MARCO PARA EL INTERCAMBIO DE DATOS EN LA PRÁCTICA

PIM Protection Information Management
For Quality Protection Outcomes

MARCO PARA EL INTERCAMBIO DE DATOS EN LA PRÁCTICA

A. Declaración de confianza

Existe una responsabilidad ética para quienes tengan información y datos de compartirlos de una forma segura y útil con otros actores que estén en la posición o tengan la responsabilidad de responder a las problemáticas planteadas.

Un entorno de confianza y las maneras en las que la confianza se puede crear, mantener y fortalecer, requiere trabajar con un espíritu y una práctica de confianza, con al menos un mínimo enfoque compartido para asegurar las buenas prácticas. Este enfoque se describe en los elementos del ***Marco***.

La declaración de confianza será un documento entre dos partes en el cual se pondrán de acuerdo como indicación de su compromiso con el ***Marco*** al compartir datos. La declaración también puede extenderse a los donantes, quienes tienen la responsabilidad y la influencia para facilitar el intercambio de datos y la cooperación entre las partes interesadas.

Declaración de confianza:

Reconocemos los beneficios de compartir datos en una manera responsable, segura y con un propósito definido para mejorar las respuestas que promueven la seguridad, la dignidad, los derechos y capacidades de las poblaciones afectadas.

Entendemos los riesgos de compartir y de no compartir, y nos comprometemos a compartir y recibir los datos y la información según los principios humanitarios y en línea con los principios de protección y de gestión de la información [PIM] y las respectivas políticas organizaciones.

Con el Marco para el Intercambio de Datos en la Práctica, contribuiremos a crear un entorno que fortalezca la coordinación y la colaboración dentro y fuera de la comunidad humanitaria para el intercambio de datos.

Si se presenta una ruptura de la confianza establecida bajo el ***Marco,*** los actores de interés involucrados deberán entender el porqué de la ruptura y sus implicaciones según el ***Marco.*** El ***Marco*** podría ser renegociado según los detalles de dichos términos, o podría dejar de existir entre las contrapartes.

B. Principios PIM

Esta sección resume los mínimos principios compartidos que subyacen y caracterizan el manejo, intercambio y uso responsable de los datos y la información, independientemente de sus propósitos, métodos o resultados (productos) específicos.

- **Centrado en las personas e inclusivo:** las actividades de información y datos se deben guiar por los intereses, el bienestar y los derechos de la población afectada y sus comunidades de acogida, quienes deben participar y ser incluidas en todas las fases pertinentes. Las actividades deben incluir una perspectiva de edad, género y otros aspectos de la diversidad.

- **No hacer daño:** las actividades de información y datos deben incluir una evaluación de riesgos y tomar medidas, si es necesario, para mitigar los riesgos identificados. La evaluación de riesgos debe considerar las consecuencias negativas que puedan derivarse de la recopilación de datos y las subsecuentes acciones o la prestación de servicios durante todo el tiempo en que se realice la actividad de gestión datos e información.

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

- **Consentimiento informado y confidencialidad:** la información personal puede recopilarse únicamente después de que la persona en cuestión haya proporcionado su consentimiento informado, y dicha persona debe tener conocimiento del propósito de la recopilación. Además, la confidencialidad debe explicarse claramente a la persona antes de que se pueda recopilar la información

- **Responsabilidad de los datos, protección y seguridad:** La responsabilidad por los datos va más allá de la privacidad y la protección de datos. Implica un conjunto de principios, propósitos[4] y procesos que buscan guiar el trabajo humanitario y aprovechar los datos para mejorar la vida de las poblaciones afectadas y las comunidades de acogida de manera responsable. Al mismo tiempo que se adhiere a las normas internacionales de protección y seguridad de datos. Las actividades de datos e información deben cumplir con el derecho internacional y las normas de protección y seguridad de datos. Las personas involucradas 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 gestión de datos e información son responsables de garantizar que las actividades de gestión de datos e información sean llevadas a cabo por personal de gestión y protección de la información que cuente con las competencias básicas de datos e información y que haya recibido una formación adecuada.

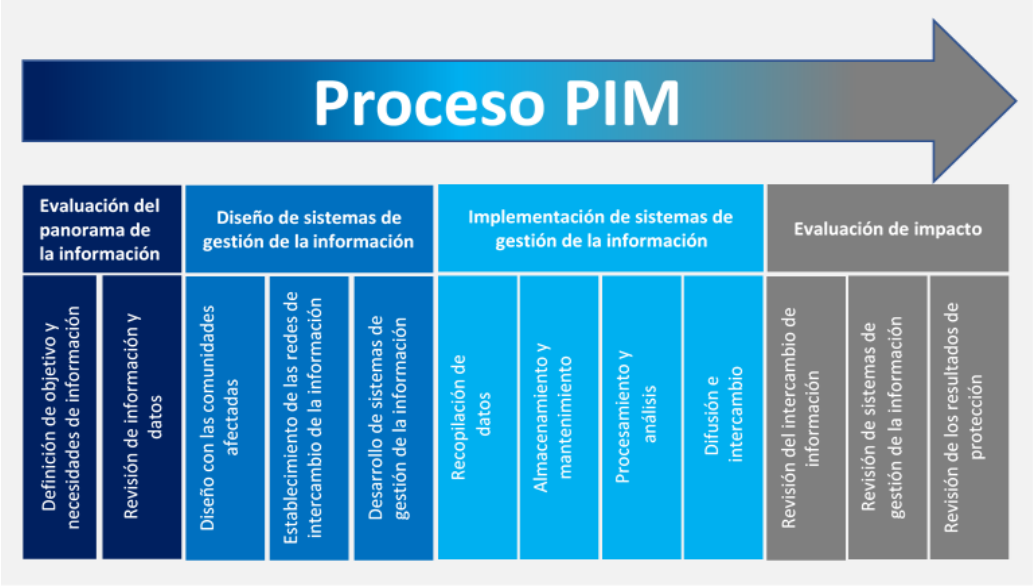
- **Imparcialidad:** todos los pasos del ciclo de datos e información deben realizarse de manera objetiva, imparcial y transparente, al tiempo que se identifican y minimizan sesgos.

- **Coordinación y colaboración:** todos los actores que implementan actividades de información y datos deben adherirse a los Principios PIM y promover la más amplia colaboración y coordinación entre los agentes humanitarios y, externamente, con y entre otros interesados. 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, construir sobre los esfuerzos y mecanismos existentes.

C. Proceso para la gestión de datos

[4] Basado parcialmente en el trabajo de OCHA Building Data Responsibility into Humanitarian Action, OCHA Policy and Studies Series. Mayo 2016 pp. 4.

Un entorno que conduzca al intercambio de datos requiere de procesos compartidos y comúnmente entendidos para la gestión de datos, ofreciendo una orientación clara sobre los pasos necesarios que fomenten las buenas prácticas.



Puede encontrar orientación adicional sobre el proceso compartido para la gestión de datos **aquí**.

Mapeo y entendimiento del ecosistema de datos según el contexto

Al comenzar el mapeo de los datos, información y análisis disponibles, es importante entender el panorama de sistemas de datos y gestión de la información[5]. En un primer paso, identifique los actores clave y los sistemas de información de datos:

- ¿Quién tiene qué información y datos?
- ¿Qué sistemas están en operación, dónde y por quién?
- ¿Qué tipos de datos, información y análisis están produciendo estos sistemas o son capaces de producirlos?

Recomendamos mapear los sistemas, las partes interesadas y los niveles y tipos de datos producidos siguiendo las categorías de la Matriz PIM[6], ya que esto puede ayudar a comprender cómo interactúan los sistemas y la información, qué datos se están generando, y cómo se utilizan los datos o la información.

D. Competencias básicas

Para procesar los datos de forma segura y responsable, los profesionales que comparten y reciben datos para la respuesta humanitaria requieren un conjunto de habilidades y conocimiento, combinados con la actitud correcta y la mentalidad para facilitar un uso y manejo de los datos e información seguro, responsable y con un propósito definido. Las competencias mínimas relevantes se encuentran **disponibles aquí**.

E. Evaluación conjunta de beneficios y riesgos

El objetivo de una evaluación conjunta de beneficios y riesgos es asegurar que los beneficios y riesgos del intercambio de información se hayan evaluado de manera sistemática y colaborativa, y que se hayan identificado las acciones para maximizar los beneficios y reducir los riesgos.

Es crucial que la evaluación ***se realice de forma conjunta*** para identificar todos los aspectos de

[5] La Matriz PIM se puede utilizar para evaluar, organizar y entender el panorama de la información. La guía de la Matriz PIM disponible aquí.

[6] La Matriz PIM está disponible para descargas aquí.

la ecuación de Beneficios y Riesgos. Un entendimiento más amplio puede informar las condiciones del intercambio de datos, lo que incluye informar los medios, modalidades y frecuencia de un acuerdo específico de intercambio de datos.

Las **Preguntas** clave y **acciones** clave, junto con la debida orientación, se describen a continuación. Las preguntas tienen la intención de guiar la identificación y evaluación conjuntas de los beneficios y riesgos y los pasos respectivos en un escenario dado de intercambio de datos. A esto le sigue una lista de medidas propuestas que se pueden tomar para maximizar los beneficios y reducir los riesgos.

Estas preguntas y acciones son indicativas en lugar de prescriptivas, y algunas preguntas o medidas adicionales pueden ser necesarias o relevantes dependiendo del contexto. Se invita a los colegas a que revisen y adapten las preguntas modelo y las acciones de acuerdo con sus necesidades.

E.1. PASO1 Evalúe el panorama de información desde una perspectiva del intercambio de datos

P1. ¿Qué necesitamos saber? ¿El propósito de compartir información beneficia la seguridad y la dignidad de las poblaciones afectadas? ¿Es crucial? ¿Cuáles son los impactos negativos o los daños potenciales de no compartir los datos?

→ **QUÉ HACER: Defina el propósito y los resultados potenciales del ejercicio de intercambio de datos**

- Identifique los objetivos específicos de protección (propósito) y las actividades que se informarán por los datos o la información compartida, y cómo las organizaciones con las que se compartirá la información van a utilizarla.
- Acuerde los beneficios esperados del ejercicio de intercambio y las alternativas e impactos potenciales de no compartir.
- Acuerde los impactos negativos potenciales de compartir: p. ej. identifique los riesgos para las personas o para los colegas, y los asuntos legales y éticos relacionados con el intercambio de datos.
- Considere el marco legal nacional para cualquier obligación de compartir información dentro del proceso de evaluación del riesgo, así como los riesgos potenciales que el marco legal nacional puede acarrear para los sujetos que proveen sus datos.

→ **QUÉ HACER: Articular las razones para compartir**

- Identifique y documente el razonamiento detrás del intercambio al contestar las siguientes preguntas:
  - ¿Cuál es la naturaleza del intercambio? – ¿Se recopilan los datos para diversos propósitos o se comparten los datos para un nuevo propósito? ¿Están compartiendo los datos a través de un proceso colaborativo y con un propósito definido, o recolectaron los datos, pero tienen propósitos diferentes? ¿El intercambio está pensado para construir sobre datos ya existentes?
  - ¿Los usos planeados y los propósitos definidos para los cuales se recopilaron los datos o la información son compatibles? ¿El uso planeado es compatible con los principios compartidos?

P2. ¿Cómo podemos maximizar los beneficios de los datos (y su recopilación) y el intercambio de estos dentro y fuera del sector humanitario?

→ **QUÉ HACER: Trabajar con las partes interesadas dentro del contexto de un marco de confianza**

- Consulte a los socios para identificar oportunidades de colaboración e intercambio de datos. Esto ayudará a evitar la duplicación de esfuerzos de recopilación de datos, así como las cargas innecesarias y los riesgos para los sujetos que proveen sus datos.
- Evalúe los riesgos y beneficios de involucrar diferentes partes interesadas en la red de intercambio de datos e información, según el propósito definido y los mandatos organizacionales.
    - Las diferentes partes interesadas necesitarán acceso a los distintos niveles de detalles y tipos de información, dependiendo del propósito definido y del riesgo.
- Considere las motivaciones para compartir con el fin de organizar los tipos de colaboradores de datos y sus respectivas motivaciones[7]. Mapee las partes interesadas desde una perspectiva de intercambio de datos. Para la comunidad humanitaria, las principales motivaciones para compartir son: la programación, respuesta e incidencia.
- Asegure que los datos o la información que se van a compartir y procesar estén alineados con los principios articulados en este *Marco.* Evite utilizar o compartir datos que no se hayan recopilado, procesado o utilizado de acuerdo con los procedimientos fundamentales de protección de datos.

[7] Basado parcialmente en el trabajo de GovLab en esta área, disponible en: **http://datacollaboratives.org/**; consultado el 25 de octubre de 2017.

P3. ¿Los actores que recopilan y reciben datos demuestran las competencias clave requeridas y el respeto de los mínimos principios y procesos requeridos? ¿Los usuarios de los datos o la información demuestran un entendimiento de los estándares relevantes (Principios PIM), los procedimientos y las políticas?

→ **QUÉ HACER: Entender las habilidades y capacidades**

- Confirme que ambas organizaciones tengan protocolos de intercambio de datos o apoyen el *Marco,* según se describe en este documento.
- Identifique las políticas y guías relevantes de protección de datos. La mayoría de las organizaciones deben tener dichas políticas y prácticas, las cuales abordan la protección de datos, la seguridad y las violaciones.
- Asegure que los roles de los socios reflejen la experticia técnica, la habilidad y la voluntad de manejar y utilizar los datos de manera competente, incluyendo a los supervisores y encuestadores.

ACCIONES: Maximizar *Pasos mínimos para maximizar los beneficios*	ACCIONES: Mitigar *Pasos mínimos para mitigar los riesgos*
• Promueva la colaboración y coordine transparentemente con las partes interesadas (incluyendo poblaciones afectadas) sobre las necesidades de recolección de datos, áreas de intervención, metodologías de recopilación de datos, intercambio para extender la cobertura geográfica, reducir la duplicación, maximizar el uso y el análisis conjunto. • Busque más allá de los socios actuales para evaluar si hay otros actores o beneficios que puedan derivarse de la recolección/intercambio de datos (incluyendo las comunidades afectadas, Gobierno y el sector privado). • Promueva la transparencia en los procedimientos/metodologías de recolección de datos e inquietudes para maximizar la usabilidad de los datos • Asegure que las intenciones del intercambio de datos para mejorar los resultados/asistencia para las comunidades afectadas sean expresadas claramente y entendidas. • Identifique los conjuntos o sub-conjuntos de datos mínimos requeridos para el intercambio de datos. • Acordar un mecanismo de retroalimentación sobre cómo el intercambio de datos ha sido útil o un beneficio.	• Reduzca la cantidad de datos sensibles recopilados al mínimo. • Busque el consentimiento del originador(es) de los datos cuando sea relevante, ¿cuál es el propósito, el alcance y las sensibilidades? • Asegure que las recomendaciones de la Evaluación de Impacto de la Protección de Datos estén adheridas. • Revise los marcos legales relevantes. • Revise e implemente los protocolos de intercambio de información inter-agenciales. • Respete las políticas internas de protección/intercambio de datos. • Fortalezca las capacidades de los usuarios de los datos en los principios PIM y proceso PIM y en el tema a abordar. • Asegure que haya un consentimiento informado de la población afectada si se recopilan datos sensibles.

E.2. PASO 2 Diseñe un Sistema de GI desde una perspectiva del intercambio de datos

P1. ¿Cuáles son los datos específicos que se deben compartir? ¿Cuál es el nivel de detalle y el tipo de los datos que se van a compartir (personales y/o sensibles, tendencias, estadísticas, análisis, resultados)?

→ **QUÉ HACER: Evaluar los datos compartidos requeridos para la toma de decisiones**

- Entienda y documente el uso planeado y el propósito que justifican la razón para compartir. Refleje y documente el razonamiento para obtener los datos en primer lugar: ¿los datos se recopilaron para informar lo siguiente?:
  - Conocimiento de la situación y respuesta
  - Diseño y entrega de servicios públicos
  - Creación y transferencia de conocimiento
  - Predicciones y proyecciones
  - Evaluación y valoración del impacto.
- Identifique el tipo de datos – ej. personales, no personales, datos de protección – y la información que se van a compartir, así como sus riesgos y sensibilidades asociados. Después, siga los siguientes pasos:
  - Analice el propósito definido junto con los riesgos y beneficios esperados.
  - Refleje y documente las consideraciones legales y éticas.
  - Articule los datos primarios y los requerimientos de información.
- Entienda el nivel de los datos detallados que se van a compartir y distinga entre los datos y la información esenciales vs. los deseables a través de los siguientes pasos:
  - Basado en el propósito definido para el ejercicio específico de intercambio de datos, categorice los posibles datos que se van a compartir en al menos dos niveles: datos cruciales que se necesitan para la toma de decisiones y la respuesta, y datos no cruciales que podrían contribuir a la toma de decisiones.
  - Luego, asegure que el intercambio de datos se centre en los datos o la información críticos para la toma de decisiones.
- Documente cómo la recopilación y el intercambio de datos de identificación personal son esenciales para el bienestar y la protección del individuo(s) de interés.

P2. ¿Cuáles son los resultados de la revisión secundaria de datos respecto a las necesidades de datos compartidos?

→ **QUÉ HACER: Realice y revise los resultados de una revisión secundaria de datos**

- Utilice una revisión secundaria de datos para identificar los riesgos y beneficios alrededor del posible intercambio de datos o información, relacionado con ciertos tipos de categorías de datos o de métodos de recopilación de datos, así como de puntos específicos en el tiempo.
  - Documente los beneficios y riesgos del intercambio de datos en contextos similares.
- Documente los datos existentes que son relevantes para el propósito actual.

- Después de la revisión secundaria de datos, revise y examine los datos cruciales requeridos para la toma de decisiones (es decir, actualice la lista previa de datos requeridos).

P3. ¿Ha definido claramente cuáles son los datos personales y sensibles en su contexto específico?

→ **QUÉ HACER: Entienda la naturaleza de los datos que se comparten desde una perspectiva de protección de datos**

- Refleje y documente lo que constituye los datos sensibles dentro de un contexto operacional específico. Este es el conjunto de información que puede ser mal utilizado intencional o accidentalmente para dañar el bienestar y el interés físico, legal, material o psicosocial del sujeto que provee los datos (individuos, grupos, comunidades).

- Defina conjuntamente un sistema de clasificación para adaptar los protocolos basado en las evaluaciones del riesgo y la sensibilidad de los datos, calificando el daño potencial como bajo, moderado o alto.

- Revise conjuntamente y de manera periódica la definición de lo que constituye datos o información sensibles para su contexto, basado en el acuerdo específico de intercambio de datos y las partes interesadas involucradas.

NOTA: Para detalles adicionales para identificar el tipo y la sensibilidad de los datos, vea el *Anexo 1: Definiciones y conceptos compartidos.*

P4. ¿Cómo ha tomado en cuenta los impactos presentes y futuros del intercambio de datos en la seguridad y protección de los individuos y comunidades, así como de los recopiladores de los datos?

→ **QUÉ HACER: Evalúe el contexto actual y potencial a futuro**

- Examine el contexto (entorno social, político y de seguridad) desde una perspectiva de intercambio de datos e información. Considere cuidadosamente los futuros y posibles cambios en escenarios que pueden afectar los beneficios y los riesgos.
    - Tenga en cuenta que los datos recolectados para un propósito específico pueden ser usados en el futuro para otro propósito y que la información puede volverse más sensible con el tiempo, dependiendo de cómo se utiliza o de cómo evoluciona el contexto político y de seguridad.
- Acuerde y documente de manera conjunta el marco de tiempo que se debe utilizar para los datos e información que se van a compartir.
    - Planee revisar periódicamente si las necesidades de datos o información cambiaron desde el propósito original para el cual se recopilaron los datos. En ese caso, se necesita un nuevo propósito que debe ser definido y aplicado de forma conjunta.

P5. Si se van a compartir los datos personales, ¿Se obtuvo el consentimiento informado para dicho propósito?

→ **QUÉ HACER: Revise los procesos de recolección de datos sobre el consentimiento informado**

- La información no puede usarse para propósitos que son incompatibles con el propósito para el cual fue originalmente recolectada, y en el caso de los datos personales, para lo que se estipuló en el consentimiento.
- Identifique las limitaciones con el consentimiento informado recibido anteriormente respecto al propósito definido.
- Los datos no deben usarse o compartirse para otros propósitos sin el consentimiento adicional. Se requiere una nueva evaluación de los riesgos y beneficios si los datos compartidos se van a utilizar para un nuevo(s) propósito(s).

P6. ¿Cuáles son las necesidades de un acuerdo de intercambio de datos? ¿Son apropiadas para el contexto?

→ **QUÉ HACER: Establezca acuerdos y procesos de intercambio de datos**

- Documente y mantenga un análisis del tipo de datos que se van a compartir dentro de la red, articulando cuál es la forma, la frecuencia, a través de cuáles canales, y en qué nivel de agregación. Rastree quién tendrá acceso a la información compartida y para qué propósito.
- Cuáles son las prácticas reales dentro de la red de intercambio de información (ej. la autocensura, la toma informal de decisiones sobre cómo compartir datos, etc.).
- Incluya 'líneas rojas' o umbrales que puedan requerir medidas reparadoras o de mitigación, o la cesación de las actividades o procesos.
- Tome decisiones informadas colectivas sobre cómo proceder con el acuerdo dado de intercambio de datos e información.

ACCIONES: Maximizar *Pasos mínimos para maximizar los beneficios*	ACCIONES: Mitigar *Pasos mínimos para mitigar los riesgos*
• Asegure que la metodología sea adecuada para el propósito, proporcional y transparente. • Asegure la transparencia en la historia de los datos (trazabilidad) adjuntando metadatos de una manera estandarizada en todos los conjuntos de datos. • Identifique todos los actores que pueden utilizar los datos para beneficiar a la población afectada (incluyendo cómo y de qué maneras se podrán beneficiar) • Establezca protocolos y el alcance (incluyendo los métodos / enfoques técnicos para asegurar un acceso significativo y seguro a los datos). • Construya mecanismos de retroalimentación para la población afectada y los miembros de la red de intercambio de información. • Use el lenguaje humanitario de intercambio (HXL, por sus siglas en inglés) y otros estándares relevantes para la interoperabilidad y tome todas las acciones razonables para prevenir la duplicación (incluyendo el intercambio).	• Establezca mecanismos para la rectificación y preparación para las poblaciones afectadas en referencia a sus datos. • Establezca protocolos y mecanismos claros para cualquier escenario de una brecha de datos (incluyendo informar a las partes interesadas y documentar incidentes críticos). • Establezca y aténgase a un plan de retención de datos. • Establezca y socialice los POEs para la red de intercambio de información, articulando la rendición de cuentas individual y organizacional, los roles y responsabilidades a lo largo del ciclo de datos. • Refleje la sensibilidad de los datos en el diseño del mecanismo de intercambio de información. • Capacite a los profesionales (usuarios de los datos y proveedores) en la práctica responsable de datos.

E.3. PASO 3 Implemente sistemas de GI

P1. ¿Han surgido nuevos beneficios o riesgos en la etapa de implementación? ¿Se han implementado con éxito las acciones de prevención y mitigación identificadas en el Paso 2 ('Revisión de datos e información')?

→ **QUÉ HACER: Monitoree activamente los riesgos y beneficios durante y después de que ocurra el intercambio de datos**

- Revise el plan de intercambio con los socios de intercambio de datos y documente lo siguiente:
  - ¿La implementación sigue el plan y el diseño acordados? Si no es así, ¿cuándo ocurrió la variación en el proceso y por qué?
  - ¿Se necesitan revisiones del mecanismo de intercambio de datos para mejorar el intercambio o resolver algunos problemas?
- Revise y documente los beneficios o los daños que resultan del intercambio.
  - ¿El propósito y/o el entorno (tiempo, contexto, capacidad) han cambiado de tal forma que puedan impactar el acuerdo de intercambio de datos?
  - ¿Todas las partes – incluyendo a las comunidades afectadas – han comunicado con claridad los beneficios y riesgos como resultado del intercambio de datos?
- Esté atento a las señales de riesgos que se pueden crear por la actividad del intercambio de datos o de las posibles fallas en las medidas de mitigación.

ACCIONES: Maximizar *Pasos mínimos para maximizar los beneficios*	**ACCIONES: Mitigar** *Pasos mínimos para mitigar los riesgos*
• Comprenda e invierta en las capacidades, competencias y aptitudes técnicas, humanas e institucionales que sean necesarias para implementar un enfoque de intercambio de datos. • Utilice un enfoque de fases para implementar modalidades de intercambio de datos, especialmente con los 'nuevos' sistemas y/o enfoques. • Cuando sea posible, revise periódicamente y ajuste el enfoque de implementación y el sistema de GI basado en la experiencia. • Asegure que se provea el marco y el contexto necesarios cuando los datos y análisis se compartan para respaldar una interpretación + uso acertados y beneficiosos. • Documente cómo se usan los datos; comparta dentro de la red de intercambio de información.	• Documente los riesgos y daños realizados; apoye el reporte de incidentes críticos / el monitoreo y la rastreabilidad. • Tome acciones correctivas cuando se realicen daños; documente estas acciones con relación a un enfoque sistemático. • Ofrezca una variedad de actividades de capacitación y de desarrollo de capacidades relacionadas con los estándares, procedimientos y políticas para el intercambio de datos. • Realice auditorías/revisiones regulares de la capacidad de los usuarios y del uso del sistema.

E.4. PASO 4 Evalúe el impacto (del intercambio)

P1. ¿Cuáles fueron los impactos del intercambio de datos?

- Revise y documente el intercambio de información:
  - ¿Fue menos o más que suficiente para el propósito?
  - ¿Se lograron los beneficios esperados?

P2. ¿Ha podido evaluar el acuerdo de intercambio de datos?

- Revise y documente el proceso y los procedimientos reales de intercambio de datos
  - ¿La información identificada se compartió según lo planeado?
  - ¿Se mitigaron de manera efectiva los riesgos?
  - ¿Hubo algunos beneficios y/o riesgos que no anticipó? ¿Cómo se abordaron?
- Documente y acuerde las fuentes relevantes (fondos, personas, etc.) para respaldar el intercambio, e identifique y abogue de manera conjunta para obtener más o menos recursos (sistema, personas, dinero) en el futuro.

P3. ¿Se compartió la información con las poblaciones afectadas según lo planeado? ¿Cuál fue la retroalimentación y cómo se consideró de acuerdo con el uso y acceso a la información?

→ **QUÉ HACER: Asegure que los respondientes tienen la información que necesitan (incluyendo a las poblaciones afectadas)**

- Trabaje con la comunidad para aprobar las solicitudes de datos e información que se presenten. Este proceso debe asegurar que estas solicitudes no tengan sesgos. También deben enfocarse en un propósito definido comúnmente acordado, que sea proporcional y pueda aportar resultados de protección en nombre de las personas de interés, reflejando también los principios acordados.

ACCIONES: Maximizar *Pasos mínimos para maximizar los beneficios*	**ACCIONES: Mitigar** *Pasos mínimos para mitigar los riesgos*
• Proporcione retroalimentación a los proveedores de datos sobre la utilidad y el impacto del uso de datos e información, incluyendo un diálogo abierto sobre la calidad y relevancia de los datos. • Busque retroalimentación de las comunidades afectadas sobre la disponibilidad y la utilidad de la información y las modalidades para compartir esa información. • Reconozca los recursos (humanos y financieros) y fuentes de los datos originales; incluyendo recomendaciones para la recaudación de fondos, capacidades y competencias institucionales (atribución apropiada) • Implemente los hallazgos y recomendaciones de las evaluaciones (para ajustar el marco de intercambio).	• Sea transparente en cuanto a los cuellos de botella y problemas a resolver para rectificar los retos para compartir e intercambiar datos – incluyendo los roles y responsabilidades. • Reconozca riesgos imprevistos y medidas de mitigación y trabaje para mejorarlos/resolverlos de manera coordinada y colaborativa en un entorno de confianza. • Trabaje hacia la expansión de la inclusión de otras partes interesadas en el marco de intercambio de datos – por ejemplo, mostrando estudios de caso positivos.

ANEXO Definiciones y conceptos compartidos

El objetivo de esta sección es definir un conjunto mínimo de términos para facilitar una discusión normativa del intercambio de datos e información y del *Marco*.

¿Qué responsabilidades mínimas tienen los proveedores de datos para los usos secundarios de los datos?

Para más detalles, por favor consulte la Sección E, Evaluación Conjunta de Beneficios y Riesgos.

¿Qué es el riesgo en el contexto del intercambio de datos e información?

El riesgo varía según el contexto, el tiempo y las personas involucradas. Puede incluir amenazas inmediatas o posteriores a la vida, la seguridad, la identidad o la libertad, tanto al nivel individual como colectivo.

La propuesta de abordar las complejidades alrededor de los riesgos se enfocará en cómo comenzar a construir un perfil de riesgo que sea específico para la situación, basándose en un propósito definido y en la intención detrás de los datos que se van a compartir. La meta es monitorear/identificar el riesgo, así como mitigarlo de manera regular.

Para detalles y consideraciones adicionales, por favor consulte la Sección E, Pasos 1 y 2, que abordan el propósito definido, así como el contexto y la temporalidad.

¿Cuál es la información de identificación personal vs. la que no identifica a las personas?

La tecnología moderna continúa desafiando las definiciones actuales de la información que identifica y que no identifica a las personas. Al tratarse de datos humanos, todo esto tiene el riesgo de ser personalmente identificable.

Recomendamos enfocarse más bien en cómo prevenir el uso perjudicial y cómo evaluar el riesgo mediante la operacionalización de una evaluación conjunta de riesgos y beneficios. Al hacer esto, se pueden aclarar las acciones necesarias para evaluar o prevenir el riesgo, basándose en una serie de pasos. El análisis conjunto de los riesgos y beneficios para un proceso particular de intercambio de datos sería entonces el componente de este proceso compartido.

¿Qué es el consentimiento informado?

El 'consentimiento' significa que los sujetos que proveen los datos aprueban voluntariamente que la información sea usada o compartida según se ha explicado. Para que el consentimiento sea 'informado' implica que los sujetos que proveen los datos deben recibir explicaciones, en un lenguaje simple, sobre la identidad de quien recopila los datos o de otros actores, así como del propósito, alcance, método, uso planeado y riesgos potenciales de la provisión de los datos, y también sobre el significado de confidencialidad.

Así, el consentimiento informado se otorga de manera libre y voluntaria según un entendimiento claro de los hechos, implicaciones y consecuencias futuras de una acción. Dependiendo de las circunstancias, puede ser verbal, escrito o provisto de otra forma según los procedimientos de Determinación del Interés Superior[8], en representación de un menor de edad.

El consentimiento se entiende como voluntariamente otorgado y solo cuando el sujeto que provee los datos tiene una elección genuina y puede rehusarse o retirar el consentimiento sin detrimento alguno.

Para ver detalles adicionales, por favor consulte la Sección E, Paso 2, sobre el 'consentimiento informado'.

[8] *Convención de los Derechos de la Niñez, Comité de los Derechos de los Niños,* GC No. 14 (2013), sobre el derecho del niño/a de que sus intereses superiores sean tomados en cuenta como una consideración primaria (art. 3, para. 1), disponible en línea en: **www2.ohchr.org/English/bodies/crc/ docs/GC/CRC_C_GC_14_ENG.pdf**, consultado el 9 de abril de 2018.

¿Cuál es la diferencia entre datos personales y los datos no personales?

Los datos personales, o la información de identificación personal (IIP), son datos de identificación a través de los cuales se puede identificar directa o indirectamente (en combinación con otra información o por medios razonablemente usados relacionados con esos datos) a una persona. Esto puede incluir, por ejemplo, una identificación como un nombre, número de documento, datos de ubicación, material audiovisual o un identificador virtual. La información de identificación personal también incluye: país de asilo, número de registro individual, ocupación, estatus, religión y grupo étnico. También incluye datos biométricos, como fotografías, huellas digitales, características faciales o patrones del iris, así como cualquier expresión de opinión sobre el individuo, como una evaluación de su estatus legal y/o sus necesidades específicas.[9]

¿Cuáles son los datos sensibles vs. los que no son sensibles?

Los datos sensibles de protección son datos o información cuya divulgación o acceso no autorizado pueden causar:

- Daño (como sanciones, discriminación, represión o estigma) a cualquier persona, incluyendo la fuente de información u otros grupos o personas identificables; o
- Un impacto negativo en la capacidad de una organización de llevar a cabo sus actividades, como lo es un daño reputacional.

La sensibilidad de los datos se define en relación con el contexto particular y el nivel de agregación, y puede cambiar con el tiempo. Por lo tanto, los mismos datos pueden no tener el mismo nivel de sensibilidad en diferentes contextos.

Los datos y la información de protección que no contengan datos personales pueden ser, sin embargo, sensibles. Puede relacionarse con comunidades y otros grupos[10], individuos anónimos, o eventos o asuntos específicos. En conflictos armados y otras situaciones de violencia, hay varios aspectos relacionados con la situación humanitaria, de derechos humanos, política o de seguridad, que pueden exacerbar los riesgos para las personas.

De igual manera, los datos agregados o seudonimizados[11] pueden seguir siendo sensibles. Los individuos o grupos se pueden seguir identificando, especialmente según su ubicación y el tamaño de la muestra, y por tanto pueden estar expuestos a daños si los datos acerca de ellos son divulgados.

No es posible, por lo tanto, proponer una lista definitiva de los tipos de datos o información que constituyen la información sensible. Sin embargo, algunos tipos clave de información pueden pertenecer a esta categoría, como la información sobre la naturaleza de las violaciones que afectan a individuos o grupos específicos, detalles sobre víctimas y testigos, la afiliación de los perpetradores, detalles operacionales relacionados con operaciones militares o con la seguridad, etc.

La privacidad, seguridad e integridad de los individuos o grupos pueden ponerse en riesgo incluso cuando no se recopilan y procesan datos personales. Al reconocer esto, los actores de protección como buena práctica aplican los estándares que se derivan desde los principios de protección de datos hasta la información y datos sensibles que se usan para propósitos de protección, al punto que sea necesario dada la sensibilidad particular de los datos.

---

[9] *Normativa profesional relativa a la labor de protección, capítulo 6,* 2018

[10] Estos datos o información se pueden referir a la ‘información identificable de la comunidad’ o ‘datos identificables demográficamente’ (IIC / IID)

[11] *Normativa profesional relativa a la labor de protección, capítulo 6*, 2018: ‘La seudonimización’ de los datos significa reemplazar cualquier característica identificable de datos con un seudónimo o con un valor que no permita identificar directamente al sujeto que provee los datos. Por ejemplo, ”Jane Doe” podría seudonimizarse como ”POC 15364”. La seudonimización se debe distinguir de la anonimización, ya que proporciona una protección limitada para la identidad de los sujetos que proveen sus datos en muchos casos, debido a que permite la identificación por medios indirectos. Cuando se utiliza un seudónimo, es frecuentemente posible identificar al sujeto que provee los datos al analizar los datos subyacentes o relacionados.

El diagrama de abajo, de los Estándares Profesionales para el Trabajo de Protección, (2018, pág. 112)[12] ilustra las relaciones entre tipos de datos e información:

Diagrama: Relaciones entre los tipos de datos e información

NOTA: esta es la primera versión del documento en español. Se aceptan comentarios y recomendaciones. Puede escribir al correo pimtraining@drc.ngo

[12] *Normativa profesional relativa a la labor de protección, capítulo 6, 2018*