**PlagiTracker**

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

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

1. **Loguearse en el sistema**
   1. **Breve descripción del caso de uso**

El caso de uso describe el proceso mediante el cual un usuario se autentica en el sistema de detección de plagio para acceder a las funcionalidades del sistema, como la visualización de reportes de plagio.

1. **Flujo de Eventos**
   1. **Flujo Básico**

|  | **ACTOR** | **SISTEMA** |
| --- | --- | --- |
| 1 | El docente accede a la página de inicio del sistema. | Muestra la página de inicio del sistema. |
| 2 | El docente hace clic en el enlace o botón para iniciar sesión. | Muestra el formulario de inicio de sesión. |
| 3 | El docente ingresa su nombre de usuario y contraseña en el formulario de inicio de sesión. | Recibe el nombre de usuario y la contraseña ingresados. |
| 4 | El docente hace clic en el botón de "Iniciar sesión". | Validar las credenciales ingresadas, Si las credenciales son correctas, autentica al usuario y muestra la página de inicio con las funcionalidades disponibles |

* 1. **Flujos Alternativos**
     1. *Credenciales Incorrectas*

|  | **ACTOR** | **SISTEMA** |
| --- | --- | --- |
| 1 | El docente ingresa su nombre de usuario y contraseña en el formulario de inicio de sesión. | Valida las credenciales ingresadas. |
|  | El docente recibe un mensaje de error indicando que las credenciales son incorrectas. | Muestra un mensaje de error indicando que el nombre de usuario o la contraseña son incorrectos. |
| 2 | El docente decide reingresar sus credenciales. | Reinicia el campo de entrada y muestra nuevamente el formulario de inicio de sesión para que el docente pueda intentar de nuevo. |

1. **Requisitos Especiales**
   1. **El sistema debe cifrar las contraseñas almacenadas en la base de datos.**

Para garantizar la seguridad de la información de los usuarios, todas las contraseñas deben ser cifradas antes de ser almacenadas en la base de datos, evitando así que sean accesibles en texto plano en caso de una brecha de seguridad.

* 1. **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.

1. **Precondiciones**
   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.

* 1. **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.

1. **Post Condiciones**
   1. **El usuario ha sido autenticado y tiene acceso al sistema**

Antes de que un usuario pueda iniciar sesión, debe estar registrado en el sistema y tener una cuenta activa con un nombre de usuario y una contraseña válidos.

* 1. **Si el inicio de sesión falla, el usuario recibe una notificación y tiene la oportunidad de corregir su información**

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.