




# SISTEMA DE RECUPERACIÓN DE CONTRASEÑA - GUÍA DE CONFIGURACIÓN

---

## BACKEND IMPLEMENTADO

Archivos Creados/Modificados:

1.  **backend/api/auth.php** - Añadidos 2 endpoints:
  - `POST /api/auth/forgot-password`
  - `POST /api/auth/reset-password`
2.  **backend/utils/Auth.php** - Añadidos 2 métodos:
  - `Auth::forgotPassword($email)`
  - `Auth::resetPassword($token, $new_password, $confirm_password)`
3.  **backend/utils/EmailService.php** - Nuevo servicio de emails:
  - `EmailService::enviarRecuperacionPassword($email, $token)`
  - Template HTML profesional incluido
  - Modo desarrollo (logs sin enviar email real)
  - Integración con Brevo API

---

## CONFIGURACIÓN REQUERIDA

### 1. Variables de Entorno en Render.com

Ve a tu servicio backend en Render → Environment → Add Environment Variable:

```
# API Key de Resend (obligatorio para producción)
RESEND_API_KEY=re_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

# URL del frontend (para enlaces en emails)
FRONTEND_URL=https://galitroco-frontend.onrender.com

# Email remitente (opcional - usa onboarding@resend.dev si no tienes dominio)
RESEND_FROM_EMAIL=onboarding@resend.dev
```

### 2. Obtener API Key de Resend

#### Paso 1: Crear Cuenta (Si aún no la tienes)

- Ve a: **<https://resend.com>**
- Click en **"Start Building"** o **"Sign Up"**

- Usa GitHub para login rápido o email
- Plan gratuito: **3,000 emails/mes + 100 emails/día**

## Paso 2: Obtener API Key

1. Login en Resend
2. Dashboard → **API Keys** (menú lateral)
3. Click "**Create API Key**"
4. Configuración:
  - **Name:** **GaliTroco Production**
  - **Permission:** **Sending access** (Full access)
  - **Domain:** **All Domains** (o tu dominio si lo tienes)
5. Click "**Add**"
6. ⚠ **IMPORTANTE:** Copia la key INMEDIATAMENTE (solo se muestra una vez)
7. Pégalas en Render como **RESEND\_API\_KEY**

## Paso 3: Email Remitente (Opciones)

### Opción A: Email de Testing (Más rápido)

```
RESEND_FROM_EMAIL=onboarding@resend.dev
```

- ☒ Funciona inmediatamente
- ☒ Perfecto para desarrollo y testing
- ⚠ Limitado a 100 emails/día
- ⚠ No personalizable

### Opción B: Dominio Propio (Producción)

1. En Resend → **Domains** → **Add Domain**
2. Añade tu dominio: **galitroco.com**
3. Configura DNS records (SPF, DKIM, DMARC)
4. Espera verificación (~15 minutos)
5. Usa: **noreply@galitroco.com**

```
RESEND_FROM_EMAIL=noreply@galitroco.com
```

**PARA TFM:** Usa **onboarding@resend.dev** (funciona perfectamente)

---

## TESTING EN DESARROLLO LOCAL

Modo Desarrollo (Sin API Key)

Si **NO** configuras **BREVO\_API\_KEY**, el sistema funciona en **modo desarrollo**:

- ☒ No envía emails reales
- ☒ Escribe en logs de PHP
- ☒ Puedes ver el token y link de recuperación en consola

### Ver logs en XAMPP:

```
# Ver últimas líneas del log
tail -f D:\xampp\apache\logs\error.log

# O en el archivo de logs de PHP
tail -f D:\xampp\php\logs\php_error_log
```

## Testing Manual con Thunder Client/Postman

### 1. Solicitar Recuperación de Contraseña

```
POST http://localhost:8000/backend/api/auth.php/forgot-password
Content-Type: application/json

{
  "email": "usuario@ejemplo.com"
}
```

### Respuesta esperada:

```
{
  "success": true,
  "message": "Si el email está registrado, recibirás instrucciones para
recuperar tu contraseña"
}
```

### En logs verás:

```
=== MODO DESARROLLO - EMAIL NO ENVIADO ===
Destinatario: usuario@ejemplo.com
Token: 1a2b3c4d5e6f7g8h9i0j...
Link de recuperación: http://localhost:4200/reset-password?
token=1a2b3c4d5e6f7g8h9i0j...
=====
```

### 2. Restablecer Contraseña con Token

POST http://localhost:8000/backend/api/auth.php/reset-password

Content-Type: application/json

```
{
  "token": "1a2b3c4d5e6f7g8h9i0j...",
  "new_password": "NuevaPass123",
  "confirm_password": "NuevaPass123"
}
```

### Respuesta esperada:

```
{
  "success": true,
  "message": "Contraseña actualizada correctamente. Ya puedes iniciar sesión"
}
```

---

## VALIDACIONES IMPLEMENTADAS

### Forgot Password:

- ☒ Email válido (formato)
- ☒ No revela si email existe (seguridad)
- ☒ Token aleatorio seguro (64 caracteres)
- ☒ Expiración 1 hora
- ☒ Protección contra timing attacks

### Reset Password:

- ☒ Token existe y no expiró
- ☒ Token no fue usado previamente
- ☒ Contraseñas coinciden
- ☒ Mínimo 8 caracteres
- ☒ Al menos 1 letra y 1 número
- ☒ Cierra todas las sesiones activas (seguridad)
- ☒ Marca token como usado

---

## SEGURIDAD IMPLEMENTADA

### Protecciones:

1. **No revela información:** Mismo mensaje si email existe o no
2. **Tokens seguros:** `bin2hex(random_bytes(32))` (64 caracteres)
3. **Expiración corta:** 1 hora por defecto
4. **Un solo uso:** Token se marca como usado

5. **Cierre de sesiones:** Al cambiar contraseña, cierra todas las sesiones
6. **Logs de auditoría:** Registra todos los intentos
7. **Timing attack protection:** `usleep()` para emails no existentes
8. **Contraseña fuerte:** Requiere letras y números

Base de Datos:

```
-- Tabla ya creada en schema.sql
CREATE TABLE password_resets (
  id SERIAL PRIMARY KEY,
  email VARCHAR(255) NOT NULL,
  token VARCHAR(255) UNIQUE NOT NULL,
  fecha_creacion TIMESTAMP DEFAULT NOW(),
  fecha_expiracion TIMESTAMP DEFAULT (NOW() + INTERVAL '1 hour'),
  usado BOOLEAN DEFAULT FALSE
);

CREATE INDEX idx_password_resets_token ON password_resets(token);
CREATE INDEX idx_password_resets_email ON password_resets(email);
```

---

## TEMPLATE DE EMAIL

El email que reciben los usuarios incluye:

- ☒ Header profesional con gradiente
- ☒ Botón grande "Restablecer Contraseña"
- ☒ Link alternativo (copia y pega)
- ☒ Aviso de expiración (1 hora)
- ☒ Nota de seguridad
- ☒ Footer con branding
- ☒ Diseño responsive (móvil y desktop)
- ☒ Estilos inline (compatibilidad con email clients)

**Vista previa:** El template HTML está en `EmailService.php` línea 95-270

---

## TROUBLESHOOTING

Problema: No recibo emails en producción

**Solución:**

1. Verifica `RESEND_API_KEY` en Render
2. Verifica `RESEND_FROM_EMAIL` (usa `onboarding@resend.dev` para testing)
3. Revisa logs de Render: `render logs --service galitroco-backend --tail`
4. Busca errores: `grep -i "error enviando email" logs`
5. Verifica en Resend Dashboard → **Logs** (muestra todos los emails enviados)

Problema: Error "Token inválido o expirado"

**Solución:**

1. El token expira en 1 hora
2. Cada token solo se puede usar una vez
3. Verifica en BD: `SELECT * FROM password_resets WHERE email='usuario@ejemplo.com' ORDER BY fecha_creacion DESC LIMIT 1;`

Problema: Email va a spam

**Solución:**

1. Con `onboarding@resend.dev` raramente va a spam
2. Si usas dominio propio:
  - En Resend → Domains → Verify DNS
  - Configura SPF, DKIM y DMARC records
  - Espera 24-48h para propagación DNS
3. Pide a usuarios revisar carpeta spam/promotions

---

## CHECKLIST PRE-PRODUCCIÓN

Antes de desplegar a producción:

- ☐ Cuenta de Resend creada (o ya tienes)
- ☐ API Key de Resend obtenida
- ☐ Variable `RESEND_API_KEY` añadida en Render
- ☐ Variable `FRONTEND_URL` configurada en Render
- ☐ Variable `RESEND_FROM_EMAIL` configurada (usa `onboarding@resend.dev`)
- ☐ Testing en local con modo desarrollo (sin API key)
- ☐ Testing en producción con email real
- ☐ Verificar que emails no van a spam
- ☐ Logs revisados sin errores
- ☐ (Opcional) Dominio propio verificado en Resend

---

## PRÓXIMOS PASOS

### 1. Implementar Frontend:

- Crear componente `forgot-password.component.ts`
- Crear componente `reset-password.component.ts`
- Actualizar `auth.service.ts`
- Añadir rutas
- Link en `login.component.html`

### 2. Testing Completo:

- Flujo completo usuario a usuario

- Diferentes navegadores
- Testing móvil

### 3. Mejoras Opcionales:

- Rate limiting (máx 3 intentos por hora)
- Email de confirmación de cambio
- Historial de cambios de contraseña

---

## SOPORTE

Si tienes problemas:

1. Revisa logs de Render
2. Verifica configuración de Brevo
3. Comprueba que BD tiene la tabla `password_resets`
4. Testing en local primero (modo desarrollo)

---

**¡Backend completado! Ahora continuamos con el Frontend.** 🦄