiento
CEO / Gerencia	Aprobar el procedimiento, asegurar recursos, validar excepciones de alto impacto, recibir reportes ejecutivos de riesgo y autorizar aceptación de riesgo residual crítico o alto cuando aplique.
Oficial de Seguridad	Coordinar la gestión de vulnerabilidades, validar el alcance de análisis, autorizar herramientas junto con TI, revisar resultados, clasificar riesgos, dar seguimiento al plan de remediación y conservar evidencia documental.
Área de Tecnología de la Información / Proveedor TI	Mantener inventario técnico, preparar activos, ejecutar o acompañar escaneos, implementar hardening, parches, cambios de configuración, segmentación, reglas de firewall, actualizaciones y evidencias de cierre.
Responsable del activo o servicio	Validar criticidad del activo, autorizar ventana de análisis, evaluar impacto operativo, atender hallazgos asignados, aprobar remediaciones y aceptar resultados de revalidación.
Desarrollo / DevOps	Corregir vulnerabilidades de aplicación, dependencias, configuración, CI/CD, secretos, repositorios y despliegues; integrar pruebas de seguridad en el ciclo de liberación.
Proveedor externo de pruebas / SMARTCONSULTING MÉXICO	Ejecutar análisis o pruebas de penetración autorizadas, respetar alcance, documentar hallazgos, entregar reporte técnico, evidencia de ejecución y recomendaciones de remediación.

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

Usuarios custodios de equipos	Permitir revisiones de seguridad en equipos asignados, aplicar parches, reportar incidentes y cumplir restricciones de uso relacionadas con el monedero electrónico.
Representante legal / Apoderado legal	Firmar y rubricar el procedimiento y sus actualizaciones cuando se requiera evidencia formal ante revisión interna o verificación tecnológica.

7. TIPOS DE ACTIVOS CUBIERTOS

Tipo de activo	Ejemplos	Frecuencia mínima sugerida	Consideración de riesgo
Activos críticos del monedero	API, Portal Clientes, ERP, base de datos, QR, autenticación, facturación, consumos y trazabilidad.	Trimestral y ante cambios mayores	Alta criticidad por impacto operativo, fiscal y de seguridad.
Infraestructura de red y perímetro	FortiGate, VPN IPSEC, switches, routers, reglas, segmentos de gestión, enlaces con estaciones.	Semestral y ante cambios de red	Riesgo de exposición, movimiento lateral, acceso remoto no autorizado.
Servidores y plataformas	Producción, QA, desarrollo, DRP, hipervisores VMware, IIS, SQL Server, PostgreSQL, runners.	Trimestral o semestral según criticidad	Riesgo de servicios expuestos, parches faltantes y configuraciones inseguras.
Aplicaciones y código	App móvil, backend, portal, dependencias, librerías, repositorios, pipelines.	En cada liberación mayor y mínimo semestral	Riesgo de fallas OWASP, secretos, dependencias vulnerables o endpoints expuestos.
Equipos de empleados	Laptops, estaciones de trabajo, celulares, equipos de administradores, soporte y desarrollo.	Semestral y al alta/baja/cambio de custodio	Riesgo de malware, credenciales expuestas, cifrado ausente o privilegios excesivos.
Estaciones y terceros conectados	Equipos de estaciones, proveedores, enlaces, terminales y componentes de integración.	Anual o conforme contrato/alcance	Riesgo por dependencia de terceros y exposición de interconexiones.

8. LINEAMIENTOS GENERALES

- Todo análisis de vulnerabilidades deberá estar calendarizado o justificado por evento extraordinario.
- El inventario de activos sujetos a análisis deberá mantenerse actualizado antes de cada ejecución.

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

- No se podrán utilizar herramientas de escaneo, explotación, fuzzing o análisis profundo sin autorización previa **conforme al PR-SF-014 y los formatos FO-SF-0054, FO-SF-0055 y FO-SF-0056.**
- Los análisis deberán ejecutarse dentro del alcance aprobado, sin exceder rangos IP, dominios, aplicaciones, cuentas o ventanas autorizadas.
- Las pruebas de penetración sobre activos críticos deberán contar con reglas de enfrentamiento, autorización expresa, responsables, contactos de emergencia y criterios de suspensión.
- Los hallazgos deberán clasificarse con base en severidad técnica, criticidad del activo, exposición, impacto operativo, impacto fiscal y probabilidad de explotación.
- Toda vulnerabilidad deberá contar con responsable, acción correctiva, SLA, evidencia esperada y estatus de seguimiento.
- Las vulnerabilidades críticas o altas deberán informarse de inmediato al Oficial de Seguridad y al responsable del activo.
- Toda remediación deberá validarse mediante reescaneo, revisión técnica o evidencia equivalente antes de cerrarse.
- La aceptación de riesgo residual deberá ser excepcional, justificada, temporal, autorizada y revisable.
- Los resultados técnicos y reportes de vulnerabilidades son información confidencial y deberán resguardarse con acceso restringido.

9. PROCEDIMIENTO OPERATIVO

Identificación y actualización del inventario

1. El Oficial de Seguridad y TI actualizan la matriz FO-SF-0122 con todos los activos relacionados con el monedero electrónico, equipos de empleados y equipos de red.
2. Cada activo deberá contar, como mínimo, con identificador, nombre, tipo, responsable, ubicación, ambiente, IP/FQDN, sistema operativo o tecnología, criticidad, exposición y relación con el monedero.
3. Cuando exista un nuevo activo, cambio de arquitectura, modificación de conectividad, alta de estación, nuevo endpoint o cambio de proveedor, el activo deberá incorporarse a la matriz antes de entrar en operación.
4. Los activos no inventariados no deberán quedar excluidos del análisis cuando soporten, administren o protejan procesos del monedero electrónico.

Calendarización anual

1. El Oficial de Seguridad elaborará el **FO-SF-0120** Calendario anual de análisis de vulnerabilidades, considerando criticidad, exposición, historial de hallazgos y ventanas operativas.
2. Mientras no existan operaciones productivas, podrán ejecutarse análisis en horario abierto, previa coordinación con TI y proveedores.
3. Una vez iniciada la operación productiva, los análisis intrusivos o que puedan afectar disponibilidad se realizarán preferentemente fines de semana después de las 20:00 horas.
4. Los análisis no intrusivos, autenticados o de código podrán ejecutarse en horarios laborales si no afectan disponibilidad ni integridad de la operación.

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

5. Cualquier análisis fuera de calendario deberá documentarse como revisión extraordinaria por cambio, incidente, auditoría, nueva amenaza, liberación relevante o requerimiento de dirección.

Autorización de herramientas

1. Antes de ejecutar herramientas como Nmap, Greenbone/OpenVAS, OWASP ZAP, Nuclei, Trivy, Dependency-Check, Gitleaks, SonarQube, scripts de verificación o cualquier herramienta equivalente, el solicitante deberá llenar **FO-SF-0054.**
2. El Oficial de Seguridad y TI evaluarán objetivo, alcance, privilegios, impacto, controles compensatorios y evidencia esperada.
3. La herramienta autorizada se registrará o actualizará en FO-SF-0055, manteniendo un registro independiente del inventario general de software.
4. Cada ejecución deberá documentarse en FO-SF-0056, indicando fecha, responsable, activos, comandos o configuración general, evidencia y cierre.
5. Si la herramienta permite explotación, evasión de controles, prueba de contraseñas, análisis intrusivo, captura de tráfico o acceso privilegiado, deberá existir autorización reforzada y ventana específica.

Preparación de la ejecución

1. El responsable técnico confirma que el alcance, credenciales, contactos, ventanas, respaldos y monitoreo estén definidos antes de iniciar.
2. Se valida si el análisis será no autenticado, autenticado, de caja negra, caja gris, de aplicación, infraestructura, código, contenedor, red o endpoint.
3. Se notifica a las áreas involucradas cuando exista riesgo de alertas, consumo de recursos, bloqueo de cuentas o afectación de servicios.
4. En producción se verifica que exista punto de reversa, respaldo o procedimiento de contingencia cuando el análisis pueda modificar o estresar servicios.
5. Se documentan restricciones: no denegación de servicio, no extracción de datos reales, no modificación de información productiva, no uso de credenciales fuera del alcance y suspensión inmediata ante afectación.

Ejecución del análisis de vulnerabilidades

1. El análisis se ejecuta únicamente sobre activos autorizados en **FO-SF-0121 y FO-SF-0122**.
2. Para infraestructura se podrán utilizar herramientas de descubrimiento, puertos, versiones, configuración TLS, exposición de servicios y vulnerabilidades conocidas.
3. Para aplicaciones web y API se podrán utilizar pruebas OWASP, revisión de cabeceras, autenticación, autorización, rate limiting, CORS, Swagger/OpenAPI, control de sesión y errores.
4. Para código y dependencias se podrán utilizar análisis estático, revisión de secretos, dependencias vulnerables, contenedores, configuración y pipelines.
5. Para equipos de empleados se revisarán parches, EDR/antimalware, cifrado, cuentas privilegiadas, firewall local, configuración segura, software no autorizado y cumplimiento de políticas.
6. Para equipos de red se revisarán servicios de administración, SNMP, versiones, ACL, cifrado, reglas expuestas, credenciales por defecto, respaldo de configuración y segmentación.

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

7. Al terminar, se resguardan reportes, logs, capturas, exportaciones y observaciones técnicas en el repositorio de evidencias autorizado

Clasificación de vulnerabilidades

1. El Oficial de Seguridad revisa los hallazgos y elimina falsos positivos documentando la justificación.
2. Cada hallazgo se registra en **FO-SF-0124** con severidad, CVSS o criterio equivalente, activo afectado, descripción, impacto, probabilidad y evidencia.
3. La severidad podrá ajustarse considerando exposición pública, datos sensibles, rol del activo, controles compensatorios, facilidad de explotación y afectación a continuidad o cumplimiento fiscal.
4. Los hallazgos críticos y altos se notifican de inmediato al responsable del activo y a Gerencia cuando el riesgo lo amerite.

Registro de resultados

1. Los resultados se documentan en **FO-SF-0123**, incluyendo resumen ejecutivo, herramientas utilizadas, alcance, activos evaluados, fecha de ejecución, hallazgos, clasificación y recomendaciones.
2. Los reportes técnicos originales de las herramientas deberán conservarse como anexos o evidencia asociada.
3. Cuando se trate de prueba de penetración, el reporte se documentará en **FO-SF-0127** y deberá incluir metodología, limitaciones, hallazgos, evidencia, impacto y recomendaciones.
4. Los resultados se consideran confidenciales y se comparten únicamente con responsables autorizados.

Plan de remediación y seguimiento

1. Cada vulnerabilidad confirmada se registra en **FO-SF-0125** con responsable, acción correctiva, SLA, prioridad, fecha compromiso y evidencia de cierre esperada.
2. El responsable del activo deberá proponer la acción técnica: parche, actualización, hardening, deshabilitación de servicio, cambio de configuración, segmentación, restricción por ACL, rotación de credenciales, actualización de certificado, corrección de código o control compensatorio.
3. El Oficial de Seguridad dará seguimiento periódico hasta obtener evidencia de implementación.
4. Si el SLA no puede cumplirse, el responsable deberá justificar causa, riesgo residual, medida temporal y nueva fecha compromiso aprobada.

Validación de remediación y cierre

Una vulnerabilidad no podrá cerrarse únicamente con declaración del responsable; deberá contar con evidencia técnica verificable.

La validación podrá consistir en reescaneo, prueba puntual, revisión de configuración, captura de política, log, salida de comando, ticket de cambio, reporte actualizado o acta de cierre.

El cierre se documentará en FO-SF-0128, indicando resultado de validación, fecha, responsable validador, evidencia y estatus final.

Cuando el hallazgo persista, se mantiene abierto, se actualiza el plan de remediación y se reasigna fecha compromiso.

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

Aceptación de riesgo residual

Cuando una vulnerabilidad no pueda remediarse de inmediato por restricción técnica, contractual, operativa o dependencia de proveedor, podrá someterse a aceptación temporal de riesgo residual.

La aceptación deberá incluir justificación, activo afectado, impacto, controles compensatorios, vigencia, responsable y autorización de Gerencia u Oficial de Seguridad según criticidad.

Las vulnerabilidades críticas no deberán aceptarse sin control compensatorio y aprobación de alto nivel.

Toda aceptación deberá revisarse antes de su vencimiento y no constituye cierre definitivo salvo que se documente la eliminación del riesgo o su reducción a nivel aceptable.

Pruebas de penetración para activos críticos

Los activos críticos del monedero electrónico deberán someterse a pruebas de penetración de forma programada y ante cambios relevantes de arquitectura, exposición pública o funcionalidad crítica.

Antes de ejecutar la prueba se deberá completar **FO-SF-0126** con alcance, reglas de enfrentamiento, exclusiones, horarios, contactos, criterios de suspensión y autorización.

La ejecución deberá evitar afectación productiva no autorizada, extracción innecesaria de datos, persistencia, modificación de saldos, manipulación de consumos o alteración de evidencias fiscales.

Los resultados se registrarán en **FO-SF-0127 y se integrarán al FO-SF-0125** para seguimiento de remediación.

El cierre técnico se validará mediante **FO-SF-0128**.

Reporte ejecutivo y comunicación

El Oficial de Seguridad consolidará resultados por periodo, severidad, activo, responsable, SLA y estatus.

Gerencia recibirá un resumen ejecutivo con vulnerabilidades críticas/altas, tendencias, riesgos pendientes y necesidades de recursos.

No se compartirán detalles técnicos de explotación fuera de los responsables autorizados.

Cuando un hallazgo represente incidente de seguridad, se activará el procedimiento de atención de incidentes correspondiente.

10. CRITERIOS DE CLASIFICACIÓN Y TIEMPOS DE REMEDIACIÓN

Severidad	Criterio general	SLA máximo sugerido	Escalamiento
Crítica	Explotación probable o confirmada, exposición pública, acceso no autorizado, ejecución remota, afectación a	72 horas	Oficial de Seguridad, Gerencia y responsable del activo.

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

	información fiscal, saldos, QR, consumos o continuidad crítica.		
Alta	Vulnerabilidad explotable con impacto alto, servicio sensible expuesto, credenciales, administración remota insegura, ausencia de control clave o componente crítico desactualizado.	15 días naturales	Oficial de Seguridad y responsable del activo.
Media	Debilidad relevante con explotación condicionada, configuración insegura, versión vulnerable no crítica, cabeceras ausentes, segmentación parcial o control incompleto.	30 días naturales	Responsable del activo y TI.
Baja	Riesgo limitado, mejora de hardening, exposición menor, información no sensible o recomendación de configuración.	60 días naturales	Responsable del activo.
Informativa	Observación técnica, mejora preventiva o buena práctica sin riesgo inmediato identificado.	90 días o plan de mejora	Seguimiento ordinario.

11. INDICADORES DE CUMPLIMIENTO

Indicador	Forma de medición	Meta sugerida
Cobertura de activos	Activos analizados / activos sujetos a análisis en FO-SF-0122.	>= 95% por ciclo.
Cumplimiento de calendario	Análisis ejecutados / análisis programados en FO-SF-0120.	>= 90% anual.
Cierre en SLA	Hallazgos cerrados dentro de SLA / hallazgos cerrados.	>= 85%.
Vulnerabilidades críticas abiertas	Número de vulnerabilidades críticas vencidas.	0.
Reincidencia	Hallazgos repetidos por activo o causa raíz.	Tendencia decreciente.
Validación de cierre	Hallazgos cerrados con evidencia validada / hallazgos cerrados.	100%.

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

12. INCUMPLIMIENTOS Y EXCEPCIONES

Se considerará incumplimiento del procedimiento:

- Ejecutar análisis o pruebas sin autorización formal.
- Analizar activos fuera del alcance aprobado.
- No registrar herramientas en el padrón independiente cuando corresponda.
- No documentar resultados, evidencias, hallazgos o cierre.
- Cerrar vulnerabilidades sin evidencia técnica suficiente.
- No atender vulnerabilidades críticas o altas dentro del SLA sin justificación y autorización.
- Omitir el reporte de hallazgos críticos, incidentes o afectaciones al servicio.
- Compartir reportes técnicos con terceros no autorizados.

Toda excepción deberá documentarse por escrito, indicar motivo, vigencia, controles compensatorios, responsable, riesgo residual y autorización correspondiente. Las excepciones vencidas deberán considerarse vencimiento de control y registrarse como observación de seguridad.

13. PERIODICIDAD DE REVISIÓN

Revisión Ordinaria

Este documento deberá ser revisado de manera integral cada 6 meses, contados a partir de su última fecha de autorización, para asegurar su alineación con los objetivos estratégicos de **SENDERO FUEL** y los requisitos del Anexo 10 de la RMF vigente.

Revisión Extraordinaria

Se realizarán revisiones y actualizaciones inmediatas a este documento cuando se presente cualquiera de los siguientes supuestos:

Cambios Legislativos: Modificaciones en la Ley del ISR, el Código Fiscal de la Federación o la Resolución Miscelánea Fiscal que afecten la operación de monederos electrónicos.

Incidentes de Seguridad: Tras la ocurrencia de un incidente crítico que involucre a un proveedor y que revele deficiencias en los controles actuales.

Cambios Tecnológicos: Implementación de nuevas tecnologías en el monedero electrónico o cambios significativos en la infraestructura de Tecnologías de la Información (TIC) de la empresa

Resultados de Auditoría: Hallazgos derivados de verificaciones independientes o inspecciones de la autoridad que exijan robustecer los controles con terceros.

Responsable de la Revisión

La Dirección de **SENDERO FUEL**, en conjunto con el responsable de seguridad de la información, serán los encargados de validar las actualizaciones, asegurar su comunicación formal al personal y gestionar el control de versiones correspondiente.

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

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

14. GLOSARIO

Término	Definición
LFPDPPP	Ley Federal de protección de datos en propiedad de particulares.
Certificado SSL	El SSL (Secure Socket Layer) es un protocolo de seguridad para lograr que la transmisión de datos entre un servidor y un usuario, o viceversa, a través de Internet, sea completamente segura. El SSL es un protocolo abierto, por lo que puede ser empleado por cualquier fabricante de aplicaciones para Internet, siendo una de sus grandes ventajas el hecho de que se pueda utilizar con cualquiera de los servicios de Internet (WWW, FTP, noticias, correo), aunque lo más normal es que se utilice para el tráfico a través de la WWW. El protocolo se basa en la utilización de un sistema de cifrado que emplea algoritmos matemáticos y un sistema de claves que solamente conocen el usuario y el servidor. Estas claves permiten la encriptación de los datos para que nadie que no las tenga pueda leer su contenido.
Acuerdo de nivel de servicio	Herramienta que ayuda a proveedores y clientes o usuarios de un servicio a llegar a un consenso en términos de las características con las que se debe entregar un servicio, por ejemplo: Tiempo de respuesta, horario de disponibilidad, personal asignado, etc.
Arquitectura de Información	Se encarga del análisis, estructura y presentación de la información, se considera arquitectura de información al resultado de alinear la arquitectura de sistemas con la arquitectura de seguridad.
Arquitectura de Sistemas	Organización de un sistema, que incluye sus componentes, relaciones entre sí, así como los principios que gobiernan su diseño.
Cartera de proyectos	Conjunto de proyectos tecnológicos desarrollados para responder a las necesidades de la Institución.
Catálogo de Servicios	Contiene los servicios tecnológicos que se proporciona en este momento a sus clientes y sienta las bases para la posterior definición de los niveles de servicio que los clientes requieren. Puede ser usado para mostrar un perfil de Proveedor de Servicios TIC (Tecnología de Información y Comunicaciones) a la organización del cliente y da a los usuarios una visión de los servicios proporcionados.
Incidente	Cualquier evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio.
Indicadores de desempeño	Medida usualmente cuantitativa que ofrece información relevante para evaluar el cumplimiento de los objetivos de un plan, programa o proyecto.

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

Marco de trabajo	Conjunto de buenas prácticas, expresado como un conjunto de procesos repetibles creado por la Institución.
Plan estratégico	Es un documento oficial en él se reflejan cual será la estrategia a seguir por el rol responsable de la entrega de servicios de TI en el mediano y largo plazo.
Plan de implantación	Es el conjunto de actividades organizadas y proyectadas para que un sistema de información sea liberado a producción.
Plan de pruebas	Es el conjunto de pruebas organizadas y proyectadas para verificar que un sistema genera los resultados esperados.
Emergencia	Situación o asunto imprevisto que requieren una especial atención y deben solucionarse lo antes posible.
Plan táctico	El conjunto de actividades organizadas y proyectadas a corto plazo para lograr los objetivos planteados por el rol responsable de entrega de servicios de TI.
Portafolio de programas de inversión	Instrumento mediante el cual se fijan las metas que se obtendrán con la ejecución de un conjunto de proyectos de inversión en TI.
Problema	Causa desconocida de uno o más incidentes
Servicio	Es un conjunto de recursos de TI que brindan una capacidad y cumplen con una o más necesidades, está enfocado al cumplimiento de los objetivos del negocio y es percibido por el cliente como una solución coherente. Un medio de entregar valor a los clientes facilitando los resultados que los clientes quieren lograr.
TI	Tecnología de información.

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

CERTIFICADO DE INTEGRIDAD DIGITAL

SHA-256: 92b402Ea59ef2a12dee193E1780d8d230e2750c6f2f432e63ad1eb2c0d1f81cf0

Este documento es una copia fiel generada por el sistema el 2 de septiembre de 2026, 12:28 p.m..

PR-SF-023 · Versión 1 · Estado: draft

David Orlando Navarro Santiesteban

Representante Legal

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