

---

**Universidad La Salle**

---

**Sistema de Detección de Plagio Académico  
PlagiTracker**

**Caso de Uso: Loguearse en el sistema**

PlagiTracker
Caso de Uso: Loguearse en el sistema

# Caso de Uso: Loguearse en el sistema

## 1. Loguearse en el sistema

### 1.1 Breve descripción del caso de uso

Este caso de uso describe el proceso mediante el cual un usuario (docente o alumno) se autentica en el sistema de detección de plagio para acceder a sus funcionalidades.

## 2. Flujo de Eventos

### 2.1 Flujo Básico

	ACTOR	SISTEMA
1	El usuario accede a la página de inicio del sistema.	Muestra la página de inicio del sistema con las opciones de <i>"Try PlagiTracker as a Student"</i> si se quiere ingresar como alumno y <i>"Try PlagiTracker as a Teacher"</i> si se quiere ingresar como docente.
2	El usuario hace clic en una de las dos opciones si quiere ingresar como docente o alumno.	Redirige a la página de Login respectiva (docente o alumno).
3	El usuario ingresa su correo y contraseña en los campos del formulario de inicio de sesión y hace clic en el botón de <i>"Login"</i> .	Valida las credenciales, autentica al usuario y redirige a la página principal con las funcionalidades disponibles.

### 2.2 Flujos Alternativos

#### 2.2.1 Campos incompletos en el formulario

	ACTOR	SISTEMA
1	El usuario no llena todos los campos y hace clic en el botón <i>"Login"</i> .	Muestra un mensaje de error debajo de cada campo incompleto del formulario, indicando que se debe llenar el respectivo campo (no se borran los campos anteriormente llenados). En caso esté vacío el campo de <b>Email</b> se muestra el mensaje: <i>"Email required"</i> y en caso de que esté vacío el campo de <b>Password</b> se muestra el mensaje <i>"Password required"</i> .

#### 2.2.2 Credenciales Incorrectas

	ACTOR	SISTEMA
--	-------	---------

PlagiTracker
Caso de Uso: Loguearse en el sistema

1	El usuario ingresa credenciales incorrectas y hace clic en el botón de "Login".	Muestra un mensaje de error debajo del formulario <i>"Unauthorized. Please check your credentials"</i> indicando que el correo(Email) o la contraseña(Password) son incorrectos, Además informa la cantidad de intentos restantes para iniciar sesión exitosamente con el mensaje: <i>"# login attempts remaining"</i> .
2	El usuario ingresa nuevamente sus credenciales y hace clic en el botón de "Login".	Si las credenciales son correctas, el sistema permite el acceso al usuario; de lo contrario, el número de intentos restantes disminuye y el ciclo se repite hasta que los intentos se agoten.

### 2.2.3 Número Máximo de Intentos Fallidos

	ACTOR	SISTEMA
1	El usuario supera el número permitido de intentos fallidos. Se permitirá un máximo de 3 intentos fallidos antes de bloquear temporalmente por 10 minutos el acceso.	Bloquea temporalmente por 10 minutos la cuenta y muestra un mensaje: <i>"Your account is locked. It will be unlocked on( :DD/MM/YYYY - HH:MM:SS)"</i> , con una fecha y hora en la que el usuario pueda intentar iniciar sesión nuevamente.

### 2.2.4 Error de inicio de sesión por fallo en el servidor:

	ACTOR	SISTEMA
1	El sistema experimenta un error durante la autenticación (por ejemplo, falla de base de datos).	Redirige a una página, la cual muestra un error <i>"500 server error"</i> en esta página dirá que hay errores en el servidor.

PlagiTracker
Caso de Uso: Loguearse en el sistema

### 3. Requisitos Especiales

#### 3.1 El sistema debe cifrar las contraseñas almacenadas en la base de datos

El sistema debe cifrar las contraseñas almacenadas en la base de datos utilizando el estándar de cifrado avanzado (AES) en su configuración AES-128. Esto asegura un nivel adecuado de seguridad ante posibles brechas. La clave secreta (*PLAGITRACKER\_ENCRYPT\_KEY*) y el vector de inicialización (IV) (*PLAGITRACKER\_IV*) deben generarse de manera segura y mantenerse en variables de entorno, evitando su codificación estática en el código.

#### 3.2 El sistema debe tener un mecanismo para prevenir ataques de fuerza bruta

El sistema debe permitir un número limitado de intentos de inicio de sesión fallidos antes de mostrar un mensaje que avise al usuario de que intente más tarde. Esto ayuda a prevenir que se realicen intentos automáticos repetidos para adivinar la contraseña.

#### 3.3 Manejo de campos incompletos

Si el docente intenta iniciar sesión sin rellenar los campos, el sistema debe mostrar un mensaje de error solicitando completar todos los campos obligatorios.

### 4. Precondiciones

#### 4.1 El usuario debe tener una cuenta registrada en el sistema

El sistema debe permitir un número limitado de intentos de inicio de sesión fallidos antes de mostrar un mensaje que avise al usuario de que intente más tarde. Esto ayuda a prevenir que se realicen intentos automáticos repetidos para adivinar la contraseña.

#### 4.2 El sistema debe estar operativo y accesible

Si las credenciales ingresadas son incorrectas, el sistema debe notificar al usuario sobre el error y permitirle reingresar la información correcta para intentar iniciar sesión nuevamente.

### 5. Post Condiciones

#### 5.1 El usuario ha sido autenticado y tiene acceso al sistema

Si las credenciales son correctas, el usuario es autenticado y se le redirige a la página principal con las funcionalidades habilitadas.

#### 5.2 Si el inicio de sesión falla (credenciales incorrectas o sistema inaccesible), el usuario puede intentarlo nuevamente

El sistema debe estar en funcionamiento y accesible a través de la red para que el usuario pueda acceder a la página de inicio de sesión y realizar el proceso de autenticación.