

---

**Universidad La Salle**

---

**CodeGuardGT**  
**Realización de Caso de Uso: Cambiar Contraseña**  
**Predeterminada**  
**Versión:2.0**

CodeGuardGT
Caso de Uso: Cambiar Contraseña Predeterminada

## Caso de Uso: Cambiar Contraseña Predeterminada

### 1. Comparación entre Entregas de Estudiantes

#### 1.1 Breve descripción del caso de uso

En este caso se describe el proceso por el cual un usuario registrado en CodeGuardGT puede cambiar la contraseña predeterminada (DNI), esto lo hará a través menú lateral izquierdo desplegable, en la pestaña de perfil, este mostrará un cambio de contraseña después de los datos personales del usuario, solo funcionará si se llenan los campos correspondientes y se da al botón de guardar.

### 2. Definiciones, Acrónimos, y Abreviaturas

- **CodeGuardGT:** Aplicativo para la detección de plagio en código SQL.
- **SQLAlchemy:** Biblioteca de Python.
- **Selenium:** Herramienta de automatización de navegadores web.
- **Caso de uso:** Descripción de cómo los usuarios interactúan con el sistema para lograr un objetivo.
- **MODAL:** mensaje emergente que retorna la aplicación, sea favorable o errónea.
- **Contraseña:** Palabra “Contraseña” en el aplicativo.
- **Api:** Una API (Interfaz de Programación de Aplicaciones) es un conjunto de reglas y protocolos que permite que diferentes aplicaciones se comuniquen entre sí, facilitando el intercambio de datos y funciones.
- **Hashea:** Encriptación de contraseñas basándose en la función Hash (toma como entrada una cadena de texto y genera una salida de longitud fija).
- **Usuario:** Administradores, estudiantes y profesores.

### 3. Referencias

#### 3.1 Flujo Básico de Cambiar Contraseña Predeterminada

ACTOR	SISTEMA
1. El “Usuario” ingresa al Sistema.	2. El sistema carga la página de LOGIN cargando un formulario donde solicitará DNI y contraseña.
3. El “Usuario” ingresa sus credenciales.	
4. El “Usuario” hace clic en el botón “Iniciar Sesión”.	5. El sistema verifica las credenciales ingresadas.
	6. El sistema redirecciona a la pantalla principal del “Usuario”.

CodeGuardGT
Caso de Uso: Cambiar Contraseña Predeterminada

7. El “Usuario” interactúa con el menú lateral izquierdo desglosable y selecciona el apartado “Mi Perfil”.	8. El sistema carga la página de perfil del usuario, mostrando la información actual.
	9. El sistema carga la información del perfil del usuario logueado y abajo un pequeño formulario donde solicita la Antigua Contraseña y la Nueva Contraseña.
10. El “Usuario” llena ambos campos.	
11. El “Usuario” hace clic en el botón “Actualizar Contraseña”.	12. El sistema envía los datos ingresados (contraseña antigua y contraseña nueva) al servidor para su validación.
	13. El sistema valida si el usuario existe.
	14. El sistema valida ambos campos han sido enviados correctamente.
	15. El sistema verifica si la contraseña antigua es correcta.
	16. El sistema “hashea” la nueva contraseña.
	18. El sistema actualiza la contraseña del usuario en la base de datos.
	17. El sistema retorna un mensaje de “Contraseña actualizada exitosamente”.

CodeGuardGT
Caso de Uso: Cambiar Contraseña Predeterminada

#### 4. Flujos Alternativos

##### 4.1 Flujo alternativo 1: *Usuario no encontrado - Solo en Api (paso 13)*

ACTOR	SISTEMA
1. Desde el punto 11	
	2. El sistema no encuentra el “Usuario”
	3. El sistema bota un mensaje de error “Usuario no encontrado”
	4. Regresa al paso 10

##### 4.2 Flujo alternativo 2: *Campos No Llenos (paso 14)*

ACTOR	SISTEMA
1. Desde el paso 11	
	2. El sistema detecta que faltan campos en el formulario y muestra una Alerta: “Completa este campo”.
	3. Regresa al paso 10

##### 4.3 Flujo alternativo 3: *Contraseña Antigua Incorrecta (paso 15)*

ACTOR	SISTEMA
1. Desde el paso 11	
	2. El sistema detecta que la contraseña antigua no coincide, muestra un mensaje de error: “La contraseña antigua no es correcta”
	3. Regresa al paso 10

#### 5. Requisitos Especiales

- **Seguridad:** La nueva contraseña debe cumplir con políticas de seguridad

estrictas, como contener al menos 8 caracteres, incluir letras mayúsculas, minúsculas, números, y símbolos especiales.

- **Encriptación:** Las contraseñas deben ser encriptadas utilizando un algoritmo de hash seguro (como bcrypt) antes de ser almacenadas en la base de datos.
- **Validación en Tiempo Real:** El sistema debe proporcionar validación en tiempo real para asegurar que la nueva contraseña cumple con los criterios de seguridad antes de ser enviada al servidor.
- **Tiempo de Respuesta:** El servidor debe procesar la solicitud de cambio de contraseña en menos de 3 segundos para una experiencia fluida de usuario.
- **Autenticación de Dos Factores (Opcional):** Se recomienda implementar autenticación de dos factores (2FA) como un paso adicional para aumentar la seguridad del cambio de contraseña, especialmente para cuentas de alto nivel (docentes).

## 6. Precondiciones

- **Usuario Autenticado:** El usuario debe haber iniciado sesión correctamente con sus credenciales (DNI y contraseña predeterminada) antes de acceder a la opción de cambiar la contraseña. El usuario puede ser de cualquiera de los siguientes roles: “Usuario Administrador”, “Usuario Docente”, o “Usuario Alumno”.
- **Acceso a la Página de Perfil:** El usuario debe tener acceso a la página “Mi Perfil” donde se realiza el cambio de contraseña.
- **Disponibilidad del Servidor:** El servidor debe estar disponible para procesar la solicitud de validación y actualización de la contraseña en la base de datos.
- **Campos Obligatorios Completos:** El usuario debe ingresar tanto la contraseña antigua como la nueva contraseña en el formulario.

## 7. Postcondiciones

- **Contraseña Actualizada:** La nueva contraseña del usuario debe estar correctamente almacenada en la base de datos y ser encriptada de manera segura.
- **Confirmación de Éxito:** El sistema debe mostrar un mensaje confirmando que la contraseña ha sido actualizada exitosamente.
- **Sesión de Usuario Activa:** El usuario debe permanecer autenticado y su sesión no debe ser interrumpida después del cambio de contraseña.
- **Notificación:** En caso de implementar, se puede enviar una notificación por correo electrónico o a través de la aplicación para informar al usuario que su contraseña ha sido cambiada.