

Flujo de Activación de Pacientes en eSalud

Resumen General

Preparado por Omar Ahumada G.

Fecha: 06-02-2025

El proceso de activación de pacientes es un flujo crítico de seguridad que permite a los nuevos pacientes crear su cuenta de usuario de manera segura y controlada.

1. Creación Inicial del Paciente

Características

- Creado por Admin/Staff sin usuario asociado
- Genera token de activación único
- Token con validez temporal de 24 horas

Proceso

1. Registro inicial de paciente en el sistema
2. Generación automática de token de activación
3. Almacenamiento seguro del token hasheado

2. Envío de Correo de Activación

Características

- Genera enlace de activación firmado
- Utiliza Mailable de Laravel
- Incluye instrucciones claras

Componentes del Correo

- Token de activación
- Enlace firmado y temporal
- Instrucciones de activación
- Información de expiración

3. Formulario de Activación

Validaciones Previas

- Verificar integridad del token
- Comprobar no expiración
- Validar solicitud firmada

Campos del Formulario

- Correo electrónico
- Contraseña (con requisitos estrictos)
- Confirmación de contraseña

4. Requisitos de Seguridad para Contraseña

- Longitud mínima: 12 caracteres
- Combinación de:
 - Mayúsculas
 - Minúsculas
 - Números
 - Caracteres especiales
- Validación de complejidad
- Prevención de contraseñas comunes

5. Creación de Usuario

Proceso

1. Crear usuario vinculado al paciente

2. Establecer rol 'paciente'
3. Marcar cuenta como activa
4. Eliminar token de activación

6. Post-Activación

- Redirección a página de login
- Mostrar mensaje de activación exitosa
- Permitir inicio de sesión inmediato

7. Manejo de Errores

Escenarios contemplados:

- Token inválido
- Token expirado
- Contraseña no cumple requisitos
- Intentos de activación agotados

Eventos del Sistema

- PacienteRegistrado
- TokenActivacionGenerado
- CuentaActivada

Consideraciones Adicionales de Seguridad

- Tokens hasheados, no almacenados en texto plano
- Registro de intentos de activación
- Protección contra ataques de fuerza bruta
- Límite de intentos de activación
- Bloqueo por IP tras múltiples intentos fallidos

Archivos y Métodos Clave

Modelo de Paciente

- **Archivo:** `app/Models/Paciente.php`
- **Métodos Principales:**
 - `generarTokenActivacion()` : Genera token de activación
 - `enviarCorreoActivacion()` : Envía correo de activación
 - `verificarTokenActivacion()` : Verifica la validez del token
 - `booted()` : Método de creación automática de token

Servicio de Activación

- **Archivo:** `app/Services/PacienteActivacionService.php`
- **Métodos Principales:**
 - `generarTokenActivacion()` : Genera token único
 - `generarUrlActivacion()` : Crea URL firmada de activación
 - `enviarCorreoActivacion()` : Gestiona envío de correo

Controlador de Activación

- **Archivo:** `app/Http/Controllers/Paciente/ActivacionController.php`
- **Métodos Principales:**
 - `mostrarFormularioActivacion()` : Muestra formulario de activación
 - `activar()` : Procesa solicitud de activación
 - `completarActivacion()` : Finaliza proceso de activación

Rutas

- **Archivo:** `routes/web.php`
- **Rutas de Activación:**
 - `paciente.activacion.formulario` : Muestra formulario
 - `paciente.activacion.completar` : Procesa activación

Correo de Activación

- **Archivo:** `app/Mail/PacienteActivacionMail.php`
- **Método Principal:** `build()` : Construye correo de activación

Ejemplo de Validación de Contraseña

```
'password' => [  
  'required',  
  'confirmed',  
  'min:12',  
  'regex:/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]+$/'  
]
```

Recomendaciones de Implementación

- Usar HTTPS
- Implementar headers de seguridad
- Deshabilitar autocompletado en formulario
- Implementar Content Security Policy
- Registrar eventos con IP y timestamp
- No loguear datos sensibles

Control de Versiones

- Versión: 1.0
- Fecha de Última Actualización: 2025-02-09
- Responsable: Equipo de Desarrollo eSalud