

# Documento de Análisis - Iteración 4

---

## *1. Introducción*

---

En la Iteración 4, el objetivo principal es desarrollar funcionalidades que permitan una gestión segura y estructurada de los permisos de acceso a metadatos y activos de datos, conforme a los roles de los usuarios definidos en el sistema. Los principales roles que interactuarán con estas funciones son:

- Gestores de Seguridad: Encargados de configurar y administrar los permisos de acceso.
- Usuarios de Metadatos: Usuarios que pueden ver y gestionar permisos sobre los datos que necesitan para su labor.

## *2. Objetivos del Análisis*

---

- Identificar las necesidades de los diferentes roles de usuario en cuanto a la gestión de permisos de acceso.
- Definir los requisitos de seguridad para asegurar que solo usuarios autorizados puedan modificar o visualizar permisos.
- Facilitar la integración de los nuevos requisitos funcionales en la infraestructura de seguridad actual del sistema.

## *3. Contexto y Justificación*

---

Actualmente, el sistema necesita una funcionalidad más robusta para administrar los accesos, especialmente en entornos con diferentes niveles de usuarios que requieren control granular sobre la visibilidad y edición de los datos. La implementación de estos requisitos permitirá cumplir con las políticas de seguridad organizativas y mejorar la trazabilidad de accesos.

## *4. Requisitos Funcionales Analizados*

---

- Para los Usuarios de Metadatos:
  - Necesidad: Acceso controlado y seguro a metadatos de diversos activos.
  - Descripción del Requisito: Los usuarios de metadatos deben tener acceso a los activos y sus metadatos dentro de las restricciones de seguridad establecidas.
- Para los Gestores de Seguridad:
  - Necesidad: Controlar y definir los permisos de acceso en función de las políticas de seguridad organizativas.
  - Descripción del Requisito: Los gestores de seguridad serán responsables de crear y administrar permisos de acceso para otros usuarios del sistema.

## *5. Casos de Uso Relevantes*

---

- CDU7 - Gestionar permisos de acceso:
  - Actor Principal: Gestores de seguridad, Usuarios de metadatos.
  - Descripción: Este caso de uso permite a los gestores configurar permisos para garantizar que cada usuario tenga el acceso adecuado de acuerdo con su rol, y a los usuarios de metadatos, gestionar los permisos de compartición y autorización.

## *6. Conclusiones del Análisis*

---

La fase de análisis sugiere que, para cumplir con los requisitos de la Iteración 4, se requiere una estructura de permisos de acceso con configuraciones detalladas. Esta implementación mejorará el cumplimiento de políticas, garantizará la confidencialidad y permitirá a los usuarios de metadatos trabajar de manera más eficiente.