ACUERDO DE TRANSFERENCIA DE INFORMACIÓN Y SEGURIDAD

ACUERDO DE TRANSFERENCIA DE INFORMACIÓN Y SEGURIDAD que celebran, por una parte, SENDERO FUEL, S.A. DE C.V., RFC SFU250224248, representada por DAVID ORLANDO NAVARRO SANTIESTEBAN, en lo sucesivo “SENDERO FUEL”; y por la otra, ENERFUEL TECH, S. DE R.L. DE C.V., RFC GTE130116TH7, representada por MARÍA ELODIA ROBLES BURGUEÑO, en lo sucesivo “ENERFUEL TECH”; conjuntamente, “LAS PARTES”.

Antecedentes

LAS PARTES mantienen una relación de prestación de servicios de soporte técnico y servicios informáticos integrales. La documentación contractual revisada contempla, entre otras actividades, soporte de infraestructura, mantenimiento de redes, instalación y mantenimiento de software, desarrollo de aplicaciones, seguridad informática y administración de información mediante servidores. Este Acuerdo establece los requisitos específicos para las transferencias y accesos a información relacionados con dichos servicios y con el monedero electrónico de combustibles.

1. Objeto y finalidad

El presente Acuerdo tiene por objeto establecer las condiciones técnicas, organizativas y contractuales bajo las cuales ENERFUEL TECH podrá recibir, consultar, transmitir, procesar, almacenar o tener acceso a información relacionada con la operación del monedero electrónico de combustibles, exclusivamente para la prestación de los servicios autorizados por SENDERO FUEL. El Acuerdo complementa el contrato principal y prevalece en materia de seguridad y transferencia de información cuando establezca obligaciones más estrictas.

2. Definiciones

- Información: cualquier dato, documento, registro, credencial, configuración, código, log, respaldo, dato transaccional, fiscal, operativo, técnico o de seguridad que sea comunicado o accesible con motivo de los servicios.
- Transferencia: cualquier envío, consulta, réplica, sincronización, acceso remoto, transmisión por API, VPN, portal, respaldo, correo autorizado o medio electrónico entre las Partes o sus sistemas.
- Información crítica: credenciales, secretos, configuraciones de seguridad, datos transaccionales del monedero, bases de datos, código fuente, respaldos, llaves criptográficas, logs y evidencias de seguridad.
- Incidente de seguridad: evento que afecte o pueda afectar confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la Información.

3. Principios de tratamiento y transferencia

- Limitación de finalidad: utilizar la Información únicamente para los servicios expresamente autorizados.
- Necesidad de conocer y mínimo privilegio: limitar el acceso a personal y cuentas indispensables.
- Prohibición de copia, extracción, duplicación o uso fuera de canales aprobados salvo autorización escrita.
- Integridad y trazabilidad: conservar registros que permitan identificar origen, destino, fecha, usuario, activo y resultado cuando técnicamente aplique.
- Retención mínima necesaria: no conservar Información por más tiempo del requerido por el servicio, la política de retención aplicable o la ley.
- No transferencia a terceros, filiales o subcontratistas fuera de los autorizados conforme a este Acuerdo.

4. Canales y mecanismos autorizados

Las transferencias deberán realizarse únicamente por canales aprobados y configurados de forma segura. Según la naturaleza del servicio, podrán utilizarse VPN/IPsec, HTTPS/TLS 1.2 o superior, SSH/SFTP, APIs autenticadas, consolas administrativas protegidas, repositorios de respaldo cifrados y demás mecanismos formalmente autorizados. Queda prohibido usar servicios personales de almacenamiento, correo personal, mensajería no autorizada o medios removibles no aprobados.

5. Controles mínimos de seguridad

Dominio	Obligación mínima
Control de acceso	Cuentas nominativas o de servicio controladas; mínimo privilegio; revisión periódica; MFA para accesos administrativos/remotos cuando esté disponible.
Cifrado	Cifrado en tránsito mediante protocolos vigentes y cifrado en reposo para información crítica cuando la plataforma lo soporte.
Integridad	Firmas, hashes, validaciones de aplicación, controles FIM o mecanismos equivalentes en flujos críticos.
Antimalware	Controles preventivos y detectivos en endpoints/servidores y filtrado perimetral o WAF según aplique.
Registros	Logs de accesos, cambios y eventos relevantes; protección contra alteración y acceso no autorizado.
Respaldo/continuidad	Mecanismos de respaldo y restauración para los componentes cuya indisponibilidad pueda afectar al servicio.
Segregación	Separación lógica de ambientes, redes y privilegios administrativos conforme a la arquitectura del servicio.

6. Prevención de los riesgos del punto 50 del Anexo 10

Riesgo	Medida contractual mínima
Intercepción	Uso de canales cifrados y autenticados; no exposición directa innecesaria.
Copia no autorizada	Mínimo privilegio, restricción de exportaciones, descargas y medios no autorizados.
Modificación	Validaciones de integridad, control de cambios y registro de modificaciones.
Borrado	Restricción de permisos de eliminación, retención, inmutabilidad o respaldo cuando aplique.
Pérdida	Confirmación de transferencias críticas, respaldo, reintentos y procedimientos de recuperación.
Código malicioso	Antimalware/XDR, IPS/IDS, WAF, escaneo/validación de archivos y monitoreo SIEM según el servicio.

7. Personal autorizado y confidencialidad

ENERFUEL TECH se obliga a mantener una relación actualizada del personal autorizado que pueda acceder a la Información, aplicar controles de alta, modificación y baja de accesos, y asegurar que dicho personal se encuentre sujeto a obligaciones de confidencialidad y seguridad equivalentes a las aquí establecidas. Las obligaciones de confidencialidad sobrevivirán a la terminación de la relación contractual por el plazo definido en el contrato principal o, en ausencia de éste, por cinco años.

8. Incidentes de seguridad

ENERFUEL TECH notificará sin demora indebida cualquier Incidente de seguridad que afecte o pueda afectar la Información. Para los servicios directamente relacionados con el monedero, la notificación inicial deberá realizarse dentro de las dos horas siguientes a su detección, o dentro del plazo más estricto previsto en el contrato principal. La notificación incluirá, en la medida disponible: fecha y hora, sistemas afectados, tipo de información, alcance estimado, medidas de contención y responsable de seguimiento.

- Preservar logs y evidencia técnica relevante.
- Cooperar en análisis forense, contención, remediación y notificaciones regulatorias que correspondan.
- No comunicar externamente el incidente sin coordinación previa, salvo obligación legal.

9. Subcontratación y cadena de suministro

ENERFUEL TECH no podrá incorporar subcontratistas que tengan acceso, almacenen, procesen o transporten Información sin autorización escrita de SENDERO FUEL. Los subcontratistas autorizados deberán quedar sujetos a obligaciones de seguridad equivalentes o superiores a las de este Acuerdo. ENERFUEL TECH conservará responsabilidad por el cumplimiento de dichos terceros en el ámbito de los servicios contratados.

10. Derecho de auditoría y evidencia

SENDERO FUEL podrá solicitar evidencia razonable del cumplimiento de este Acuerdo, incluyendo configuraciones, reportes, bitácoras, certificaciones, resultados de pruebas, tickets y contratos con subproveedores, respetando restricciones de seguridad y confidencialidad. ENERFUEL TECH atenderá requerimientos de verificación relacionados con el Anexo 10, auditorías internas o externas y revisiones de seguridad.

11. Retención, devolución y eliminación

Al finalizar el servicio o cuando SENDERO FUEL lo solicite y no exista obligación legal de conservación, ENERFUEL TECH deberá devolver o eliminar de manera segura la Información y sus copias bajo su control, incluyendo repositorios temporales y credenciales. Cuando sea solicitado, emitirá constancia de devolución o eliminación. Los respaldos sujetos a políticas de retención podrán expirar conforme a su ciclo normal, manteniéndose protegidos durante dicho periodo.

12. Protección de datos personales

Las Partes tratarán los datos personales conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y demás disposiciones aplicables. El acceso a datos personales se limitará a la finalidad del servicio y se aplicarán medidas administrativas, técnicas y físicas apropiadas.

13. Vigencia y supervivencia

El presente Acuerdo permanecerá vigente mientras exista transferencia o acceso a Información con motivo de los servicios. Las obligaciones de confidencialidad, devolución/eliminación, cooperación en incidentes y responsabilidad que por su naturaleza deban sobrevivir permanecerán aplicables después de su terminación.

14. Integración contractual

Este Acuerdo se considera complementario al contrato principal. En caso de contradicción, prevalecerá la disposición que otorgue mayor protección a la Información, salvo prohibición legal o acuerdo expreso posterior firmado por representantes autorizados.

15. Vigencia

Las PARTES acuerdan que el presente **Acuerdo de Transferencia de Información / Adenda de Seguridad y Transferencia de Información** surtirá efectos a partir del **1 de julio de 2026**, independientemente de la fecha en que sea materialmente suscrito por sus representantes, reconociendo expresamente las PARTES dicha fecha como el inicio de la aplicación de las obligaciones de seguridad, confidencialidad y protección de la información aquí establecidas.

El presente instrumento permanecerá vigente durante todo el tiempo en que subsista la relación contractual, comercial o de prestación de servicios entre las PARTES que dé origen a la transferencia, acceso, alojamiento, tratamiento, almacenamiento, transmisión, respaldo, administración o cualquier otra forma de manejo de información relacionada con los servicios contratados.

En caso de que el contrato principal, orden de servicio, anexo, cotización o instrumento del cual derive la relación entre las PARTES establezca una vigencia determinada, el presente Acuerdo o Adenda permanecerá vigente, como mínimo, durante el mismo periodo. Cuando la relación contractual principal sea de vigencia indefinida, el presente instrumento tendrá igualmente vigencia indefinida mientras subsista la prestación de los servicios o exista información de la otra PARTE bajo custodia, tratamiento o control de cualquiera de ellas.

La terminación, rescisión, vencimiento o cancelación del contrato principal **no extinguirá automáticamente las obligaciones derivadas del presente instrumento** cuando todavía exista información de la otra PARTE bajo posesión, custodia, tratamiento, respaldo o control de la contraparte o de alguno de sus subcontratistas.

Por lo anterior, las obligaciones relativas a:

a) confidencialidad y no divulgación;
b) protección de información y datos personales;
c) restricciones de uso, copia y transferencia;
d) conservación de registros y evidencia de auditoría;
e) notificación, investigación y atención de incidentes de seguridad;
f) devolución, eliminación, destrucción segura o transferencia de la información al término del servicio;
g) cooperación con auditorías, revisiones regulatorias o requerimientos de autoridad; y
h) responsabilidad respecto de subcontratistas o terceros que hayan tenido acceso a la información,

continuarán vigentes aun después de terminada la relación contractual, hasta que se haya acreditado documentalmente la devolución, eliminación o destrucción segura de la información y hayan concluido los periodos de conservación establecidos por la legislación aplicable.

Las obligaciones de **confidencialidad** sobrevivirán a la terminación del presente instrumento por un periodo mínimo de **cinco años**, sin perjuicio de que, tratándose de datos personales, secretos industriales,

credenciales, llaves criptográficas, información de seguridad o cualquier otra información cuya protección deba mantenerse por disposición legal o por su propia naturaleza, dichas obligaciones subsistirán durante todo el tiempo en que la información conserve ese carácter protegido.

La terminación del presente instrumento no liberará a ninguna de las PARTES de las responsabilidades derivadas de actos, omisiones, incidentes o incumplimientos ocurridos durante su vigencia.

Anexo A. Matriz de transferencias autorizadas

Flujo / información	Origen ↔ destino	Canal mínimo	Restricciones
Administración de servidores y aplicaciones	SENDERO FUEL ↔ ENERFUEL TECH	VPN/Guacamole/HTTPS/SSH según aplique	MFA, cuenta nominativa/servicio controlado, sesión registrada
Soporte a aplicaciones y APIs	Sistemas del monedero ↔ personal técnico autorizado	HTTPS/TLS, consola segura, repositorio autorizado	No extracción a dispositivos personales; tickets y logs
Código/configuración	Repositorio autorizado ↔ equipo técnico	Canal corporativo cifrado / repositorio de control de versiones	Control de cambios, revisión, trazabilidad
Logs y evidencias de seguridad	Wazuh/Sophos/FortiGate/WAF ↔ personal autorizado	Consolas HTTPS/TLS	Sólo lectura salvo rol autorizado; no borrado
Respaldos/recuperación	Veeam/StoreOnce/Wasabi ↔ operadores autorizados	Canales nativos cifrados	Retención, inmutabilidad cuando aplique, mínimo privilegio

EL CLIENTE
SENDERO FUEL, S.A. DE C.V.
David Orlando Navarro Santiesteban - Apoderado Legal

EL PROVEEDOR
ENERFUEL TECH, S. DE R.L. DE C.V.
María Elodia Robles Burgueño - Apoderada Legal