Propuesta de organización estratégica de carpetas y protocolo de manejo de la información

Convenio CA 02-25 CPE-Fundación Shaia

Introducción 1

Propuesta de estructura estratégica de carpetas 2

Protocolo de manejo de la información 4

Principios de gestión de la información 5

Clasificación de la información del proyecto 5

Flujo de gestión de la información del proyecto 6

1. Generación o recolección de información 6
2. Registro y organización de la información 6
3. Revisión y control de versiones 6
4. Uso y circulación de la información 7
5. Conservación de la información 7
6. Archivo final del proyecto 7

Normas de uso y seguridad de la información 8

Control de acceso a la información 8

Protección de datos personales 8

Seguridad en el almacenamiento de la información 8

Uso responsable de la información 9

Gestión de incidentes de seguridad 9

Frecuencia de actualización 9

Roles y niveles de acceso 10

Responsables internos 10

Seguimiento y cumplimiento 11

Introducción

En el marco del convenio entre Fundación Shaia y Computadores para Educar, se presenta la siguiente propuesta de organización estratégica de la información del proyecto.

El objetivo es garantizar una gestión ordenada, trazable y segura de los documentos generados durante la ejecución del convenio, facilitando el seguimiento, la transparencia y los procesos de auditoría.

La propuesta incluye:

• Una estructura estratégica de carpetas organizada según los componentes del convenio.

• Un protocolo de manejo de la información que establece lineamientos de uso, seguridad, acceso y actualización de la documentación del proyecto.

La propuesta se fundamenta en los principios de confidencialidad, acceso controlado, protección de datos personales y buenas prácticas de gestión documental establecidas en la Política de tratamiento de datos personales de Computadores para Educar, en cumplimiento de la Ley 1581 de 2012.

Propuesta de estructura estratégica de carpetas

Carpeta	Subcarpeta nivel 01	SUBCARPETA siguientes niveles
Informes	Informe 1	•
	Informe 2	•
	Informe final	•
Reuniones y comités	Comités técnicos	•
	Seguimientos	•
HV y soportes equipo	Jose Rafael Espinosa	•
	Fernando Díaz del Castillo	•
	David Méndez	•

	José Luis Sánchez	●
	Auxiliar administrativo	●
	Profesionales de campo	● Magdalena ● Valle del Cauca ● Putumayo
	Nogales +	●
Componente 1	Fortalecimiento estratégico	●
	Propuestas de aprendizaje innovadoras	● Propuesta 1 ● Propuesta 2 ● Propuesta 3 ● Propuesta 4 ● Propuesta 5 ● Propuesta 5
Componente 2	0. Alistamiento y pre-arranque	● Plan operativo ● Propuesta Testbed CPE ● Actualización de la política de tratamiento y uso de datos ● Protocolo Suspensión de Actividades

	1. Diseño Conceptual del Testbed	● Marco conceptual del testbed
		  ○ Versiones previas
		  ○ Versión final
		● Matriz de dimensiones, indicadores, e instrumentos
		  ○ Versiones previas
		  ○ Versión final
		● Caja de herramientas del Testbed
		  ○ Instrumentos T0
		  ▪ Versiones previas
		  ▪ Versión final
		  ○ Instrumentos T1
		  ▪ Versión final
		  ▪ Versión final
		  ○ Instrumentos T2
		  ▪ Versión final
		  ▪ Versión final
		● Plan de monitoreo y aprendizaje del testbed

	2. Implementación del *Testbed*	• Plan de implementación del trabajo de campo • Base de datos de implementación del Testbed • Registro de hallazgos por institución y territorio
	3. Sistematización de aprendizajes	• Marco integrado de aprendizajes del testbed • Orientaciones estratégicas para ajuste y escalamiento
	4. Carpeta temporal	
Documentos transversales		

Esta propuesta no es estática y va a presentar cambios que se discutirán en las reuniones de seguimiento. Por ejemplo, en la subcarpeta "propuestas de aprendizaje innovadoras", cada subcarpeta contenida va a contener el título de la propuesta de aprendizaje o un descriptor sobre el contenido.

Las subcarpetas que más van a estar sujetas a cambios serán las del componente 2, especialmente las "2. Implementación del Testbed" y "3. Sistematización de aprendizajes". Esto porque a medida que avance el proyecto se irá ajustando el contenido y su forma de guardarlo. Para dar un ejemplo, es muy posible que la carpeta que contenga la implementación del Testbed se ajuste a contener carpetas por territorio, por institución o por herramienta. Cada uno de estos cambios serán discutidos y aprobados por ambas partes. Como paso previo a la organización de las carpetas, para la implementación de los testbeds, se va a contar con una carpeta temporal, que permita poder subir información o archivos que están aún en proceso de discusión o revisión. Una vez estos archivos sean revisados por el equipo, se organizarán en sus carpetas correspondientes.

Adicionalmente, en la carpeta documentos transversales, van a incluirse otros documentos del convenio, tales como la propuesta técnica, la minuta o este documento. Son aquellos que afectan directamente la totalidad del convenio e incluyen elementos administrativos, técnicos y financieros que no existen en las otras carpetas.

Protocolo de manejo de la información

El presente protocolo establece los lineamientos técnicos, operativos y administrativos para la gestión, almacenamiento, uso, actualización,

circulación y protección de la información generada en el marco del convenio entre Fundación Shaia y Computadores para Educar.

Su propósito es asegurar que la información producida durante la ejecución del convenio sea gestionada conforme a los principios de seguridad de la información, protección de datos personales, trazabilidad documental y acceso controlado, garantizando el cumplimiento de la normativa colombiana y las políticas institucionales de Computadores para Educar.

Este protocolo aplica a todos los documentos, registros y bases de datos generados durante el proyecto, incluyendo:

- documentos técnicos del proyecto
- informes de avance y productos contractuales
- instrumentos de recolección de información
- registros de implementación del Testbed
- bases de datos del proyecto
- documentos administrativos del equipo
- información de instituciones educativas participantes

De acuerdo con la Política de Tratamiento de Datos Personales de Computadores para Educar, cualquier información que contenga datos personales debe ser tratada garantizando la confidencialidad, seguridad y uso responsable de los datos, evitando accesos no autorizados o divulgación indebida de la información.

Principios de gestión de la información

La gestión de la información del proyecto se regirá por los siguientes principios:

- Confidencialidad: la información generada en el proyecto solo podrá ser consultada por personas autorizadas. Se deberán aplicar controles de acceso que eviten la divulgación indebida de la información.
- Integridad: la información deberá mantenerse completa, veraz y sin modificaciones no autorizadas. Los documentos oficiales deberán conservarse en las carpetas definidas dentro de la unidad compartida del proyecto.
- Disponibilidad: la información deberá permanecer disponible para los actores autorizados del proyecto, facilitando los procesos de seguimiento, monitoreo, evaluación y auditoría.

- Legalidad: el tratamiento de datos personales deberá cumplir con la Ley 1581 de 2012, el Decreto 1377 de 2013 y las políticas institucionales de Computadores para Educar.
- Minimización de datos: solo se recolectarán los datos estrictamente necesarios para el desarrollo de las actividades del proyecto.
- Responsabilidad en el tratamiento de la información: los integrantes del equipo del proyecto deberán garantizar el uso adecuado y responsable de la información a la que tengan acceso.

Clasificación de la información del proyecto

Con el fin de fortalecer la gestión y protección de la información, se establece la siguiente clasificación:

Tipo de información	Descripción	Ejemplos
Información pública	Información que puede ser divulgada sin restricciones	informes finales publicados, productos de conocimiento aprobados por CPE como tales
Información de uso interno	Información utilizada para la gestión del proyecto que no requiere difusión pública	actas de reunión, documentos de trabajo, informes preliminares
Información restringida	Información que contiene datos personales o información sensible del proyecto	bases de datos del Testbed, información de participantes, registros institucionales

La información clasificada como restringida deberá contar con controles adicionales de acceso y protección.

Flujo de gestión de la información del proyecto

La gestión de la información del proyecto seguirá el siguiente flujo:

1. Generación o recolección de información

La información del proyecto podrá generarse mediante:

- elaboración de documentos técnicos
- desarrollo de instrumentos de investigación o monitoreo
- registro de actividades de campo
- recolección de información institucional o educativa

En caso de recolectarse datos personales, se deberá garantizar que el tratamiento de los datos tenga una finalidad legítima asociada al proyecto. Este protocolo de recolección de datos será acordado entre las partes en las siguientes reuniones de seguimiento y antes de ir a campo.

2. Registro y organización de la información

Una vez generada, la información deberá ser almacenada en la unidad compartida del proyecto, siguiendo la estructura de carpetas establecida anteriormente.

Los documentos deberán:

- ubicarse en la carpeta correspondiente
- mantener un nombre claro que permita identificar su contenido
- incluir versión o fecha cuando corresponda

3. Revisión y control de versiones

Los documentos técnicos del proyecto deberán pasar por procesos de revisión interna antes de considerarse versiones finales.

Para ello se utilizarán las carpetas “versiones previas” y “Versión final” en caso de los testbeds y en para el componente 1, los archivos contendran la fecha y número de versión en caso de ser necesario.

Esto permite garantizar trazabilidad documental y control de cambios.

4. Uso y circulación de la información

La información del proyecto podrá ser utilizada para:

- desarrollo de actividades técnicas del convenio
- elaboración de informes contractuales
- análisis de resultados del Testbed
- monitoreo y evaluación del proyecto
- auditorías institucionales

La circulación de documentos deberá realizarse a través de canales institucionales autorizados.

5. Conservación de la información

La información deberá conservarse durante la ejecución del proyecto y el periodo requerido para procesos de cierre contractual, auditoría o verificación institucional según el covenio y las leyes que apliquen. En todo caso, la Fundación Shaia hará entrega de la carpeta compartida y perderá el acceso a

la misma en cuanto se acabe el proyecto. En caso que haya documentación adicional para productos de conocimiento, esto quedará establecido por decisión del comité técnico.

6. Archivo final del proyecto

Al finalizar el convenio se consolidará un archivo final organizado, que incluirá:

- informes finales
- productos del convenio
- documentación metodológica
- registros de implementación
- bases de datos consolidadas

Este archivo servirá como soporte institucional del proyecto.

Normas de uso y seguridad de la información

Las normas de uso y seguridad buscan garantizar la adecuada protección de la información generada en el proyecto y evitar riesgos asociados a pérdida, divulgación indebida o acceso no autorizado.

Estas normas se basan en:

- la Política de tratamiento de datos personales de computadores para educar
- la legislación colombiana en materia de protección de datos personales
- estándares internacionales de seguridad de la información.

Control de acceso a la información

El acceso a la información se regirá por el principio de acceso mínimo necesario, según el cual cada usuario solo podrá acceder a la información requerida para el cumplimiento de sus funciones.

Los accesos serán asignados conforme a los roles definidos en el proyecto y deberán ser administrados por el responsable del proyecto.

Protección de datos personales

Cuando la información del proyecto incluya datos personales, se deberán aplicar las siguientes medidas:

- restringir el acceso a las bases de datos que contengan información personal
- utilizar los datos exclusivamente para los fines del proyecto
- evitar la divulgación no autorizada de información personal
- anonimizar o eliminar los datos cuando ya no sean necesarios para el proyecto

Estas medidas buscan proteger los derechos de los titulares de los datos, incluyendo el derecho a conocer, actualizar y rectificar su información personal.

Seguridad en el almacenamiento de la información

La información del proyecto se almacenará en la plataforma establecida por CPE que permite garantizar su protección mediante:

- control de accesos
- uso de contraseñas seguras
- respaldo periódico de la información
- monitoreo del acceso a documentos sensibles

Estas medidas buscan evitar la pérdida, alteración o divulgación indebida de la información.

Uso responsable de la información

Las personas con acceso a la información del proyecto deberán:

- utilizar la información únicamente para fines relacionados con el convenio
- evitar compartir documentos con terceros sin autorización
- respetar la confidencialidad de la información institucional
- proteger los documentos frente a accesos indebidos

El incumplimiento de estas normas podrá generar restricciones de acceso a la información del proyecto.

Gestión de incidentes de seguridad

En caso de identificarse incidentes de seguridad de la información, tales como:

- pérdida de documentos
- acceso no autorizado a bases de datos
- divulgación indebida de información
- modificación no autorizada de archivos

se deberá informar inmediatamente al supervisor del convenio para activar las medidas de control y mitigación correspondientes según protocolos internos de CPE.

Frecuencia de actualización

La actualización de la información de la unidad compartida se realizará al menos una vez a la semana.

Cada semana se deberá:

• Cargar los documentos generados durante la ejecución del proyecto.

• Actualizar versiones de documentos en desarrollo.

• Archivar las versiones finales en las carpetas correspondientes.

Este proceso permitirá garantizar la trazabilidad y el seguimiento permanente del proyecto.

Roles y niveles de acceso

El acceso será únicamente por la cuenta y contraseña entregada por CPE, la cual funcionará como un acceso común a todo el equipo. Sin embargo, para transparencia de quién tendría el acceso completo a las carpetas, habrán dos niveles: el editor y el lector.

Los editores tendrán el usuario y la contraseña proveídos por CPE, y serán los únicos que tengan esa información. Al tener ese rol de editor, con control sobre usuario y contraseña, se le dará un acceso restringido, a ciertos correos siempre institucionales, a algunas personas del equipo. Esto permitirá una mayor eficiencia para el caso de miembros del equipo, como los enlaces, que puedan cargar información cuando sea necesario, y que puedan ver los archivos, pero que no puedan ni borrar, ni editar ninguno de ellos.

Los accesos a la unidad compartida estarán definidos según los siguientes roles:

- Gerente del proyecto – Fundación Shaia; Nivel de acceso: Editor
- Auxiliar administrativo – Fundación Shaia; Nivel de acceso: Editor
- Líder delegado de Nogales +; Nivel de acceso: Editor
- Especialista en innovación educativa – Fundación Shaia; Nivel de acceso: Restringido
- Enlaces territoriales: Restringido

Definición de niveles:

Editor

• Crear documentos

• Editar documentos

• Organizar carpetas

• Actualizar información

Restringido

• Consultar documentos

• Descargar archivos

• Cargar archivos

• No modificar ni eliminar información

Responsables internos

Los responsables del manejo y organización de la información serán:

Gerente del proyecto – Fundación Shaia

Responsable de supervisar la organización de la unidad compartida, garantizar el cumplimiento del protocolo y autorizar accesos a la información.

Auxiliar administrativo

Responsable de apoyar la organización de los documentos técnicos y pedagógicos del proyecto, así como de verificar la consistencia de la documentación y la facilidad en su lectura según títulos y descriptores.

Seguimiento y cumplimiento

El cumplimiento de este protocolo se verificará mediante:

• Revisión periódica de la organización de carpetas.

• Verificación de la actualización semanal de la información.

• Control de accesos a la unidad compartida.

Estas acciones permitirán garantizar una adecuada gestión documental del convenio.