EVIDENCIA DE GESTIÓN DE INCIDENTE EN GLPI

Levantamiento, clasificación, atención, remediación y cierre conforme al PR-SF-022 - Proceso de gestión de incidentes

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

Propósito del expediente

Documentar de forma visual y trazable cómo debe registrarse y atenderse un incidente en GLPI, desde su detección y registro inicial hasta el cierre, conservación de evidencias y actualización de la base de conocimientos.

1. Fundamento y correspondencia con PR-SF-022

El procedimiento PR-SF-022 establece que GLPI es la herramienta oficial para registrar, clasificar, atender, escalar, documentar y cerrar incidentes y problemas relacionados con la operación del monedero electrónico. El ticket debe conservar trazabilidad de fechas, responsables, clasificación, acciones, evidencias, aprobaciones, escalamiento, remediación y cierre.

Etapa PR-SF-022	Evidencia gráfica
Detección y registro inicial	Pantallas 1 y 2
Clasificación inicial	Pantalla 3
Contención y escalamiento	Pantalla 4
Recolección y preservación de evidencia	Pantalla 5
Investigación y causa raíz	Pantalla 6
Remediación y recuperación	Pantalla 7
Evaluación PR-SF-001 / SAT y cierre	Pantalla 8
Base de conocimientos	Pantalla 9
Resumen de trazabilidad	Pantalla 10

2. Datos del incidente de referencia

• El incidente se origina por una alerta de monitoreo que detecta errores HTTP 503 intermitentes en el Portal Clientes.

• El activo principal asociado es SRV-MON-APP-PR (172.16.52.10), ubicado en el Centro de Datos NGX. El servicio afectado es https://clientes.ener-go.mx.

• La clasificación inicial es SEV-2 Alto debido a la degradación parcial del servicio, sin evidencia de afectación a confidencialidad o integridad de información de contribuyentes.

• El incidente se escala a ENERFUEL TECH para diagnóstico técnico y se mantiene coordinación con el Oficial de Seguridad y Atención a Clientes.

3. Evidencia 1 - Detección y listado de tickets

La vista debe mostrar el ticket dentro del listado de incidentes y permitir identificar ID, título, estado, prioridad, responsable asignado y última actualización. La evidencia debe relacionar el evento de monitoreo con el servicio y activo afectados.

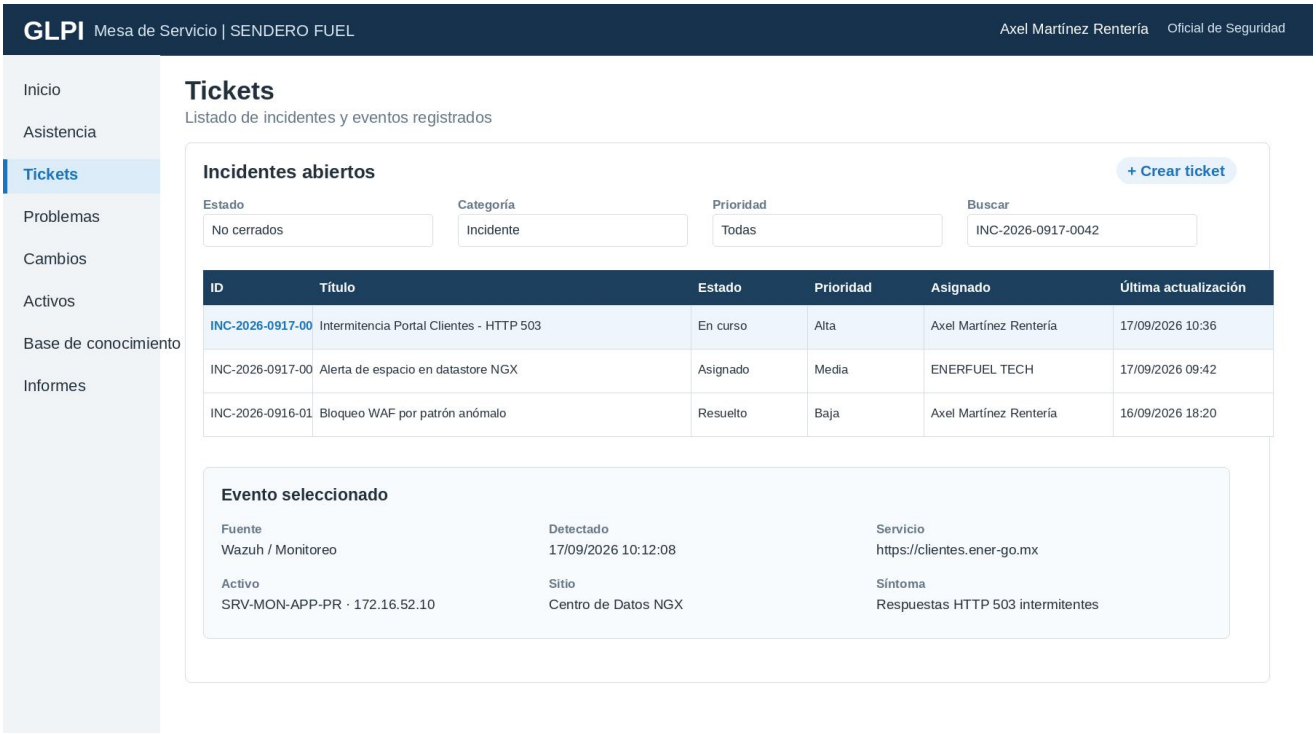


Figura 1. Detección y listado de tickets.

4. Evidencia 2 - Registro inicial del incidente

El formulario debe contener los campos mínimos de PR-SF-022: tipo, categoría, título, reportante, activo, proceso, ubicación, proveedor involucrado, fecha/hora de detección y descripción del impacto inicial.

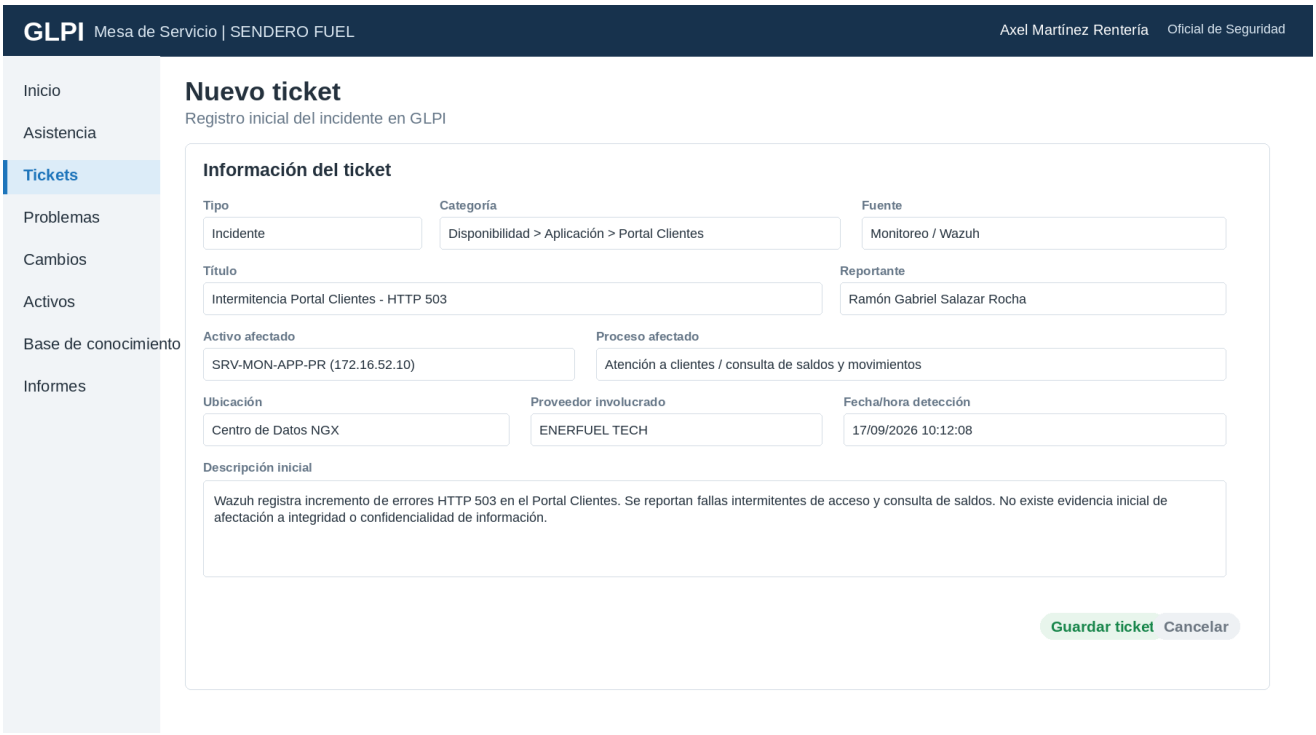


Figura 2. Registro inicial del incidente.

Elementos que deben ser visibles: ID/título del ticket, reportante, fecha y hora, categoría, activo, proceso afectado, descripción inicial y proveedor.

5. Evidencia 3 - Clasificación y severidad

La pantalla debe mostrar la severidad validada, impacto, urgencia, categoría, responsables, activo, servicio, SLA y evaluación inicial sobre información de contribuyentes y necesidad de activar BCP/DRP o PR-SF-001.

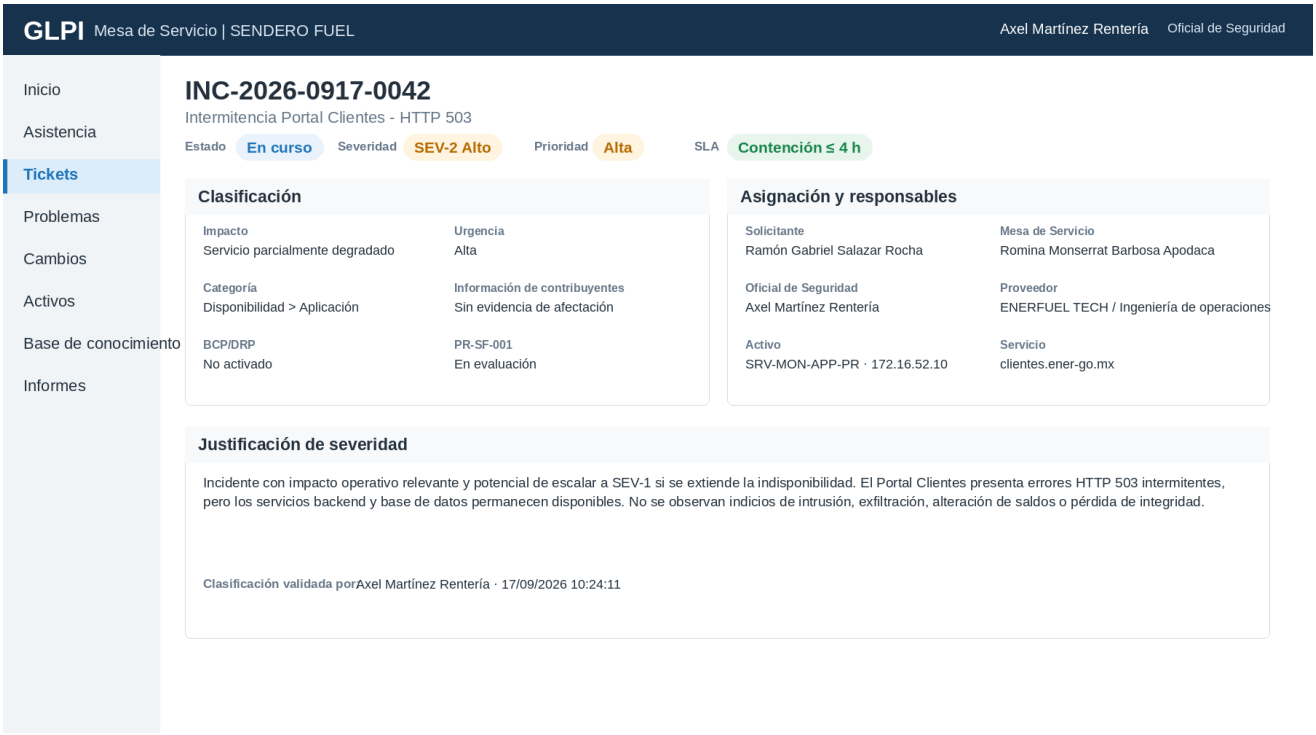


Figura 3. Clasificación y severidad.

Elementos que deben ser visibles: severidad, prioridad, impacto, urgencia, activo, servicio, responsables, SLA, evaluación de información de contribuyentes y escalamiento.

6. Evidencia 4 - Contención, escalamiento y seguimiento

La línea de tiempo debe conservar cada seguimiento con fecha/hora, responsable y acción realizada. Debe evidenciar el escalamiento a ENERFUEL TECH, preservación previa de evidencia, contención aplicada, estabilización y validaciones.

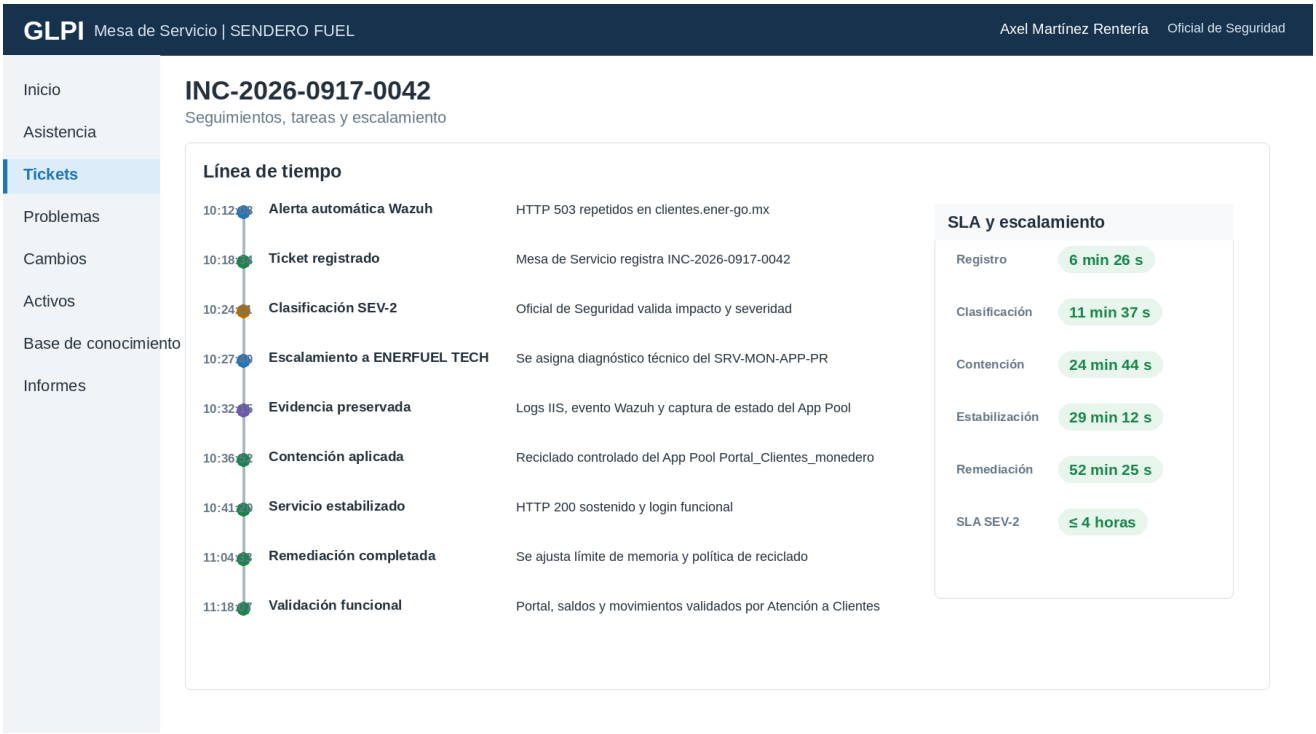


Figura 4. Contención, escalamiento y seguimiento.

Elementos que deben ser visibles: fecha/hora de cada seguimiento, responsable, escalamiento a proveedor, contención, preservación de evidencia y estabilización.

7. Evidencia 5 - Evidencia técnica adjunta y preservación

La pestaña de documentos debe mostrar los logs, capturas y reportes asociados al incidente. Para evidencia crítica conviene registrar origen, fecha/hora e integridad o referencia de hash, además de evitar adjuntar datos personales innecesarios.

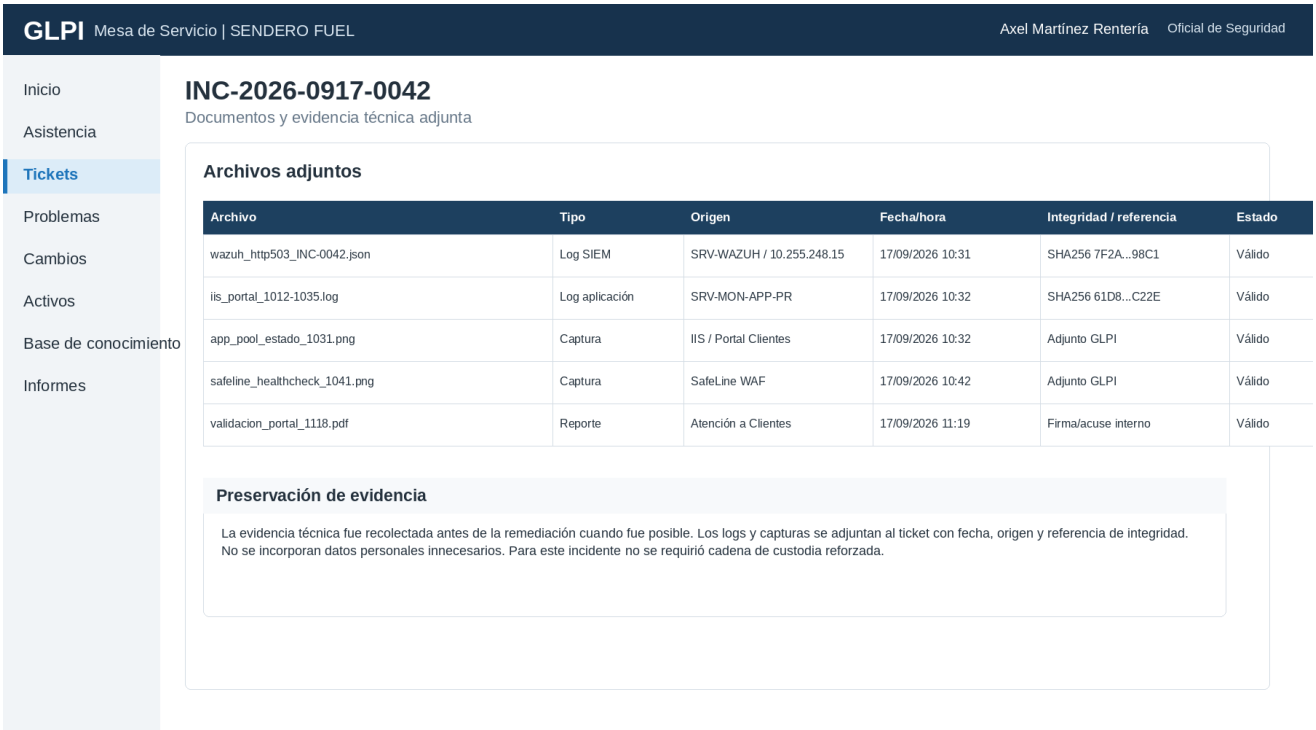


Figura 5. Evidencia técnica adjunta y preservación.

Elementos que deben ser visibles: nombre de archivo, tipo, origen, fecha/hora, referencia de integridad y estado del adjunto.

8. Evidencia 6 - Investigación, causa raíz y problema relacionado

El diagnóstico debe identificar síntoma, componente, causa probable, causa raíz, periodo afectado, transacciones potencialmente impactadas, contención y remediación. Si existe recurrencia, debe abrirse o vincularse un problema en GLPI.

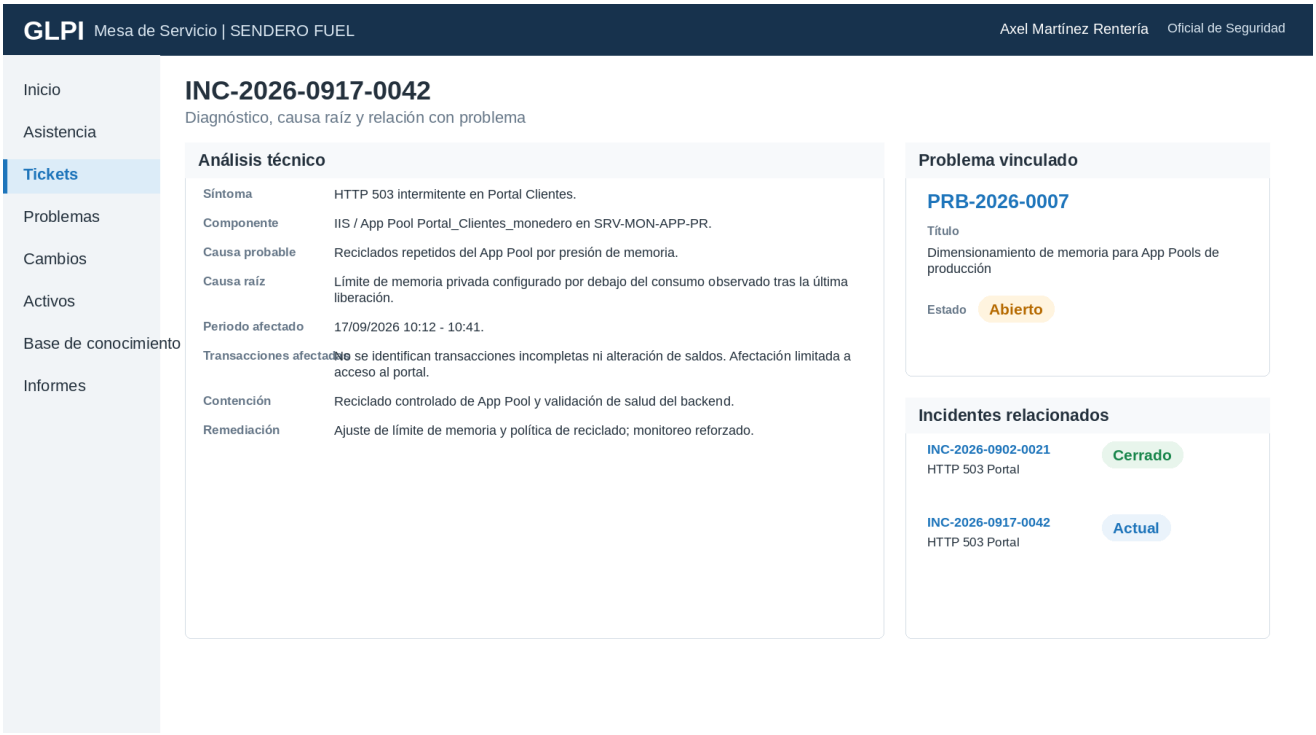


Figura 6. Investigación, causa raíz y problema relacionado.

Elementos que deben ser visibles: síntoma, causa probable, causa raíz, periodo afectado, acciones y vínculo a problema cuando exista recurrencia.

9. Evidencia 7 - Remediación, recuperación y validación funcional

La evidencia debe mostrar acciones correctivas, responsable, resultado y validaciones posteriores. Para el monedero deben comprobarse, según aplique, disponibilidad, autenticación, consulta de saldos, movimientos y ausencia de errores persistentes.

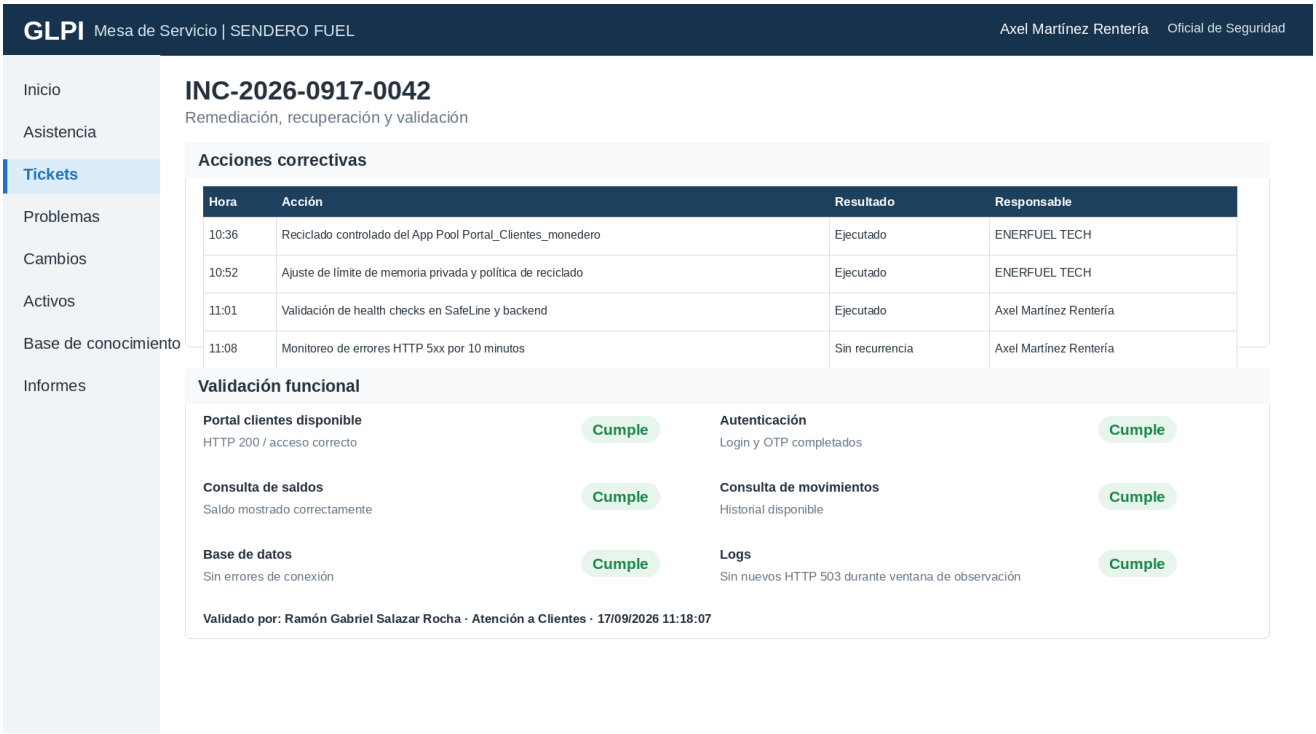


Figura 7. Remediación, recuperación y validación funcional.

Elementos que deben ser visibles: acción correctiva, resultado, responsable, pruebas funcionales y validación por el dueño del proceso.

10. Evidencia 8 - Evaluación regulatoria, cierre y lecciones aprendidas

El cierre debe conservar la evaluación de afectación a confidencialidad, integridad y disponibilidad, la decisión sobre PR-SF-001, validación del dueño del proceso, fecha de solución, fecha de cierre, tiempo total, acciones preventivas y lecciones aprendidas.

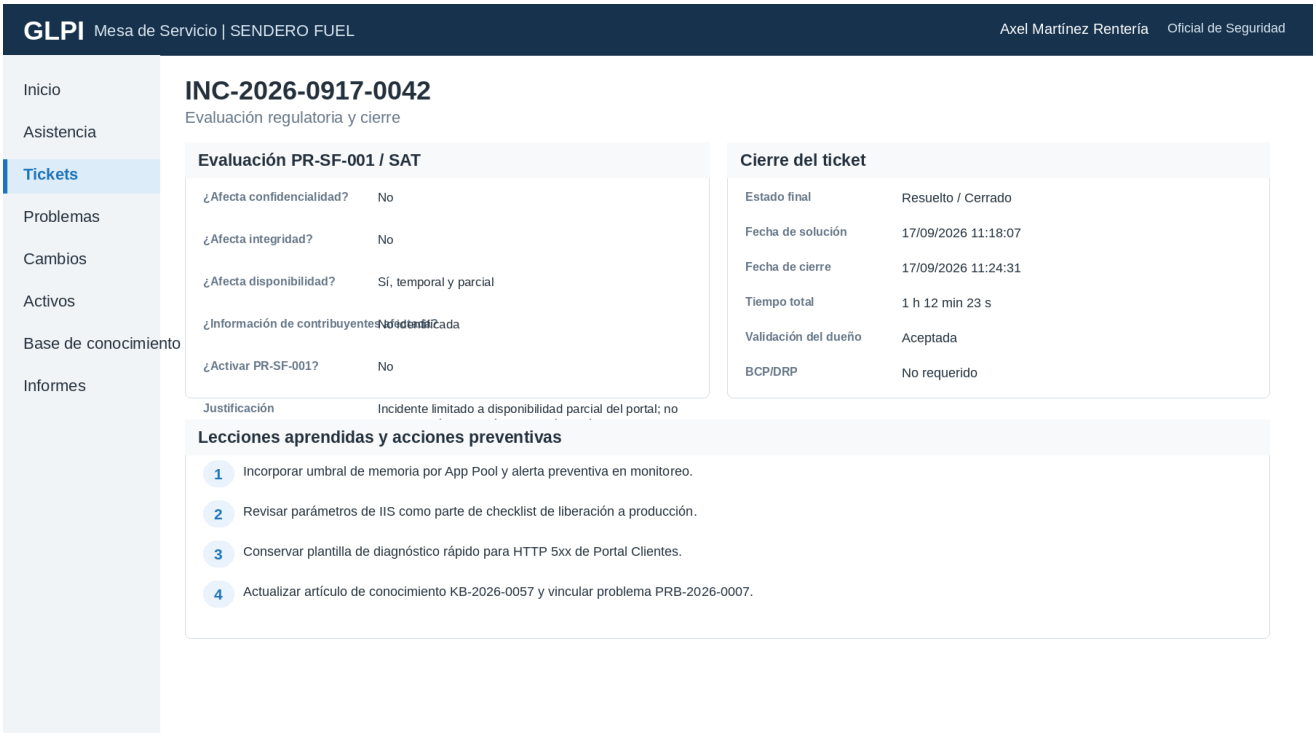


Figura 8. Evaluación regulatoria, cierre y lecciones aprendidas.

Elementos que deben ser visibles: evaluación CIA, decisión PR-SF-001, fecha de solución/cierre, validación y lecciones aprendidas.

11. Evidencia 9 - Base de conocimientos

Para incidentes SEV-1, SEV-2 o problemas recurrentes, la base de conocimientos debe incluir síntomas, diagnóstico, causa conocida, solución, prevención y referencias a tickets/problemas relacionados.



Figura 9. Base de conocimientos.

12. Evidencia 10 - Resumen de trazabilidad para auditoría

La vista de cierre permite confirmar que todas las etapas exigidas por PR-SF-022 cuentan con evidencia y que los tiempos de atención quedaron dentro de los niveles definidos para SEV-2.

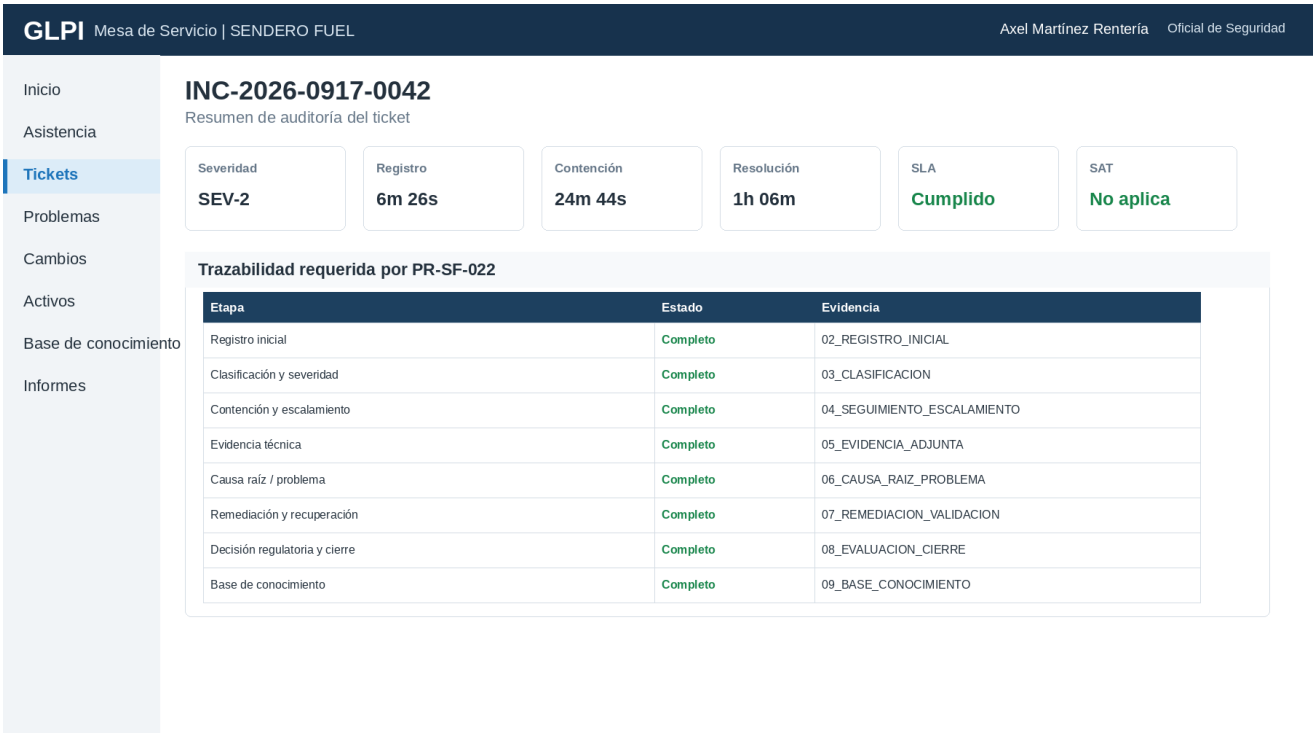


Figura 10. Resumen de trazabilidad para auditoría.