

INFORME DE SITUACIÓN: RESPUESTA A AUDITORÍAS Y ANÁLISIS DE MADUREZ (SEPT 2026)

1. Resumen Ejecutivo

A fecha de 22 de septiembre de 2026, la plataforma de la Real Federación Hípica Española (RFHE) ha completado un ciclo intensivo de correcciones tras recibir los informes de auditoría técnica (Informes 7, 8 y el análisis de madurez de infraestructura).

Partiendo de valoraciones iniciales, el estado actual del proyecto refleja una mitigación casi total de los hallazgos críticos y altos en el código de la API y el Frontend. Los avances más significativos incluyen

- el **endurecimiento de la seguridad en producción** (corrigiendo una configuración errónea de variables de entorno que mantenía apagadas las protecciones)
- el cierre de **fugas de datos por falta de comprobación de ámbito**
- y una transición completa hacia una **infraestructura modular y gestionada mediante GitOps**.

Aunque se han identificado y resuelto vulnerabilidades críticas, se ha optado por aceptar ciertos riesgos residuales bajo justificación técnica, como el cifrado a nivel de campo (diferido hasta completar la migración de legado) y la reutilización de justificantes de pago en procesos manuales.

2. Madurez de la Plataforma e Infraestructura

El análisis de madurez técnica del 23 de septiembre de 2026 indica un cambio estructural de una arquitectura monolítica a una organización por responsabilidades separadas.

2.1 Evolución de Riesgos Estructurales

Hallazgo Original	Estado Actual	Evidencia de Mejora
Secretos/State versionados	Corregido	Uso de backends S3 con bloqueo (use_lockfile) y eliminación de secretos en archivos versionados.
Producción desde develop	Corregido	Despliegue limitado a tags vX.Y.Z con ejecución manual y protección de ramas.
Versión de Kubernetes obsoleta	Corregido	Actualización de la versión 1.29 a la 1.35 en todos los entornos.
Tooling mutable	Parcial	Fijación de versiones en imágenes de CI (Terraform 1.9.8, TFlint 0.59.1).

2.2 Avances en GitOps y Seguridad de Red

- **Adopción de Argo CD:** Se ha implementado un flujo GitOps operativo para el entorno de desarrollo, con políticas de sincronización automática y reparación autónoma (selfHeal).

- **Hardening de Workloads:** Implementación de NetworkPolicies para delimitar el tráfico, uso de PodDisruptionBudgets (PDB) para asegurar disponibilidad y restricciones de seguridad en el Gateway para segmentar namespaces.

3. Análisis Técnico: Frontend (admin-rfhe-ui)

El Informe 7 identificó 42 hallazgos. La respuesta técnica del 21 de septiembre de 2026 confirma que **ninguno de los seis hallazgos críticos permanece abierto**.

3.1 Mitigación de Hallazgos Críticos y Altos

- **Control de Accesos (CRIT-01 a CRIT-03):** Se han eliminado las vulnerabilidades en el Wizard de Schedule que permitían ediciones con permisos nulos. Se implementó una garantía por tests (role-routes.test.ts) que impide que cualquier ruta administrativa quede sin protección centralizada.
- **Cabeceras de Seguridad (HIGH-12):** Se identificó que el sitio en producción solo devolvía cabeceras de servidor y control de caché. Se ha configurado el proxy Nginx para incluir X-Frame-Options, HSTS y Content-Security-Policy-Report-Only.
- **Internacionalización (i18n):** Se ha alcanzado la paridad en español e inglés (5.747 claves), quedando pendientes ~500 claves en idiomas regionales (ca/eu/gl) correspondientes a pantallas de administración profunda.

3.2 Rectificación de Errores del Informe

El análisis destaca que varios puntos calificados como críticos por la auditoría eran **falsos positivos** debidos a la limitación del ZIP auditado:

- **CI/CD:** El proyecto contaba con una pipeline obligatoria (test, lint, build) antes del informe, gestionada en un repositorio de infraestructura no incluido en el paquete de auditoría.
- **Fallback SPA:** Se verificó que el servidor Nginx en producción gestiona correctamente los refrescos de ruta (200 OK) mediante la configuración del proxy.

4. Análisis Técnico: API (admin-rfhe-api)

El Informe 8 presentó 53 hallazgos (10 críticos). Tras la iteración de septiembre, se han corregido 20 hallazgos adicionales, centrando los esfuerzos en el endurecimiento efectivo del entorno de ejecución.

4.1 El Error de Configuración de Entorno (CRIT-06 / HIGH-13)

Se descubrió que la seguridad en producción estaba **desactivada de facto**. El código aplicaba protecciones solo si `NODE_ENV === "production"`, pero los secretos de producción estaban configurados como pre-production.

- **Consecuencia:** Las cookies se emitían sin el flag Secure, el nivel de log estaba en debug (provocando fugas de datos personales) y los guards de arranque estaban inactivos.
- **Corrección:** Se unificó el criterio de "entorno productivo" para incluir production, pre-production y staging, forzando el endurecimiento de seguridad independientemente del nombre del entorno.

4.2 Autorización y Fugas de Datos (CRIT-04 y CRIT-05)

Se confirmaron fallos de autorización donde el sistema validaba el rol del usuario pero no el ámbito del objeto:

- **Detalle de Concurso:** Usuarios autenticados podían ver metadatos de documentos y campos internos de fases que debían estar restringidos.
- **Histórico de Programa:** Se permitía el acceso a aprobaciones y rechazos de cualquier concurso conociendo solo su ID.
- **Solución:** Implementación de proyecciones restringidas para usuarios sin ámbito y adición de comprobaciones de propiedad en los controladores.

4.3 Reorganización a Monolito Modular (ADR-0015)

Más allá de la auditoría, el equipo realizó una refactorización estructural para mitigar problemas de acoplamiento:

- **Estructura:** Se pasó de una organización por capas técnicas a 26 módulos de dominio (Package by Feature).
- **Fronteras Verificadas:** Se implementaron reglas de Lint para impedir importaciones cruzadas no autorizadas entre módulos, convirtiendo errores de arquitectura en fallos de análisis estático.

5. Riesgos Aceptados y Decisiones de Diseño

La dirección técnica ha documentado áreas donde la corrección inmediata no se considera prioritaria o eficiente:

1. **Cifrado a nivel de campo (CRIT-10):** Desactivado hasta finalizar la migración de datos de legado. El riesgo se considera mitigado por el control de acceso a la base de datos y cifrado en tránsito, aunque los datos de ~1.200 personas permanecen en claro actualmente.
2. **Reutilización de Justificantes (HIGH-11):** Se permite técnicamente que un mismo archivo de pago se adjunte a dos solicitudes. Se acepta el riesgo dado que existe una revisión humana obligatoria que detectaría la duplicidad de la transferencia.
3. **Códigos de Acceso en Correos (MED-11):** Se mantiene el envío de códigos de acceso en correos de restablecimiento para facilitar la recuperación de cuentas de sistema y comités, según el ADR-0014.

6. Pendientes y Próximos Pasos

El plan de acción inmediato se divide en tareas de infraestructura y despliegue final:

- **Infraestructura:**
 - Desplegar la configuración de cabeceras de seguridad en producción tras validar la CSP en modo report-only.
 - Implementar imágenes Docker multietapa para eliminar dependencias de desarrollo y documentación en los artefactos de producción.
 - Configurar el límite de peticiones (Rate Limit) en el Gateway.
- **Desarrollo:**
 - Finalizar las 505 traducciones pendientes en catalán, euskera y gallego para las pantallas de administración.
 - Activar reglas de Lint type-aware de forma progresiva por módulos.
- **API:**
 - Corregir el residuo de getDraftSchedule para asegurar que el permiso NONE bloquee el acceso incluso a nivel de lectura.
 - Establecer el trabajo de migración previo al despliegue en la pipeline para evitar ejecuciones concurrentes de esquemas.