GESTIÓN RESPONSABLE DE LOS DATOS DURANTE TODO EL PROCESO

OXFAM

¿QUÉ ES LA GESTIÓN RESPONSABLE DE DATOS?

Este documento sirve de orientación para todas las personas que vayan a gestionar, compartir o acceder a datos de programas sobre distintas cuestiones de gestión responsable que surjan a lo largo del **ciclo de vida de los datos**.

Se centra principalmente en la gestión responsable de los datos en crisis humanitarias, desde la perspectiva de su recogida. No obstante, los principios, herramientas y enfoques se pueden aplicar en otros ámbitos.

La gestión responsable de datos se basa en tratar con respeto la información que recogemos y defender los derechos de las personas que la proporcionan. Estos datos pueden ser respuestas a encuestas, información de registro, fotografías, historias, etc.

La gestión responsable de los datos no tiene por qué ser restrictiva. Al contrario, puede fortalecer y facilitar la contribución que estos datos aportan a la hora de realizar un trabajo de calidad. Debe considerarse como un marco para asegurar que las personas que recogen los datos son responsables, rinden cuentas y trasmiten el mensaje de la población afectada.

El marco reglamentario (leyes y otras normas) sobre la gestión de datos se encuentra en constante cambio, al igual que la tecnología de recogida y gestión de la información. Por lo tanto, la gestión responsable de datos es un proceso en constante evolución a través del que se decide en qué momento y de qué manera se recogerán dichos datos y cuáles serán las pautas de gestión de riesgos.

1 ELABORE UN PLAN

Defina claramente el propósito de la recogida de los datos.

Los beneficios que espera de los datos deben ser proporcionales a los riesgos. Debe guiarse por los intereses y el bienestar de la población afectada.

Evalúe los métodos y las herramientas disponibles para encontrar aquellos que se adecuen al contexto y su propósito.

Reduzca al máximo las preguntas y compruebe de manera rigurosa si realmente son imprescindibles. Compruebe que la información no esté ya disponible en ninguna fuente fiable.

Decida si necesita realizar una **evaluación de impacto sobre la intimidad y la protección de datos**.

Los datos personales son muy sensibles y requieren la adopción de medidas de protección especiales, como almacenarlos de manera independiente (sin incluir las respuestas de las personas encuestadas), o incluir esta información de manera **anónima**.

Piense desde el principio en cómo se asegurará de conseguir un **consentimiento realmente informado**. Explique claramente qué es el consentimiento e informe a las comunidades del destino de esos datos.

Compruebe si existen riesgos de parcialidad en su enfoque y metodología. Reflexione sobre cómo comprobará que sus datos sean correctos.

2 EVALÚE LOS RIESGOS

La recogida de datos puede poner en riesgo a las personas que los facilitan. Evalúe los riesgos y tome medidas para evitar cualquier consecuencia negativa a las personas encuestadas (p.ej.: garantizando la seguridad y la confidencialidad de los datos).

Pida consejo a expertos técnicos acerca de los riesgos específicos y reflexione sobre las pautas que seguirá si surge algún problema o **se filtran los datos.**

3 FORME A LOS ENCUESTADORES/AS

Las formaciones para las personas que van a recoger los datos deberán incluir:

- Aspectos a tener en cuenta para la gestión responsable de los datos.
- El proceso de consentimiento: aquello que las personas que proporcionan la información deben saber sobre el uso que se le dará.
- Casos reales para hacer que la formación sobre sistemas y protocolos sea lo más real posible.

4 ASEGÚRESE DE QUE DISPONE DE CONSENTIMIENTO INFORMADO

Otorgar consentimiento no se reduce a marcar una casilla sino que se basa en tratar con dignidad y respeto a las personas que proporcionan los

datos y garantizar que se respetan los requisitos legales sobre datos personales.

Explique a estas personas cómo utilizará sus datos y la razón por la que los necesita. ¿Cómo los almacenará? ¿Con quién los compartirá? ¿Cómo se asegurará de que estos terceros no los comparten con otros agentes? ¿Qué sucede si las personas que proporcionan los datos cambian de idea sobre su consentimiento? ¿Cómo pueden ponerse en contacto con usted?

Pregúnteles si desean recibir información sobre el uso que se ha dado a los datos, y cómo desean recibirla.

Ofrézcales la oportunidad de revocar su consentimiento y elabore un «plan B» que recoja este caso.

5 GESTIÓN DE DATOS

TRANSFERENCIA

Utilice dispositivos portátiles y tecnologías de uso compartido con prudencia. **Cifre** los datos cuando corresponda y establezca sistemas que permitan eliminar a distancia los datos de los teléfonos.

En caso de que esté utilizando documentos impresos, transpórtelos con cuidado cuando esté en el terreno. Cifre los archivos digitales en el punto de entrada de datos.

ACCESO

Establezca cuentas individuales con contraseñas de usuario para garantizar los derechos de acceso a las fuentes de datos digitales. Establezca el acceso en función de los contenidos que necesite cada usuario.

Cada persona que recoja o utilice los datos es responsable de su gestión. Una posibilidad consiste en hacer responsable de la protección de los datos a un miembro del equipo y garantizar que el resto comprenda su función y la rendición de cuentas.

ALMACENAMIENTO

Investigue detenidamente la seguridad de los datos, la ubicación del almacenamiento en la nube y las opciones de la base de datos.

Reflexione sobre opciones seguras de almacenamiento para aquellos datos en formato impreso. De ser posible, guárdelos en una caja fuerte o en un armario bajo llave.

INTERCAMBIO/PUBLICACIÓN

Establezca un **acuerdo de intercambio de datos** con las organizaciones con las que vaya a compartirlos; incluya también una guía de gestión de datos. Solicite asesoramiento jurídico de ser necesario.

Estos principios se aplicarán independientemente de cuál sea la identidad de la tercera parte: un Gobierno, otra ONG, una empresa privada, una entidad bancaria, etc.

No comparta ningún dato si no cuenta con el consentimiento de las personas que los proporcionaron.

Algunas organizaciones comparten o publican los datos. Solicite asesoramiento especializado y analice los riesgos y sensibilidades antes de compartir cualquier **conjunto de datos**. No basta con eliminar los nombres para ocultar la identidad de las personas.

6 DESTINO DE LOS DATOS

Pueden utilizarse para fines de lobby, incidencia política o para realizar ajustes a programas.

Piense en las personas que representan los datos. ¿Existe un equilibrio de género?

Según los datos, ¿hay algún sesgo en esta decisión?

7 PROPIEDAD Y FEEDBACK

¿Cómo puede promover que las personas se sientan propietarias de los datos que han proporcionado?

Reúnase con ellas para validar los resultados y asegurarse de que estos representan su opinión en la medida de lo posible. Infórmeles del uso que se dará a los datos.

8 CONSERVACIÓN/ELIMINACIÓN/ ARCHIVO DE DATOS

Decida con antelación durante cuánto tiempo necesitará disponer de los datos. Recuerde que estos pierden relevancia con mucha rapidez.

Eliminar un documento en formato digital no es igual que quemar o destruir uno en papel, ya que pueden quedar copias en su computadora. (p.ej.: carpetas de descarga, archivos, etc.; lo que se conoce como registros digitales).

DEFINICIONES

De manera anónima: en teoría, se refiere a procesos para dificultar o hacer que sea imposible identificar a una persona concreta a partir de un conjunto de datos. En la práctica, a menudo es posible reagrupar distintas informaciones para revelar identidades.

Filtración de datos: divulgación intencionada o accidental de información en un entorno no fiable.

Proceso de gestión de datos: flujo de información a través de un sistema, desde su creación a su eliminación, pasando por el almacenamiento.

Conjunto de datos: agrupación de datos relacionados entre sí.

Acuerdo de intercambio de datos: marco para el intercambio de datos que establece cómo se transmitirán, almacenarán y utilizarán los datos.

Cifrado: conversión de datos a un formato en el que no puedan ser leídos con facilidad por personas no autorizadas.

Consentimiento informado: acuerdo que se proporciona de manera libre y voluntaria y se basa en el reconocimiento y la comprensión de los hechos, implicaciones y futuras consecuencias de una acción. Las personas deben ser conscientes de su derecho a negar su consentimiento y ser capaces de ejercerlo. Existen situaciones en las que no es posible obtener el consentimiento informado, como en el caso de los menores o personas discapacitadas.

Datos personales: información que puede utilizarse, por sí sola o junto a otra información, para identificar a una persona concreta.

Evaluación de impacto sobre la intimidad: herramienta para identificar y reducir riesgos para la intimidad.

Para más información, puede consultar:
www.oxfam.org.uk/responsibledata

GESTIÓN RESPONSABLE DEL CICLO DE LOS DATOS