**GOBERNANZA DE DATOS**

**Presentado por: GRUPO 1**

**CINDY JOHANNA ZAPATA ROMERO**

**HECTOR GEOVANY BELLO SANTAMARÍA**

**MARIO GUERRA GUALY**

**LEANDRO REYES JORDÁN**

**Docente:**

**CARLOS ISAAC ZAINEA MAYA**

**UNIDAD DE ESTUDIO:**

**GERENCIA DE PROYECTOS PARA CIENCIA DE DATOS**

**MAESTRÍA - GRUPO 1 - M1V - VIRTUAL - 2025**

**FACULTAD DE INGENIERÍA**

**BOGOTÁ, 01 DE MARZO DE 2025**

**UNIVERSIDAD EAN**

**Tabla de contenido**

[INTRODUCCIÓN 3](#_Toc191565102)

[NORMAS Y ESTÁNDARES APLICADOS 3](#_Toc191565103)

[PRIVACIDAD Y SEGURIDAD DE DATOS 3](#_Toc191565104)

[CONTROL Y AUDITORÍA DE DATOS 4](#_Toc191565105)

# INTRODUCCIÓN

Este documento describe las políticas de gobernanza de datos implementadas en el proyecto, garantizando la calidad, seguridad y cumplimiento normativo de los datos utilizados. La gobernanza de datos permite una gestión eficaz, asegurando integridad, trazabilidad y acceso controlado a la información.

La implementación de estas políticas de gobernanza de datos asegura la confiabilidad, seguridad y cumplimiento normativo del proyecto, la cual debe ser acompañada con una revisión periódica de estas políticas para garantizar su efectividad y alineación con cambios regulatorios y tecnológicos.

# NORMAS Y ESTÁNDARES APLICADOS

Para garantizar la coherencia y fiabilidad de los datos, el proyecto adopta los siguientes estándares y mejores prácticas:

* ISO 27001: Seguridad de la información y gestión de riesgos.
* ISO 8000: Calidad de datos y gestión de información.
* GDPR (Reglamento General de Protección de Datos): Regulaciones sobre privacidad y protección de datos personales en la UE.
* Ley de Protección de Datos Personales (según legislación de Colombia): Cumplimiento de normativas nacionales aplicables.
* Principios FAIR: Asegurar que los datos sean Encontrables, Accesibles, Interoperables y Reutilizables.

# PRIVACIDAD Y SEGURIDAD DE DATOS

El proyecto implementa medidas estrictas para proteger la privacidad y seguridad de los datos:

* Cifrado de datos: Se utilizan algoritmos de cifrado AES-256 para datos almacenados y TLS para datos en tránsito.
* Control de acceso: Políticas de acceso basadas en roles (RBAC) para garantizar que solo usuarios autorizados puedan acceder a información sensible.
* Anonimización y seudonimización: Aplicación de técnicas de ocultamiento de identidad en datos personales.
* Almacenamiento seguro: Uso de entornos en la nube certificados con cumplimiento de normativas internacionales.
* Planes de contingencia: Respaldos periódicos y protocolos de recuperación ante incidentes.

# CONTROL Y AUDITORÍA DE DATOS

Para garantizar la integridad y calidad de los datos, se han establecido los siguientes mecanismos de control y auditoría:

* Trazabilidad y linaje de datos: Registro de cambios y movimientos de datos dentro del sistema.
* Auditorías periódicas: Evaluaciones regulares del cumplimiento de normativas y buenas prácticas.
* Monitoreo continuo: Implementación de herramientas de detección de anomalías y acceso no autorizado.
* Gobernanza de metadatos: Definición de catálogos de datos para facilitar su gestión y reutilización.
* Políticas de retención y eliminación de datos: Definición de períodos de conservación y procedimientos de eliminación segura.