



Ministerio de  
**ECONOMÍA**  
Y  
**FINANZAS PÚBLICAS**  
ESTADO PLURINACIONAL DE BOLIVIA

**GUÍA OPERATIVA**  
**CAMBIO DE CONTRASEÑA POR**  
**CADUCIDAD**  
**SISTEMA DE GESTIÓN PÚBLICA - SIGEP**



## **Guía Operativa**

### **Cambio de Contraseña por caducidad**

#### **Sistema de Gestión Pública - SIGEP**

Ministerio de Economía y Finanzas Públicas

Viceministerio de Presupuesto y Contabilidad Fiscal

Dirección General de Sistemas de Gestión de Información Fiscal

**2017**

## Contenido

---

1. GENERALIDADES.....	3
2. ADVERTENCIA DE CADUCIDAD DE LA CONTRASEÑA.....	3
3. CAMBIO DE CONTRASEÑA.....	4
4. RECOMENDACIONES.....	5

# CAMBIO DE CONTRASEÑA POR CADUCIDAD

## 1. GENERALIDADES

Las contraseñas de acceso al Sistema de Gestión Pública (SIGEP) como a cualquier otro sistema informático tienen un tiempo de caducidad o tiempo máximo de uso, lo que significa que cuando la contraseña caduque, se requerirá de forma obligatoria al usuario que realice el cambio de la misma en el sistema. Los usuarios deben cambiar su contraseña periódicamente en el SIGEP por motivos de seguridad.

Las contraseñas en el SIGEP caducan en seis (6) meses, tiempo que será contabilizado a partir del último cambio de contraseña efectuado por el usuario.

Si el usuario cambia su contraseña en un menor tiempo, el sistema no requerirá un cambio obligatorio de contraseña.

## 2. ADVERTENCIA DE CADUCIDAD DE LA CONTRASEÑA

El usuario con contraseña próxima a expirar que se conecte al SIGEP observará un mensaje de advertencia de caducidad, tal como muestra la Fig. 1:

**Fig. 1**  
**Advertencia de caducidad de la contraseña**



Dicho mensaje se actualizará automáticamente y mostrará la cantidad de días restantes para la caducidad de la contraseña, para que el usuario cambie de contraseña en el sistema.

Una vez que se llegue al tiempo para cambio voluntario de la contraseña haya vencido y si el usuario notificado no ha procedido con el cambio de contraseña, cuando se conecte al sistema

se visualizará por defecto la pantalla de cambio de contraseña, impidiendo realizar otra operación diferente mientras no se realice el cambio requerido.

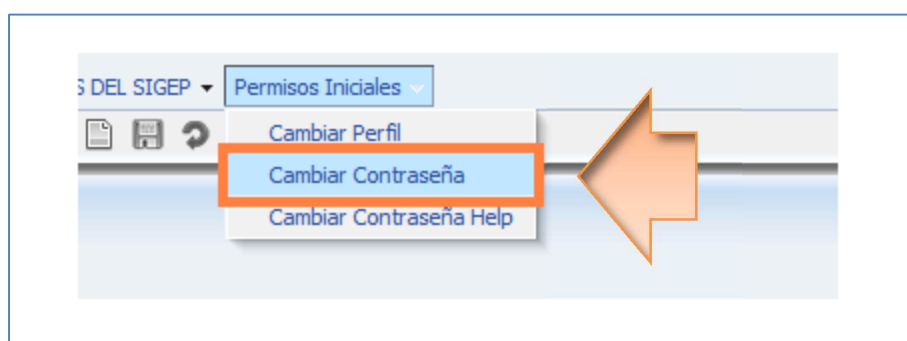
### 3. CAMBIO DE CONTRASEÑA

Para realizar el cambio de contraseña siga la ruta del menú horizontal que se muestra a continuación:

Permisos Iniciales ► Cambiar Contraseña

Tal como muestra la siguiente figura 2:

**Fig. 2**  
**Ruta para cambiar la contraseña**



A continuación visualizará la pantalla mostrada en la Fig. 3, en esta pantalla digite los datos requeridos por el sistema:

- a) **Contraseña a cambiar:** Digite su contraseña actual, con la cual ingresó al sistema.
- b) **Nueva contraseña:** Digite la nueva contraseña, para lo cual deberá considerar los siguientes criterios a efectos de lograr contraseñas más seguras:
  - Debe tener mínimo 10 y máximo 14 caracteres (obligatorio)
  - Debe ser diferente de la contraseña actual (obligatorio)
  - Puede contener caracteres alfanuméricos y caracteres especiales que figuran en el teclado estándar como guión bajo (\_), punto (.), pesos (\$), numeral (#) entre otros.
  - Se debe evitar que la contraseña contenga el nombre de usuario o cualquier otra información personal (cumpleaños, nombres de hijos, cónyuges, etc.).
  - Se debe evitar utilizar serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)
- c) **Repita la nueva contraseña:** Digite nuevamente la nueva contraseña para confirmar el cambio.

Seguidamente, presione el botón Guardar y el cambio se efectuará cuando el usuario ingrese nuevamente al sistema (Ver Fig. 3).

**Fig. 3**  
**Cambio de contraseña**

The image shows a web form titled "Cambio de Contraseña". It contains three input fields for passwords, each with a callout bubble: 'a)' points to the "Contraseña a cambiar:" field, 'b)' points to the "Nueva contraseña:" field, and 'c)' points to the "Repita la nueva contraseña:" field. All fields are masked with dots. Below the fields is a "Guardar" button, which is highlighted with an orange box and a large orange arrow pointing towards it from the right.

## 4. RECOMENDACIONES

Se recomienda a los usuarios:

- No almacenar las contraseñas en un lugar público y al alcance de otras personas.
- No compartir las contraseñas por ningún medio.
- Nunca utilizar la opción de "Guardar contraseña" que en ocasiones se despliega en el navegador. Pues es más seguro que el usuario introduzca su contraseña cada vez que ingresa el sistema.

Los datos de acceso al sistema (usuario y contraseña) son personales y privados.

Los datos registrados en el SIGEP con el usuario asignado son de completa responsabilidad de la persona que se consigne como titular de dicho usuario.