PIM Protection Information Management

Principios de la Gestión de Información de Protección (PIM)[1]

Basándose en la definición acordada de la Gestión de Información de Protección (PIM), los participantes debatieron en profundidad para desarrollar los siguientes principios centrales y orientadores cuando se realizan acciones de PIM – principios que se construyen sobre discusiones y foros inter-agenciales previos. Estos principios subyacen y caracterizan todos los sistemas de PIM, independientemente de sus propósitos, métodos o productos[2].

Centralidad en las personas e inclusión: las actividades de datos e información deben guiarse por los intereses, el bienestar y los derechos de la población afectada y la comunidad de acogida, quienes deben participar y ser incluidos en todas las fases pertinentes.

Evitar acciones con daño: las actividades de datos e información deben incluir una evaluación de riesgos y toma de medidas para mitigar los riesgos identificados, si es necesario. La evaluación de riesgos debe tener en cuenta las consecuencias negativas que puedan derivarse de la recopilación de datos y las acciones posteriores o la prestación de servicios durante el tiempo que se lleve a cabo la actividad de datos e información.

Propósito definido: dado el carácter sensible y a menudo personal de la información de protección, los datos y las actividades de información deben satisfacer necesidades y propósitos específicos. El objetivo debe estar claramente definido y comunicado, además de ser proporcional tanto al riesgo identificado como a los costos frente a la respuesta esperada, y estar dirigido a la acción para lograr resultados de protección, incluyendo el intercambio y coordinación de los datos y la información de protección.

Consentimiento informado y confidencialidad: la información personal puede recopilarse solo después de que la persona en cuestión haya proporcionado su consentimiento informado, y esa persona debe estar consciente del propósito de la recopilación. Además, la confidencialidad debe explicarse claramente a la persona antes de que se pueda recopilar la información.

Responsabilidad, protección y seguridad de los datos: la responsabilidad de los datos va más allá de la privacidad y la protección de los datos. Implica un conjunto de principios, propósitos[3] y procesos que buscan guiar el trabajo humanitario y aprovechar los datos para mejorar las vidas de las poblaciones afectadas y la de las comunidades de acogida de manera responsable, al mismo tiempo que se adhieren a las normas internacionales de protección y seguridad de datos. Las actividades de recolección de datos e información deben cumplir con el derecho internacional[4] y las normas de protección y seguridad de

[1] Desarrollados por los participantes en la Primera Reunión de Trabajo de PIM llevada a cabo en Copenhague entre el 26-29 de mayo de 2015. Los principios PIM tienen en consideración los 'Principios de la Gestión e Intercambio de Información Humanitaria', promocionados por el Simposio Global +5 en Ginebra (2007) y la 'Normativa profesional relativa a la labor de protección, Gestión de datos sensibles de protección', Capítulo 6 (2013).

[2] Para conocer cómo operacionalizar estos principios, diríjase a la página web de PIM: http://pim.guide/

[3] Basado en parte en el trabajo de OCHA '*Building Data Responsibility into Humanitarian Action, OCHA Policy and Studies Series*, mayo 2016; p. 4.

[4] Incluyendo las 'Directrices para la regulación de los archivos de datos personales informatizados' de la Asamblea General de las Naciones Unidas de 1990.

los datos. Las personas tienen derecho a que sus datos sean protegidos de acuerdo con las normas internacionales de protección de datos.

Competencia y capacidad: los actores que participan en actividades de recolección de datos e información son responsables de garantizar que las actividades de recopilación de datos e información sean llevadas a cabo por personal de protección y gestión de la información que haya sido equipado con las competencias básicas de recopilación de datos e información y que haya recibido una formación adecuada.

Imparcialidad: todos los pasos del ciclo de datos e información deben llevarse a cabo de manera objetiva, imparcial y transparente, al mismo tiempo que se identifican y minimizan los sesgos.

Coordinación y colaboración: todos los actores que ejecutan actividades de datos e información deben adherirse a los principios mencionados anteriormente y promover la más amplia colaboración y coordinación de las actividades relacionadas a la gestión de datos e información, internamente entre los actores humanitarios y externamente con y entre otras partes interesadas. En la medida de lo posible, las actividades de datos e información deben evitar la duplicación de otras actividades de datos e información y, en su lugar, se deberán aprovechar los esfuerzos y mecanismos existentes.