🔍 ANÁLISIS DE RIESGOS Y AUDITORÍA DEL SISTEMA IA SCHOOL

Fecha de Auditoría: 7 de Febrero 2026
Versión del Sistema: 2.5
Auditor: Sistema de Análisis IA

📊 RESUMEN EJECUTIVO

El sistema IA School es una plataforma SaaS robusta con **51 páginas** y **128+ endpoints API**. Esta auditoría identifica **riesgos críticos**, **vulnerabilidades potenciales** y **recomendaciones de mejora**.

Estado General: 🟡 BUENO (Requiere Mejoras Puntuales)

Categoría	Estado	Puntuación
Seguridad de APIs	🟡	75/100
Integridad de Datos	🟢	85/100
UX/UI	🟡	70/100
Escalabilidad	🟡	72/100
Correlación de Módulos	🟢	80/100
Manejo de Errores	🟡	68/100

🚨 RIESGOS CRÍTICOS IDENTIFICADOS

1. Race Conditions en Pagos y Contribuciones

Severidad: ALTA 🔴
Ubicación: `/api/vocal/funds/[id]/contributions`, `/api/charges/[id]/payments`

Problema:
- No hay bloqueo optimista ni transacciones atómicas completas
- Múltiples usuarios podrían registrar el mismo pago simultáneamente
- Posible duplicación de registros o montos incorrectos

Solución Recomendada:

```
// Usar transacciones con aislamiento
await prisma.$transaction(async (tx) => {
  const existing = await tx.payment.findFirst({ where: { ... } });
  if (existing) throw new Error('Pago ya registrado');
  // Crear pago
}, { isolationLevel: 'Serializable' });
```

---

2. Falta de Rate Limiting en Endpoints Críticos

Severidad: ALTA 🔴
Ubicación: Todos los endpoints `/api/*`

Problema:
- Sin protección contra ataques de fuerza bruta
- Vulnerable a DDoS en operaciones costosas (IA, generación PDF, emails)
- El chatbot podría ser abusado para generar costos excesivos

Solución Recomendada:
- Implementar rate limiting por IP y por usuario
- Límites específicos: Login (5/min), Chatbot (20/min), Tips IA (10/hora)

---

3. Sesiones JWT Sin Revocación

Severidad: MEDIA 🟡
Ubicación: `lib/auth-options.ts`

Problema:
- Una vez emitido un JWT, no puede ser revocado
- Si un usuario es desactivado, su sesión sigue válida hasta expirar
- No hay logout real del lado del servidor

Solución Recomendada:
- Implementar lista negra de tokens (Redis/DB)
- Verificar estado activo del usuario en cada request
- Reducir tiempo de expiración del token

---

4. Falta de Auditoría de Acciones Críticas

Severidad: MEDIA 🟡
Ubicación: Múltiples endpoints

Problema:
- No se registra quién ve información médica sensible
- Acciones financieras sin trail de auditoría completo
- Cambios en becas/descuentos sin log

Acciones Sin Auditar:
- Consulta de expedientes médicos
- Eliminación de pagos

- Modificación de becas asignadas
- Acceso a información psicológica

---

5. Exposición de Datos Sensibles en Responses

Severidad: MEDIA 🟡
Ubicación: Múltiples APIs

Problema:
- Algunos endpoints devuelven más datos de los necesarios
- Información médica podría filtrarse en includes de Prisma
- IDs internos expuestos innecesariamente

⚠️ RIESGOS OPERACIONALES

6. Correlación Problemática: Becas + Pagos

Severidad: MEDIA 🟡

Escenario de Riesgo:
1. Admin crea beca con 50% descuento
2. Se asigna a estudiante
3. Sistema genera cargos sin aplicar descuento automáticamente
4. Padre paga monto completo
5. Reclamación y proceso de reembolso

Estado Actual: El sistema de becas existe pero NO está integrado automáticamente con la generación de cargos.

Solución: Integrar `Scholarship` → `Charge` → `Payment` en cadena.

---

7. Sincronización B2B vs Servicios Individuales

Severidad: MEDIA 🟡

Problema:
- Si un colegio entra en morosidad B2B (no paga su 50%)
- El sistema suspende el colegio
- Pero los padres ya pagaron sus mensualidades
- ¿Qué pasa con el servicio a los padres?

Solución Recomendada:
- Modo “Solo Lectura” en lugar de suspensión total
- Notificar a padres sobre situación
- Período de gracia extendido para operaciones críticas (calificaciones)

---

8. Dependencia de Servicio de IA

Severidad: BAJA 🟢

Problema:
- Chatbot, Tips, Análisis de Sentimiento dependen de API externa
- Si la API falla, múltiples funciones se degradan
- No hay fallback para operaciones críticas

Solución: Implementar respuestas de fallback y caché de tips populares.

🖥️ ANÁLISIS UX/INTERFAZ

Problemas Identificados:

Problema	Impacto	Prioridad
Dashboard de PROFESOR usa vista de PADRE	Confusión de roles	ALTA
Dashboard de VOCAL usa vista de PADRE	Falta funcionalidad específica	ALTA
No hay confirmación en acciones destructivas	Errores irreversibles	MEDIA
Carga lenta en directorio con muchos usuarios	Performance	MEDIA
Sin modo offline real para PWA	UX móvil	BAJA
Tablas no responsivas en móvil	Usabilidad	MEDIA

🔐 ANÁLISIS DE SEGURIDAD

Headers de Seguridad (Middleware)

✅ X-Content-Type-Options: nosniff
✅ X-Frame-Options: SAMEORIGIN
✅ X-XSS-Protection: 1; mode=block
✅ Referrer-Policy: strict-origin-when-cross-origin
⚠️ Content-Security-Policy: NO IMPLEMENTADO
⚠️ Strict-Transport-Security: NO IMPLEMENTADO

Validación de Entrada

✅ Prisma previene SQL Injection
⚠️ Algunas APIs no validan tipos estrictamente
⚠️ Falta sanitización de HTML en campos de texto largo

Autenticación

✅ Passwords hasheados con bcrypt
✅ JWT para sesiones
⚠️ Sin 2FA
⚠️ Sin protección contra credential stuffing
⚠️ Sin bloqueo de cuenta por intentos fallidos

📈 ANÁLISIS DE ESCALABILIDAD

Puntos de Bottleneck:

1. **Consultas N+1 en APIs de listado**
   - `/api/groups/my-groups` hace múltiples queries
   - `/api/announcements` no optimiza lectura de status

2. **Sin paginación en algunos endpoints**
   - Directorio de estudiantes
   - Historial de pagos
   - Lista de documentos

3. **Generación de PDF síncrona**
   - Certificados y constancias bloquean el request
   - Deberían ser trabajos en background

🔄 CORRELACIONES DE MÓDULOS

Matriz de Dependencias

```
                    Pagos  Becas  Asist  Calif  Enferm  Tienda  Vocal
Pagos (Charges)      ✓      →      -      -      -       ←      ←
Becas (Scholarship)  ←      ✓      -      →      -       -      -
Asistencia           -      -      ✓      →      →       -      -
Calificaciones       -      ←      ←      ✓      -       -      -
Enfermería           -      -      ←      -      ✓       -      -
Tienda (Store)       →      -      -      -      -       ✓      -
Vocal (Funds)        →      -      -      -      -       -      ✓

→ = Afecta a    ← = Afectado por    - = Sin relación
```

Integraciones Faltantes:

- ❌ Becas → Cargos (descuento automático)
- ❌ Asistencia → Notificaciones automáticas
- ❌ Calificaciones → Becas académicas

- ❌ Enfermería → Alertas a padres
- ❌ Store → Pagos unificados

💡 MEJORAS ADICIONALES RECOMENDADAS

Funcionalidad

1. **Dashboard específico para PROFESOR** con:
   - Tareas pendientes de calificar
   - Asistencia del día
   - Mensajes de padres
   - Calendario de clases

2. **Dashboard específico para VOCAL** con:
   - Fondos activos
   - Pagos pendientes de su grupo
   - Avisos del grupo
   - Calendario de actividades

3. **Sistema de Ciclos Escolares** para:
   - Promover alumnos automáticamente
   - Histórico de calificaciones por año
   - Reportes comparativos

4. **Recibos PDF de Pagos** para:
   - Comprobante fiscal
   - Referencia SPEI
   - QR de verificación

Seguridad Avanzada

1. **Verificación en Signup** (ver sección siguiente)
2. **Logs de Auditoría** completos
3. **2FA Opcional** para admins
4. **Alertas de actividad sospechosa**

🔐 RECONOCIMIENTO FACIAL Y VERIFICACIÓN SEGURA

¿Es Posible? SÍ ✅

Opciones Técnicas:

Opción A: Face API con IA (Recomendada para verificación)

Cómo funciona:

1. Usuario toma selfie durante signup
2. Sistema guarda embedding facial (no la foto)
3. En login, compara selfie en vivo con embedding guardado
4. Requiere “liveness detection” para evitar fotos

Pros:
- Alta seguridad
- Difícil de falsificar con liveness
- Conveniente para padres

Contras:
- Requiere consentimiento explícito (GDPR/LFPDPPP)
- Costo adicional por API de reconocimiento
- Problemas de accesibilidad
- Puede fallar con cambios físicos (barba, lentes)

Opción B: Web Authn / Passkeys (Más Moderna)

Cómo funciona:
1. Usuario registra dispositivo con Face ID/Touch ID
2. Autenticación biométrica local
3. No se envía dato biométrico al servidor

Pros:
- Más privado (biometría nunca sale del dispositivo)
- Soportado nativamente en iOS/Android
- Sin costo de API externa
- Estándar FIDO2

Contras:
- Requiere dispositivo compatible
- Fallback necesario para dispositivos viejos

Opción C: Verificación de Identidad (KYC Lite)

Cómo funciona:
1. Usuario sube foto de INE/Pasaporte
2. Sistema verifica documento con OCR
3. Selfie comparado con foto del documento
4. Se valida que persona = documento

Pros:
- Verifica identidad real
- Útil para contexto escolar (seguridad)
- Una vez por registro

Contras:
- Proceso más largo
- Requiere manejo seguro de documentos
- Costo por verificación ($2-5 USD)

Recomendación:

Para IA School, sugiero implementar:

1. **Signup:** Verificación con selfie + documento (opcional, configurable por escuela)
2. **Login:** WebAuthn/Passkeys como método principal
3. **Fallback:** Email/Password + OTP por SMS/Email

Implementación Propuesta:

```
// Flujo de signup seguro
1. Usuario ingresa datos básicos
2. Verificación de email (código 6 dígitos)
3. [Opcional] Verificación facial:
   - Selfie en vivo con liveness detection
   - Comparación con foto de documento
4. Términos y condiciones aceptados
5. Cuenta creada con nivel de verificación registrado

// Flujo de login con Face ID
1. Usuario ingresa email
2. Sistema detecta si tiene Passkey registrado
3. Si sí: Autenticación con Face ID/Touch ID
4. Si no: Password + OTP opcional
```

📋 PLAN DE ACCIÓN PRIORIZADO

Fase 1: Crítico (1-2 semanas)

- [ ] Implementar rate limiting
- [ ] Agregar transacciones atómicas en pagos
- [ ] Verificar usuario activo en middleware
- [ ] Content Security Policy

Fase 2: Alta Prioridad (2-4 semanas)

- [ ] Dashboards específicos (Profesor, Vocal)
- [ ] Integración Becas → Cargos
- [ ] Sistema de auditoría
- [ ] WebAuthn/Passkeys login

Fase 3: Media Prioridad (1-2 meses)

- [ ] Ciclos escolares
- [ ] Recibos PDF
- [ ] KYC lite opcional
- [ ] Modo offline mejorado

Fase 4: Mejoras Continuas

- [ ] Optimización de queries
- [ ] Tests automatizados
- [ ] Monitoreo de performance

📝 CONCLUSIÓN

El sistema IA School tiene una **base sólida** pero requiere atención en:
1. **Seguridad transaccional** en operaciones financieras
2. **Rate limiting** para proteger recursos

3. **Dashboards específicos** por rol
4. **Verificación de identidad mejorada** (factible con múltiples opciones)

El reconocimiento facial **SÍ es posible** y recomiendo WebAuthn/Passkeys como solución principal por ser más privada y moderna, con KYC lite opcional para escuelas que requieran verificación de identidad estricta.

Documento generado automáticamente - Febrero 2026