EnerGo

DOC-SF-057

Esquemas de alta disponibilidad

del monedero electrónico de combustibles

SENDERO FUEL

Documento descriptivo de los esquemas de alta disponibilidad implementados para las actividades relacionadas con el monedero electrónico de combustibles, conforme al punto 57 del Anexo 10 de la RMF 2026 aplicable a **SENDERO FUEL**.

Índice

1. Definición y objetivo del documento
2. Alcance
3. Requisito normativo que atiende el documento
4. Descripción general del esquema de alta disponibilidad
5. Arquitectura de alta disponibilidad
6. Componentes críticos por centro de datos
7. Esquema de disponibilidad por capas
8. Servicios críticos del monedero electrónico
9. Roles y responsabilidades
10. Monitoreo, tickets y evidencias de disponibilidad
11. Criterios de activación, operación y retorno

1. Definición y objetivo del documento

Para **SENDERO FUEL**, la alta disponibilidad del monedero electrónico de combustibles significa contar con una arquitectura tecnológica, operativa y de soporte que permita mantener disponibles los servicios críticos del monedero, reducir puntos únicos de falla y habilitar mecanismos de continuidad cuando exista afectación en infraestructura, comunicaciones, servicios aplicativos, base de datos, seguridad perimetral o componentes de soporte.

El objetivo de este documento es describir, de manera clara y verificable, los esquemas de alta disponibilidad implementados por **SENDERO FUEL** para las actividades relacionadas con el monedero electrónico, incluyendo infraestructura principal, sitio alterno, componentes redundantes o en standby, servicios críticos, monitoreo, soporte, criterios de activación, evidencias técnicas y relación con otros controles del Anexo 10.

2. Alcance

El alcance del presente documento comprende los componentes tecnológicos, operativos y de soporte que permiten la disponibilidad del monedero electrónico de combustibles de **SENDERO FUEL**. Incluye la infraestructura ubicada en el centro de datos principal NGX, el centro de datos alterno ASSETEL, la oficina administrativa, la conectividad segura mediante VPN IPSEC, los ambientes de producción, QA/pruebas y desarrollo, la aplicación móvil, los servicios API, el Portal Clientes Monedero, el ERP monedero, la base de datos, los componentes de seguridad perimetral, los sistemas de respaldo, las herramientas de monitoreo y los mecanismos de atención mediante GLPI.

Este documento no sustituye al Plan de Continuidad del Negocio ni al Plan de Recuperación de Desastres; los complementa desde una perspectiva de disponibilidad tecnológica. El punto 57 se enfoca en describir el esquema de alta disponibilidad, mientras que los puntos 58 y 59 documentan los planes, escenarios, pruebas y resultados de continuidad y recuperación.

3. Requisito normativo que atiende el documento

El punto 57 del Anexo 10 de la RMF 2026 requiere documentación que describa los esquemas de alta disponibilidad que la persona moral implementa para las actividades relacionadas con el monedero electrónico. En atención a dicho requisito, este documento identifica los servicios críticos, la arquitectura implementada, los componentes de respaldo, los mecanismos de monitoreo y las evidencias que permiten demostrar que el monedero cuenta con medidas de disponibilidad alineadas a su operación.

Elemento normativo	Respuesta documental en este documento
Esquemas de alta disponibilidad	Se describen NGX como sitio principal, ASSETEL como sitio alterno/standby, virtualización, almacenamiento, respaldos, seguridad perimetral, conectividad VPN IPSEC y servicios críticos.
Actividades relacionadas con el monedero electrónico	Se cubren autorización de transacciones, consulta de saldos, administración de tarjetas/dispositivos, generación de QR, registro de consumos, compensación/liquidación y soporte operativo.
Evidencia de implementación	Se incluye matriz de activos, diagrama de arquitectura, capas de disponibilidad, monitoreo, tickets GLPI, respaldos, pruebas BCP/DRP y evidencias técnicas requeridas.

4. Descripción general del esquema de alta disponibilidad

El esquema de alta disponibilidad de **SENDERO FUEL** se basa en una arquitectura de sitio principal y sitio alterno. El centro de datos NGX opera como infraestructura principal para las actividades productivas del monedero electrónico. El centro de datos ASSETEL cuenta con infraestructura espejo en modalidad standby para soportar recuperación y continuidad tecnológica ante fallas mayores o indisponibilidad del sitio principal.

El modelo adoptado no se documenta como una operación activa-activa, sino como un esquema principal-respaldo con componentes redundantes, réplicas en standby, respaldos y capacidad de activación coordinada. Este enfoque permite que las actividades críticas del monedero puedan mantenerse o restablecerse conforme a los criterios definidos en BCP/DRP y a la validación técnica de ENERFUEL TECH, proveedor relacionado con la operación tecnológica del monedero.

Nivel	Descripción del esquema	Objetivo de disponibilidad
Sitio principal	NGX aloja activos productivos del monedero, virtualización, almacenamiento, firewall, switch, servidores de aplicación, base de datos, servicios y herramientas de soporte.	Mantener la operación ordinaria del monedero electrónico.
Sitio alterno	ASSETEL aloja infraestructura de respaldo y réplicas/standby para servidores críticos del monedero.	Permitir activación de contingencia o recuperación ante indisponibilidad del sitio principal.
Servicios de soporte	GLPI para tickets, SOPHOS para monitoreo/antivirus/XDR, respaldos y bitácoras técnicas.	Detectar, registrar, escalar y evidenciar eventos que afecten disponibilidad.
Conectividad	VPN IPSEC y controles perimetrales FortiGate para comunicaciones con estaciones, usuarios y servicios.	Asegurar transferencia controlada y operación segura del monedero.

5. Arquitectura de alta disponibilidad

La arquitectura de alta disponibilidad se sustenta en la separación física y lógica entre centro de datos principal, centro de datos alterno, oficina administrativa y canales externos. Esta separación permite reducir el impacto de fallas localizadas, controlar la interconexión entre sitios y mantener un punto de recuperación tecnológica ante eventos que afecten la operación del monedero.

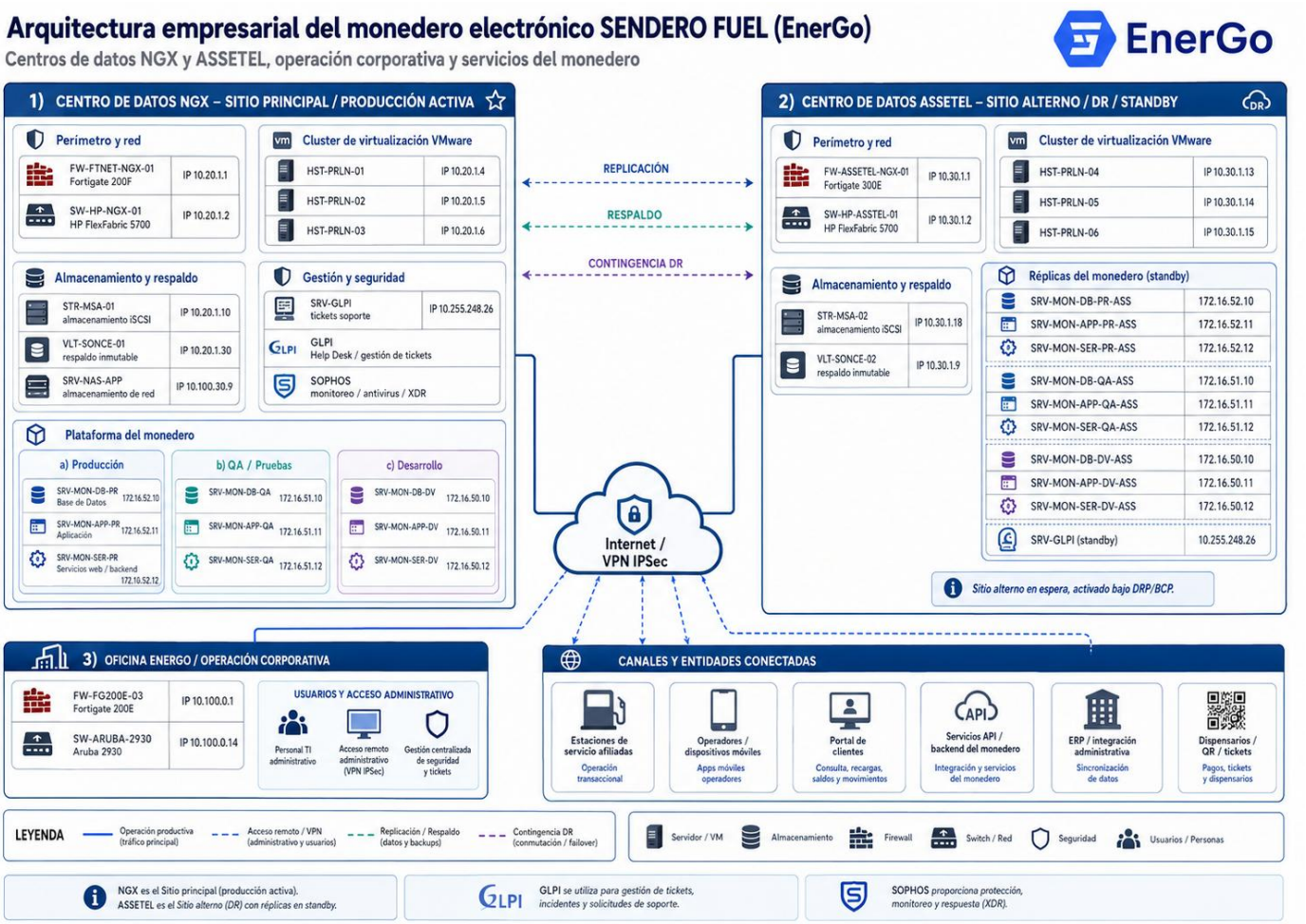


Figura 1. Arquitectura empresarial del monedero electrónico SENDERO FUEL: NGX como sitio principal y ASSETEL como sitio alterno/standby.

La figura anterior permite identificar las capas que intervienen en la disponibilidad: perímetro y red, cluster de virtualización VMware, almacenamiento, respaldo, gestión de seguridad, plataforma del monedero y réplicas de servicios. Asimismo, muestra la conectividad segura hacia canales y entidades conectadas, incluyendo estaciones de servicio afiliadas, operadores/dispositivos móviles, Portal Clientes, servicios API/backend, ERP/integración administrativa y dispensarios/QR/tickets.

6. Componentes críticos por centro de datos

Con base en el inventario de activos de **SENDERO FUEL**, los componentes críticos se agrupan por ubicación. Para efectos del punto 57, se consideran relevantes aquellos activos que participan en operación principal, respaldo, seguridad, monitoreo, conectividad, almacenamiento, virtualización o recuperación del monedero electrónico.

Ubicación	Cantidad de activos	Principales activos identificados
Centro de datos NGX	20	GLPI, SOPHOS, SW-HP-NGX-01, FW-FTNET-NGX-01, HST-PRLN-01, HST-PRLN-02, HST-PRLN-03 y 13 activos adicionales
Centro de datos Assetel	17	SW-HP-ASSTEL-01, FW-ASSETEL-NGX-01, HST-PRLN-04, HST-PRLN-05, HST-PRLN-06, STR-MSA-02, VLT-SONCE-02 y 10 activos adicionales
Oficina EnerGo	2	SW-ARUBA-2930, FW-FG200E-03

6.1 Inventario operativo de alta disponibilidad

No.	Activo	Función / descripción	IP	Ubicación	Estado
1	GLPI	Software para la gestión del Help Desk	N/A	Centro de datos NGX	Activo
2	SOPHOS	Monitoreo/Antivirus/XDR	N/A	Centro de datos NGX	Activo
3	SW-HP-NGX-01	Switch Core, interconecta todos los dispositivos del centro de datos	10.20.1.2	Centro de datos NGX	Activo
4	FW-FTNET-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	10.20.1.1	Centro de datos NGX	Activo
5	SW-HP-ASSTEL-01	Switch Core, interconecta todos los dispositivos del centro de datos	10.30.1.2	Centro de datos Assetel	Activo
6	FW-ASSETEL-NGX-01	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	10.30.1.1	Centro de datos Assetel	Activo
7	SW-ARUBA-2930	Switch Core, interconecta todos los dispositivos del centro de datos	10.100.0.14	Oficina EnerGo	Activo
8	FW-FG200E-03	Firewall perimetral, gestiona los enlaces de Intrnet, IDS, IPS, Filtrado web, etc	10.100.0.1	Oficina EnerGo	Activo
9	HST-PRLN-01	Host de virtualizacion VMWare	10.20.1.4	Centro de datos NGX	Activo
10	HST-PRLN-02	Host de virtualizacion VMWare	10.20.1.5	Centro de datos NGX	Activo
11	HST-PRLN-03	Host de virtualizacion VMWare	10.20.1.6	Centro de datos NGX	Activo
12	STR-MSA-01	Dispositivo de Almacenamiento de datos de red ISCSI, almacena las VM de VMWare	10.20.1.10	Centro de datos NGX	Activo
13	VLT-SONCE-01	Almacenameinto inmutable de respaldos para máquinas virtuales de VMWare	10.20.1.30	Centro de datos NGX	Activo
14	HST-PRLN-04	Host de virtualizacion VMWare	10.30.1.13	Centro de datos Assetel	Activo
15	HST-PRLN-05	Host de virtualizacion VMWare	10.30.1.14	Centro de datos Assetel	Activo
16	HST-PRLN-06	Host de virtualizacion VMWare	10.30.1.15	Centro de datos Assetel	Activo
17	STR-MSA-02	Dispositivo de Almacenamiento de datos de red ISCSI, almacena las VM de VMWare	10.30.1.18	Centro de datos Assetel	Activo
18	VLT-SONCE-02	Almacenameinto inmutable de respaldos para máquinas virtuales de VMWare	10.30.1.9	Centro de datos Assetel	Activo
19	SRV-MON-DB-PR	Servidor de Produccion de Base de Datos de monedero	172.16.52.10	Centro de datos NGX	Activo
20	SRV-MON-APP-PR	Servidor de Produccion de Aplicacion de monedero	172.16.52.11	Centro de datos NGX	Activo
21	SRV-MON-DB-QA	Servidor de Pruebas de Base de Datos de monedero	172.16.51.10	Centro de datos NGX	Activo
22	SRV-MON-APP-QA	Servidor de Pruebas de Aplicaion de monedero	172.16.51.11	Centro de datos NGX	Activo
23	SRV-MON-DB-DV	Servidor de Desarrollo de Base de Datos de monedero	172.16.50.10	Centro de datos NGX	Activo
24	SRV-MON-APP-DV	Servidor de Desarrollo de Aplicaion de monedero	172.16.50.11	Centro de datos NGX	Activo
25	SRV-MON-SER-PR	Servidor de Produccion para Servicios web y backend del monedero	172.16.52.12	Centro de datos NGX	Activo
26	SRV-MON-SER-QA	Servidor de Pruebas para Servicios web y backend del monedero	172.16.51.12	Centro de datos NGX	Activo
27	SRV-MON-SER-DV	Servidor de Desarrollo para Servicios web y backend del monedero	172.16.50.12	Centro de datos NGX	Activo
28	SRV-NAS-APP	Almancenamiento de red.	10.100.30.9	Centro de datos NGX	Activo
29	SRV-GLPI	Tickets Soporte	10.255.248.26	Centro de datos NGX	Activo
30	SRV-MON-DB-PR-ASS	Replica Servidor de Produccion de Base de Datos de monedero, apagado en Standby	172.16.52.10	Centro de datos Assetel	Activo
31	SRV-MON-APP-PR-ASS	Replica de Servidor de Produccion de Aplicacion de monedero, apagado en standby	172.16.52.11	Centro de datos Assetel	Activo
32	SRV-MON-DB-QA-ASS	Replica de Servidor de Pruebas de Base de Datos de monedero, apagado, en standby	172.16.51.10	Centro de datos Assetel	Activo
33	SRV-MON-APP-QA-ASS	Replica de Servidor de Pruebas de Aplicaion de monedero, apagado en standby	172.16.51.11	Centro de datos Assetel	Activo
34	SRV-MON-DB-DV-ASS	Replica decServidor de Desarrollo de Base de Datos de monedero, apagado en standby	172.16.50.10	Centro de datos Assetel	Activo
35	SRV-MON-APP-DV-ASS	Replaica de Servidor de Desarrollo de Aplicaion de monedero, apagadpo en standby	172.16.50.11	Centro de datos Assetel	Activo
36	SRV-MON-SER-PR-ASS	Replica de Servidor de Produccion para Servicios web y backend del monedero, apagado en standy	172.16.52.12	Centro de datos Assetel	Activo
37	SRV-MON-SER-QA-ASS	Servidor de Pruebas para Servicios web y backend del monedero	172.16.51.12	Centro de datos Assetel	Activo
38	SRV-MON-SER-DV-ASS	Replica de Servidor de Desarrollo para Servicios web y backend del monedero, apagado en standby	172.16.50.12	Centro de datos Assetel	Activo
39	SRV-GLPI	Rteplica de Servidor de GLPI Tickets Soporte, apagado en standby	10.255.248.26	Centro de datos Assetel	Activo

7. Esquema de disponibilidad por capas

La alta disponibilidad se documenta por capas para demostrar que la disponibilidad del monedero no depende de un solo componente. Cada capa aporta controles específicos para prevenir, detectar, contener o recuperar fallas.

Capa	Componentes	Esquema de alta disponibilidad	Evidencia esperada
Centro de datos	NGX y ASSETEL	NGX funciona como sitio principal y ASSETEL como sitio alterno/DR en standby. La separación entre sitios reduce dependencia de una sola ubicación.	Diagrama de arquitectura, inventario de activos, actas de prueba DRP, evidencia de conectividad entre sitios.
Virtualización	Hosts VMware HST-PRLN-01 a HST-PRLN-06	La virtualización permite alojar servidores del monedero en hosts administrados y facilitar recuperación o reasignación de cargas ante falla de host.	Capturas de vCenter/VMware, estado de hosts, datastore, uso de CPU/RAM y disponibilidad de VMs.
Perímetro y red	FortiGate, switches HP/Aruba, VPN IPSEC	Control de tráfico, segmentación, comunicación segura con estaciones y conectividad entre sitios.	Configuración de VPN, estado de túneles, reglas firewall, logs FortiGate, estado de interfaces.
Aplicación y servicios	API, Portal, ERP, servidores APP/SER	Separación de ambientes producción, QA y desarrollo; servicios API y portal con autenticación y endpoints de salud.	Prueba de acceso, endpoint Status, logs de aplicación, estado de IIS/App Pool o servicios API.
Base de datos	SRV-MON-DB-PR y réplicas ASSETEL	Base de datos productiva con respaldo/standby para recuperación y continuidad transaccional.	Estado de motor, respaldos, validación de restauración, consistencia e integridad de datos.
Almacenamiento y respaldo	MSA, StoreOnce, NAS, respaldos	Almacenamiento centralizado y respaldos para reducir riesgo de pérdida de información y recuperación de servicios.	Reportes de respaldo, pruebas de restauración, estado de almacenamiento, capacidad y alertas.
Monitoreo y soporte	GLPI, SOPHOS, bitácoras	Registro de incidentes, eventos, cambios, alertas y trazabilidad de disponibilidad.	Tickets GLPI, alertas SOPHOS/XDR, bitácoras, reportes de monitoreo.

8. Servicios críticos del monedero electrónico

La alta disponibilidad se orienta a mantener activos o recuperables los servicios que impactan directamente la operación del monedero. Para **SENDERO FUEL**, los procesos críticos previamente definidos son la autorización de transacciones y la compensación/liquidación. A partir de dichos procesos se identifican servicios técnicos, dependencias y métricas operativas.

Servicio crítico	Dependencias principales	Riesgo de indisponibilidad	Esquema de continuidad/HA
Autenticación de usuarios y conductores	API, Portal/App, base de datos, tokens, OTP, Device header.	Impide acceso a clientes, beneficiarios, operadores o personal autorizado.	Validación de servicios API, monitoreo de login, disponibilidad de base de datos, soporte GLPI y escalamiento con ENERFUEL TECH.
Consulta de saldos y parámetros	Portal/App, API, base de datos, conectividad segura.	Impide determinar monto/volumen disponible y reglas de carga.	Servicios productivos en NGX y réplicas/standby en ASSETEL; validación funcional en pruebas BCP/DRP.
Generación y validación de QR	API, app móvil, reglas de negocio, base de datos, servicios de notificación.	Impide autorización de carga o puede afectar operación en estaciones.	Validación de QR dinámico, trazabilidad por consumo, monitoreo de respuestas y recuperación desde sitio alterno.
Autorización de carga	API, base de datos, estación, VPN IPSEC, firewall, dispensario.	Interrumpe la actividad central del monedero.	Conectividad VPN IPSEC, reglas perimetrales, monitoreo de estaciones y procedimiento de escalamiento.
Registro de consumo y evidencias	Base de datos, tablas de consumo, fotos, OCR, firma, documentos.	Afecta trazabilidad fiscal, operativa y conciliación.	Respaldos, registros transaccionales, bitácoras, validación de integridad y recuperación.
Compensación/liquidación	ERP/Portal, reportes, base de datos, movimientos y saldos.	Afecta conciliación financiera y operación administrativa.	Validación operativa por Crédito y Cobranza, respaldos, reportes y disponibilidad de plataforma.

9. Roles y responsabilidades

La operación de alta disponibilidad requiere coordinación técnica y funcional. Los roles se establecen para asegurar que cualquier evento de indisponibilidad sea detectado, registrado, evaluado, escalado y resuelto con evidencia suficiente.

Rol / responsable	Responsabilidad en alta disponibilidad	Evidencia que genera o resguarda
Gerente General / Romina Monserrat Barbosa Apodaca	Coordina la respuesta operativa, valida comunicación con áreas internas y mantiene relación directa con ENERFUEL TECH para soporte del monedero.	Tickets GLPI, comunicaciones, actas de prueba, seguimiento de escalamiento.
Oficial de Seguridad / Axel Martínez Rentería	Valida controles de seguridad, bitácoras, evidencias, monitoreo, incidentes y cumplimiento documental.	Bitácoras, alertas, evidencias de acceso, reportes de revisión.
Coordinador de Mantenimiento de Cartera / Raúl Ernesto Galindo	Valida continuidad operativa asociada a clientes, cartera y seguimiento comercial-operativo.	Registros operativos, evidencias de consulta y seguimiento.
Coordinador de Atención a Clientes / Ramón Gabriel Salazar Rocha	Valida la disponibilidad funcional de acceso, portal, saldos, movimientos y atención a usuarios.	Capturas de prueba, reportes de atención y tickets.
Coordinador de Crédito y Cobranza / Francisco Ricardo López Dimas	Valida continuidad de compensación/liquidación, saldos, pagos y reportes.	Registros de conciliación, evidencia de reportes y validaciones.
Ingeniero de operaciones / ENERFUEL TECH	Ejecuta soporte técnico, diagnóstico, activación de sitio alterno, validación de servicios y restauración.	Bitácoras técnicas, evidencia de conectividad, estado de servicios y cierre de soporte.
Administrador de infraestructura	Opera hosts, almacenamiento, firewall, switches, respaldos y conectividad entre sitios.	Capturas de vCenter, firewall, almacenamiento, respaldos, VPN y monitoreo.

10. Monitoreo, tickets y evidencias de disponibilidad

Todo evento, incidente, problema, requerimiento de soporte o actividad de validación asociada con disponibilidad debe registrarse en GLPI. GLPI funciona como repositorio operativo para tickets, seguimiento, responsables, fechas, evidencias, resolución y cierre. Las alertas de seguridad o disponibilidad generadas por SOPHOS, FortiGate, VMware, almacenamiento, respaldos o servicios aplicativos deberán vincularse al ticket correspondiente cuando impliquen afectación real o potencial al monedero.

Fuente de monitoreo	Qué debe monitorearse	Umbral o evento relevante	Evidencia
VMware / vCenter	Hosts, VMs, datastores, CPU, RAM, snapshots, estado de servicios.	Host caído, VM apagada, datastore >80%, CPU/RAM sostenido >75%, snapshot no autorizado.	Capturas, reportes de salud, logs de host/VM.
FortiGate	Interfaces, VPN IPSEC, reglas, IDS/IPS, amenazas, tráfico permitido/denegado.	Túnel VPN caído, alto volumen de bloqueos, caída de interfaz, cambios no autorizados.	Logs FortiGate, estado VPN, capturas de reglas.
Switches	Puertos, uplinks, errores, caída de enlace, utilización.	Puerto crítico caído, errores CRC, saturación de enlace.	Estado de puertos y bitácoras de red.
Almacenamiento/respaldos	MSA, StoreOnce, NAS, jobs de backup, capacidad, restauraciones.	Backup fallido, capacidad >80%, error de disco, restauración no validada.	Reporte de backup, prueba de restauración, alertas de almacenamiento.
Servicios API / Portal / ERP	Endpoint Status, App Pool/IIS, servicios API, respuestas HTTP, autenticación.	HTTP 5xx, caída de pool, tiempos de respuesta altos, errores de autenticación masivos.	Logs de aplicación, pruebas de acceso, capturas de portal.
Base de datos	Disponibilidad del motor, jobs, consistencia, respaldos, crecimiento.	Servicio detenido, error de conexión, crecimiento anormal, respaldo fallido.	Logs DB, reporte de jobs, evidencia de respaldo/restauración.
GLPI	Tickets de incidentes, cambios, soporte y problemas.	Ticket crítico sin atención dentro de SLA, reincidencia o evento de disponibilidad.	Ticket, tiempos, responsable, cierre y evidencia adjunta.
SOPHOS/XDR	Alertas de malware, comportamiento anómalo, salud de endpoints/servidores.	Alerta crítica, equipo sin agente, detección de código malicioso.	Consola SOPHOS, alertas y acciones de contención.

10.1 Registro mínimo del ticket GLPI

- Fecha y hora de detección del evento.
- Activo, servicio o ubicación afectada.
- Tipo de evento: alerta, incidente, problema, cambio, mantenimiento o prueba.
- Impacto estimado en autorización de transacciones, consulta de saldos, QR, consumos o compensación/liquidación.
- Responsable asignado y proveedor involucrado, en su caso ENERFUEL TECH.
- Acciones realizadas, evidencia adjunta y resultado obtenido.
- Fecha y hora de cierre, validación funcional y lecciones aprendidas.

11. Criterios de activación, operación y retorno

El esquema de alta disponibilidad debe activarse de forma controlada cuando un evento comprometa la operación normal del monedero. La activación puede consistir en reasignación de servicios, recuperación de una VM, restauración de respaldo, intervención de red, corrección de seguridad, escalamiento con proveedor o activación del sitio alterno ASSETEL.

Escenario	Criterio de activación	Acción de alta disponibilidad	Validación de retorno
Caída de servidor APP/API	Servicio no responde, HTTP 5xx persistente o VM indisponible.	Reiniciar servicio/VM, validar dependencias, escalar a ENERFUEL TECH; si persiste, evaluar activación en ASSETEL.	Acceso al portal/app, login, consulta de saldos, prueba de QR.
Indisponibilidad de base de datos	Falla de conexión, servicio detenido, corrupción o error crítico.	Diagnóstico, restauración o activación de réplica/standby conforme DRP.	Consulta de tablas críticas, consumo controlado, integridad de registros.
Falla de red o VPN IPSEC	Túnel caído, pérdida de conectividad con estaciones o centro alterno.	Revisión FortiGate, enlaces, reglas, renegociación de túnel, escalamiento a proveedor.	Ping, trazas, estado de túnel, prueba de autorización estación-monedero.

Escenario	Criterio de activación	Acción de alta disponibilidad	Validación de retorno
Falla de almacenamiento	Datastore no disponible, errores de disco, capacidad crítica.	Contención, liberación de espacio, reparación, restauración desde respaldo o failover según alcance.	Estado de datastore, ejecución de VM, validación de aplicación y DB.
Incidente de seguridad	Alerta crítica SOPHOS/XDR, tráfico malicioso o compromiso de servicio.	Aislar activo, analizar impacto, registrar GLPI, aplicar remediación y validar continuidad.	Servicios limpios, logs revisados, aplicación disponible, cierre de incidente.
Indisponibilidad de NGX	Afectación del sitio principal o imposibilidad de operar servicios críticos.	Activación coordinada de ASSETEL como sitio alterno/standby conforme DRP.	Pruebas funcionales completas, registros, bitácoras y cierre de activación.

11.1 Retorno a operación normal

El retorno a operación normal debe ejecutarse únicamente cuando el responsable técnico y el responsable funcional confirmen estabilidad del servicio. La decisión debe quedar documentada en GLPI y, si se activó ASSETEL, también en el acta o bitácora DRP correspondiente. Antes de cerrar el evento se debe validar que no exista pérdida de información, que los respaldos estén actualizados, que los logs sean consistentes y que las áreas operativas confirmen funcionamiento de los servicios críticos.

12. Matriz de riesgos de disponibilidad y controles

La siguiente matriz relaciona los riesgos de disponibilidad más relevantes del monedero electrónico con los controles de alta disponibilidad implementados o documentados por **SENDERO FUEL**.

Riesgo de disponibilidad	Impacto potencial	Control / esquema HA	Evidencia de control
Falla del centro de datos principal NGX	Interrupción de servicios productivos del monedero.	Sitio alterno ASSETEL en standby y DRP documentado.	Diagrama, inventario ASSETEL, acta DRP, evidencia de activación.
Falla de host VMware	Indisponibilidad de VM del monedero.	Cluster de virtualización con múltiples hosts y capacidad de recuperación/reasignación.	Estado de hosts, VMs, recursos y logs VMware.
Falla de almacenamiento	Pérdida temporal de acceso a datos o VMs.	MSA, StoreOnce, NAS y respaldos; restauración controlada.	Reporte de respaldos, alertas de almacenamiento, pruebas de restauración.
Caída de VPN o firewall	Sin comunicación con estaciones o sitios remotos.	FortiGate, VPN IPSEC, reglas de firewall y monitoreo de túneles.	Logs FortiGate, estado VPN, tickets GLPI.
Error de aplicación/API	No se pueden autorizar transacciones o consultar saldos.	Monitoreo de servicios, endpoints de salud, separación de ambientes y escalamiento técnico.	Logs API/Portal/ERP, capturas de Status, validación funcional.
Error de base de datos	Impacto en saldos, consumos, QR, reportes y conciliación.	Respaldos, réplica/standby, restauración y validación de integridad.	Logs DB, evidencia de backup/restauración, consultas de validación.
Malware o ataque a servicios	Afectación de disponibilidad o integridad operativa.	SOPHOS/XDR, FortiGate, segmentación, monitoreo y PR-SF-021.	Alertas SOPHOS, tickets GLPI, bitácoras de incidente.
Cambio no controlado	Interrupción por liberación o configuración incorrecta.	Gestión de cambios PR-SF-022, QA, CI/CD y reverso.	Tickets/cambios GLPI, evidencia de pruebas y liberación.