**Documento de Especificación de Requisitos 1**

| **Grupo** | 3 | |
| --- | --- | --- |
| **Proyecto** | “TreeSolution” (TS) | |
| **Especificación de Requisitos** | 1 | |
| **Requisito Funcional** | Inicio de Sesión | |
| **Encargado** | Cjuno Chacca, Roggelio | |
| **Control de Versión** | 1.0 | 22/04/2024 |

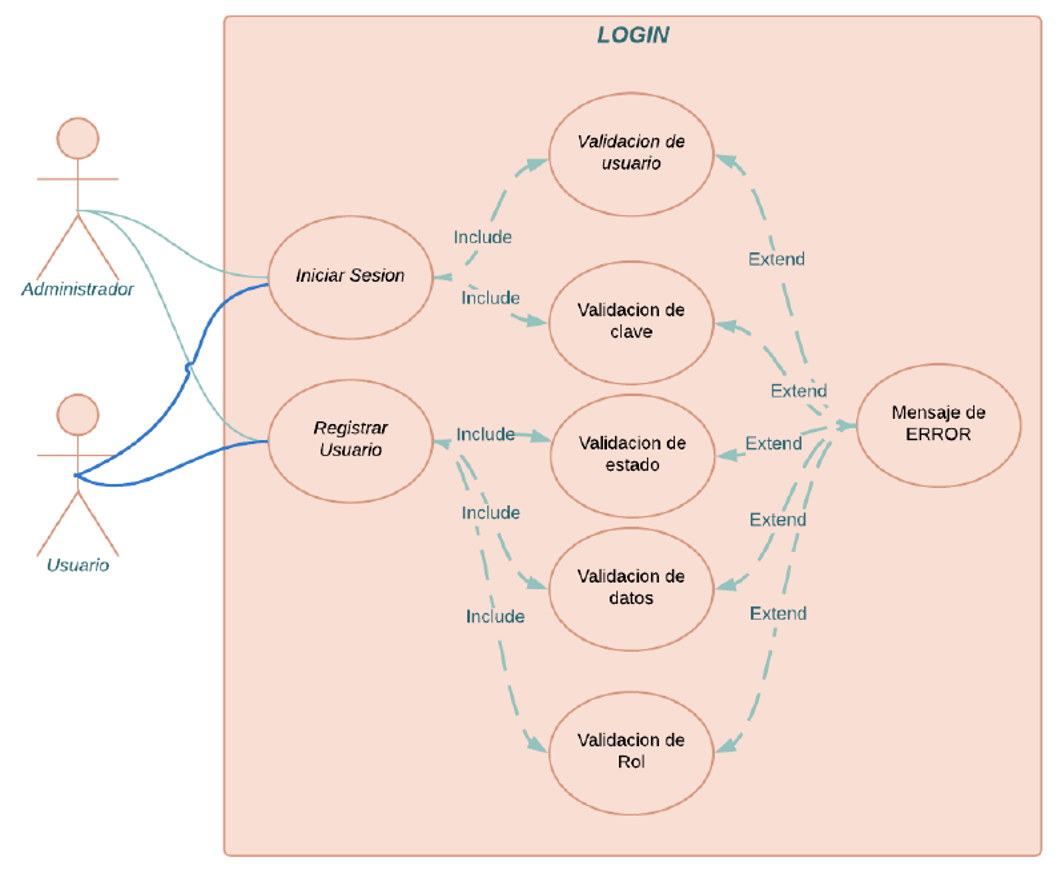
1. **Requisito Funcional**

| **ID** | **Nombre** | **Descripción** | **Usuario** |
| --- | --- | --- | --- |
| RF001 | Sistema de inicio de sesión | El sistema debe permitir el registro y el inicio de sesión al sistema. | Gerente, Empleado |

1. **Caso de Uso : Sistema de inicio de sesión**
   1. **Descripción**:

El sistema de inicio de sesión permite al gerente y empleados autenticarse de manera segura en la aplicación de software. Este requisito define los comportamientos necesarios para garantizar un acceso controlado y protegido al sistema por parte de ambos tipos de actores..

* 1. **Actores**
     1. **Principales**
        1. **Gerente**: Representa al que administra todo el sistema informático.
     2. **Secundarios**
        1. **Usuario** : Representa a las entidades externas que solicitan productos de la empresa, en este caso ropa deportiva, y están sujetas a ser facturadas por ellos.
  2. **Condiciones**
     1. **Precondiciones**
* El sistema está en un estado operativo y disponible para su uso.
* El empleado tiene credenciales válidas para acceder al sistema .
  + 1. **Postcondiciones**
* El usuario ha sido autenticado exitosamente por el sistema.
* Se ha concedido al usuario acceso a las funciones y datos autorizados según su rol y nivel de permisos.
* Se ha registrado la actividad de inicio de sesión, incluyendo la fecha, hora y la identificación del usuario, para fines de auditoría y seguimiento.
* Se ha cargado la interfaz de usuario principal o la pantalla de inicio correspondiente al usuario autenticado.
  1. **Diagrama de Caso de Uso**



1. **Requisitos No Funcionales**

| **ID** | **Nombre** | **Descripción** | **Usuario** |
| --- | --- | --- | --- |
| RNF1 | Seguridad | * El sistema debe utilizar un protocolo de autenticación seguro, como HTTPS, para proteger las credenciales del usuario durante la transmisión. * Debe implementarse un mecanismo de protección contra ataques de fuerza bruta para evitar intentos repetidos de inicio de sesión con credenciales incorrectas. * Se deben seguir las mejores prácticas de seguridad de contraseñas, como el uso de contraseñas fuertes, el almacenamiento seguro de contraseñas y la implementación de políticas de caducidad y cambio de contraseñas. | Empleado, Cliente |