

# Prueba de Caja Negra REQ-009

---

*“Título proyecto: Gestión de Fideicomisos”*

## **Integrantes:**

Kevin Andino  
Luis Calle  
Denisse Quishpe  
Madellyn Tasipanta.

**Fecha: 2026/01/17**

**Captura de la pantalla de la**

**Ejecución:**

**REQ 009- Vencimiento y renovación**

**obligatoria de contraseña**

### **Paso 1: Intento de Acceso Estándar**

**Título: Interfaz de Inicio de Sesión**

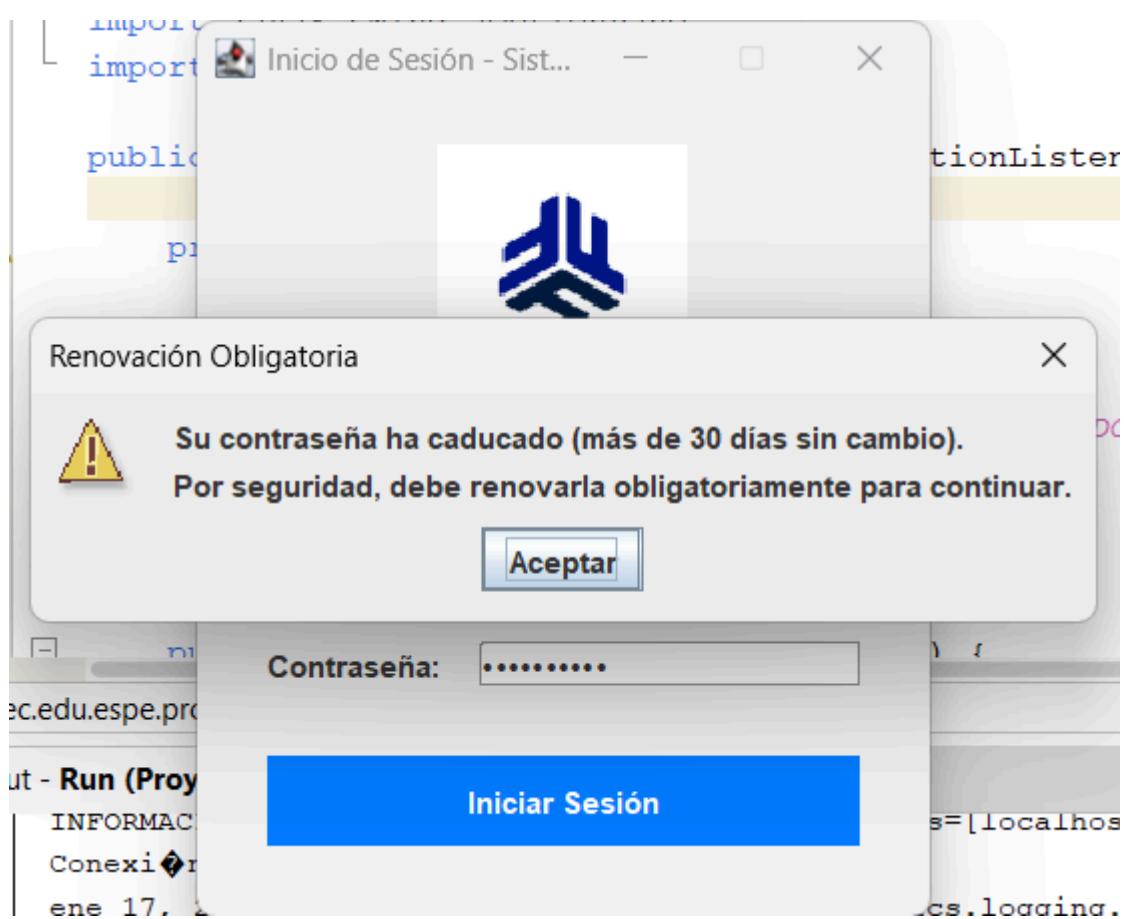
**Descripción:** El flujo comienza en la pantalla de "Acceso al Sistema", donde el usuario ingresa sus credenciales habituales (**Usuario y Contraseña**). En este punto, el sistema actúa como una caja negra que, tras recibir los datos, no solo valida la veracidad de la clave, sino que también consulta en la base de datos la fecha del último cambio realizado por dicho usuario.



### **Paso 2: Detección de Caducidad (Regla de Negocio)**

**Título: Notificación de Renovación Obligatoria**

**Descripción:** Al detectar que han transcurrido más de 30 días desde la última actualización de la clave, el sistema interrumpe el proceso de inicio de sesión. Se despliega una ventana emergente de advertencia informando que la contraseña ha caducado y que, por políticas estrictas de seguridad, es imperativo renovarla para poder acceder a las funciones del software.



### Paso 3: Gestión de Cambio de Credenciales

#### Título: Formulario de Actualización de Usuario

**Descripción:** El sistema redirige de forma automática al usuario a la interfaz de "Configuración de Usuario". Aquí se requiere el ingreso de la contraseña actual como método de validación de identidad, seguido de la nueva clave y su respectiva confirmación. Este paso asegura que solo el propietario de la cuenta pueda realizar el cambio obligatorio.

Configuración de Usuario

## Datos y Herramientas de Usuario

Usuario Login:  Cambiar Usuario

---

Contraseña actual:

Contraseña Nueva:  Cambiar Contraseña

Confirmar Contraseña:

### Paso 4: Validación de Integridad y Seguridad

#### Título: Control de Diferencia de Contraseñas

**Descripción:** Durante el proceso de cambio, el sistema valida que la nueva contraseña no coincida con la anterior. Si el usuario intenta burlar la renovación ingresando la misma clave caducada, el sistema emite una alerta indicando que "la nueva contraseña debe ser diferente a la actual", garantizando así que se cumpla el objetivo de rotación de seguridad del requisito.

Configuración de Usuario

## Datos y Herramientas de Usuario

Usuario Login:  Cambiar Usuario

Seguridad

Contraseña  Por seguridad, la nueva contraseña debe ser diferente a la actual.

Aceptar

Contraseña

Confirmar Contraseña:

## Paso 5: Confirmación de Renovación Exitosa

### Título: Finalización y Reautenticación

**Descripción:** Una vez procesada una clave válida, se muestra el mensaje de "¡Renovación exitosa!". El sistema solicita un nuevo ingreso para asegurar que el token de sesión se genere con las nuevas credenciales. Esta confirmación cierra el ciclo del REQ 009, dejando al usuario listo para operar con una cuenta actualizada y protegida.

