Documentación de Requisitos y Casos de Uso - Iteración 4

Introducción

Este documento describe los requisitos funcionales y los casos de uso para la Iteración 4 del proyecto. En esta iteración, el objetivo principal es gestionar permisos de acceso, facilitando la compartición de datos y su autorización. Se enfoca en roles específicos de usuarios, como los gestores de seguridad y los usuarios de metadatos, permitiéndoles interactuar con los metadatos y controlar los permisos de acceso de acuerdo con las políticas de seguridad establecidas.

Casos de Uso

CDU7 - Gestionar permisos de acceso

Este caso de uso permite a los gestores de seguridad y a los usuarios de metadatos gestionar y compartir los permisos de acceso de manera estructurada y segura. Los usuarios con el rol de gestores de seguridad podrán definir y administrar los permisos de acceso para distintos tipos de usuarios, como implicados y gestores, de acuerdo con los niveles de seguridad requeridos.

1. **Actor Principal**: Gestores de seguridad, Usuarios de metadatos.

2. **Descripción**: Los gestores de seguridad configuran los permisos de acceso para asegurar que cada tipo de usuario (implicados, gestores) tenga acceso a los recursos de acuerdo con su rol. Además, los usuarios de metadatos pueden visualizar los metadatos disponibles y gestionar los permisos de compartición y autorización para su uso.

Requisitos Funcionales

Para los usuarios con el rol de Usuarios de Metadatos

RF.UM.01 - Acceder a los metadatos

Descripción: Los usuarios de metadatos podrán acceder a los distintos tipos de activos de datos y a sus metadatos, siempre que cumplan con las restricciones de seguridad establecidas.

Objetivo: Facilitar el acceso controlado y seguro a los metadatos, asegurando la accesibilidad de los datos según las políticas de seguridad de la organización.

Para los usuarios con el rol de Gestores de Seguridad

RF.GS.01 - Administrar permisos de acceso

Descripción: Los gestores de seguridad podrán definir y gestionar los permisos de acceso para cada tipo de usuario, incluyendo roles como implicados y gestores. Esta capacidad asegura que cada usuario acceda a los recursos que necesita de acuerdo con su función.

Objetivo: Mantener un entorno de seguridad gestionado para que los permisos se asignen de acuerdo con los requisitos de confidencialidad y acceso de la organización.