🔒 Reporte de Auditoría de Seguridad - INMOVA API

Fecha: 18/12/2025, 20:19:19

Total de Rutas Auditadas: 526

📊 Resumen Ejecutivo

Severidad	Cantidad	Porcentaje
🔴 **CRÍTICO**	3	0.6%
🟠 **ALTO**	108	20.5%
🟡 **MEDIO**	378	71.9%
🔵 **BAJO**	0	0.0%
✅ **SEGURO**	37	7.0%

🎯 Métricas de Seguridad

- **Con Autenticación (getServerSession):** 413/526 (78.5%)
- **Con Verificación de Sesión:** 35/526 (6.7%)
- **Con Verificación de Roles:** 66/526 (12.5%)
- **Con Manejo de Errores:** 520/526 (98.9%)

🔴 PROBLEMAS CRÍTICOS (Acción Inmediata Requerida)

`/api/auth/validate-password`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/stripe/webhook`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/users/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

🟠 PROBLEMAS DE ALTA PRIORIDAD

`/api/ai/detect-business-model`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/ai/detect-intent`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/analytics/web-vitals`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/approvals/[id]`

- **Métodos:** PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/approvals/request`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/approvals`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/approvals/stats`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/audit-logs`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-propietario/login`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-propietario/logout`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-propietario/me`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/forgot-password`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/login`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/logout`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/me`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/register`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-proveedor/reset-password`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/auth-tenant/[...nextauth]`

- **Métodos:** N/A
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/automation/run`

- **Métodos:** GET, POST
- **Problemas:**

- ❌ No tiene verificación de autenticación (getServerSession)

`/api/b2b-billing/webhook`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/buildings`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/announcements`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/engagement`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/events/[id]/attendees`

- **Métodos:** POST, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/events/[id]`

- **Métodos:** GET, PATCH, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/events`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/posts/[id]/reactions`

- **Métodos:** POST, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/posts/[id]`

- **Métodos:** GET, PATCH, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/community/posts`

- **Métodos:** GET, POST

- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/cron/process-contract-renewals`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/cron/process-payment-reminders`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/cron/process-preventive-maintenance`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/cron/process-scheduled-reports`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/csrf-token`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/dashboard/analytics`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/dashboard`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/dashboard/stats-cached-example`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/digital-signature/[id]/reject`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/digital-signature/[id]/sign`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/digital-signature/webhook`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/docs`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/expenses/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/expenses`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/landing/capture-lead`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-logs`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-preferences`

- **Métodos:** GET, PUT
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-rules/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-rules`

- **Métodos:** GET, POST
- **Problemas:**

- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-templates/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/notification-templates`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/owner-notifications`

- **Métodos:** GET, PATCH
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/accept-invitation`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/calculate-commissions`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/commissions`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/dashboard`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/invitations`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/login`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/partners/register`

- **Métodos:** POST

- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/payments/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ⚠️ Ruta crítica sin verificación de roles específicos

`/api/payments/receipt/[id]`

- **Métodos:** GET
- **Problemas:**
- ⚠️ Ruta crítica sin verificación de roles específicos

`/api/portal-inquilino/invitations/validate`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-inquilino/login`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-inquilino/maintenance`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-inquilino/password-reset/confirm`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-inquilino/password-reset/request`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-inquilino/register`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-propietario/documents`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-propietario/maintenance`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-propietario/messages`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-propietario/settings`

- **Métodos:** GET, PUT
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/availability`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/chat/conversations`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/chat/messages`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/dashboard`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/invoices/[id]/pdf`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/invoices/[id]`

- **Métodos:** GET, PATCH
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/invoices/[id]/submit`

- **Métodos:** POST
- **Problemas:**

- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/invoices`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/quotes/[id]`

- **Métodos:** GET, PATCH
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/quotes`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/reviews`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/work-orders/[id]/accept`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/work-orders/[id]/reject`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/portal-proveedor/work-orders/[id]/start`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/providers/performance/[id]`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/providers/recommend`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/providers`

- **Métodos:** GET, POST

- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/providers/stats`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/push/vapid-keys`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/push-notifications/public-key`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/reports`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/scheduled-reports/[id]`

- **Métodos:** POST, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/scheduled-reports`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/signup`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/str/channel-manager/dynamic-rules`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/str/channel-manager/metrics`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/str/channel-manager/pricing`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/str/channel-manager`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/suggestions/[id]`

- **Métodos:** GET, PATCH, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/suggestions`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/suggestions/stats`

- **Métodos:** GET
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/support/categorize-ticket`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/support/knowledge-search`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/support/tickets/analyze`

- **Métodos:** POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/tasks/[id]`

- **Métodos:** GET, PUT, DELETE
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/tasks`

- **Métodos:** GET, POST
- **Problemas:**

- ❌ No tiene verificación de autenticación (getServerSession)

`/api/tenants`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

`/api/users`

- **Métodos:** GET, POST
- **Problemas:**
- ❌ No tiene verificación de autenticación (getServerSession)

🟡 PROBLEMAS DE PRIORIDAD MEDIA (Mostrando 20 de 378)

- `/api/accounting/[provider]/config` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/[provider]/disconnect` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/[provider]/test` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/a3/create-invoice` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/a3/register-payment` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/a3/status` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/a3/sync-customers` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/alegra/create-invoice` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/alegra/register-expense` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/alegra/register-payment` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/alegra/status` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/alegra/sync-customers` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/analytics` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/balance` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/cash-flow` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/contasimple/customers` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/contasimple/expenses` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/contasimple/invoices` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/contasimple/payments` - ⚠️ Tiene getServerSession pero no verifica if (!session)
- `/api/accounting/contasimple/status` - ⚠️ Tiene getServerSession pero no verifica if (!session)

💡 Recomendaciones de Acción

Inmediatas (Hoy)

1. **Proteger rutas críticas:** Agregar `getServerSession()` en todas las rutas marcadas como CRÍTICO
2. **Verificar sesiones:** Añadir `if (!session) return NextResponse.json({ error: 'Unauthorized' }, { status: 401 })`
3. **Rutas /api/admin/*:** Verificar que solo `super_admin` pueda acceder

Esta Semana

1. Implementar middleware de autenticación centralizado
2. Añadir verificación de roles en rutas sensibles
3. Implementar rate limiting en rutas de autenticación y pago

Este Mes

1. Añadir manejo de errores consistente en todas las rutas
2. Implementar logging de accesos a rutas críticas
3. Crear tests automatizados de seguridad

📝 Ejemplo de Ruta Segura

```
import { NextRequest, NextResponse } from 'next/server';
import { getServerSession } from 'next-auth';
import { authOptions } from '@/lib/auth';

export async function POST(request: NextRequest) {
  try {
    // 1. Verificar autenticación
    const session = await getServerSession(authOptions);
    if (!session) {
      return NextResponse.json(
        { error: 'Unauthorized' },
        { status: 401 }
      );
    }

    // 2. Verificar roles (para rutas críticas)
    const allowedRoles = ['super_admin', 'administrador'];
    if (!allowedRoles.includes(session.user.role)) {
      return NextResponse.json(
        { error: 'Forbidden - Insufficient permissions' },
        { status: 403 }
      );
    }

    // 3. Validar input
    const body = await request.json();
    // ... validación con zod o similar

    // 4. Lógica de negocio
    // ...

    return NextResponse.json({ success: true });
  } catch (error) {
    console.error('Error en ruta:', error);
    return NextResponse.json(
      { error: 'Internal server error' },
      { status: 500 }
    );
  }
}
```

Generado automáticamente por el script de auditoría de seguridad