PLAN DE GESTIÓN DE DATOS

(Plantilla CONCYTEC)

1. Información general del proyecto

Ítem	Descripción
Título del proyecto	"Reformas institucionales y cadenas de valor: Estudio comparativo de capacidades de gestión en gobiernos locales de Arequipa y Cajamarca, 2001 – 2021"
Investigador principal (Apellidos y nombres, ORCID, afiliación)	Rolando Rojas Rojas https://orcid.org/0000-0002-6258-4932 Instituto de Estudios Peruanos
Colaboradores (Apellidos y nombres, ORCID, afiliación, rol)	Marcos Garfias Dávila https://orcid.org/0000-0001-5445-6634 Instituto de Estudios Peruanos
Breve descripción del proyecto	Este estudio partió de la posibilidad de hallar indicios suficientes que permitan afirmar que, a lo largo de estas dos últimas décadas, las reformas institucionales del Estado, o al menos parte de ellas, han encontrado en algunos gobiernos locales de Arequipa y Cajamarca condiciones favorables para desarrollarse. Proponemos que estas reformas propiciaron que la articulación entre el gobierno distrital con el provincial y regional fueron más efectivas.
Fuente de financiamiento del proyecto	PROCIENCIA, CONCYTEC
Código del proyecto (Al momento de la postulación, señale el código del concurso, luego de adjudicado, reemplazar por código del proyecto)	Código de postulación: E041-2022-03 Código de proyecto: **PE501078780-2022-PROCIENCIA**
Versión del PGD (control de versiones)	1

2. Creación y/o recopilación de los datos de investigación

¿Qué tipo de datos utilizará y/o generará? *[Realizar una breve descripción de todos los datos que tiene previsto generar/recopilar o reutilizar durante del desarrollo del proyecto de investigación. Para cada conjunto de datos, especifique su contenido, tipo, alcance y formato. Justifique la elección del formato considerando el almacenamiento, respaldo y accesos necesarios, teniendo en cuenta su volumen.* *La tabla 1describe el tipo de datos que puede generar o utilizar, de acuerdo al vocabulario controlado de la Confederación de Repositorios de Acceso Abierto (COAR) disponible en: https://vocabularies.coar-repositories.org/resource_types/]*
1.Encuestas estructuradas (fuente interna)

Contenido: Variables cuantitativas a servidores y funcionarios municipales, sobre percepciones en la mejora de la gestión, así como del impacto del proceso de descentralización y de las reformas del servicio civil.
Tipo COAR: Datos de encuesta
Alcance: 111 encuestas, 13 variables cada una.
Formato: captura de encuestas.
Justificación; Formato .jpg Volumen estimado: 8 MB por encuesta, total: 900 MB.
Formato: resultado de encuestas.
Justificación: Formato .cvs, compatible con software estadístico, fácil de almacenar y con respaldo regular en repositorios institucionales.

2.Narrativas cualitativas (fuente interna)
Contenido: Grabaciones de entrevistas a servidores y funcionarios de gobiernos locales.
Tipo COAR: Datos grabados.
Alcance: 42 entrevistas, 39 horas de grabación.
Formato: MP3 para grabaciones
Volumen estimado: 4.8 GB para grabaciones (MP3)
Justificación: El MP3 asegura almacenamiento eficiente.

3.Análisis documental (fuente externa)
Contenido: Datos compilados de documentos oficiales sobre reforma de la gestión a nivel de gobiernos municipales y políticas de transporte público (2000-2021).
Tipo COAR: Datos compilados.
Alcance: 20 documentos revisados.
Formato: PDF
Volumen estimado: 200 KB a 1 MB por documento. Total: 20 MB.
Justificación: Formatos que garantizan organización, análisis estructurado y durabilidad, con almacenamiento en repositorios institucionales y respaldo periódico.

¿Qué formato y cantidad de datos utilizará y/o generará?
[Indique los formatos de archivo y software específicos que se utilizarán para gestionar los datos a lo largo del proyecto. Considere que los formatos deben facilitar el intercambio, la accesibilidad a largo plazo y la interoperabilidad con otras herramientas.
Se recomienda el uso de formatos abiertos y estándares aceptados de acuerdo al área de conocimiento (ej., .txt, .csv, .tif, .tfw, etc) para asegurar la compatibilidad con diferentes sistemas y software a lo largo del tiempo.]

Se usó formatos estándar y reconocidos para garantizar el intercambio y la accesibilidad

1.Encuestas estructuradas: Los datos cuantitativos se gestionarán en archivos .CVS, un formato abierto, ideal para análisis estadístico en software como SPSS. Con un total de 111 encuestas y 13 variables por participante, se estima un volumen de 7 MB.

3.Narrativas cualitativas: Las grabaciones de entrevistas se almacenarán en formato .MP3, que garantiza compresión eficiente y calidad adecuada. Se estima un volumen de 4.8 GB para las grabaciones.

4.Análisis documental: Los datos compilados de documentos oficiales se almacenarán en formatos .PDF por su capacidad para organizar y analizar la información de manera estructurada, además de su durabilidad. Volumen estimado: 20 MB para 20 documentos.

¿Va a contar con datos reutilizados o reutilizables? ¿propios o de otras fuentes? *[Los datos a emplear podrán provenir de investigaciones realizadas por el equipo, de instituciones gubernamentales como el INEI, o de bases de datos de acceso abierto disponibles en línea. En el caso de datos de terceros, se deberá contar con las autorizaciones necesarias para su uso y reconocimiento de autoría.* *Especifique las fuentes utilizando preferentemente identificadores persistentes (DOI, handle, url, etc).]*
Se utilizaron datos propios y datos reutilizados provenientes de fuentes externas: Datos propios: Recopilados directamente por el equipo de investigación a través de entrevistas en profundidad y encuestas estructuradas; y que por tanto no han sido utilizados previamente en otros proyectos. Datos reutilizados: Se usaron datos secundarios obtenidos de instituciones gubernamentales y publicaciones académicas: - INEI (Instituto Nacional de Estadística e Informática): Bases de datos demográficas de las regiones de Arequipa y Cajamarca. - Plataforma del Estado Peruano, normas, informes y memorias sobre la gestión municipal y las reformas del servicio civil. -Repositorio Nacional Digital del Perú (RENARE): Documentos y publicaciones científicas relevantes disponibles bajo acceso abierto. -Bases de datos académicas: Artículos y reportes de bases de datos como Scopus, SciELO y Redalyc, utilizando identificadores persistentes como DOI para garantizar la trazabilidad y correcta citación.

3. Organización de los datos (estructuras de carpetas, convenciones de nomenclaturas de archivos, versiones de archivos)

¿Qué estándares o metodologías usará para la recolección y/o creación de los datos? *[Describa la estrategia a usar en la generación o recolección de los datos, así como los estándares (nacionales o internacionales) que utilizará.]*
1.Recolección y generación de datos Datos cualitativos: Se emplearon entrevistas haciendo uso de guías semiestructuradas. Datos cuantitativos: Las encuestas estructuradas se diseñarán siguiendo estándares estadísticos aceptados, con preguntas cerradas y escalas validadas, como la escala Likert, para asegurar la fiabilidad de los resultados. 2.Estándares nacionales e internacionales Normas nacionales: Se cumplirán las directrices éticas y metodológicas del Ministerio de Salud del Perú (Resolución Ministerial Nº 233-2020-MINSA), asegurando el consentimiento informado y la protección de datos personales. Estándares internacionales: Declaración de Helsinki (2013): Para garantizar el respeto y protección de los participantes.
¿Cómo estructurará y denominará las carpetas y archivos? *[Considere la forma en que organizará los datos durante la investigación, mencionando por ejemplo la convención de nomenclatura, la organización de las carpetas donde almacenará los datos.]*
Los datos serán organizados del siguiente modo: .

1.Estructura de carpetas: Las carpetas estarán organizadas de manera jerárquica según los siguientes criterios:

-Nivel 1: Etapas del proyecto (01. Diseño / 02. Recolección / 03. Análisis / 04. Informe).
-Nivel 2: Tipos de datos (Entrevistas / Encuestas / Documentos).
-Nivel 3: Ubicación y fechas (Arequipa_2023 / Cajamarca_2023).

2.Convención de nomenclatura: Los archivos seguirán un esquema estandarizado para facilitar su identificación y búsqueda:

Formato: Proyecto_TipoDato_Ubicación_Fecha
Modelo:
-Entrevistas:
-Gestión_municipal_Entrevista_Cajamarca_2023
- Gestión_municipal a_Entrevista_Cajamarca_2025
-Encuestas estructuradas:
- Gestión_municipal _Encuesta_Cajamarca_2023
- Gestión_municipal _Encuesta_Arequipa_2023
-Análisis documental:
- Gestión municipal _Documento_Arequipa_2023
- Gestión_municipal _Documento_Cajamarca_2023
-Informe:
- Gestión_municipal _Reporte_Entrevistas_2023
- Gestión_ municipal _Reporte_Encuestas_2023

¿Cómo gestionará las versiones?
[Describa la forma de organización o estructura de los datos considerando el uso de disposiciones para controlar las versiones. Especifique de qué manera cada versión será identificada y almacenada, y cómo se garantizará la integridad de los datos, su recuperación y/o colaboración.]

Mediante una estructura que permita identificar, almacenar y rastrear los cambios realizados en los datos a lo largo del proyecto

1.Control de versiones: Cada archivo incluirá un sufijo en su nombre para indicar la versión, utilizando un esquema estandarizado:

Formato: V1, V2, V3, ..., Final
Ejemplos:
Gestión_municipal_Encuesta_Arequipa_2025_V1
Gestión_municipal _Engrevista_ Cajamarca_2025_Final
La versión Final indicará el archivo aprobado para análisis o reporte.

2.Almacenamiento de versiones: Todas las versiones serán almacenadas en carpetas específicas según su estado:
Carpeta "Borradores": Contendrá las versiones iniciales de los archivos.
Carpeta "Revisados": Almacenará versiones actualizadas tras revisión.
Carpeta "Final": Incluirá únicamente los archivos aprobados para uso definitivo.

3.Integridad y recuperación: Se realizarán respaldos automáticos y manuales en repositorios digitales institucionales y copias periódicas en discos externos y plataformas en la nube (Google Drive).
Un registro de cambios será mantenido en un archivo maestro que documente las modificaciones realizadas en cada versión, incluyendo fecha, responsable y descripción del cambio.

4.Colaboración: Se utilizarán herramientas de colaboración como Google Drive para compartir archivos, con permisos controlados para evitar ediciones no autorizadas.

Las versiones compartidas incluirán una marca de tiempo y estarán restringidas al equipo autorizado, garantizando un trabajo colaborativo ordenado.

¿Qué procesos usará para asegurar la calidad de los datos?
[Describa los procedimientos que utilizará para asegurar la calidad de los datos, incluyendo la limpieza de datos, la transformación y la estandarización. Incluya información sobre software a utilizar, algoritmos, flujos de trabajo científico, entre otros.]

1.Criterios de calidad:

Integridad: Los datos recolectados serán verificados periódicamente para asegurar que estén completos.

Consistencia: Los datos serán revisados para identificar discrepancias o errores en las entradas.

2.Procesos para asegurar la calidad:

Limpieza de datos:

Se eliminarán duplicados y cualquier error de escritura y de datos mediante herramientas como Microsoft Excel.

En los datos cualitativos, se verificará periódicamente la fidelidad de las grabaciones.

Transformación de datos:

Los datos cuantitativos serán organizados en formatos tabulares (.CSV) para análisis estadístico con SPSS.

Estandarización de datos:

Se emplearán formatos consistentes para todos los datos (ejem., .CSV, .JPEG, .TXT) asegurando su interoperabilidad.

Las variables en las encuestas serán codificadas siguiendo convenciones uniformes (e.g., escala Likert de 1 a 5).

3.Flujo de trabajo científico: Se utilizará un flujo de trabajo estructurado que incluye:

Revisión inicial de los datos recolectados.

Aplicación de procedimientos de limpieza y transformación.

Validación mediante triangulación de datos cualitativos y cuantitativos para detectar inconsistencias.

4.Software utilizado:

SPSS para análisis estadístico y control de calidad de datos cuantitativos.

Microsoft Excel para validaciones iniciales y verificación manual de datos tabulares.

4. Documentación de los datos durante la fase de recopilación y análisis de la investigación

¿Qué información es necesaria para que los datos puedan ser leídos e interpretados en el futuro?
[Describa el tipo de documentación que se asociará a los datos para mantenerlos compresibles y utilizables, para usted y para ayudar a otros a entenderlos y reutilizarlos (bitácoras, cuadernos de laboratorio, procedimientos, normativa, entre otros). Debe incluir los detalles básicos que le permitirán a las personas encontrar los datos; la identificación de las personas que los crearon o contribuyeron a hacerlo; el título, la fecha de creación y las condiciones para su acceso.
La documentación podría incluir detalles de la metodología usada, información sobre análisis y procedimientos, la definición de variables, el vocabulario, las unidades de medida, los supuestos. Los metadatos de archivos asociados, como word, pdf, excel, se pueden generar en la misma aplicación.]

Se asociará documentación detallada con aspectos metodológicos, técnicos y contextuales:

1.Tipos de documentación asociada:

Bitácoras de campo: Registro de actividades realizadas durante la recolección de datos, incluyendo ubicación, fecha, participantes y observaciones relevantes.
Procedimientos metodológicos: Descripción de las metodologías utilizadas para la recopilación y análisis, incluyendo el diseño de entrevistas y cuestionarios.
Normativa aplicada: Referencias a las regulaciones nacionales e internacionales seguidas durante el proyecto, como la Resolución Ministerial Nº 233-2020-MINSA y la Declaración de Helsinki.
Definición de variables: Diccionario de datos que describa cada variable utilizada, su significado, formato, valores posibles y unidades de medida (e.g., escala Likert, categorías cualitativas).
Flujo de trabajo: Instrucciones detalladas sobre cómo se procesaron los datos, incluyendo pasos de limpieza, codificación y estandarización.

2.Metadatos asociados:
Título: Nombre del archivo que indique su contenido.
Autores: Identificación de quienes contribuyeron al archivo.
Fecha: Registro de la fecha de creación y última modificación del archivo.
Condiciones de acceso: Detalles sobre permisos de uso, licencias y posibles restricciones.
Detalles técnicos: Software utilizado para generar y analizar datos, como SPSS o Microsoft Excel.

3.Documentación en archivos digitales:
Metadatos: Los archivos (.docx, .csv, .pdf, .jpeg) generarán metadatos automáticamente o manualmente en las herramientas utilizadas.
Archivo README: Cada carpeta incluirá un README general que describa su contenido, estructura y propósito.
Documentación clave: Procedimientos y resultados se registrarán en archivos .pdf para durabilidad y accesibilidad.

Describa la forma en que reportará los metadatos
[Considere las "Directrices para repositorios institucionales de la Red Nacional de Repositorios Digitales de Ciencia, Tecnología e Innovación de Acceso Abierto (RENARE)" o Guía Alicia 2.0.1 (Disponible en https://hdl.handle.net/20.500.12390/2231) o las "Directrices de la Red Nacional de Información en Ciencia, Tecnología e Innovación para administradores de sistemas de gestión de información científica" (Disponible en: https://hdl.handle.net/20.500.12390/3690). Completar la plantilla de la tabla 2]

La información de los metadatos será reportada según las Directrices para repositorios institucionales de RENARE y la Guía Alicia 2.0.1:

- Autor (dc.contributor.author): Identificación de los investigadores responsables.
- Título (dc.title): Nombre descriptivo que refleje el contenido del conjunto de datos.
- Editorial (dc.publisher): Institución encargada de la publicación, como el repositorio asignado.
- Fecha de publicación (dc.date.issued): Fecha de generación o publicación de los datos.
- Tipo de publicación (dc.type): Clasificación del contenido, como "Datos cualitativos" o "Datos cuantitativos".
- Versión de la publicación (dc.type.version): Detalle sobre versiones, si corresponde.
- Formato y tamaño (dc.format, dc.format.size): Formato del archivo (ejem., .CSV, .JPEG, .PDF) y su tamaño aproximado.
- Idioma (dc.language.iso): Idioma de los datos, principalmente español.
- Nivel de acceso (dc.rights): Condiciones de acceso, como licencias.
- Condición de licencia (dc.rights.uri): Detalles de la licencia, si aplica.
- Fecha de fin de embargo (dc.date.embargoEnd): Fecha de finalización de restricciones, si corresponde.
- Resumen (dc.description.abstract): Breve descripción del propósito, metodología y alcance.
- Referencia bibliográfica (dc.identifier.citation): Citas relacionadas, si aplica.

- Materia (dc.subject): Palabras clave del contenido (ejem., gestión municipal, servicio civil.
- Campo del conocimiento OCDE (dc.subject.ocde): Clasificación temática según el OCDE.
- Identificador Handle (dc.identifier.uri): Identificador único para el acceso.
- ISBN (dc.identifier.isbn): Obligatorio si está relacionado con publicaciones aplicables.
- Recurso del cual forma parte (dc.relation.isPartOf): Vínculo con otros recursos, si corresponde.
- Patrocinio (dc.description.sponsorship): Información de los patrocinadores, si aplica.

5. Cumplimiento de aspectos éticos y legales

¿Ha considerado los aspectos éticos en relación con la creación y el uso de los datos?
[La gestión de datos debe considerar aspectos éticos fundamentales como la privacidad, la confidencialidad y el consentimiento informado. Es crucial establecer medidas de protección de datos, como la anonimización y la obtención de consentimiento previo, especialmente cuando se trabaja con datos de personas. Además, se deben respetar los derechos de los pueblos indígenas y garantizar la soberanía de sus datos. Por ejemplo: El tratamiento de los datos será totalmente anónimo y no será incluida ninguna información de carácter ideológico, orientación sexual, racial o religioso.]

1.Consentimiento informado:
- Todos los participantes recibirán información clara y comprensible sobre los objetivos, procedimientos, beneficios y posibles riesgos del estudio.
- Se utilizarán formularios diseñados asegurando el consentimiento voluntario previo a la participación.

2.Confidencialidad y anonimato:
- Los datos personales serán tratados de forma estrictamente confidencial y anonimizada, eliminando cualquier información que pueda identificar a los participantes.
- No se incluirán datos sensibles relacionados con ideología, orientación sexual, raza, religión o cualquier otro aspecto que pueda comprometer la privacidad de los involucrados.
- Los datos anonimizados se utilizarán únicamente con fines de investigación y bajo las condiciones establecidas en el consentimiento informado.

3. Medidas de protección de datos:
- Todos los datos recopilados serán almacenados en repositorios digitales seguros y protegidos por sistemas de acceso restringido.
- Se establecerán políticas de acceso que limiten el manejo de los datos a miembros autorizados del equipo de investigación, minimizando riesgos de filtraciones o usos no autorizados.

¿Cómo ha previsto identificar y tratar los aspectos legales?
[En proyectos colaborativos con instituciones externas, es fundamental establecer acuerdos claros sobre autorías, derechos de propiedad intelectual y condiciones de uso de los datos. Se recomienda consultar las políticas de cada institución involucrada y considerar los aspectos legales pertinentes.
La reutilización de datos de terceros requiere obtener los permisos correspondientes y respetar las restricciones de uso establecidas por sus autores. Asimismo, los datos que involucren información personal o confidencial deberán ser tratados de acuerdo con las normas de protección de datos y los consentimientos informados otorgados por los participantes.
En el marco de la Ley 30035 se debe utilizar la licencia Creative Commons Atribución/Reconocimiento 4.0 Internacional (CC BY) como licencia por defecto para los resultados de investigación. Sin embargo, se reconocen las particularidades de cada proyecto y se permite el uso de otras licencias o derechos de autor cuando sea necesario.]

A través de los siguientes lineamientos:

- Derechos de propiedad intelectual y autoría: Se reconocerá la contribución de cada participante conforme a su aporte.
- Condiciones de uso de datos: Cuando los datos involucren información personal o confidencial, su tratamiento se ajustará a las normativas de protección de datos y a los consentimientos informados otorgados por los participantes.
- Licenciamiento y acceso abierto: En cumplimiento de la Ley 30035, los resultados del proyecto se publicarán bajo la licencia Creative Commons Atribución 4.0 Internacional (CC BY) como estándar, permitiendo su uso, distribución y modificación con la debida atribución. No obstante, se podrán aplicar otras licencias en función de la naturaleza del proyecto.
- Cumplimiento legal: Se garantiza el cumplimiento de normativas aplicables, como propiedad intelectual, protección de datos y confidencialidad.

6. Prácticas de administración de datos para almacenar y proteger sus datos (copias de seguridad, almacenamiento, archivado)

¿Tiene suficiente capacidad de almacenamiento?
[Describa dónde se almacenarán los datos (local o externo) y la capacidad o limitaciones de depósito de los dispositivos o plataformas seleccionadas y su localización física, así como la mención de la institución o responsables a cargo.]

Los datos del proyecto se almacenarán en una combinación de almacenamiento local e institucional. Se utilizarán servidores internos con una capacidad de 15 GB. Además, se empleará almacenamiento en la nube con Google Drive institucional y repositorios de datos abiertos en la plataforma RENARE, dependiendo del tipo de información. La administración y supervisión estarán a cargo del equipo del grupo de investigación (GI).

¿Cómo se respaldarán los datos?
[Si los datos se almacenan en los repositorios institucionales, identifique con qué frecuencia se realizará el respaldo de los datos, así como la cantidad de copias que manejará. Solicite apoyo al gestor del repositorio institucional de la institución a la cual está afiliado para conocer la política institucional alineada a las "Directrices para repositorios institucionales de la Red Nacional de Repositorios Digitales de Ciencia, Tecnología e Innovación de Acceso Abierto (RENARE)" o Guía Alicia 2.0.1 (Disponible en https://hdl.handle.net/20.500.12390/2231) o las "Directrices de la Red Nacional de Información en Ciencia, Tecnología e Innovación para administradores de sistemas de gestión de información científica" (Disponible en: https://hdl.handle.net/20.500.12390/3690).]

Se implementará un esquema de tres copias de seguridad:

1. Copia principal: Almacenada en el servidor institucional, asegurando acceso interno seguro y administración centralizada.
2. Copia secundaria: Resguardada en un almacenamiento en la nube institucional con cifrado de extremo a extremo, garantizando integridad y accesibilidad remota bajo protocolos de seguridad establecidos.
3. Copia archivada: Guardada en un dispositivo físico (NAS o disco duro externo), protegido en una ubicación segura con acceso restringido para garantizar su integridad ante fallos en las copias digitales.

Para asegurar el cumplimiento de estándares de gestión y preservación de datos, se seguirá la política institucional de almacenamiento alineada con las Directrices RENARE y la Guía Alicia 2.0.1.

¿Quién será responsable de hacer los respaldos y la recuperación de los datos?
[Indique quien es el responsable de la custodia y respaldo de los datos. Si escoge un proveedor de respaldo, debe asegurarse que no existan conflictos con las políticas institucionales o a nivel gubernamental, por ejemplo, en el caso de datos sensibles.]

El responsable técnico y el coinvestigador. Ambos tendrán la responsabilidad de conservar una copia de seguridad en su almacenamiento personal, fortaleciendo la integridad y recuperación de la información.
En caso de considerar las opciones de respaldo institucionales ¿qué hará en caso de que accidentalmente se pierdan? *[Puede considerar hacer referencia al plan de acción o los lineamientos con los que cuente la institución responsable al respecto.]*
Se aplicará un protocolo que incluirá: 1.Restauración inmediata desde la última copia de seguridad disponible. 2.Validación de integridad para asegurar que los datos recuperados no presenten alteraciones o corrupción. 3.Notificación al equipo de TI, quien investigará la causa de la pérdida y aplicará medidas preventivas. 4.Implementación de acciones correctivas, como revisión de políticas de acceso, fortalecimiento de seguridad y automatización de respaldos. 5. Se seguirá el plan de acción institucional, priorizando la recuperación de los datos críticos en el menor tiempo posible, garantizando su continuidad y disponibilidad para los investigadores.

7. Acceso y seguridad de los datos de investigación

¿Cuáles son los riesgos relacionados con la seguridad de los datos y cómo se manejarán esos riesgos? *[Describa las estrategias para manejar los riesgos ante la desaparición involuntaria d los datos o el robo de estos, priorice implementar un enfoque integral de seguridad de datos. Puede considerar hacer referencia a los lineamientos con los que cuente la institución al respecto.]*
Los riesgos incluyen pérdida involuntaria, robo de datos y accesos no autorizados. Para prevenirlo se adoptarán las siguientes medidas: 1.Respaldo regular: Se realizarán copias de seguridad automáticas y programadas en múltiples ubicaciones seguras (local y en la nube) para minimizar el impacto de fallos o pérdidas accidentales. 2.Monitoreo continuo: Se utilizarán herramientas de detección de intrusos y monitoreo de actividad para identificar accesos sospechosos o intentos de vulneración. 3. Plan de recuperación ante desastres: Se establecerá un protocolo documentado para la rápida restauración de datos en caso de pérdida o ataque cibernético, asegurando la continuidad del proyecto. 4. Además, se consultarán y adoptarán los lineamientos institucionales en ciberseguridad para reforzar la protección de los datos, alineando estas medidas con normativas vigentes y buenas prácticas en seguridad informática.
¿Cómo controlará el acceso a los datos para mantener su seguridad? *[Para garantizar la seguridad de los datos, es esencial implementar un sistema de control de acceso robusto. Esto implica autenticar a los usuarios de manera segura, otorgar permisos específicos según sus roles, encriptar los datos tanto en reposo como en tránsito, y monitorear constantemente la actividad del sistema. Puede considerar hacer referencia a los lineamientos con los que cuente la institución al respecto.]*
Se implementarán las siguientes medidas: 1.Sistema de gestión de usuarios: Se asignarán cuentas individuales con permisos específicos según el rol del colaborador. 2.Autenticación robusta: Se exigirán contraseñas seguras y autenticación multifactor (MFA) para prevenir accesos no autorizados. 3. Revisión periódica: Se auditarán los permisos regularmente para alinearlos con las necesidades del proyecto.

4. Se aplicarán políticas institucionales de control de acceso y seguridad para fortalecer la protección de los datos.
¿Cómo conseguirá que las personas colaboradoras tengan acceso a los datos de forma segura? *[Para garantizar la seguridad de los datos, es esencial implementar un sistema de control de acceso robusto. Esto implica autenticar a los usuarios de manera segura, otorgar permisos específicos según sus roles, encriptar los datos tanto en reposo como en tránsito, y monitorear constantemente la actividad del sistema. Puede considerar hacer referencia a los lineamientos con los que cuente la institución al respecto.]*
Se implementarán las siguientes medidas: 1.Plataformas seguras certificadas: Las que incluirán repositorios digitales y sistemas de almacenamiento en la nube cifrado. 2.Control de roles y permisos: Se aplicará un modelo de mínimos privilegios, asegurando que cada colaborador tenga acceso solo a los datos para sus funciones. 3. Capacitación y concienciación: Dirigidas a los colaboradores, enfatizando la importancia de las buenas prácticas en seguridad de datos, la identificación de amenazas y el correcto uso de las plataformas asignadas.
Si se generan o colectan datos en campo ¿Cómo garantizará su transferencia segura a su sistema principal de seguridad? *[Describa las medidas que abarquen tanto el aspecto técnico como el organizacional. Puede considerar hacer referencia a los lineamientos con los que cuente la institución al respecto.]*
La transferencia de datos generados en campo se realizará con protocolos de seguridad para evitar pérdidas o accesos no autorizados: 1. Protocolos seguros: Transferencia mediante SFTP, HTTPS o herramientas institucionales certificadas para garantizar comunicación cifrada. 2. Redes confiables: Uso exclusivo de redes seguras o VPN institucional, evitando redes públicas no verificadas. 3. Copias locales temporales: Mantener una copia cifrada en dispositivos hasta confirmar la transferencia. 4. Verificación de integridad: Validación posterior de los datos y eliminación segura de copias temporales. Estas medidas cumplirán con las directrices institucionales para minimizar riesgos en la transferencia de datos, garantizando la protección y disponibilidad de los datos recolectados en campo.

8. Selección de datos para su reutilización y preservación

¿Cuáles datos tienen valor a largo plazo? ¿Cuáles deberían de retenerse, compartirse o conservarse? ¿Qué criterios usará para decidir esto? *[La gestión de datos va más allá del simple almacenamiento. Resguardar implica una gestión activa de la información, seleccionando aquellos datos que poseen un valor duradero y estratégico. A través de criterios rigurosos, podemos determinar cuáles deben ser conservados, compartidos o eliminados, asegurando así la optimización de nuestros recursos y el cumplimiento de las normativas vigentes]*
Los datos que poseen valor a largo plazo incluyen las narrativas cualitativas y los resultados cuantitativos de las encuestas. Estos serán retenidos, compartidos y conservados conforme a estos criterios: Criterios para la decisión: 1.Valor científico: Datos con potencial para generar conocimiento, validar hipótesis o realizar análisis longitudinales. 2.Reutilización: Datos anonimizados y estructurados para facilitar análisis comparativos en nuevos proyectos. 3.Cumplimiento normativo: Resguardo de datos que cumplan con estándares éticos y legales.

4.Impacto social y estratégico: Información que pueda influir en políticas públicas o intervenciones educativas y sociales.
5.Demanda potencial: Datos susceptibles de ser consultados por otras comunidades académicas o sectores interesados.
6. Los datos irrelevantes o duplicados serán eliminados tras validar su falta de utilidad, asegurando una gestión eficiente y responsable.

¿Cuáles datos deben ser conservados o destruidos, de acuerdo con regulaciones contractuales y legales de su institución?
[La reutilización de datos puede generar un gran valor, ya sea a través de la validación de resultados, la generación de nuevos conocimientos o la mejora de la enseñanza. Para maximizar ese potencial, es necesario establecer criterios claros para la selección y conservación de los datos. Estos criterios deben considerar tanto las exigencias legales o normativas, así como el valor intrínseco de los datos como los costos asociados a su gestión. Además, es fundamental planificar la preservación a largo plazo, asegurando la accesibilidad y la integridad de los datos para futuras generaciones de investigadores y usuarios.]

Datos que serán conservados:
1. Aquellos esenciales para la reproducibilidad científica.
2. Datos requeridos por políticas de acceso abierto.
3. Información de alto valor para futuras investigaciones.

Datos que serán destruidos:
1. Cuando expire el período de retención establecido en contratos o normativas.
2. Si contienen información sensible sin consentimiento explícito para su conservación.
3. Si su almacenamiento implica un riesgo innecesario o un alto costo sin justificación científica.

¿Cuánto tiempo los datos serán conservados y preservados?
[Considere que tiempo que los datos deben ser conservados y preservados depende de diversos factores, como la legislación vigente, el valor científico o comercial de los datos, y los costos de almacenamiento. Para tomar esta decisión, se deben evaluar criterios como la necesidad actual y futura de los datos, su valor intrínseco, los riesgos de pérdida y los costos asociados a su gestión.]

1.Normativas: Algunos datos deben conservarse entre 5 y 10 años, según regulaciones legales y científicas.
2.Valor a largo plazo: Datos de alto impacto podrán preservarse indefinidamente en repositorios especializados.
3.Costos: Se evaluará periódicamente la viabilidad de continuar su almacenamiento.
4.Propiedad y regulaciones: Si los datos están sujetos a normativas específicas, se garantizará su resguardo hasta cumplir los plazos establecidos.
5. Como estándar, los datos críticos serán almacenados por al menos 10 años, asegurando su accesibilidad para futuras investigaciones.

¿Cuál es el plan para el almacenamiento de los datos a largo plazo?
[Describa el tipo de almacenamiento y curaduría por parte de las personas investigadoras de las bases de datos con valor de largo plazo.
Considere una estrategia integral que combine la tecnología adecuada con una gestión cuidadosa por parte de los investigadores, a fin de garantizar la preservación de la información valiosa para futuras generaciones de investigadores y usuarios.]

Se seguirá el siguiente plan integral:
1. Repositorio institucional: Se almacenarán los datos en plataformas certificadas que cumplan con estándares de preservación digital.
2. Almacenamiento redundante: Se utilizarán servidores locales y en la nube para minimizar el riesgo de pérdida.
3. Curaduría y mantenimiento: Se realizarán revisiones periódicas para evitar la degradación de los datos.

4. Metadatos estandarizados: Se documentarán los datos para facilitar su recuperación y reutilización en el futuro.
5. Cifrado y control de acceso: Se aplicarán medidas de seguridad para proteger la integridad y confidencialidad de la información.

Se adoptarán mejores prácticas internacionales y directrices institucionales para asegurar la accesibilidad y conservación a largo plazo.

¿Dónde o en cuál repositorio?
[Garantizar el depósito oportuno de los datos de investigación en las plataformas alineadas a la Ley 31250 y la Ley 30035, que cumplan con las características técnicas y normativas para tales fines.]

En repositorios que cumplan con la Ley 31250 y la Ley 30035:
1. RENARE: para almacenamiento a nivel nacional.
2. Repositorio institucional: IEP.
3. Almacenamiento en la nube: Infraestructura certificada para datos con restricciones de acceso.

9. Compartir los datos de investigación

¿Cómo se enterarán los potenciales usuarios de la disponibilidad de los conjuntos de datos?
[La visibilidad de los conjuntos de datos es crucial para fomentar su reutilización y maximizar su impacto. Explique qué estrategias, herramientas y/o plataformas disponibles aplicará para tales fines. Al hacer que tus datos sean fácilmente describibles y accesibles, estarás contribuyendo al avance de la ciencia y la innovación.]

Para ello se establecerá la siguiente ruta:

1. Estrategias:
- Difusión en repositorios: Los datos primarios serán depositados en RENARE y repositorios institucionales para asegurar su acceso.
- Promoción en publicaciones: Referenciados en artículos científicos con identificadores persistentes (DOI).
- Colaboración científica: Divulgados en redes académicas y foros especializados.

2. Herramientas:
- Identificadores persistentes: DOI y Handle para garantizar trazabilidad.
- Documentación: Archivos README y metadatos para describir contenido y metodología.
- Políticas de acceso: Uso de licencias abiertas (ejem., Creative Commons).

3. Plataformas disponibles:
- Repositorios nacionales: RENARE para acceso y preservación.
- Redes científicas: Publicación en ResearchGate y otros espacios colaborativos.

¿Con quién compartirá los datos y bajo qué condiciones?
[Tome en cuenta las implicaciones éticas, legales y sociales en su justificación. Considere el uso de licencias de uso, compatibles con el acceso abierto.]

Con la comunidad científica, instituciones académicas, organismos gubernamentales y el público en general, siempre que su difusión no comprometa la privacidad, confidencialidad o integridad de los sujetos involucrados. Se priorizará el acceso abierto, garantizando un equilibrio entre la transparencia y la protección de la información.

Condiciones de uso:
1. Licencia Creative Commons (CC BY 4.0): Permitirá la reutilización de los datos con atribución adecuada a los autores originales, fomentando el acceso abierto y la colaboración científica.

2. Acceso restringido en casos específicos: Datos sensibles o sujetos a acuerdos contractuales requerirán permisos especiales, garantizando que su uso se ajuste a los términos establecidos por la institución. 3. Uso ético y legal: Se exigirá que los usuarios acepten condiciones que prohíban la manipulación indebida de los datos y respeten los principios éticos de investigación. 4. Autorización para reutilización académica y de innovación: Se permitirá la reutilización con fines científicos, educativos y de desarrollo tecnológico, promoviendo su impacto en futuras investigaciones. 5. Se seguirán las normativas nacionales e institucionales sobre protección de datos y acceso abierto, asegurando que el uso y la difusión de la información cumplan con los más altos estándares éticos y legales.
¿Compartirá los datos a través del repositorio, atendiendo solicitudes directas u otro mecanismo? *[Considere que la forma de compartir los datos involucra varios factores, como el tipo de datos, las políticas institucionales, las consideraciones éticas y las necesidades de los usuarios. Mencione el nombre y URL del repositorio o plataforma respectiva, la oficina y entidad que la gestiona, así como los datos de contacto.]*
Los datos serán compartidos a través de diversos mecanismos: 1. Repositorio institucional: Se almacenarán en RENARE o repositorios universitarios, asegurando disponibilidad y preservación digital. 2. Solicitudes directas: Datos con restricciones éticas o contractuales. Los investigadores enviarán una solicitud justificando su uso y aceptando las condiciones de acceso.
¿Cuándo estarán a disposición los datos? *[Considere fechas de embargo relacionadas en los datos, en caso de corresponder.]*
Desarrollo: En 10 meses aproximadamente.

10. Restricciones al compartir los datos

    Determine si los datos tienen restricciones debido a aspectos de confidencialidad, consentimiento o sensibilidad de los datos. Considere si un acuerdo de confidencialidad brindaría suficiente protección para los datos. Recuerde que el compartir datos debe garantizar el cumplimiento de los principios FAIR. (Ver https://www.go-fair.org/fair-principles)

¿Qué acciones implementará para evitar o minimizar las restricciones?
1. Anonimización de datos 2. Consentimiento informado ampliado 3. Uso de acuerdos de confidencialidad 4. Evaluación y clasificación de sensibilidad 5. Seguridad en el almacenamiento.
¿Por cuánto tiempo necesitará un uso exclusivo de los datos y por qué?
- Datos cuantitativos (encuestas): 12 meses para verificar su validez luego de trascurrido el tiempo de publicación de resultados. - Datos cualitativos (narrativas): 12 meses debido a la complejidad de la anonimización, codificación y análisis.
¿Se necesitarán acuerdos de algún tipo para compartir los datos?
Sí, los siguientes: 1. Acuerdos de uso de datos anonimizados (en mi alcance):

Los datos anonimizados serán compartidos bajo licencias abiertas como Creative Commons, asegurando condiciones claras, como atribución adecuada y prohibición de usos comerciales. Se incluirá una cláusula para prevenir intentos de reidentificación de los participantes.

2. Acuerdos de confidencialidad (requeriré su implementación):
En casos donde los datos no puedan ser completamente anonimizados (ejem., narrativas sensibles), solicitaremos que las instancias correspondientes implementen acuerdos de confidencialidad para regular el acceso y uso exclusivo a los fines declarados. Estos acuerdos deberán ser firmados por usuarios externos antes de acceder a los datos restringidos.

3. Acuerdos institucionales (en coordinación con otras instancias):
Solicitaremos a la institución que gestione convenios con entidades externas interesadas en los datos, garantizando que estas cumplan con normativas éticas y legales, y que manejen los datos de forma segura. Estos convenios asegurarán la protección de los derechos de los participantes y la integridad de los datos compartidos.

4. Políticas de repositorios (dependiente de las plataformas):
Al depositar los datos en repositorios como RENARE, cumpliremos con las condiciones establecidas por la plataforma. Si se requiere involucrar a departamentos técnicos o administrativos, haremos las solicitudes necesarias para garantizar el cumplimiento de los estándares.:

11. Responsabilidades y recursos

Resuelva las responsabilidades de las personas involucradas sobre el manejo de los datos y del plan de gestión de datos. Considere cualquier recurso necesario para ejecutar el plan (software, hardware, conocimientos técnicos, etc.). Cuando se necesiten recursos específicos, estos deben describirse y justificarse.

¿Quién(es) será(n) responsable(s) del manejo de los datos y cuáles serán sus responsabilidades en este manejo?
1. Investigador principal y el coinvestigador: Supervisarán la recopilación, almacenamiento y uso adecuado de los datos, asegurando que se sigan los protocolos establecidos. 2. Gestor de datos institucional: Aplicará medidas de cifrado, control de accesos y resguardo seguro de la información, minimizando riesgos de pérdida o filtración. Además, velará por la preservación y publicación en repositorios científicos, asegurando el cumplimiento de los principios FAIR. Cada responsable deberá seguir el Plan de Gestión de Datos (PGD) y cumplir con normativas éticas y legales para garantizar la transparencia y reutilización de la información.
¿Quién es la persona responsable de la implementación del plan de gestión de datos, y de garantizar su escrutinio y revisión?
El Investigador Principal (IP) junto al coinvestigador serán responsables de implementar el Plan de Gestión de Datos (PGD). Además, un gestor de datos institucional supervisará periódicamente su aplicación, garantizando la alineación con las políticas institucionales y normativas nacionales, asegurando la integridad, seguridad y disponibilidad de los datos.
¿Cómo estarán distribuidas las responsabilidades entre las diversas entidades participantes? (En el caso de proyectos con otras instituciones)
Desarrollo:

¿La propiedad de los datos y las responsabilidades para la gestión de los datos de investigación serán parte de algún convenio?

Desarrollo:

¿Qué recursos requiere para ejecutar el plan de gestión de datos?

1. Infraestructura de almacenamiento: Servidores institucionales, almacenamiento en la nube y dispositivos de respaldo físico para garantizar la seguridad y accesibilidad de los datos.
2. Software especializado: Herramientas de gestión como OpenRefine, Dataverse y DMPTool, para la organización, limpieza y preservación de datos.
3. Capacitación del equipo: Formación en estándares de metadatos, anonimización y protocolos de seguridad para asegurar el cumplimiento normativo.
4. Soporte técnico: Personal capacitado en administración de bases de datos y ciberseguridad, asegurando la correcta implementación de las estrategias de resguardo y acceso.

¿Se requiere tener adicionalmente el apoyo de especialistas, por ejemplo, para dar entrenamiento o para administrar datos científicos?

Sí, se requerirá el apoyo de los siguientes especialistas:

1. Gestión de datos científicos: Para que especialistas en manejo de información garanticen que los datos cumplan con los principios FAIR (Encontrables, Accesibles, Interoperables y Reutilizables), asegurando su correcta organización y preservación en repositorios científicos.
2. Anonimización de datos sensibles: Se requerirá apoyo técnico para aplicar métodos de anonimización y enmascaramiento de datos personales, garantizando el cumplimiento de normativas de protección de datos y confidencialidad.
3. Capacitación del equipo de investigación: Se requerirán talleres de formación en almacenamiento, respaldo, preservación digital y buenas prácticas en el manejo de datos, para mejorar las competencias del equipo en la gestión de información científica.
4. Repositorios digitales y acceso abierto: Se requerirán especialistas en metadatos y curaduría digital para proporcionar asesoría en la integración de los datos en plataformas de preservación certificadas, asegurando su disponibilidad a largo plazo.

¿Se requiere hardware o software adicional al existente en la institución?

Sí, los detallados a continuación:

- Hardware: Servidores adicionales o almacenamiento en la nube, dispositivos de respaldo cifrados (NAS, discos duros) y equipos para recolección en campo (sensores, grabadoras).
- Software: Herramientas de análisis (SPSS), bases de datos (PostgreSQL, MySQL) y plataformas de respaldo y cifrado (Veracrypt, AWS Backup).