CaLP
The Cash Learning Partnership

CAJA DE HERRAMIENTAS PARA LA RESPONSABILIDAD EN LA GESTIÓN DE DATOS

GUÍA PRÁCTICA PARA PROFESIONALES DE PROGRAMAS DE TRANSFERENCIAS MONETARIAS

ÍNDICE Y AGRADECIMIENTOS

ÍNDICE

AGRADECIMIENTOS

La Caja de Herramientas para la Responsabilidad en la Gestión de Datos – Guía Práctica para profesionales de Programas de Transferencias Monetarias fue comisionada por CaLP con fondos de la Oficina Federal de Relaciones Exteriores de Alemania.

La investigación de esta publicación fue realizada entre junio y septiembre de 2020 por Linda Raftree, consultora independiente.

Esta publicación fue elaborada por Linda Raftree con el apoyo y la supervisión editorial y de contenido de Anna Kondakhchyan de CaLP. Este es un trabajo colaborativo, que recibió insumos invaluables de muchas organizaciones y profesionales en materia de PTM que, de manera generosa, contribuyeron con sus ideas y su tiempo al proceso de investigación a través de entrevistas a actores clave y fuentes de datos.

Un agradecimiento especial a los miembros del Comité Asesor por su apoyo inestimable en guiar el desarrollo de la Guía práctica y en revisar los borradores. Los miembros son: Amos Doornbos (World Vision International), James Eaton-Lee (Oxfam), Stuart Campo (OCHA HDX), Jenny Caswell (GSMA), Jo Burton (CICR), Gabriele Erba (Unicef) y Rosa Akbari (Mercy Corps).

Los puntos de vista que se expresan en la presente publicación son únicamente de los autores y no son necesariamente los puntos de vista de los donantes ni de las agencias miembro de CaLP.

CaLP es una red mundial dinámica de más de 90 organizaciones que se dedica a la tarea fundamental de establecimiento de políticas, prácticas e investigación en materia de Programas de Transferencias Monetarias (PTM) humanitarios y asistencia financiera en general.

Para obtener más información, favor visitar el sitio web de CaLP en el enlace www.calpnetwork.org

Siga a CaLP en Twitter: @calpnetwork

PRÓLOGO

Si bien todos los programas humanitarios recopilan grandes cantidades de datos, en los Programas de Transferencias Monetarias (PTM) recopilamos grandes volúmenes de datos que con frecuencia se intercambian con múltiples agentes. Gran parte de los datos que recopilamos son altamente sensibles y privados, y los recopilamos de y sobre personas muy vulnerables. Es importante diseñar nuestros programas y gestionar los datos a modo de reducir la posibilidad de que estos datos sean utilizados —ya sea accidental o deliberadamente— en una manera que cause daño o que excluya injustamente a personas o grupos designados, de la recepción de beneficios.

Los tipos de daños asociados con los datos y las tecnologías digitales incluyen:

- **Riesgo de lesión**, por ejemplo, cuando los datos se utilizan para identificar, localizar y específicamente causar daño físico, emocional o psicológico a una persona o grupo.[1]
- **Negación de servicios o discriminación** basado en los datos, esto incluye la pérdida de oportunidades y pérdidas económicas cuando los datos se utilizan para decidir la elegibilidad a ciertos servicios o beneficios.[2]
- **Violaciones de los derechos humanos**, tales como la pérdida de la dignidad, libertad o privacidad, cuando los datos se utilizan en maneras que deshumanizan a las personas, cuando las decisiones las toman algoritmos computarizados, o cuando la recopilación de datos es invasiva o los datos se recopilan, procesan e intercambian sin permiso, o cuando las personas deben dar sus datos a cambio de un servicio vital o del acceso a otro derecho.[3]
- **Focalización y acoso intencional** de poblaciones vulnerables a través de nuevas tecnologías. Como se menciona en el informe del Relator especial sobre tecnologías digitales y el estado de bienestar, el uso de las tecnologías para identificar fraudes o violaciones de las condiciones impuestas a los destinatarios al recibir asistencia en efectivo u otras prestaciones sociales, permite que se recopile información digital y que se almacene por un período de tiempo indefinido. Esto significa que se mantienen cantidades enormes de información indefinidamente y que podrían utilizarse en contra de alguien.[4]
- **Erosión de las estructuras sociales o democráticas**, por ejemplo, a través de la manipulación, la ampliación de los desequilibrios de poder o la desinformación.[5]

La gestión y el intercambio de datos son componentes críticos de los PTM; trabajamos con datos sensibles en todo el proceso de los programas de transferencias monetarias. De modo que, de la misma manera que el salvaguardar, el proteger y el "no causar daño" son partes esenciales de los PTM y de otros programas humanitarios, la responsabilidad en la gestión de datos debe incorporarse en todo lo que hacemos como profesionales en PTM. Si bien esta guía práctica está dirigida a los PTM, gran parte de la orientación también puede extenderse a otros programas humanitarios.

CASILLA 1: ¿QUÉ ES LA RESPONSABILIDAD EN LA GESTIÓN DE DATOS?

La responsabilidad en la gestión de datos va más allá de la privacidad de los datos y de la protección de datos, pues incluye principios, procesos y herramientas que respaldan una gestión segura, ética y eficiente de los datos.[6]

1 Véase el marco de Microsoft 'Types of Harm' (Tipos de daños) para realizar un examen más a fondo de este tema.
2 See Alston, P. (2019) 'Report of the Special Rapporteur on extreme poverty and human rights' (Informe del Relator Especial sobre la pobreza extrema y los derechos humanos), que estudia el papel que desempeñan las Tecnologías Digitales y el Estado de Bienestar. Presentando en la 74° Sesión de la Asamblea General de la ONU, en el tema de Promoción y protección de los derechos humanos: preguntas sobre derechos humanos, incluyendo enfoques alternativos para mejorar el goce de los derechos humanos y la libertad fundamental.
3 Véase el General Data Protection Regulation (GDPR) (2018) donde se enumeran los derechos de las personas a las que se refieren los datos, incluido el derecho de un individuo a negarse al tratamiento de sus datos, el derecho a no ser categorizado en un perfil por los datos, el derecho a que no se tomen decisiones automáticas que afecten la vida de una persona, así como el derecho a impugnar una decisión automática y a pedir que esta sea revisada por un humano.
4 Alston (2019).
5 Marco de Microsoft, 'Types of Harm' (Tipos de daños).
6 OCHA (2016) 'Think Brief: Building Data Responsibility into Humanitarian Action' (Informe de Pensamiento: Incorporando la responsabilidad en la gestión de datos en las medidas humanitarias).

Puntos clave a tomar en cuenta:

- **La responsabilidad en la gestión de datos es más que solo datos.** Al igual que otros bienes de valor, los datos se han convertido en un lujo. Los datos individuales, por lo general, se convierten en información valiosa que es utilizada por diferentes agentes para todo tipo de fines —tanto beneficiosos como perjudiciales—. Se ha creado todo un ecosistema en torno a los datos recopilados y procesados a través de los PTM. Los datos pueden otorgar poder y beneficios económicos a individuos, agencias humanitarias, gobiernos locales y nacionales, Proveedores de Servicios Financieros (PSF), supervisores externos (third-party monitors, TPM por sus siglas en inglés), compañías tecnológicas y actores no gubernamentales, ya que todos estos manejan datos en PTM.
- **La responsabilidad en la gestión de datos requiere contextualización, creatividad, capacidad y colaboración.** Una variedad de agentes recopila, gestiona, utiliza e intercambia datos en los PTM. Hay diferentes mandatos y motivaciones, dinámicas de poder y niveles de capacidades y conocimientos organizacionales en juego. Será necesario encontrar maneras ágiles y adaptables para mitigar los riesgos y daños asociados con los datos, en especial en contextos frágiles o afectados por un conflicto. La responsabilidad en la gestión de datos va a depender de todo aquel que participe en el ciclo de programa, desde los encuestadores individuales y el personal en primera línea pasando por los equipos de coordinación de país, PSF, socios y donantes. A veces, la protección de datos también puede poner en riesgo al personal humanitario y a los trabajadores en primera línea.
- **La responsabilidad en la gestión de datos no es una actividad individual; requiere de equipos integrales.** Será necesario involucrar a diferentes partes de su organización y múltiples tipos de conocimientos a medida que incorpore la protección de datos y mitigación de posibles daños relacionados a los PTM. Para esto será necesario contar con capacidades técnicas como son seguridad de la información, administración de los sistemas de datos, análisis y arquitectura de datos; administración legal y comercial, cumplimiento y entendimiento de las finanzas; género, inclusión, protección y bienestar; y competencias interpersonales como la negociación y construcción de consenso.

En esta guía práctica, ofrecemos varias maneras de incorporar la responsabilidad en la gestión de datos en la planificación, el diseño, la implementación y las actividades de monitoreo, evaluación, rendición de cuentas y aprendizaje (MEAl, por sus siglas en inglés) del programa. La guía práctica ofrece un "estándar de oro" al cual las organizaciones deben aspirar alcanzar, e identifica las implicaciones tanto legales como éticas de las que debemos ser conscientes al tratar los datos. Reconocemos que no siempre será posible alcanzar el estándar de oro. Siempre habrá contrapartidas en cuanto a velocidad, presupuesto y otros factores a considerar, y sabemos que los profesionales de PTM serán arrastrados en diferentes direcciones. No obstante, en aquellos casos en los que nuestra capacidad organizacional no satisfaga los estándares legales y éticos, es posible que sea necesario interrumpir las actividades debido a que nuestra recopilación de datos podría conducir a daños o infringir la ley.

Los datos son la extensión de una persona. Debemos tratar los datos de una persona con el mismo respeto y cuidado con el que trataríamos a la persona física, si estuviera parada frente a nosotros.

¿PARA QUÉ OTRA GUÍA PRÁCTICA?

En 2016, ELAN produjo el "Data Starter Kit" (kit inicial sobre datos)[7], una de las primeras guías prácticas en abordar el tema de la responsabilidad en la gestión de datos en los sectores humanitario y de desarrollo. El "Data Starter Kit" ha sido un recurso básico para la comunidad de CaLP y más ampliamente para los profesionales responsables de los datos en todo el mundo. Tomando en cuenta el modo en que el mundo de los Programas de Transferencias Monetarias (PTM) ha cambiado desde 2016, CaLP sintió que era necesario actualizar el "Data Starter Kit" para enfrentar los retos actuales. El enorme volumen de PTM ha aumentado de $2.800 millones en 2016 a $5.600 millones en 2019, lo que significa que hoy en día, los PTM constituyen aproximadamente 18 % de toda la ayuda humanitaria internacional.[8]

Además, hay un creciente énfasis en la calidad, y los PTM están atravesando un cambio en sus roles y en sus alianzas. Cada vez más los PTM requieren coordinación entre varios socios para alcanzar una mayor escala y sostenibilidad. La coordinación entre actores clave se da entre los ministerios gubernamentales, agencias de la ONU, el Movimiento Internacional de la Cruz Roja y de la Medialuna Roja, ONGs Internacionales y organizaciones locales; así como cada uno de sus respectivos sistemas de datos. Los PTM involucran a muchos más socios y con frecuencia requieren que estos socios implementadores utilicen grandes sistemas establecidos, muchos de los cuales proponen la incorporación de la identidad digital o la biometría para la identificación. Cada vez más, los PTM dependen de medios digitales, por tanto, es más probable que también se involucren bancos, operadores de redes móviles (mobile network operators, MNO por sus siglas en inglés), microfinancieras, y una variedad de nuevos proveedores de tecnología financiera.

7 ELAN (2016) 'Data Starter Kit' (Kit inicial sobre datos).
8 Cash Learning Partnership (2020) 'State of the World's Cash 2020'.

CASILLA 2: ¿QUÉ ES EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS?

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) entró en vigencia en mayo de 2018. Por lo general, se le considera la regulación sobre privacidad de datos más robusta del mundo. La mayoría de las organizaciones con base en la UE están obligadas a cumplir con el RGPD y muchos países en otras partes del mundo basan sus propias regulaciones de privacidad en el RGPD. La ONU y el CICR no están sujetos al RGPD porque disfrutan de ciertos privilegios e inmunidades debido a su posición como organizaciones internacionales.

La cantidad de datos que los socios de los PTM recopilan, almacenan, utilizan e intercambian aumenta de manera consistente. A la vez, en países de todo el mundo se desarrollan y entran en vigor nuevas y actualizadas leyes sobre la privacidad de datos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE). Estas leyes introducen nuevos requisitos para las organizaciones que manejan datos personales y sensibles. La concientización también se ha incrementado respecto al manejo seguro de datos, a nuestra obligación de cuidar, a la responsabilidad de proteger a los participantes de nuestros programas, así como la obligación de no causar daño con los datos.

En este contexto, ofrecemos una guía práctica para la responsabilidad en la gestión de datos actualizada con el fin de reflexionar sobre estos importantes cambios.

CASILLA 3: ¿QUÉ TIPO DE DATOS ABARCA ESTA GUÍA PRÁCTICA?

El término "dato" en estas hojas de orientación (tomando prestado de OCHA[9] y CICR[10]) incluye tanto datos sensibles como datos no personales, incluidos los siguientes:

1. datos sobre las personas afectadas por una crisis y sus necesidades (p. ej., datos personales de las personas receptoras de PTM);
2. datos sobre el contexto en el cual ocurre una crisis (p. ej., información sobre las comunidades que reciben transferencias monetarias);
3. datos sobre la respuesta por parte de las organizaciones y las personas que intentan ayudar (p. ej., localización de puntos de distribución de asistencia en efectivo o planes de las actividades de recopilación de datos).

Dato personal es la información que se relaciona con una persona física identificada o identificable.

Dato sensible es un dato que, en caso de ser divulgado o de tener acceso a él sin una autorización adecuada, podría resultar en:

- daños a una persona (como sanciones, discriminación y amenazas de seguridad), incluyendo la fuente de información u otras personas o grupos identificables;
- un efecto negativo sobre la capacidad de una organización de realizar sus actividades o sobre la percepción del público de esa organización.

Los datos tienen niveles de sensibilidad que varían dependiendo del contexto, por lo que en la presente guía no ofrecemos una lista definitiva de puntos de datos sensibles.

9 OCHA (2019), 'Data Responsibility Guidelines: Working Draft' (Lineamientos sobre la responsabilidad en la gestión de datos: borrador de trabajo).
10 CICR (2020), 'Data Protection Handbook' (Manual de protección de datos).

¿CÓMO ESTÁ ESTRUCTURADA ESTA GUÍA PRÁCTICA?

En la presente guía práctica, nos enfocamos en la responsabilidad en la gestión de datos en los PTM a través del lente del ciclo de vida de los datos. Debe señalarse que el ciclo de vida de los datos no es un circuito único. En cambio, es una gráfica visual, útil como guía, para pensar sobre los datos de manera holística. Esperamos que reconsidere el ciclo de vida de los datos a medida que su programa se desarrolle y se implementen actividades adicionales relacionadas con los datos.

CASILLA 4: CICLO DE VIDA DE LOS DATOS

El ciclo de vida de los datos es útil para guiar las actividades generales relacionadas con datos en una respuesta en su conjunto y para actividades de recopilación de datos individuales en diferentes fases de una respuesta. (El ciclo de vida que se utiliza aquí es ilustrativo. Es posible que las organizaciones tengan su propia versión del ciclo de vida de los datos).

Para facilidad de uso, la presente guía práctica se divide en 7 hojas de orientación que abordan temas relacionados con el contexto y la capacidad organizativa; el diseño y la planificación; y la ejecución. En breve, las hojas de orientación abarcan los siguientes aspectos:

CONTEXTO Y CAPACIDAD ORGANIZATIVA (HOJA DE ORIENTACIÓN 1)

En la fase temprana, se deben tomar decisiones de alto nivel respecto a la capacidad de las organizaciones para implementar los PTM de manera segura y ética. Esto incluye evaluar el panorama de datos en general, el contexto nacional, el contexto legal y las dinámicas de poder relacionadas con los datos en los PTM. También incluye evaluar los aspectos relacionados con el cumplimiento, las relaciones entre los datos y los sistemas que serán utilizados (y con frecuencia requeridos) por donantes, consorcios, agencias de la ONU, el Movimiento Internacional de la Cruz Roja y de la Medialuna Roja, organizaciones no gubernamentales (ONG) nacionales e internacionales, gobiernos, los proveedores de servicios financieros y otros socios en programas de transferencias monetaria.

En esta etapa, la evaluación de la capacidad organizativa incluye las habilidades, los conocimientos y los recursos para proteger los datos y para usar herramientas y procesos digitales de manera responsable en el contexto anterior. Muchos de los aspectos que exponemos en la hoja de orientación 1 pueden incorporarse en la preparación y análisis de situación de PTM existentes.

CASILLA 5: LEGAL VERSUS ÉTICO

Al hacer algo de manera legal, se preguntará *¿podemos* hacer esto? Al hacer algo de manera ética, se preguntará *¿debemos* hacer esto? A veces lo que es legal, no es ético.

DISEÑO Y PLANIFICACIÓN (HOJA DE ORIENTACIÓN 2)

La fase de diseño y planificación ayuda a las organizaciones a establecer su enfoque de recopilación y gestión responsable de datos dentro de las diversas fases del ciclo de programa de los PTM (focalización, inscripción y registro, implementación y MEAL). Es probable que cada etapa del ciclo de programas de transferencias monetarias requiera de algún tipo de recopilación, captura y gestión de datos a lo largo del ciclo de vida de los datos. Por ejemplo, evaluaciones de necesidades y vulnerabilidades, que por lo general se realizan en fases tempranas para ayudar a las agencias a comprender las necesidades específicas de las poblaciones afectadas. Estas evaluaciones deben guiar las decisiones posteriores respecto a la modalidad de asistencia en efectivo más apropiada para el contexto, el valor y frecuencia de las transferencias, las alianzas y participación de terceros, y el proceso general de inicio a fin, incluido qué datos se recopilarán y de qué modo, y qué sistemas se utilizarán para el almacenamiento y el análisis de datos. Los aspectos que se abarcan en esta fase se alinean con las fases típicas de análisis de respuesta y el diseño de los PTM.

GESTIÓN DE DATOS DURANTE LA EJECUCIÓN (HOJAS DE ORIENTACIÓN 3–7)

Posterior a las etapas de diseño y planificación, la respuesta pasa a la ejecución. Durante las fases de ejecución del PTM, las organizaciones recopilan datos de las poblaciones afectadas con el fin de seleccionar, inscribir y registrar, y de distribuir asistencia en efectivo o cupones.[11] También realizan actividades de monitoreo y recopilan retroalimentación de las poblaciones afectadas con el fin de mejorar la rendición de cuentas y adaptar las iniciativas del programa. La recopilación de datos durante la fase de ejecución se vuelve más frecuente y más granular. Es posible que los riesgos y daños sean exacerbados debido al aumento de datos personales y otras formas de datos sensibles o datos grupales que se estén manejando o intercambiando. Las agencias también deben tomar en cuenta qué les ocurre a los datos de las poblaciones afectadas cuando un programa se cierra o se entrega su gestión a otra entidad, como, por ejemplo, cuando un PTM humanitario se transfiere a agencias de protección social gubernamentales o a otros socios para el desarrollo.

Utilizar un enfoque de ciclo de vida de los datos para guiar la recopilación y la gestión de datos generales de un programa y para planificar e implementar procesos específicos de recopilación y gestión de datos en las diferentes etapas de la ejecución de un PTM, puede ayudar a las organizaciones a maximizar los beneficios de los datos y a identificar y mitigar los riesgos y daños durante la ejecución del mismo. Las hojas de orientación 3–7 pueden servir a las organizaciones en el desarrollo de planes para cada etapa del ciclo de vida de datos; para luego regresar a finalizar el diseño y plan general de datos (hoja de orientación 2).

11 Los programas de entrega de efectivo tienden a involucrar cantidades mayores de recopilación de datos, tratamiento de datos, y de intercambio de datos y coordinación entre agencias, mientras que la asistencia por medio de cupones podría implicar menos intercambio de datos, porque con frecuencia se maneja internamente y requiere menos intercambio de datos y coordinación con otros agentes de los PTM.

LISTA DE ACRÓNIMOS

AAP	Rendición de cuentas a poblaciones afectadas (siglas en inglés)
ACNUR	Alto Comisionado de las Naciones Unidas para los Refugiados
CaLP	Cash Learning Partnership
CDR	Registro de detalles de llamadas (siglas en inglés)
CICR	Comité Internacional de la Cruz Roja
DPO	Oficial de protección de datos (siglas en inglés)
EIPD	Evaluación del impacto de la privacidad de los datos personales
GAFI	Grupo de Acción Financiera Internacional
GTM	Grupo de Trabajo de Transferencias Monetarias
IASC	Comité Permanente Inter Agencial
ID	Identificación
INGO	Organización no Gubernamental Internacional (siglas en inglés)
ISP	Protocolos de intercambio de información (siglas en inglés)
KYC	Conocer a tu cliente (siglas en inglés)
LI	Organización no Gubernamental Internacional (siglas en inglés)
MEAL	Monitoreo, evaluación, rendición de cuentas y aprendizaje (siglas en inglés)
MNO	Monitoreo, evaluación, rendición de cuentas y aprendizaje (siglas en inglés)
OCHA	Oficina de Coordinación de Asuntos Humanitarios
ONG	Organización no Gubernamental
ONU	Organización de las Naciones Unidas
PEA	Análisis de economía política
PI	Interés público (siglas en inglés)
PIA	Evaluación de impacto sobre la privacidad (siglas en inglés)
PMA	Programa Mundial de Alimentos
POE	Procedimiento Operacional Estándar
PSF	Proveedor de Servicios Financieros
PTM	Programas de Transferencias Monetarias
RBA	Evaluación de riesgos y beneficios (siglas en inglés)
RCRCM	Movimiento Internacional de la Cruz Roja y de la Medialuna Roja (siglas en inglés)
RGPD	Reglamento General de Protección de Datos
SCOPE	Sistema de registro de destinatarios PMA (siglas en inglés)
UE	Unión Europea
Unicef	Fondo de las Naciones Unidas para la Infancia

HOJA DE ORIENTACIÓN 1

EVALUACIÓN DEL CONTEXTO Y LAS CAPACIDADES

A la hora de planificar un programa, incluso un PTM, es necesario evaluar el contexto general en el que se está trabajando y la capacidad de la organización, antes de planificar detalladamente el programa. En este nivel, el interés es determinar si la organización puede implementar un programa de manera segura y ética en un contexto específico.

Esta evaluación de alto nivel debe incluir una revisión de las obligaciones y las capacidades para recopilar y gestionar responsablemente los datos que se necesitan para el programa. Es probable que también incluya evaluaciones de la normativa, evaluaciones de viabilidad, el alcance de los servicios de liquidez y financieros, un estudio de las estrategias de los donantes y otras consideraciones generales.

Revisar el contexto y las capacidades relacionadas con los datos en este punto ayuda a garantizar que los datos necesarios para poner en marcha el programa se pueden recopilar, procesar y gestionar de manera responsable, y a entender cuáles son las compensaciones que se pueden hacer para poder tomar decisiones clave. Una evaluación de alto nivel de las áreas, que se detallan a continuación, puede ayudar a determinar si se está responsablemente equipado para proceder con una propuesta o respuesta. Si, al realizar el primer examen, los riesgos y daños (a las poblaciones afectadas, a su organización, a sus socios o a su personal) relacionados con los datos superan los beneficios, deberá rediseñar, renegociar o repensar el programa antes de proceder a la etapa de propuesta. Las áreas clave especificadas a continuación quizá ya estén incluidas en sus procesos ordinarios de toma de decisión e investigación previos a la propuesta. Las enumeramos de todos modos, pues con frecuencia las organizaciones no se centran lo suficiente en su responsabilidad hacia los datos durante los pasos previos a la propuesta.

IDENTIFICACIÓN DE PRINCIPIOS DE ALTO NIVEL QUE GUÍAN EL ENFOQUE DE SU ORGANIZACIÓN

Los actores humanitarios ya han desarrollado o adoptado diferentes conjuntos de principios que pueden ayudar al pensamiento en el alto nivel de liderazgo de la organización, sobre la responsabilidad en la gestión de datos en los PTM. Su organización podría aplicar uno o más de estos principios, o seguir sus propios principios. Los principios de alto nivel pueden ayudarle a definir más adelante las "líneas rojas" que su organización se niega a cruzar a nivel operativo, y los criterios que entran en juego para las decisiones de "ir / no ir".

La hoja de orientación 1 ofrece una guía sobre cómo evaluar el contexto y las capacidades relacionadas con los datos, antes de embarcarse en un PTM. Los recursos y la capacidad de su organización determinarán la profundidad y el rigor de su enfoque a estas evaluaciones. Incluso si sus recursos son limitados, es importante que al menos considere cada uno de estos elementos al hacer una evaluación rápida, pues su evaluación del contexto y de la capacidad podría alertarle de una situación en la que no es aconsejable avanzar.

- *CaLP´s Protecting Beneficiary Privacy Principles and Operational Standards (Principios y estándares operativos para la protección de la privacidad de personas beneficiarias de CaLP) (2013)*
- *Principles for Digital Payments in Humanitarian Response (Principios para pagos digitales en respuestas de ayuda humanitaria) (2015)*
- *UN Personal Data Protection and Privacy Principles (Principios de protección y privacidad de datos personales de la ONU) (2018)*
- *EU's General Data Protection Regulation (GDPR) Data Protection Principles (Principios de protección de datos personales de la Regulación de Protección General de Datos de la UE) (2018)*
- *ICRC Data Processing Principles (2020), (Principios de tratamiento de datos del CICR) (2020), páginas 35–43*

Los principios deben incorporarse a los procesos comerciales. A medida que trabaje con esta guía práctica, revise y establezca dónde encajan los principios y las políticas de su organización en sus operaciones. ¿Existen documentos o pasos transferible —como listas de verificación, marcos de evaluación de riesgos o herramientas de selección— relacionados con la responsabilidad en la gestión de datos, que quizás podría necesitar incorporar en algún proceso actual? ¿Hay alguien a quien acudir para recibir consejos cuando tenga dudas?

Algunas organizaciones podrían considerar la creación de un comité interno de ética de datos que revise el uso ético de los datos y otros aspectos éticos de los programas. En el siguiente enlace puede encontrar orientación sobre cómo **establecer un comité de ética** que revise el uso responsable de datos y tecnología.

ENTENDER LA ECONOMÍA POLÍTICA DE LOS DATOS EN SU CONTEXTO OPERATIVO

Los datos son poder. En la mayoría de los contextos humanitarios, quien controla más datos tiene más poder y toma el control de la respuesta. Esto puede significar que las agencias compitan por los datos y presionen para adoptar ciertos sistemas para centralizar su gestión. Las agencias que poseen la mayor cantidad de datos o que promueven sus sistemas como el predeterminado, tienden a estar en mejor posición para acceder a fondos. Entidades individuales que poseen gran volumen de datos también pueden negociar más fácilmente con las autoridades locales en situaciones en las que los PTM humanitarios se integran con los esfuerzos gubernamentales de protección social. En una época en la que los fondos son cada vez más escasos para el trabajo asistencial, los datos son una fuente de tensión debido al poder y a la financiación que pueden conferir.

CASILLA 6: ¿QUÉ ES UN "ANÁLISIS DE ECONOMÍA POLÍTICA" (PEA)?

Un Análisis de economía política (PEA, por sus siglas en inglés) es una forma estructurada de examinar las dinámicas de poder y la influencia de las fuerzas económicas y sociales en un contexto determinado. El PEA es un proceso de comprensión de las dinámicas contextuales y de cómo las diferentes intervenciones, o las posibles intervenciones (incluyendo las humanitarias), podrían interactuar con esas dinámicas, e influenciarlas. El PEA incluye una reflexión sobre aspectos como los siguientes:

- influencias fundacionales (como la historia o la geografía);
- impacto de eventos inmediatos y actores (como cambios en el liderazgo o desastres naturales);
- y el marco institucional (incluyendo leyes formales y prácticas informales) que conforma los comportamientos y los resultados observados.

El PEA motiva a los profesionales a tomar en cuenta estas dinámicas, incentivos e intereses y a reflexionar sobre el modo en que ellos podrían ayudar a informar la práctica operativa. Los actores de los PTM pueden querer abarcar el contexto nacional o regional, así como las dinámicas de poder y las fuerzas económicas y sociales, que entran en juego en una respuesta humanitaria, incluidos los PTM.[12]

Los gobiernos también están interesados en los datos por diversas razones. Esto incluye tanto los beneficios de los datos para mejorar los programas y la toma de decisiones, como los usos menos positivos, tales como la manipulación de las listas de las personas beneficiarias de los PTM, compitiendo por el poder con otros actores no estatales durante conflictos, o la identificación nociva de personas o grupos. El sector privado y los PSF también podrían tener interés en acceder a los datos con el fin de identificar a posibles nuevos clientes a quienes ofrecer sus productos y servicios, realizar investigaciones y desarrollar nuevos productos, o monetizar los datos vendiéndoselos a otras personas.

Comprender el papel que desempeñan los datos en el contexto de trabajo es importante para determinar los posibles riesgos y daños que podrían resultar de la recopilación, el tratamiento y el intercambio de datos. Esto, a su vez, podría ayudar a resaltar las áreas en las que hay espacio para negociar una mayor responsabilidad en la gestión de datos. Realizar un "Análisis de la economía política de los datos" en relación con los PTM es una manera de establecer algunas de las dinámicas subyacentes que afectan el acceso y control de los datos. Un PEA de los datos puede ser realizado por un monitor independiente, un consultor externo y, en algunos casos, por un socio del sector privado. Los grupos de trabajo de transferencias monetarias (Cash Working Groups) que funcionan bien, pueden servir como espacio neutral donde debatir el PEA

12 Menocal, A. et. al (2018) 'Thinking and Working Politically through Applied Political Economy Analysis: A Guide for Practitioners'. (Traducción - Pensar y trabajar políticamente mediante el análisis de la economía política: Guía para profesionales). USAID.

de los datos y acordar enfoques colectivos sobre los datos que beneficien a la población afectada, en lugar de enfoques que están orientados a servir a las agendas de determinados organismos o gobiernos. Las agencias menos poderosas querrán realizar un PEA de los datos por cuenta propia y utilizarlo para encontrar estrategias que les permita navegar por las dinámicas de poder de los PTM. Otra posibilidad es realizar un PEA del contexto más amplio y general. En este caso, se debe incluir un análisis del PEA de los datos como uno de sus objetivos analíticos.

CASILLA 7: EJEMPLOS DE PREGUNTAS PARA REALIZAR UN ANÁLISIS DE ECONOMÍA POLÍTICA DE DATOS PARA LOS PTM[13]

- **Roles y responsabilidades.** ¿Quiénes son los principales grupos de interés? ¿Cuáles son los roles y mandatos, formales o informales, de los distintos actores? ¿Cuál es el equilibrio entre los distintos actores en el control de los datos?
- **Propiedad de la estructura y financiamiento.** ¿Cuál es la estructura de una respuesta de PTM? ¿Cuál es el equilibrio entre agencias, gobiernos y otros actores en términos de control de los datos y el acceso a ellos? ¿Cómo se financian los PTM y quién los financia? ¿Cuáles son los intereses de quienes proveen fondos a los PTM o los financian? ¿De qué manera están influenciados por otras agendas (por ejemplo, austeridad, preocupación por el fraude y la financiación de los contribuyentes, alianzas a nivel global e intereses particulares de ciertos países en el desarrollo o en la situación política de otros países)? Si una agencia posee y financia todos los PTM, ¿qué significa eso para la responsabilidad de los datos?
- **Dinámicas de poder.** ¿En qué medida el poder está en manos de individuos, agencias o grupos específicos? ¿De qué manera los diferentes grupos de interés (PSF, agencias de la ONU, RCRCM, ONG internacionales, ONG, empresas de tecnología y datos, poblaciones afectadas, gobiernos, medios de comunicación, fiscalizadores, etc.) tratan de influir en la gestión de los datos y quién accede a ellos y los controlan?
- **Legados históricos.** ¿Cuál es la historia de los diferentes actores en este contexto de programas o en este país? ¿Cuáles son las relaciones históricas de los distintos actores? ¿Cómo influye esto sobre las percepciones actuales de las partes interesadas?
- **Corrupción y búsqueda de beneficios.** ¿Existe corrupción, fraude o la búsqueda de beneficios en el sector humanitario, en programas de PTM o en el país en general? ¿Qué papel desempeñan los datos en ello? ¿Dónde tiene mayor prevalencia esto (por ejemplo, al momento de la focalización, inscripción, entrega, contratación)? ¿Quién se beneficia más de ello? ¿Cómo está siendo utilizado el patrocinio?
- **Implementación y entrega de los PTM.** ¿Quiénes son los principales receptores de los PTM? ¿Se incluyeron o se excluyeron determinados grupos sociales, regionales o étnicos? ¿Se ofrecen subvenciones? ¿qué grupos se benefician más de estos?
- **Ideologías y valores.** ¿Cuáles son las ideologías y los valores dominantes que conforman las opiniones en torno al sector humanitario o a los PTM? ¿En qué medida pueden influir la forma en que se implementan los PTM?
- **Toma de decisiones.** ¿Cómo se toman decisiones en el sector humanitario o en los PTM? ¿Quién participa en estos procesos de toma de decisión?
- **Problemas en la implementación.** Una vez se toman las decisiones, ¿éstas se aplican? ¿Dónde están los principales cuellos de botella del sistema? ¿La falta de aplicación se debe a la falta de capacidad o a otras razones de economía política?
- **Posibilidad de reforma.** ¿Quiénes podrían ser los "ganadores" y los "perdedores" de determinadas decisiones sobre el acceso y el control de los datos? ¿Quiénes se oponen a la configuración actual y quiénes se resistirían al cambio y por qué? ¿Qué podría negociarse para superar esta oposición?

Dependiendo de la situación, podría realizar un PEA más formal (por ejemplo, contratando a un tercero o acordando con socios la realización de uno en conjunto); o, si su equipo tiene experiencia en PTM y en el contexto, podría dirigir un taller de PEA con representantes de un grupo diverso de agentes de PTM, para extraer y evaluar temas principales.

Lo ideal sería integrar un PEA de datos (o aprender de éste) en su análisis de la situación de los PTM, en el estudio de conveniencia y viabilidad de los PTM, y en la evaluación de riesgos, beneficios y daños.

Debe orientar a los responsables de la toma de decisiones de su organización sobre los asuntos relacionados con los datos que deben tomarse en cuenta antes de firmar un contrato o un acuerdo para participar en una respuesta (por ejemplo, la decisión de "ir o no ir").

Es probable que deba hacer algo de promoción interna para concientizar más a los responsables de la toma de decisiones sobre la necesidad de estar "preparados en el tema de datos" antes de participar en un PTM.

13 Adaptado de la Guidance Note on Use of Political Economy Analysis for ADB Operations (2009) (Nota de orientación sobre el uso del análisis de la economía política para las operaciones del ADB) del Asian Development Bank. Véase la publicación completa para más información sobre el PEA. Fuentes: J. Moncrieffe y C. Luttrell. 2005. An Analytical Framework for Understanding the Political Economy of Sectors and Policy (Marco analítico para comprender la economía política de los sectores y los escenarios políticos) Arenas, Londres: Overseas Development Institute; V. Fritz, K. Kaiser y B. Levy. 2009. Problem-Driven Governance and Political Economy Analysis: Good Practice Framework (Gobernanza orientada hacia la solución de problemas y el análisis de la economía política: marco de buenas prácticas). Washington, DC: Banco Mundial.

DETERMINAR QUÉ MARCOS DE PRIVACIDAD DE DATOS NACIONAL U OTROS MARCOS JURÍDICOS APLICAN

Cada vez más, los países de todo el mundo están desarrollando o actualizando las leyes de privacidad de datos para adaptarse a las nuevas realidades de las sociedades digitales. Los actores de los PTM deben conocerlas y tener cuidado de cumplirlas. La revisión de la normativa sobre datos podría ya ser parte de su evaluación de normativas. De lo contrario, quizás quiera revisar áreas que se indican a continuación. Aunque, los mecanismos de rendición de cuentas de las leyes de privacidad de datos podrían ser débiles en algunos contextos, violar una ley de privacidad de datos podría conducir a que una organización sea multada, o a que se le prohíba operar en el país.

Las agencias con sede en Europa pueden estar sujetas al Reglamento General de Protección de Datos (RGPD) de la UE, que se considera que ofrece el nivel más alto de protección de datos del mundo. Las agencias como la ONU y el CICR disfrutan de ciertas protecciones legales con el fin de ayudarles a mantener la confidencialidad y la neutralidad en sus operaciones.[14] Si bien esta inmunidad significa que no están sujetas al RGDP, la ONU y el CICR tienen sus propias políticas de protección de datos a las que se atienen.

Puede ser complicado manejar múltiples jurisdicciones legales en una respuesta. Trabajar con equipos jurídicos y trazar un mapa de los lugares donde los datos cruzan las fronteras y a las poblaciones a las que se refieren, puede ayudarle a cumplir con estas leyes y combinaciones de leyes. Algunos contextos, por ejemplo, Bangladesh y Filipinas, tienen ciertos requisitos que entran en conflicto con el RGPD. Además, algunas regulaciones requieren que se realicen Evaluaciones de impacto sobre la privacidad de los datos (EIPD) si se alcanzan ciertos umbrales con relación al tipo y a la cantidad de datos recopilados y procesados, el nivel de sensibilidad de los datos o si se recopilan datos de poblaciones vulnerables. También pueden exigir evaluaciones que demuestren que la recopilación y el tratamiento de datos no conducen a daños, ni vulneran otros derechos, como el derecho de privacidad.

Algunas legislaciones nacionales incluyen regulaciones relacionadas con la transmisión de datos. La transmisión de datos puede producirse internamente, o entre oficinas a nivel nacional o entre países. En todos estos casos, existen normas especiales para proteger la privacidad y la seguridad de los datos personales o sensibles que están siendo transferidos. Cuando las transferencias de datos ocurren entre países, se le denomina *transferencia de datos transfronteriza*. Algunos países tienen leyes dirigidas a limitar las transferencias de datos transfronterizos. Kenia, por ejemplo, ha promulgado una ley sobre la localización de datos que limita el tipo de datos que pueden transferirse fuera del país. La UE también tiene normas específicas respecto a dónde y cuándo pueden transferirse los datos de ciudadanos de la UE, fuera de la UE. Algunos países requieren una copia de los datos almacenados a nivel local, o que los datos se procesen en el país, o que se obtenga el consentimiento del gobierno antes de transferir los datos fuera. Las organizaciones internacionales también tienen normas respecto a cuándo y dónde puede ocurrir la transmisión transfronteriza.

En algunas ocasiones, las organizaciones podrían encontrar riesgos asociados con mantener datos almacenados en el país, por ejemplo, si un gobierno está persiguiendo a un conjunto específico de personas o de grupos, y las autoridades podrían utilizar estos datos para identificar o localizar a estos grupos, o si la situación de seguridad se ha deteriorado al grado que la organización no siente que puede mantener los datos seguros y protegidos en el país. En estos casos, las organizaciones deben tomar decisiones difíciles respecto al cumplimiento de las leyes frente a poner en riesgo a las personas y podrían decidir evitar la recopilación de datos.

CASILLA 8: ASPECTOS CLAVE A REVISAR EN RELACIÓN A LA PRIVACIDAD Y LA SEGURIDAD DE LOS DATOS EN LAS REGULACIONES SOBRE PRIVACIDAD

- Tipos de datos contemplados en las leyes y políticas
- Restricciones sobre los tipos de datos que pueden recopilarse
- Requisitos para comprender y evaluar el riesgo y el impacto sobre los derechos de las personas
- Normativas específicas sobre los datos de los niños u otros datos de categoría especial, como los datos biométricos
- Especificaciones sobre el intercambio de datos
- Responsabilidades/obligaciones para quienes recopilan datos versus a quienes procesan los datos
- Restricciones sobre la posibilidad de transferir los datos fuera del país
- Restricciones sobre dónde y cómo se pueden almacenar los datos y por cuánto tiempo
- Normas relativas a si los gobiernos deben tener acceso a los datos
- Orientación sobre cómo recopilar y registrar los consentimientos
- Multas y otras medidas punitivas que pueden aplicarse a causa del mal manejo de los datos
- Derechos de los "interesados" (las personas cuyos datos están siendo recopilados o procesados)
- Mecanismos necesarios para manejar reclamaciones
- Indicaciones sobre cuándo, cómo y a quién deben notificarse las violaciones de datos
- Requisitos para contratar o asignar un responsable de protección de datos

14 Uno de los privilegios y de las inmunidades de las que disfruta el CICR y las agencias de la ONU incluye la inmunidad ante el proceso judicial. En los territorios donde operan, los gobiernos no tienen acceso a sus instalaciones, documentos ni datos. Su personal está exento de ser testigo o de ofrecer evidencia en procesos judiciales. Véase la Convention on the Privileges and Immunities of the UN (1946) (Convención sobre los privilegios e inmunidades de la ONU) para conocer ejemplos y leer más información sobre la capacidad legal del CICR.

Además de las leyes de privacidad, la legislación nacional derivada del Grupo de acción financiera internacional (GAFI)[15] o de las normas de diligencia debida del consumidor, conocidas como los requisitos de Conocimiento del cliente (KYC, por sus siglas en inglés) puede obligarle a recopilar cierta información con el fin de realizar transferencias monetarias (véase la hoja de orientación 3 para obtener más información sobre el GAFI y los requisitos de KYC).

Trabaje con el equipo legal, de privacidad y de informática y tecnología de su organización para encontrar opciones para la transmisión y el almacenamiento de los datos. Revise dónde y cómo transmiten y almacenan los datos los terceros con los que trabaje.

La publicación de la Information Technology and Innovation Foundation (ITIF) **Cross-Border Data Flows: Where are the Barriers and What Do They Cost?** (Flujo de datos transfronterizo: ¿dónde se encuentran las barreras y cuánto cuestan?) ofrece una lista (a partir del 2017) de los países que cuentan con políticas o leyes de localización de datos. También puede referirse a la publicación de DLA Piper, **Data Protection Laws of the World** (Leyes de protección de datos del mundo) (continuamente actualizada) o de Deloitte (2017), **Privacy is Paramount: Personal Data Protection in Africa** (La privacidad es fundamental: la protección de los datos personales en África).

Es posible que deba sopesar elecciones y contrapartidas difíciles, por ejemplo, si se le exige legalmente intercambiar datos con gobiernos y usted teme que esto podría poner en riesgo a las poblaciones afectadas o influir sobre el nivel de confianza en su organización. Véase la publicación del CaLP, **'Data Sharing with Governments'** (Intercambio de datos con los gobiernos).

INVESTIGAR LOS REQUISITOS DE CUMPLIMIENTO DE DATOS, SISTEMAS Y SUBSIDIOS DE DONANTES

Los donantes exigen cada vez más a los actores de los PTM que se coordinen y compartan datos. Los donantes también pueden tener requisitos específicos sobre los tipos de datos que las organizaciones deben recopilar y compartir, o sobre cómo esperan que se protejan los datos. Estos requisitos suelen figurar en los acuerdos de financiación e influirán en el modo en que pueden manejarse y almacenarse sus datos. Algunos gobiernos donantes, por ejemplo, exigen que se investigue a las personas receptoras de los PTM o que se cumplan las Normas de lucha contra el terrorismo, o de lucha contra el blanqueo de dinero; requisitos que pueden poner en riesgo a las personas receptoras de los PTM debido a la cantidad de datos personales y sensibles recopilados para realizar estas verificaciones, a la falta de claridad respecto a quién tiene acceso a estos tipos de bases de datos y a la posibilidad de errores de inclusión o de exclusión. Otros exigen que se compartan con ellos determinados datos programáticos en formatos y plazos específicos, y las organizaciones deben anonimizar o tratar de otro modo los datos antes de compartirlos para que las personas receptoras de los PTM estén protegidas. Investigar los requisitos de datos de los donantes ya puede formar parte de sus evaluaciones de viabilidad; no obstante, a veces las organizaciones no conocen lo suficientemente de cerca los requisitos que se relacionan específicamente con los datos.

Además, para algunas subvenciones o alianzas, se espera que los socios ingresen datos en sistemas específicos de la ONU, por ejemplo, el SCOPE del PMA[16], el PRIME/ProGres del Alto Comisionado de las Naciones Unidas para los Refugiados/ACNUR[17] o el Primero de Unicef[18]. En otros casos, el intercambio de datos ocurre de manera bilateral entre las ONG a través de mandatos de consorcios, estructuras de gobernanza y acuerdos de intercambio de datos. Con frecuencia, los sistemas de la ONU están configurados para recopilar datos biométricos. El intercambio de datos y el uso de estos sistemas ha sido un aspecto que provoca tensión entre las agencias de la ONU y algunos socios implementadores que tienen inquietudes sobre la protección de los datos y solidez de la seguridad de ciertas plataformas de datos. Algunas ONG han expresado su frustración respecto a los desequilibrios de poder y al espacio para negociar en torno a los requisitos de la ONU, así como a los privilegios y las inmunidades de la ONU. El intercambio de datos y el uso de estos sistemas de datos está en constante cambio, con las conversaciones y negociaciones en curso, como telón de fondo. En la actualidad, el PMA, ACNUR y Unicef trabajan para encontrar maneras de hacer que sus sistemas sean interoperables entre sí y con los gobiernos, lo que ha suscitado la preocupación por la responsabilidad en la gestión de datos entre los socios implementadores.

Es importante que en la fase previa a la propuesta se entienda cuáles son los requisitos de los donantes, y si estos se alinean con lo que su organización está y no está dispuesta a hacer. Al realizar una investigación antes de desarrollar una propuesta, podrá decidir si seguir adelante y/o cómo negociar los requisitos de datos de los donantes.

Muchos donantes han expresado que están abiertos y dispuestos a cambiar los requisitos de datos, si se plantean inquietudes legítimas. Al investigar y luego enmarcar o documentar cualquier inquietud, tendrá un argumento más sólido con el cual acercarse a un donante para negociar.

Quizás enfrente obstáculos de otros sectores de su organización con un nivel de conciencia menor respecto a los riesgos que pueden suponer los datos durante la implementación. Es importante crear alianzas dentro de su organización con el fin de defender una mayor protección de los datos y una gestión responsable de los mismos y encontrar maneras de lograr la participación de equipos aliados, como son los de seguridad, protección, legal, informática y ciberseguridad, para conseguir mayor apoyo a la responsabilidad en la gestión de datos.

15 Véase la publicación del Grupo de Acción Financiera (2020) 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: "The FATF Recommendations" (Normas internacionales para combatir el lavado de dinero y la financiación del terrorismo y la proliferación: recomendaciones del GAFI).
16 Véase el sistema SCOPE del Programa Mundial de Alimentos.
17 Véase la publicación del Alto Comisionado de las Naciones Unidas para los Refugiados Guidance on Registration and Identity Management - 3.6 Registration tools - Population Registration and Identity Management Eco-System (PRIMES) (Lineamientos sobre el registro y la gestión de la identidad 3.6 Ecosistema de registro de la población y gestión de la identidad [PRIMES]).
18 Véase el sitio web de Primero de la Unicef.

REVISIÓN DE LA CAPACIDAD DE GESTIÓN DE DATOS DE LA ORGANIZACIÓN

Las respuestas humanitarias, incluidos los PTM, dependen de múltiples actores, y la protección de datos es únicamente tan segura como el eslabón más débil. Fortalecer las políticas y prácticas de protección de datos se vuelve un tema cada vez más importante a medida que las organizaciones y las respuestas se digitalizan cada vez más, y recopilan e intercambian volúmenes mayores de datos sensibles.

Las organizaciones tendrán diferentes niveles de capacidad de gestión de datos. Esto no depende del tamaño de la organización, sino, de la importancia que le ha atribuido a este tema y de su acceso a financiación institucional en el transcurso del tiempo para mejorar la infraestructura y los sistemas de datos. **Es vital que las organizaciones no recopilen datos que no puedan mantener a salvo. Este es un concepto básico de la responsabilidad en la gestión de datos.**

Una revisión organizativa puede ayudarle a determinar si su organización y sus posibles socios tienen la capacidad de gestionar datos de manera responsable en el contexto en el que está trabajando. Esto deberá realizarse antes de firmar un compromiso formal o un compromiso de ofrecer los PTM en un contexto dado.

Puede realizar una evaluación exhaustiva de su madurez en la gestión de datos (o la de sus socios implementadores) utilizando el modelo **"Responsible Data Maturity Model for Development and Humanitarian Organizations model"** (Modelo de madurez en la gestión responsable de los datos para organizaciones de desarrollo y de ayuda humanitaria) creado para CARE. Una amplia revisión y fortalecimiento de la organización requiere tiempo y una inversión a largo plazo.

Si su organización no puede realizar una evaluación completa o separada, podría incluir una sección sobre la capacidad de responsabilidad en la gestión de datos en su evaluación general de viabilidad de los PTM. La plantilla en la casilla 9 que aparece a continuación, puede servirle para identificar las preguntas básicas que deben incluirse.

Esta **lista de verificación imprimible de la Electronic Frontier Foundation** puede ayudar a evaluar la capacidad de un socio para ofrecer seguridad y privacidad de datos al procesarlos. También es útil para evaluar a un tercero o un PSF.

Este **conjunto de preguntas** sirve de guía para consultar sobre el cumplimiento con el RGPD de un tercero o de un proveedor.

DECIDIR SI "IR, O NO IR"

En base a las investigaciones y análisis anteriores, destinadas a comprender mejor su contexto y capacidades, determine a un alto nivel si debe pasar o no a la etapa de propuesta o asociación y si debe participar en una respuesta en particular.

Como se ha señalado, si su organización ya realiza evaluaciones de viabilidad, capacidad o riesgo, los aspectos anteriores pueden integrarse a esas evaluaciones. Es importante que la responsabilidad de los datos se evalúe específicamente para estar seguro de que se tiene en cuenta en el proceso de toma de decisiones. Esta podría ser una nueva área de consideración para su organización y quizás requiera incidir ante los responsables de adoptar decisiones como tema de debate en la etapa previa a la propuesta. **Es importante destacar que a lo mejor algunos proyectos deban interrumpirse después de esta etapa de análisis inicial, o que sea necesario encontrar modalidades que no recopilen datos sensibles porque la organización o la respuesta carecen de la capacidad para recopilarlos de manera segura.**

Si su organización aún no cuenta con una plantilla o un proceso para determinar si se debe seguir adelante o no, en función del contexto y la capacidad de los datos, puede utilizar la plantilla en la casilla 9 que figura a continuación. Cuando rellene la plantilla, clasifique la posición actual de su organización y haga recomendaciones sobre medidas de mitigación que podrían cambiar la decisión de "no ir" por la de "ir". Si ya dispone de un proceso, puede incorporar las preguntas que figuran a continuación para estar seguro de abarcar la responsabilidad en la gestión de datos en las evaluaciones iniciales.

CASILLA 9: EVALUACIÓN RÁPIDA PARA "IR, O NO IR"

Si su organización aún no dispone de procesos, o necesita una plantilla de evaluación rápida, esta herramienta para decidir "ir, o no ir", podría serle de utilidad. La puede utilizar para calificar su confianza en que su organización puede gestionar los datos de forma responsable en el contexto de esta respuesta. Luego, en las casillas, ofrezca comentarios sobre por qué tiene o no confianza, y sugiera las estrategias que habría que adoptar para mejorar la confianza, por ejemplo, evaluar las habilidades, las capacidades y los recursos. Utilice las respuestas como parte de sus criterios de decisión o compártalas con quienes estén negociando su participación en la financiación. Debe intentar obtener datos de un grupo diverso, incluido personal del equipo legal, seguridad, protección, informática y ciberseguridad, datos o MEAL, y personal en primera línea. El responsable de la protección de datos y el comité de ética (u otra función similar) de su organización deberían revisar esta plantilla y apoyar la toma de decisión. Esta plantilla también puede utilizarse para evaluar el nivel de confianza en sus socios.

NIVELES DE CONFIANZA (destrezas, capacidades, recursos)	**BAJO**	**MEDIANO**	**ALTO**
Sabemos cómo serán utilizados los datos y hemos identificado a todas las partes que tendrán acceso a estos.			
Hemos evaluado la viabilidad de trabajar en este contexto sin colocar a las personas beneficiarias de los PTM, a nuestra organización o al personal, en un nivel inaceptable de riesgo de sufrir daños a causa de los datos.			
Podemos cumplir con los marcos jurídicos nacionales y globales.			
Podemos mantener la seguridad de los datos a la vez que cumplimos con los marcos legales nacionales y globales.			
Podemos cumplir con los requisitos de protección de datosde los donantes.			
Podemos mantener la seguridad de los datos a la vez que proporcionamos a los donantes los datos que necesitan.			
Podemos mantener la seguridad de los datos en los sistemas que nos exigen utilizar los donantes o los socios.			
Tenemos la capacidad de manejar los sistemas que nos exigen utilizar.			
Tenemos la capacidad general de gestionar los datos de una manera responsable en este contexto.			
Nuestros socios tienen la capacidad de gestionar los datos de una manera responsable en este contexto.			

HOJA DE ORIENTACIÓN 2

DISEÑO Y PLANIFICACIÓN

Una vez se ha tomado una decisión de alto nivel respecto a si el contexto operativo, la capacidad y las condiciones organizacionales relacionados con los datos permiten una respuesta responsable de los PTM (según la hoja de orientación 1) se debe diseñar el plan de recopilación y gestión de datos para la respuesta general. En esta fase, se incorporan las evaluaciones de contexto y de capacidad de la hoja de orientación 1. Ahora es el momento de diseñar su propuesta de los PTM y de configurar cómo gestionar los datos en el transcurso de la respuesta (las hojas de orientación 3–7 le ayudarán a elaborar los detalles de cada etapa del ciclo de vida de los datos). En esta fase quizás también realice evaluaciones de viabilidad, revisión adicional de las regulaciones, una evaluación de mercado, una evaluación de PSF, evaluaciones de necesidades y de vulnerabilidad, y tome decisiones respecto a las modalidades de los PTM más adecuadas y seguras para el contexto.[19]

Identificará a los socios y otros terceros con quienes trabajará, los sistemas que utilizará, qué aspecto tendrá el proceso general y si los PTM humanitarios se vincularán con los sistemas de protección social gubernamental. En todos estos esfuerzos, es necesario evaluar la responsabilidad en la gestión de datos. A la vez, varios factores relacionados con la responsabilidad en la gestión de datos deben influir en las decisiones sobre el diseño y la ejecución de un programa y si es seguro recopilar ciertos tipos de datos o si el riesgo relacionado con los datos es demasiado alto para las poblaciones afectadas, los trabajadores en terreno y los encuestadores, o para su organización en general.

Durante la fase de diseño y planificación, se establecerán cada uno de los procesos de datos que se producirán a lo largo de la respuesta —desde las evaluaciones de necesidades pasando por la focalización, el registro y la inscripción, y la entrega hasta el MEAL y la retroalimentación de las poblaciones afectadas— y cómo gestionar los datos de manera responsable. El diseño y la planificación de la gestión responsable de los datos le permitirán comprender cómo podría ser su respuesta con un enfoque totalmente maduro hacia la responsabilidad en la gestión de los datos, para adaptarse al tiempo y a los fondos disponibles, e identificar áreas de mejora a lo largo del tiempo.

A medida que se desarrollan las capacidades, habilidades y prácticas, de manera ideal, la responsabilidad en la gestión de datos se convertirá en una forma de pensar y no en una carga.

La hoja de orientación 2 abarca el diseño y la planificación. En la hoja de orientación 1 habrá realizado el trabajo a gran escala y ahora debe entrar en más detalle sobre cómo será la respuesta en la práctica. Esto se reflejará en su diseño de propuesta, el presupuesto, la elección de socios y otras decisiones relacionadas con la planificación.

19 Véase Mercy Corps "Cash Minimum Standards Policy" (Políticas de estándares mínimos en asistencia de efectivo) donde encontrará un resumen de las diversas evaluaciones y estándares que Mercy Corps incorpora a cada fase de una respuesta de PTM.

DETERMINAR SI UTILIZAR DATOS EXISTENTES O RECOPILAR DATOS NUEVOS

Como parte del proceso de diseño y planificación, es importante determinar si será necesario realizar un proceso completamente nuevo de recopilación de datos, o si existen listas o conjuntos de datos que pueden utilizarse para la selección, inscripción o entrega. Si estas listas están desactualizadas, son de baja calidad o han sido alteradas de una manera no autorizada, o únicamente abarcan cierta parte de la población, deben ser complementadas con datos adicionales o con un nuevo ejercicio de recopilación de datos. La duplicación de datos entre las listas nuevas y existentes puede ser un problema. En este caso, será necesario comparar las listas y evaluar la situación. Puede ser un reto que los sistemas no sean interoperables. En algunas respuestas, es posible que una organización o agencia ya haya comparado y recopilado listas y datos; no obstante, aún puede ser buena idea abogar por que los datos se actualicen, se revisen en cuanto a su calidad o sean más inclusivos.

Si su respuesta está vinculada con una iniciativa de protección social existente, será necesario armonizar los datos de las organizaciones humanitarias con los datos gubernamentales. Esto plantea preocupaciones respecto al acceso de los gobiernos a las listas de las organizaciones humanitarias. Por ejemplo, las listas de desplazados internos (IDP por sus siglas en inglés), refugiados e inmigrantes, podrían suponer un riesgo de focalización, detención, deportación u otros tipos de abuso de los gobiernos. Si tiene planes de utilizar datos existentes, es importante revisar los aspectos legales relacionados con el acceso y el uso de los datos captados para cumplir un propósito para el cual no fueron recopilados. (Véase la hoja de orientación 2, casillas 12 y 13 sobre las bases legales para el tratamiento de datos).

La COVID-19 ha presionado a muchas agencias a utilizar conjuntos de datos existentes y a realizar innovaciones en los PTM humanitarios y los esquemas de protección social. Algunas de estas innovaciones se presentan en el sitio web SocialProtection.org y en esta **entrada de blog** en particular.

Mercy Corps ofrece unos **lineamientos sobre distintos tipos de datos que pueden utilizarse o reutilizarse para la selección remota**, junto con las **ventajas y desventajas** de cada fuente.

Véase el **estudio de caso sobre enfoques emergentes para el uso de datos no tradicionales para la identificación en los PTM** de CaLP.

El GovLab documentó la manera en que realizó una **"asamblea de datos"** con el fin de comprender mejor los casos en los que los residentes de la ciudad de Nueva York se sentirían cómodos con el acceso y la reutilización de sus datos personales durante la crisis de la COVID-19. Esta metodología podría también utilizarse en otros contextos.

DECIDIR QUIÉN(ES) EJERCERÁ(N) DE CONTROLADOR(ES) DE DATOS Y PROCESADOR(ES) DE DATOS

Al inicio de una respuesta de PTM es vital comprender quién ejercerá de controlador de datos y quién ejercerá de procesador de datos, o si habrá controladores de datos conjuntos. El controlador de datos es el ente que toma decisiones sobre el modo de procesar los datos personales. El procesador recibe instrucciones del controlador respecto a qué datos personales recopilar y cómo procesarlos. Cuando las organizaciones actúan como controladores corresponsables, deciden juntos los fines y medios del tratamiento de los mismos datos personales.

CASILLA 10: ROLES Y RESPONSABILIDADES DE LOS CONTROLADORES DE DATOS Y LOS PROCESADORES DE DATOS

Las obligaciones de una organización con respecto a los datos dependen del papel que estas desempeñan en la recopilación y el tratamiento de datos. Por ejemplo, con arreglo al RGPD, las personas y las autoridades supervisoras pueden responsabilizar tanto a los controladores como a los procesadores por no cumplir con sus responsabilidades en virtud del RGPD.

Controlador de datos: se denomina controlador de datos a una entidad que, sola o en conjunto con otros, ejerce el control sobre los propósitos y los medios para procesar los datos personales. Los controladores ostentan el mayor nivel de responsabilidad en el cumplimiento de los aspectos relacionados con los datos. Ellos deben demostrar el cumplimiento con los principios de protección de datos y otros requisitos del RGPD. También son responsables del cumplimiento de sus procesadores de datos. Las autoridades supervisoras y los individuos pueden tomar medidas en contra de un controlador con respecto al incumplimiento de una de sus obligaciones. Los controladores de datos son quienes:

- deciden recolectar o procesar los datos personales;
- deciden cuál será la finalidad o el resultado del tratamiento;
- deciden qué datos personales deben recopilarse;
- deciden sobre qué personas recopilar datos personales;
- obtienen ganancia comercial u otro beneficio del tratamiento, salvo cualquier pago por servicios de parte de otro controlador;

CASILLA 10: ROLES Y RESPONSABILIDADES DE LOS CONTROLADORES DE DATOS Y LOS PROCESADORES DE DATOS (CONTINUACIÓN)

- procesan los datos personales como resultado de un contrato entre nosotros y la persona a la que se refieren los datos;
- toman decisiones sobre las personas interesadas como parte o como resultado del tratamiento;
- ejercen su criterio profesional en el tratamiento de los datos personales;
- tienen una relación directa con las personas a las que se refieren los datos;
- disfrutan de una completa autonomía respecto al modo en que se procesan los datos personales;
- han nombrado a los procesadores para procesar los datos personales en su nombre.

Controlador conjunto: Cuando dos o más controladores de datos determinan de manera conjunta los fines y la manera de procesar los mismos datos personales, se les denomina controladores conjuntos. No obstante, no se consideran controladores conjuntos si procesan los mismos datos para diferentes fines. Los controladores conjuntos deben coordinar entre sí quién asumirá la responsabilidad principal de cumplir con las obligaciones del RGPD, y en especial, con las obligaciones de transparencia y los derechos de las personas. Todos los controladores conjuntos siguen siendo responsables de cumplir con las obligaciones del controlador con arreglo al RGPD. Tanto las autoridades supervisoras como los particulares pueden tomar medidas en contra de un controlador con respecto al incumplimiento de una de esas obligaciones. Las organizaciones se consideran controladoras conjuntas, cuando ocurre alguno de los siguientes casos:

- tienen un objetivo común con otros controladores con respecto al tratamiento;
- procesan los datos personales con la misma finalidad que otro controlador;
- utilizan el mismo conjunto de datos personales (por ejemplo, una base de datos) para este tratamiento, que otro controlador;
- han diseñado este proceso con otro controlador;
- tienen normas de gestión de información comunes con otros controladores.

Procesador de datos: Se denomina procesador de datos a una entidad que procesa datos personales en nombre de un controlador de datos o con arreglo a las instrucciones de un controlador. Los procesadores de datos no tienen una finalidad o propósito personal para procesar los datos. Los procesadores no tienen las mismas obligaciones que los controladores con arreglo al RGPD y no tienen que pagar una tarifa de protección de datos. No obstante, los procesadores sí tienen obligaciones directas en arreglo al RGPD. Tanto las autoridades supervisoras como los particulares pueden tomar medidas en contra de un procesador con respecto al incumplimiento de una de esas obligaciones. Los procesadores de datos son quienes:

- cumplen las instrucciones de otra persona con respecto al tratamiento de datos personales;
- reciben los datos personales de un cliente o de un tercero o se les dice qué datos recopilar;
- no toman la decisión de recopilar datos personales de los individuos;
- no deciden qué datos personales deben recopilarse de los individuos;
- no deciden la base jurídica para el uso de esos datos;
- no deciden para qué fines se utilizarán los datos;
- no deciden si divulgar los datos, ni a quién;
- no deciden por cuánto tiempo conservar los datos;
- toman ciertas decisiones sobre el modo de procesar los datos, pero implementan estas decisiones con arreglo a un contrato con otra persona;
- no tienen interés en el resultado final del tratamiento.

(Las definiciones y las listas de cotejo fueron tomadas de la Information Commissioner's Office of the UK (Oficina del Comisionado de Información del Reino Unido) y mínimamente adaptadas).[20]

Determinar las funciones (controlador y procesador) es importante para los aspectos posteriores, tales como los acuerdos de intercambio de datos y los protocolos de transferencia de información. También es importante que, a medida que se ponga en marcha la respuesta, sea evidente quién asume la responsabilidad y rinde cuentas de determinados aspectos del tratamiento de datos. Esta información también será necesaria para informar a las personas y comunidades sobre el modo en que se manejarán sus datos.

Véase esta explicación detallada de las responsabilidades de los controladores de datos y procesadores de datos con arreglo al RGPD.

20 Information Commissioner's Office of the UK (2018) 'Guide to the General Data Protection Regulation: Controllers and Processors' (Guía para las Regulaciones Generales de Protección de datos: controladores y procesadores).

CASILLA 11: ESCENARIOS DE TRABAJO COMÚN DE LOS CONTROLADORES DE DATOS Y PROCESADORES DE DATOS

Para poder determinar quién es el controlador de datos y quién es el procesador de datos, será necesario responder a la siguiente pregunta, "¿quién toma las decisiones respecto a los sistemas que se utilizan y los datos que se recopilan?"

A continuación, ilustramos algunos posibles escenarios para la relación entre controlador y procesador.

Cuando participan un donante o una agencia de la ONU y sus socios implementadores, es posible ver uno de los siguientes escenarios:

- un donante no interventor/agencia de la ONU o una financiación que se autoabastece —el socio implementador actúa como controlador—;
- un donante normativo o una entidad de la ONU que exigen sistemas/enfoques/datos específicos —el donante actúa como controlador, el socio implementador (receptor del financiamiento) como procesador—.

En cierta medida, esta podría ser una decisión política. Aquellos socios implementadores que se sientan más fundamentados que sus donantes/agencia de la ONU, podrían querer actuar como controladores, o si prefieren reducir la responsabilidad, querrán que su donante/agencia de la ONU ejerza como controlador.

Entre ONG y ONG internacionales:

Esto podría ser muy sencillo o podría convertirse en algo más complicado si la ONG o la ONG internacional trabaja en alianza con otros, por ejemplo, un programa relacionado con un consorcio. Algunos escenarios incluyen:

- La ONG o la ONG internacional trabajan en gran parte con su propio personal sobre el terreno y una programación en papel/digital de 'circuito cerrado'. En este caso, el proceso finaliza aquí.
- En un consorcio muy plano en el que los roles son casi indistinguibles, es posible contar con controladores de datos conjuntos. Sin embargo, los equipos jurídicos pueden sentirse incómodos con esto debido a la cantidad de responsabilidades que presenta, porque se puede utilizar a cualquiera de los miembros de los controladores de datos conjuntos por el incumplimiento de cualquier otro. A los equipos de privacidad y a los equipos en el terreno quizás les parezca complejo comunicarse unos con otros en esta situación, pues inevitablemente tienen una propensión al riesgo muy distinta.
- Cuando un miembro del consorcio asume claramente el liderazgo, este podría ser el controlador o el procesador principal y emitir sub-financiaciones a otros socios. En esta configuración, el líder carga con el mayor riesgo de responsabilidad en caso de vulneración de datos.
- Cuando el consorcio tiene roles bastante separados (por ejemplo., el miembro A se encarga de la seguridad alimentaria y el miembro B presta asesoría jurídica), podrían ser controladores distintos ("Controladores en común") y limitarse a celebrar acuerdos de intercambio de datos ("para disipar dudas").

Participación de PSF:

Cuando participen un PSF es probable que se presenten dos posibilidades:

- el PSF tiene sus propias obligaciones (por ejemplo, KYC, o además vende servicios de consumo a las personas beneficiarias por medio de tarjetas en circuito abierto) —en cuyo caso podría ser un controlador aparte—. En este caso, al igual que las "funciones separadas", podría realizarse un acuerdo de intercambio de datos para disipar dudas/un controlador común. En este caso lo ideal sería realizar una evaluación de riesgos para determinar posibles responsabilidades y estrategias de mitigación de riesgo que podrían introducirse al involucrar o aceptar a un PSF.
- el PSF tiene pocas o no tiene obligaciones (raro, pero posible. Un proveedor de servicio, como un proveedor de software/hardware para los PTM, también podría caer en esta categoría) —en este caso el PSF podría ser un simple procesador—. También podría darse el caso de que sea un procesador para algunas actividades, pero un controlador para otras (por ejemplo, los clientes posiblemente ya tengan tarjetas de débito para las cuales el banco es el controlador, pero para algunas actividades actúan como procesador para una ONG internacional).

DETERMINAR UNA BASE JURÍDICA PARA EL TRATAMIENTO DE DATOS ANTES DE RECOPILAR DATOS PERSONALES O SENSIBLES

Para procesar datos personales o sensibles, es necesario haber identificado una base jurídica o legal. Puede ser útil pensar en la base jurídica para la recopilación de datos como un portal ético y legal clave para la actividad general de los datos —casi como una prueba de utilidad social que, en caso de fallar, sugiere que un uso particular de los datos puedo no ser lo mejor para la comunidad o las personas afectadas—. En las leyes nacionales, las bases jurídicas tienden a centrarse en el equilibrio entre los derechos de las personas y de los grupos y el "locus de la agencia" —o sea, el lugar donde reside el control, el poder y la misión—.

En algunos contextos, la base jurídica es muy simple y se enfoca por completo en una elección individual. En las leyes europeas y en contextos similares, la base jurídica es más matizada y ofrece distintas vías que reconocen que a veces no es posible tener una elección, por ejemplo, cuando existe una necesidad pública imperiosa, un requisito vital u otro motivo que hace necesario recopilar y procesar datos. Cuando no es posible hacer una elección, con frecuencia hay requisitos de seguimiento adicionales que deben cumplir quienes desean recopilar y procesar datos para garantizar que no se infrinjan otros derechos.

Por estos motivos, la elección correcta de la base jurídica no solo sirve como importante salvaguarda legal, sino que es un principio esencial para reconocer y comprender dónde radica el poder y definir la raíz de su actividad en el propósito social.

CASILLA 12: BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS

Por ejemplo, el RGPD enumera seis bases jurídicas para el tratamiento de datos, como se indica a continución:

- **Intereses vitales:** el tratamiento es necesario para proteger la vida de alguien en una emergencia.
- **Función pública/Interés público:** el tratamiento es necesario para poder realizar una tarea de interés público o para realizar sus funciones oficiales y esta tarea o función tienen una clara base legal.
- **Consentimiento individual:** la persona le ha ofrecido un consentimiento claro para procesar sus datos personales para un propósito específico.
- **Intereses legítimos:** el tratamiento es necesario para sus intereses legítimos o para los intereses legítimos de un tercero, salvo que exista un buen motivo para proteger los datos personales del individuo que anule estos intereses legítimos.
- **Cumplimiento de un contrato:** el tratamiento es necesario para un contrato que celebró con la persona o porque la persona le pidió tomar medidas específicas antes de celebrar un contrato.
- **Obligación legal:** el tratamiento es necesario para cumplir con la ley (esto no incluye las obligaciones contractuales).

El CICR utiliza estos mismos fundamentos jurídicos básicos para recopilar datos personales, pero combina lo contractual y lo legal en una categoría. Antes de recopilar los datos debe determinarse la base jurídica. Esta base jurídica y la finalidad de la recopilacion de datos no pueden cambiarse en el trascurso de las actividades de recopilación y tratamiento de datos. Si esto ocurre, los datos que ya han sido recopilados deben volverse a recopilar y ser tratados de acuerdo con la base jurídica actualizada.[21]

Las bases jurídicas han sido motivo de un amplio debate en el sector humanitario, en especial con respecto a cuándo usar el consentimiento, y si usar o no el consentimiento frente a otras bases jurídicas. Por lo general, el debate se centra en los verdaderos retos de asegurar un consentimiento realmente fundamentado, voluntario y revocable en escenarios de asistencia humanitaria debido a las dinámicas de poder en situaciones humanitarias (incluidos los PTM), la falta de elección y la dificultad para explicar la manera en que los datos serán procesados y compartidos, entre otros aspectos. Este debate, junto con el estudio adicional de regulaciones, tales como el RGPD, ha llevado a las organizaciones a utilizar como base jurídica del Interés legítimo o la Función pública/Interés público, en combinación con un enfoque positivo y ético al consentimiento informado. Véase la casilla 13 donde encontrará una explicación detallada de las bases jurídicas y orientación sobre qué base jurídica podría ser la más apropiada para los PTM. *Debe señalarse que esta orientación no tiene carácter de asesoramiento legal, sino que su propósito es promover que la oficina de protección de datos y el equipo legal de su organización la consideren al tomar una decisión sobre las bases jurídicas.*

21 Estas bases jurídicas fueron tomadas del Reglamento General de Protección de Datos de la UE. Será necesario revisar la legislación nacional con el fin de determinar cuáles son las bases jurídicas para un país específico. Algunas organizaciones internacionales, como la ONU y el CICR, disfrutan de privilegios e inmunidades y cumplen con sus propios principios, políticas, procesos y normas de protección de datos.

CASILLA 13: ELECCIÓN DE UNA BASE JURÍDICA PARA EL TRATAMIENTO DE DATOS

Se ha debatido ampliamente el tema de las restricciones que presenta el consentimiento informado como base jurídica para el tratamiento de datos en situaciones de ayuda humanitaria. Un nuevo punto de vista que ha surgido es que otras bases jurídicas podrían ser más adecuadas que un consentimiento. Aquí exploramos en detalle ese nuevo punto de vista.

Con arreglo al RGPD, ciertas bases jurídicas probablemente no sean adecuadas para los PTM. Por ejemplo, es poco probable que la elección de intereses vitales sea una opción sólida, incluso para casos de uso en ayuda humanitaria.[22] Asimismo, las actividades de desarrollo o de ayuda humanitaria, por lo general, no son "requeridas por ley", lo que hace de la obligación legal una opción poco probable. Debido a que las agencias no suelen firmar contratos con las comunidades con las que trabajan, la opción de cumplimiento de un contrato (con personas) es improbable.

Esto deja tres bases jurídicas para las acciones humanitarias (incluidos los PTM), que se dividen en dos grandes grupos:

Grupo 1 – El consentimiento es la única base jurídica que coloca a la agencia sobre el individuo.

Grupo 2 – La función pública/interés público e interés legítimo– hacen énfasis en equilibrar los derechos de los individuos y las necesidades de las organizaciones o de la sociedad en su conjunto, expresadas a través de sus leyes y costumbres.

Consentimiento

A pesar de que el uso del consentimiento como base jurídica no elimina la necesidad de que las organizaciones sean responsables, seguras o consideren el riesgo, su uso defiende de manera eficaz que en el contexto donde se obtiene el consentimiento, las personas estén lo suficientemente empoderadas para hacer elecciones informadas y voluntarias. El RGPD describe que para que las personas entreguen su consentimiento, las organizaciones deben ofrecer opciones fundamentadas, revocables (reversibles) en circunstancias en las cuales la persona pueda negar o rechazar otorgar el consentimiento sin sufrir consecuencias negativas.

El uso del consentimiento como base jurídica en los contextos humanitarios o de desarrollo plantea varios desafíos, como se explica a continuación:

- dado que gran parte de la programación se centra en datos, probablemente habrá consecuencias si una persona no acepta proporcionar datos. Por ejemplo, si no se ofrece la asistencia sin una inscripción o un registro previo.
- es difícil ofrecer una elección genuina o libre, dado el desequilibrio de poderes presente, en especial en un contexto de ayuda humanitaria.
- es poco frecuente que pueda ofrecerse un "derecho al olvido" o una suspensión del consentimiento, en especial, cuando existan otros requisitos como conocimiento del cliente, desviación de la ayuda, auditoría, lucha contra el fraude o monitoreo, evaluación, rendición de cuentas y aprendizaje (MEAL), que podrían exigir la retención de datos personales o sensibles y por tanto, impedir "olvidarse" de la persona.

Interés legítimo/Función pública/Interés público

Cuando no se pueda ofrecer la posibilidad de elegir, pero la actividad sigue siendo deseable para cumplir con la misión de una agencia o para que un bien social continúe siendo reconocido como bien de interés público, entonces, ya sea el interés legítimo o la función pública/el interés público podrían ser bases jurídicas adecuadas.

Podría parecer que el interés legítimo y la función pública/interés público no pertenecen a la misma categoría, pero ambos representan un "interés" o una exigencia, según se explica a continuación:

- la Organización (interés legítimo) podría tener un interés en defender el imperativo humanitario o los objetivos del programa consagrados en los estatutos, los documentos constitutivos, la misión o los objetivos caritativos de una organización; por ejemplo, es posible que una organización tenga un *"interés legítimo en cumplir con objetivos caritativos al prestar una labor vital a las comunidades a través de la entrega de ayuda en especie a través de un PTM, el cual solicita el nombre y la situación de la persona receptora para poder evaluar y prestar esa asistencia';*
- Derecho y sociedad (función pública/interés público): Una "base de interés público" podría tener su origen en la financiación institucional de donantes nacionales con un mandato explícito de prestar asistencia vital.

Ni la justificación de recopilar datos por un interés legítimo o por un interés público invalida otras obligaciones legales o las buenas prácticas en la protección de datos. Permanecen las obligaciones de informar a las personas, de emplear "un límite del propósito" y de usar la mínima cantidad de datos y de manera segura. De hecho, el RGPD expresa con claridad que si existe otra manera de lograr el mismo resultado (es decir, si los datos no son necesarios), una base jurídica no será válida.

En la mayoría de los casos, la elección final de la base jurídica será una combinación de las circunstancias específicas de una organización, el contexto legal local (en especial, si es una situación no regida por el RGPD y si el contexto es más binario) y la interpretación de la ley. **Sin embargo, nosotros sugerimos que el desequilibrio de poder, las necesidades externas, tales como KYC, y los retos y contextos cambiantes, hacen del consentimiento una mala opción para la mayoría de los casos, sino todos.**

22 El Considerando 46 aclara que la opción de Intereses vitales probablemente aplique únicamente a una estrecha gama de casos donde es necesario "salvar vidas", donde el tratamiento "no puede basarse manifiestamente en otra base jurídica". El Considerando 46 detalla de manera explícita "los fines humanitarios" como un ejemplo de tratamiento que puede servir tanto al interés público como a los intereses vitales, incluyendo el seguimiento de epidemias y su propagación o en situaciones de emergencias humanitarias. Esto sugiere claramente que para la mayoría de las intervenciones de asistencia no crítica, es poco probable que sea buena opción elegir intereses vitales para las organizaciones humanitarias.

CASILLA 13: ELECCIÓN DE UNA BASE JURÍDICA PARA EL TRATAMIENTO DE DATOS (CONT.)

Un enfoque de "interés" (es decir, función pública/interés público o interés legítimo) junto con un consenso positivo y éticamente informado, puede ofrecer lo mejor de ambos mundos, ya que:

- mantiene estándares de elección altos para las personas, basados en un panorama adecuado, completo y sensible al contexto respecto a cómo serán utilizados los datos y para qué fines;
- impone una carga mayor sobre las organizaciones de modo que rindan cuentas y reflexionen, ahora y en el futuro, sobre sus comportamientos, los riesgos a los que son expuestos los participantes y cómo podrían cambiar estos riesgos a lo largo del tiempo;
- refuerza la necesidad de valorar y comprender el contexto, en la planificación, en la contextualización, en la actuación y en la reacción.

INCORPORAR LA PRIVACIDAD POR DISEÑO

Si bien la hoja de orientación 1 señala la importancia de trabajar en el ámbito de principios de alto nivel de responsabilidad en la gestión de los datos, el RGPD —y los defensores de la privacidad— recomienda de manera específica incorporar los principios de "Privacy by Design" (Privacidad por diseño) a la fase de diseño y planificación. La premisa básica de "Privacy by Design" es que no puede garantizarse la privacidad únicamente cumpliendo con los marcos políticos y normativos. También debe incorporarse al diseño de los procesos de recopilación de datos de manera tal, que la fuerza de las medidas de privacidad sea proporcional a la fuerza de la sensibilidad de los datos que están siendo recopilados y procesados.[23] La privacidad debe venir por defecto en el modo de diseñar los procesos de datos y no como una opción de inclusión voluntaria. Los puntos en la casilla 14 son un útil recordatorio de cómo diseñar protegiendo la privacidad.

CASILLA 14: 7 PRINCIPIOS ESENCIALES QUE ORIENTAN EL PROCESO DE PRIVACIDAD POR DISEÑO

1. **Proactivo y no reactivo: preventivo y no correctivo.** Anticipe los riesgos y evite eventos de invasión a la privacidad y daños antes de que ocurran y diseñe estrategias de mitigación desde el inicio.
2. **Privacidad como configuración por defecto.** Las personas no tienen que adoptar medida alguna para proteger su privacidad. La privacidad es la modalidad incorporada por defecto en todos los entornos.
3. **Privacidad integrada al diseño.** La privacidad se integra al diseño y a la arquitectura tanto de los sistemas como de las prácticas comerciales. La privacidad es un componente esencial de la funcionalidad principal que se ofrece.
4. **Plena funcionalidad: suma positiva, no suma cero.** No se obliga a las personas a escoger entre la privacidad y el uso de una aplicación, herramienta, plataforma o servicio. Sacrificar la privacidad no es un requisito para acceder al producto.
5. **Solución integral de seguridad: protección del ciclo de vida completo.** Es posible mantener la privacidad mientras se protege la confidencialidad de los datos a través del ciclo de vida de los datos. Todos los datos se recopilan, utilizan, retienen y almacenan de manera segura y luego se destruyen de manera segura al final del proceso, sin demoras.
6. **Visibilidad y transparencia: mantener apertura.** Toda práctica o tecnología comercial deberá operar de conformidad con las promesas y los objetivos planteados, sujeto a una verificación independiente. Las personas a las que se refieren los datos tienen pleno conocimiento de qué datos personales están siendo recopilados, qué se hace con ellos, para qué propósito(s) y quién los recopila.
7. **Respeto a la privacidad del usuario: mantener la privacidad centrada en el usuario.** Los arquitectos y operadores priorizan los intereses del individuo ofreciendo medidas como una robusta privacidad por defecto, notificaciones adecuadas y potenciación de opciones fáciles de manejar. También es importante escuchar a los usuarios y responder a sus comentarios.

Véase este resumen para obtener más información sobre la Privacidad por diseño.

23 https://www.ryerson.ca/content/dam/pbdce/seven-foundational-principles/The-7-Foundational-Principles.pdf

CUMPLIR CON LA DEBIDA DILIGENCIA A SOCIOS DEL SECTOR PRIVADO, INCLUYENDO LOS PSF Y TERCERAS PARTES

Las alianzas con el sector privado forman parte cada vez más del modo en que las organizaciones gestionan los datos, ya que los datos y las herramientas digitales están cada vez más integradas en el trabajo diario de las organizaciones de ayuda humanitaria y requieren de destrezas con las que muchas organizaciones no cuentan. A veces, estas alianzas traen consigo fondos o experiencia técnica en especie. En otras ocasiones, permiten escalar y realizar iniciativas más sostenibles, lo que las hace atractivas para el sector humanitario.

Los PTM también se prestan cada vez más a través de terceros proveedores. Es posible que estas entidades estén interesadas en "hacer el bien", no obstante, su motivo principal es percibir ganancias. Quizás también tengan obligación de compartir datos con arreglo a leyes contra el terrorismo o contra el blanqueo de dinero, y esto podría influir el modo en que tratan los datos. En algunos casos, el sector privado se toma muy en serio la privacidad y la seguridad de los datos con el fin de mantener la confianza del cliente. En otros casos, los actores del sector privado podrían tener interés en monetizar los datos o en reutilizar los datos de clientes con el fin de desarrollar productos y servicios. Si ha realizado un análisis de economía política de los datos (véase la hoja de orientación 1), debería haber identificado algunas de las dinámicas de poder y posibles motivaciones de los socios del sector privado en los PTM. En la etapa de "Intercambio de datos" (hoja de orientación 6), se explica cómo establecer acuerdos para proteger los datos de las personas receptoras de los PTM y los datos organizacionales durante los PTM.

Muchas organizaciones de ayuda humanitaria tienen instaurados procesos de debida diligencia de los socios. Algunos aspectos clave respecto a la responsabilidad en la gestión de datos que deben incluirse en estos procesos, involucran asegurarse de que los socios del sector privado cumplan con los siguientes requisitos:

- ser capaces y estar dispuestos a proteger los datos según requerimiento de los actores humanitarios;
- tener instauradas políticas y prácticas robustas y responsables que protejan y aseguren los datos;
- haber respondido de una manera adecuada a filtraciones de datos o incidentes previos en relación con los datos;
- tener líneas comerciales o modelos comerciales pasados, actuales y futuros alineados con los objetivos humanitarios fundamentales y con los principios de "no causar daño";
- no tomar parte en actividades comerciales que perjudiquen a las poblaciones vulnerables a las que las agencias humanitarias aspiran a apoyar (por ejemplo, utilizar los datos para identificar a refugiados y migrantes con el fin de detenerlos o deportarlos, crear tecnologías de vigilancia que los gobiernos utilicen para identificar a poblaciones específicas con el fin de tomar medidas perjudiciales o desarrollar modelos de datos que sean utilizados para excluir a personas o a grupos vulnerables específicos de los beneficios o servicios);
- tener un compromiso firme de trabajar con los PTM y las personas beneficiarias de estos programas en modos que no sean predatorios, ni explotadores.

Algunos socios del sector privado, por ejemplo, muchos operadores de redes móviles (MNO, por sus siglas en inglés), tienen modelos comerciales que dependen de una gestión de datos segura y, por tanto, cuentan con una amplia experiencia en los aspectos de privacidad y seguridad de los datos. En algunos casos, pueden ayudar a las organizaciones humanitarias a mejorar en este aspecto.

Si va a trabajar con el sector privado en una iniciativa relacionada con datos o tecnología, puede utilizar **esta Nota Orientativa** como guía para enmarcar una asociación cuyo centro sea la responsabilidad en la gestión de datos.

Esta **lista de verificación imprimible de la "Electronic Frontier Foundation"** puede ayudarle a evaluar la capacidad de un socio para garantizar seguridad y privacidad de datos.

Este **conjunto de 7 preguntas** puede ayudarle a hacer las preguntas adecuadas a su proveedor respecto al cumplimiento con el RGPD.

ESTABLECER UN PROCESO DE GOBERNANZA DE DATOS PARA AYUDAR A GESTIONAR LA RESPONSABILIDAD Y RENDICIÓN DE CUENTAS DE LOS DATOS

Dependiendo de la estructura de los PTM y de los socios involucrados, es importante documentar quién asume la responsabilidad de la gestión general de los datos y de cada uno de los procesos de recopilación de datos en las diferentes etapas del ciclo de los PTM. Esto incluye:

- mantener una lista de inventario de datos y controlar qué socio mantiene cuáles datos, y garantizar que se cumpla con los plazos para la retención y la eliminación de los datos, y que los socios cumplan con los acuerdos de intercambio de datos y otros términos de los contratos y acuerdos relacionados con el mantenimiento, la retención y la eliminación de los datos;
- controlar quién tiene acceso a cuáles datos, incluido el manejo de cambios en los niveles de acceso del personal y de los socios;
- asegurarse de que los datos sean agregados o anonimizados tan pronto como sea posible después de ser recopilados o utilizados (dependiendo de las circunstancias);

- manejar y dar respuesta a las solicitudes de los participantes de los PTM respecto a la corrección, eliminación o cancelación de sus datos del sistema.

Asegúrese de especificar sus necesidades con respecto al mantenimiento y a la retención de datos en las etapas iniciales de planificación para garantizar que dispone del presupuesto necesario para el mantenimiento, la retención y la eliminación segura de datos. El papel que usted desempeñe en el proyecto determinará si este costo lo asumirá su organización o un socio.

PREPARARSE PARA POSIBLES INCIDENTES O VULNERACIONES CON DATOS CRÍTICOS

Los incidentes de datos críticos incluyen la filtración en la infraestructura, divulgación no autorizada o alteración de los datos y el uso de los datos recopilados con fines humanitarios para otros fines, sin un correspondiente consentimiento o acuerdo. Esto ocurre cuando la manera de gestionar los datos provoca daños a las poblaciones afectadas, las organizaciones, el personal o a otras personas o grupos. Los incidentes de datos pueden incluir el robo o la confiscación de una computadora portátil que contenga datos sensibles, una lista de personas beneficiarias de los PTM que sea alterada o compartida sin autorización, o la provisión forzada de encuestas o datos de hogares, a autoridades. Los incidentes de datos pueden incluso ocurrir sin que corra peligro la infraestructura técnica. Cuando la recopilación, el uso y el intercambio de datos conduce a la propagación de rumores negativos, sensibilidades culturales, dinámicas de poder y otros factores que tienen efectos adversos sobre las poblaciones afectadas o las organizaciones humanitarias, esto también puede considerarse un incidente de datos crítico.[24]

Basado en su análisis de contexto y capacidades (hoja de orientación 1) y en las experiencias pasadas, además del tipo de actores que podría tener interés en acceder a sus datos, redacte una lista de los tipos de incidentes de datos que podrían ocurrir durante la respuesta de los PTM y haga planes para mitigarlos en su planificación y diseño. Tendrá que plantear esta cuestión con sus organizaciones socias (en el caso de ser una organización implementadora) o con las agencias que manejen los sistemas de datos. **Al seleccionar a los socios (por ejemplo, proveedores de servicios financieros, operadores de redes móviles, etc.) que manejarán las herramientas de datos digitales y los sistemas de datos generales, es importante poner por escrito sus responsabilidades y obligaciones (además de las propias) ante los incidentes de datos críticos, como parte de su acuerdo contractual.** El equipo de seguridad de la información de su organización debe participar para apoyar este tipo de investigación, y su equipo legal puede ofrecer plantillas o la redacción que debe incluirse. Es probable que deba también involucrar al oficial de protección de datos.

Por último, querrá determinar cómo organizar la respuesta a un incidente de datos críticos notificados, documentándolo en un "protocolo de incidente de datos crítico" donde esté establecido el modo de reportar, investigar y comunicar los incidentes de datos. También establecerá el proceso por el que se pasará para determinar si va a ofrecer una compensación o apoyo a cualquier persona que se haya visto perjudicada por una filtración de datos, y de qué manera. La mayor parte de las legislaciones sobre la privacidad requiere que se reporten las filtraciones de datos a las autoridades de datos y a las personas afectadas por ello, dentro de un plazo específico. Si bien no es habitual que los actores humanitarios revelen incidentes de datos críticos o filtraciones de datos a las poblaciones afectadas, las personas tienen derecho a saber que sus datos se han visto afectados y los tipos de daños que podrían resultar, y a ser compensadas por los daños que puedan sufrir. Este aspecto está vinculado con la rendición de cuentas a las poblaciones afectadas y, por tanto, los equipos que trabajan en la rendición de cuentas a las poblaciones afectadas podrían ser buenos aliados en esta labor. Los equipos de seguridad también son excelentes aliados, si tomamos en cuenta que los incidentes de datos críticos implican dinámicas de poder y daños. Las organizaciones tienen la responsabilidad de evitar los incidentes de datos y la obligación de atender los casos, cuando estos ocurren.

Las estrategias de mitigación de incidentes de su organización deben abarcar la seguridad de los datos y los sistemas de datos, así como capacitar a las personas en la protección de los datos e incentivarlas a hacerlo. Esto va a requerir los aportes del personal, los encuestadores y otras personas que manejan datos "en el terreno" y que están familiarizadas con el contexto cotidiano de una respuesta.

Converse con los equipos de seguridad, protección, ciberseguridad, gestión de datos, protección de datos, legal, comunicación y cumplimiento de su organización; para determinar la manera de responder de manera colectiva a incidentes de datos críticos y si ya existen políticas de este tipo. Es posible que pueda emplear las experiencias y los protocolos de manejo de crisis de los equipos de seguridad y relaciones públicas de su organización para planificar y manejar los incidentes de datos críticos.

Asegúrese de incluir los incidentes de datos críticos en sus evaluaciones de riesgos, beneficios y daños o de impacto de la privacidad de los datos (véase el siguiente paso en esta hoja de orientación), junto con ejemplos de cómo mitigar los posibles daños.

24 OCHA Centre for Humanitarian Data. Note #2: Data Incident Management. Guidance Note Series: Responsible Data in Action. 2019 (Nota no 2: Gestión de incidentes de datos. Serie de notas orientadoras: responsabilidad en la gestión de datos en acción).

DESPUÉS DE PLANIFICAR TODO EL CICLO DE VIDA DE LOS DATOS (HOJAS DE ORIENTACIÓN 1–7), REALICE UNA EVALUACIÓN DE IMPACTO DE PRIVACIDAD DE LOS DATOS

La Evaluación de impacto de privacidad de los datos (EIPD) es un análisis sistemático de los posibles riesgos de privacidad a los que se exponen las personas a causa de la recopilación y el uso de datos durante la ejecución de programas.

La EIPD debe realizarse durante la etapa de planificación, pero será necesario haber elaborado planes para el ciclo de vida de datos completo (etapas 1–7) para obtener la información necesaria con la cual realizarla.

Una EIPD se concentra de manera explícita en los posibles daños a las personas cuyos datos están siendo recopilados y procesados —no es una herramienta para evaluar el riesgo y la obligación organizacional—. No obstante, si existe un alto riesgo para las personas y grupos que participan en un programa, la organización acumulará riesgos y obligaciones. La EIPD permite analizar las amenazas y los riesgos relacionados con el impacto de los datos y desarrollar estrategias de mitigación. La EIPD ayuda a las organizaciones humanitarias a proteger la privacidad de los participantes y a fortalecer la confianza pública en un programa. El Reglamento general de protección de datos (RGPD) de la UE y algunos otros marcos legales ordenan que se realicen EIPD o una evaluación de impacto sobre la privacidad en todo caso donde sea probable la existencia de un alto riesgo para la población beneficiaria. La EIPD ayuda a las organizaciones a determinar si los posibles beneficios de la recopilación sobrepasan los posibles daños y ofrece una manera de documentar los hallazgos. Se debe realizar una EIPD sin tomar en cuenta la modalidad del PTM.

Si su organización es auditada sobre sus prácticas en la gestión de los datos, tener una EIPD en sus archivos sirve para proporcionar documentación sobre el modo en que su organización identificó y mitigó los riesgos en la recopilación y el tratamiento de datos. Cuando sea posible demostrar que su organización fue exhaustiva en su gestión de datos y en la reducción de riesgos, los fallos y multas probablemente sean más pequeñas. Si se considera que su organización está actuando de una manera negligente, entonces se podrían recomendar multas mayores. Si no se realiza una EIPD, es importante también documentar los motivos por los cuales no fue posible hacerlo.

Su EIPD debe utilizarse como herramienta de planificación, junto con (o incorporado a) los demás procesos de evaluación de riesgos de su organización, con el fin de identificar las áreas de riesgo de la organización en términos de cómo su gestión de datos podría perjudicar a poblaciones afectadas y a su propia reputación, o situación legal o financiera. En la medida de lo posible, la EIPD debe ser participativa, de modo que incluya los puntos de vista de las poblaciones afectadas en la identificación y clasificación de los riesgos, y en las propuestas de estrategias de mitigación. Las preguntas de preselección de la EIPD (tales como "¿es vulnerable esta población?") se deben incorporar a otros procesos, como las listas de verificación para la planificación, las guías de diseño de programas, los marcos de aprobación y los procesos de aprobación de licitaciones para transversalizar la privacidad a la organización en general.

Si una organización descubre que, durante el proceso de EIPD, no hay apoyo disponible, ni recursos adecuados para gestionar los datos de una manera responsable, que los datos no pueden recopilarse y utilizarse de una manera responsable debido al contexto, o que las poblaciones afectadas están asumiendo riesgos por el uso de los datos que no es proporcional a los beneficios, la respuesta debe interrumpirse e implementarse un enfoque programático que utilice menos datos.

Algunas organizaciones igualmente implementarán la revisión de la EIPD como parte de sus estructuras y marcos de gobernanza. Lo importante es que exista una evaluación de riesgos específica enfocada en los datos, y que se concentre en el impacto del uso de los datos sobre las poblaciones afectadas.[25]

Aunque la hoja de orientación 1 sugiere realizar una evaluación rápida para determinar si, en general, una organización debe ocuparse de una respuesta basada en el contexto y la capacidad (véase la casilla 9), la EIPD profundiza en la evaluación de las actividades de recopilación y uso de datos dentro de la propuesta (por ejemplo, un proceso de recopilación de datos para focalización del PTM, el uso de una cierta modalidad de entrega de PTM o un proceso de encuesta o MEAL).

A continuación, algunos ejemplos de marcos y procesos de EIPD, evaluación de impacto sobre la privacidad y evaluación de riesgos y beneficios:

- CICR, **Data Protection Handbook** (Manual de protección de datos) Apéndice 1, página 299.
- Sonjara's **Benefit Risk Assessment Framework Workshop** (Taller sobre el marco de evaluación de beneficios y riesgos de Sonjara).

25 Las EIPD pueden realizarse en diferentes etapas del ciclo de programa de los PTM. Podría realizarse una EIPD general en la fase de diseño de programa que ayude a determinar si los agentes de los PTM son capaces de reducir los riesgos a la privacidad a un nivel aceptable. Los posibles riesgos a las poblaciones afectadas no deben pesar más que los posibles beneficios. Lo mismo cabe decir para las organizaciones —los procesos de recopilación de datos deben arrojar más beneficios que riesgos—. También deben realizarse EIPD para actividades de recopilación de datos específicas en el transcurso del ciclo de programa. Si se utiliza un formato estandarizado de EIPD, pueden realizarse EIPD de manera periódica y de un modo descentralizado, al inicio de nuevas actividades de recopilación de datos. Estas pueden consolidarse y utilizarse de manera periódica con el fin de servir de aprendizaje y de utilizarlas para realizar mejoras a lo largo del tiempo. La EIPD debe ser un 'documento vivo', revisado de manera periódica, por ejemplo, cuando cambian los socios, el contexto o el uso de los datos.

- Herramienta de USAID, **Benefit Risk Assessment** (Herramienta de evaluación de beneficios y riesgos), páginas 11–13, parte del documento "Considerations for Using Data Responsibly" (Consideraciones para la responsabilidad en el uso de los datos).
- **The Privacy Commissioner of New Zealand's PIA**, (Evaluación de impacto sobre la privacidad del Comisionado de Privacidad de Nueva Zelanda).
- CaLP, **Protecting Beneficiary Privacy** (Protección de la privacidad de las personas beneficiarias), páginas 19-20.
- **Assessing Harm for Tech Builders** framework (marco de evaluación de daños para los creadores de tecnología) de Microsoft.

Algunas organizaciones utilizan una evaluación de riegos y beneficios (RBA por sus siglas en inglés), la cual podría ser más útil en el contexto de la ayuda humanitaria y, siempre que abarque aspectos de privacidad de los datos, con frecuencia puede reemplazar una EIPD. Las RBA sobre datos examinan la pregunta crítica de quién se arriesga y quién se beneficia de la recopilación de datos en un intento por garantizar que las personas más vulnerables no carguen con los riesgos, mientras las organizaciones se llevan los beneficios. La nota orientativa de OCHA, **Note on Data Impact Assessments** (Nota sobre evaluaciones de impacto de los datos), abarca los diferentes tipos de evaluaciones y cómo determinar cuál es la más apropiada según el contexto.

HOJA DE ORIENTACIÓN 3

RECOPILAR O ACCEDER A DATOS

Los datos pueden utilizarse para buenos motivos, como, por ejemplo, para mejorar la focalización de los programas y reducir la duplicación y el fraude. Pero también pueden utilizarse para influir sobre los comportamientos en modos poco transparentes: para extorsionar, identificar a personas y grupos con el fin de causarles daño y para difundir información errónea. Los datos también pueden provocar daños involuntarios, a pesar de las buenas intenciones. Por todos estos motivos, y porque las personas tienen el derecho fundamental a la privacidad, es vital ser responsables en la recopilación de los datos y en el acceso a los mismos.

Se recopilan datos personales y otras formas de datos sensibles en cada etapa de los PTM, incluyendo:

- planificación y evaluaciones de necesidades
- focalización
- inscripción y registro
- implementación
- retroalimentación
- monitoreo y evaluación

La hoja de orientación 3 abarca aspectos que le ayudarán a recopilar datos necesarios de alta calidad y proporcionales a la finalidad para la cual son recopilados. En aquellos casos en los que se acceda a datos que fueron previamente recopilados o que fueron recopilados por otras organizaciones, deberá seguir aplicando esta orientación.

CASILLA 15: DEFINICIONES DE LOS DATOS: DATO PERSONAL, DATO PERSONAL SENSIBLE, DATO PERSONAL NO SENSIBLE Y METADATO

¿Qué es un dato personal?

- Es un dato que se relaciona con un individuo identificado o identificable ; esto incluye datos que identifican directamente a una persona (un nombre, un número, o una dirección IP ("Internet Protocol", por sus siglas en inglés) o identificador de "cookies") o datos que podrían posiblemente identificar a una persona (por ejemplo, porque el conjunto de datos es pequeño o los datos incluyen información, o una combinación de información, que facilita la identificación de una persona dentro de un conjunto de datos mayor).
- Un dato que identifica a una persona cuando un conjunto de datos se cruza con otro conjunto de datos.

¿Qué es un dato sensible?

- Un dato sensible incluye datos personales sensibles, los cuales, si se divulgan o se accede a ellos sin una autorización adecuada, podrían resultar en discriminación o en represión hacia la persona, hacia la fuente de la información o hacia otras personas o grupos identificables.

CASILLA 15: DEFINICIONES DE LOS DATOS: DATO PERSONAL, DATO PERSONAL SENSIBLE, DATO PERSONAL NO SENSIBLE Y METADATO (CONT.)

- Un dato personal sensible, por lo general, incluye la raza, el origen étnico, la afiliación política, la religión, la membresía a un sindicato, información genética, datos biométricos, de salud, de vida sexual o de orientación sexual; también incluye datos personales sobre personas altamente vulnerables, como niños, niñas o personas desplazadas.
- Otra información personal puede ser sensible, dependiendo del contexto y la cultura, y contextos humanitarios gran parte de los datos son altamente sensibles. Debido a que los datos tienen niveles variados de sensibilidad dependiendo del contexto, en la presente guía práctica no ofrecemos una lista definitiva de puntos de datos sensibles.
- Es bueno considerar quién decide qué es sensible y qué no lo es. Una comunidad afectada podría determinar que un campo de dato específico es sensible, incluso cuando las regulaciones de privacidad de los datos o la organización implementadora no lo categorice como tal.

¿Qué es un dato no personal sensible?

- Datos sobre el contexto en el cual ocurre una crisis (por ejemplo, información sobre las comunidades que reciben transferencias monetarias);
- Datos sobre la respuesta de las organizaciones y las personas a las que se pretende prestar asistencia (por ejemplo, ubicación de puntos de distribución de efectivo o planes de recopilación de datos).[26]

¿Qué son metadatos?

- Los metadatos son "datos sobre datos".
- Los metadatos se producen a través de los aspectos prácticos de los PTM, y diferentes obligaciones regulatorias y legales se aplican a la recopilación, el intercambio y la retención de metadatos.
- Por ejemplo, en el caso de dinero a través del teléfono móvil, los metadatos incluyen los números de teléfono del remitente y del destinatario, la fecha y hora de la transacción financiera, el número de identificación de la transacción, la ubicación y el tamaño de la transacción, la tienda donde se llevó a cabo y los agentes involucrados en ambos lados.
- Estos datos pueden utilizarse para deducir otra información e inteligencia, que podría utilizarse para crear un perfil, identificar y supervisar a los usuarios. Estos datos podrían utilizarse para deducir información sobre los comportamientos, los movimientos, las afiliaciones y otras características de las poblaciones afectadas. La capacidad de deducción sobre las personas beneficiarias es posible mucho después de finalizado un programa.[27, 28]

DETERMINAR CÓMO PROTEGER LOS DATOS SI ESTÁN SIENDO RECOPILADOS REMOTAMENTE O VÍA TELÉFONO MÓVIL

Si bien la recopilación de datos remota se ha practicado en algunos países debido a entornos de conflictos o donde se hace difícil trabajar, esta forma de recopilación se volvió más prevalente durante la pandemia de la COVID-19. Muchas organizaciones realizaron la focalización de los PTM vía llamadas telefónicas o confiando en los miembros de la comunidad para identificar y gestionar la selección de receptores de los PTM. Surgen inquietudes respecto a la confidencialidad con este tipo de recopilación de datos que puede conducir al favoritismo, a la manipulación de las listas o colocar a miembros de la comunidad en una posición en la que se vean obligados a gestionar la demanda de efectivo. Si una intervención se realiza de manera totalmente remota, no habrá un tercero externo disponible (como una organización de PTM) para señalar o prestar apoyo en estas situaciones.[29] Es más, en algunos casos se han exonerado o reducido las regulaciones de Conocimiento del cliente (KYC, por sus siglas en inglés) y cuando se han aplicado, las organizaciones han encontrado dificultades en cumplirlas cuando el registro de las personas beneficiarias se realizó por teléfono, ya que no se pudo verificar la identidad de manera directa. Si bien parte de estos datos todavía se recopilan sin el uso de mecanismos digitales remotos, la recopilación remota es una iniciativa de rápida evolución, pues muchos de los nuevos esfuerzos implican métodos de recopilación de datos digitales. Algunos ejemplos de nuevas prácticas innovadoras que están emergiendo incluyen el uso de la identificación de voz o de los "selfies" para probar la identidad. Recientemente, el GAFI señaló que la verificación de identidad remota puede ser igualmente efectiva cuando altos niveles de garantía de la identidad se puedan lograr. Esta no es una opción en la que la gente tenga que optar. Los puntos en la casilla 14 son un útil recordatorio de cómo diseñar teniendo en cuenta la protección de la privacidad.[30]

26 OCHA (2019) 'Data Responsibility Guidelines: Working Draft' (Lineamientos sobre la gestión responsable de datos: borrador de trabajo).
27 CICR Data Protection Handbook (2020) (Manual de protección de datos).
28 CICR y Privacy International (2018) 'The Humanitarian Metadata Problem: Doing No Harm in the Digital Era' (El problema de los metadatos en la ayuda humanitaria: no causar daño en la era digital).
29 Save the Children hoja de orientación: "Adaptations in how we identify, register, and verify CVA beneficiaries in the time of Covid-19" (Adaptaciones en el modo en que identificamos, registramos y verificamos a los destinatarios de PTM en tiempos de la COVID-19). (sin publicar)
30 Grupo de Acción Financiera (GAFI) (2020) 'Digital Identity' (Identidad digital).

Véase la publicación de CaLP, **"PTM en contextos afectados por la COVID-19"** para obtener una visión general de cómo las diferentes agencias se adaptan a la recopilación a distancia de datos y a otras actividades remotas.

Véase **este debate** sobre los pros y los contras y las buenas prácticas en el monitoreo remoto.

Véase **esta lista de comprobación** que contiene orientación sobre cómo recopilar datos móviles de manera segura. Esta lista puede adaptarse para la recopilación de datos móviles para PTM.

La guía práctica del PMA, **"Vulnerability Analysis & Mapping (VAM) toolkit"** (Guía práctica de análisis de vulnerabilidad y mapeo (VAM por sus siglas en inglés)) ofrece orientación sobre la responsabilidad en la realización de encuestas móviles.

UTILIZAR MÉTODOS, ENFOQUES Y HERRAMIENTAS DE RECOPILACIÓN DE DATOS INCLUSIVOS

Cuando se diseñe la recopilación de datos, en especial si se utilizan herramientas digitales, es fundamental diseñar expresamente la inclusión para evitar dejar fuera las poblaciones más vulnerables. Las mujeres tienen menos probabilidades de tener acceso a un teléfono móvil en comparación con los hombres, y esto es particularmente cierto en los contextos de ayuda humanitaria. El informe del GSMA sobre la brecha de género en la telefonía móvil 2020, por ejemplo, muestra que las mujeres tienen un 8 % menos de probabilidad que los hombres de ser propietarias de teléfonos móviles, y esta brecha aumenta al 20 % cuando se trata de Internet móvil.[31] Estas brechas pueden ser incluso mayores en contextos de ayuda humanitaria.[32] Es probable que las poblaciones más vulnerables también queden excluidas del acceso a la telefonía móvil. Asimismo, es importante que las organizaciones consideren si están siendo inclusivas respecto a las personas con discapacidades y a otros grupos que sufren discriminación. Habrá que incorporar desde el principio estos así llamados casos "extremos", en el diseño del proceso de recopilación de datos — y presupuestarlos —. Esto significa tomar medidas para diseñar diferentes tipos de acceso y buscar activamente estos casos "extremos" para garantizar que se estén probando los métodos y enfoques de recopilación de datos con estos grupos que tienen más probabilidades de quedar fuera.

El **portal de rendición de cuentas e inclusión del Comité Permanente Inter Agencial** tiene recursos y guías para garantizar la inclusión en los procesos de ayuda humanitaria.

Véase **esta Guía práctica** sobre cómo garantizar la inclusión digital de las personas con discapacidades.

La **Guía práctica sobre género y tecnología de la información y la comunicación (TIC)** ("Gender and Information Communication Technology ICT Toolkit) de USAID ofrece una serie de módulos y consideraciones para comprender el acceso de las mujeres a las TIC.

Será necesario ofrecer más de una opción o ruta para la recopilación de datos con el fin de garantizar que las personas más vulnerables (por ejemplo, los que no son de fácil acceso, las mujeres, los que no hablen idiomas más comunes) y las personas con discapacidades, no sean excluidas.

CONSIDERAR EL IMPACTO DEL CONOCIMIENTO DEL CLIENTE (KYC), EL REGISTRO DE TARJETAS SIM Y LAS MEDIDAS CONTRA EL TERRORISMO

Cuando las organizaciones de ayuda humanitaria colaboran con los Operadores de redes móviles (MNO, por sus siglas en inglés) y otros PSF, se les exige cumplir con las normas de Conocimiento del cliente (KYC, por sus siglas en inglés), de lucha contra el blanqueo de dinero, medidas de lucha contra el terrorismo y otras regulaciones y legislación diseñadas para prevenir el lavado de dinero y la corrupción. Esto significa que su organización, o los mismos receptores de los PTM, deben compartir datos personales y sensibles con terceros, incluidos fiscalizadores, para verificar la identidad de las personas beneficiarias de los PTM. Ciertos donantes requieren de una aprobación adicional como parte de las medidas de lucha contra el terrorismo. Además, más de 155 gobiernos alrededor del mundo tienen establecidas políticas de registro SIM (siglas en inglés para "suscriber identity module"), que exigen a las personas proporcionar una prueba de identidad antes de poder acceder a una tarjeta SIM.[33]

El Grupo de acción financiera internacional (GAFI), el organismo de control mundial contra el blanqueo de dinero y la financiación al terrorismo también puede ofrecer recomendaciones adicionales, en cuyo caso se incorporan a la legislación nacional, y los nuevos receptores de los PTM deben ser examinados con arreglo a estas listas. La información de KYC debe verificarse con listas establecidas por autoridades locales, incluidas personas y entidades que posiblemente están involucradas en un conflicto o una situación de violencia. En caso de encontrar una coincidencia, las personas beneficiarias de los PTM podrían ser excluidos de la asistencia, incluso si la coincidencia es un caso de identidad equivocada. En entornos de conflicto, las familias en necesidad de contar con asistencia en efectivo podrían ser de comunidades que se encuentren en este tipo de lista de control, pues con frecuencia son clasificadas por zona geográfica.

Este proceso podría ser supervisado por autoridades e incluir la obligación de presentar informes. Las medidas de lucha contra el blanqueo de dinero y las medidas de lucha contra el terrorismo a menudo son decretadas con la ayuda de programas informáticos de terceros, pero a veces es incierto lo qué ocurre con los datos que se introducen en estas bases de datos. Los gobiernos, los PSF o los MNO podrían utilizar los datos recopilados para otros fines, como la promoción de servicios financieros adicionales (u otros servicios, si los datos son vendidos o compartidos más adelante) o para determinar la solvencia de las personas.

31 GSMA (2020) 'The Mobile Gender Gap 2020' (Brecha de género en la telefonía móvil).
32 GSMA (2020) 'Bridging the mobile gender gap for refugees' (Cerrando la brecha de género de refugiados en la telefonía móvil).
33 GSMA (2020) 'GSMA Digital Identity Programme: Insights and Achievements (2016–2020)' (Programa de identidad digital de GSMA: ideas y logros (2016-2020).

Es fundamental que, al negociar el alcance de trabajo y el proceso de contratación con un PSF, se evalúen estos importantes elementos, y que las organizaciones cuenten con procesos claros para revisar cualquier documento de alcance de trabajo. Este proceso deberá coordinarse entre el equipo que gestiona los procesos de PTM directamente, y el equipo de tecnología, ya que pueden evaluar aspectos como la seguridad, el almacenamiento de los datos y los elementos del servidor, los encargados de datos y privacidad, y las adquisiciones. Esto será útil para que las organizaciones eviten brechas y vacíos, o sorpresas; por ejemplo, cláusulas de intercambio de datos que no protegen totalmente los datos de los PTM.

No todos los donantes o gobiernos nacionales exigen este tipo de examen previo, pero en los casos en que se requiera, esto debería ser explicado a las personas afectadas como parte del proceso de recopilación de datos, dándoles la opción de proporcionar o no sus datos, de inscribirse utilizando un tipo de proceso diferente o de recibir asistencia bajo otra forma de pago, como por ejemplo, ayuda en especie, efectivo en mano, cupones de un solo uso o tarjetas con circuito integrado (smart cards) anónimas. Sin embargo, no todas las agencias pueden ofrecer estas opciones, debido a su estructura, tamaño o a su dependencia de otras agencias para acceder a sistemas y fondos.

Es posible negociar con los donantes respecto a las implicaciones operativas de sus requisitos de revisión. Los donantes son cada vez más conscientes de la necesidad de gestionar los datos de manera responsable y de mitigar los riesgos relacionados con los datos. Con frecuencia ellos comprenden las contrapartidas que esto implica, por ejemplo, que el escrutinio socava los principios de imparcialidad de la ayuda humanitaria, lo que significa que habrá un margen para negociar.

Aquí puede encontrar una lista de los países que exigen el Registro de tarjeta SIM a partir de 2020.

En esta **hoja de orientación** de 2016 se discuten las medidas de KYC y algunos ejemplos de regulaciones ajustadas.

TENER EN CUENTA LOS COSTOS Y BENEFICIOS DE RECOPILAR DATOS BIOMÉTRICOS O INTRODUCIR SISTEMAS DE IDENTIFICACIÓN DIGITAL

Se citan una serie de ventajas cuando se utilizan datos biométricos para la gestión y el rastreo de la inscripción y la entrega de ayuda humanitaria, incluidos los PTM. La biometría, tales como las huellas dactilares, el escaneo del iris, el reconocimiento facial y los datos biométricos de voz, se utiliza como parte de los PTM en diferentes partes del mundo. Ellos ofrecen una forma única de identificar a una persona, incluso si no existe otro medio para probar su identidad porque sus otros documentos de identidad están perdidos o no están disponibles (con frecuencia es el caso de las personas desplazadas). Aunque la biometría se ha promovido como una forma de reducir el fraude individual, los críticos señalan que no enfrentan la corrupción y el abuso general a nivel sistemático, donde se sospecha que se produce el fraude con más frecuencia.[34] Además, la biometría ha sido cuestionada por ofrecer mayor eficiencia a las agencias sin prestar beneficios significativos a las poblaciones afectadas[35] y por una serie de otros motivos, tales como la inexactitud, el riesgo de desviar el uso y la posibilidad de que los datos biométricos puedan ser compartidos con los gobiernos. Algunas organizaciones están explorando el uso de tecnologías para preservar la privacidad, la criptología y los sistemas de registro distribuido (DLT, por sus siglas en inglés), tales como la tecnología de cadena de bloques como una forma de mantener los datos biométricos de una manera más segura, pero se requiere más trabajo en esta área.

Si se utilizan datos biométricos, debe ser proporcional a la finalidad para el cual están siendo recopilados, y las organizaciones deben poder probar que el beneficio de utilizar los datos biométricos, supera los riesgos de su uso. Debido a la naturaleza altamente sensible de los datos biométricos, siempre tendrá que realizar una EIPD, PIA o RBA antes de confirmar el uso de la biometría. Si, como agencia implementadora, se le exige utilizar la biometría porque el sistema en el que está introduciendo los datos así lo requiere, tendrá que revisar cuidadosamente su capacidad para recopilar y gestionar los datos biométricos de forma segura, y las agencias que solicitan a sus socios utilizar datos biométricos, deben asegurarse que estos socios tienen la capacidad de proteger los datos biométricos. Debido a que existe un nivel de incomodidad con la biometría en algunas comunidades afectadas, es de suma importancia ofrecer a las personas la posibilidad de elegir libremente y de forma significativa, si van a proporcionar datos biométricos para inscribirse o recibir asistencia en efectivo, además de ofrecer una alternativa que no constituya una carga para la persona. Organizaciones como Mercy Corps, están explorando otras formas de identificación que sirvan de identidad única, pero no impliquen datos biométricos. Si se explora el uso de la biometría, asegúrese de entender completamente cómo funciona una determinada solución, de principio a fin. Si la solución es demasiado difícil de entender, puede ser razón suficiente para recurrir a formas de identificación no biométricas. El CICR ha realizado una exploración detallada de cuándo y dónde podría ser apropiado utilizar la biometría y ha identificado algunos casos en los cuales son adecuados, y algunos en los que no lo son.

34 Oxfam y The Engine Room (2018) 'Biometrics in the Humanitarian Sector' (Los datos biométricos en el sector de la ayuda humanitaria).
35 Véase la carta abierta de Access Now 'Why ID' (Por qué una identificación) para obtener más información sobre los retos que plantean los datos biométricos en la labor humanitaria y en otras situaciones.

La publicación de Mercy Corps, **"Internal Primer on Biometrics"** (Guía interna sobre la biometría) ofrece una orientación detallada.

Véase el capítulo 8 sobre Datos biométricos en el manual, **"ICRC's Data Protection Handbook"** (Manual de protección de datos del CICR) donde encontrará un debate extenso sobre la biometría y cómo manejar este tipo de datos sensibles y con arreglo a qué base jurídica pueden capturarse datos biométricos en diferentes circunstancias.

Véase **este documento** para acceder a una discusión exhaustiva sobre el uso de la biometría y los sistemas de identificación y registro en crisis prolongadas y recurrentes.

Lea esta **"Carta abierta a los líderes de bancos de desarrollo internacional, la Organización de las Naciones Unidas, organizaciones de ayuda internacional, agencias de financiación y gobiernos nacionales"** para obtener un examen pormenorizado de algunas de las cuestiones y los problemas básicos con los sistemas de identificación biométrica.

COMUNICAR DE FORMA TRANSPARENTE A LAS POBLACIONES AFECTADAS SOBRE LA RECOPILACIÓN Y EL TRATAMIENTO DE LOS DATOS

Comunicarse de una manera transparente y clara con las poblaciones afectadas respecto a la recopilación y el tratamiento de datos, es una parte importante de cualquier proceso de datos y debería ser parte integral de cómo se diseña y presupuesta la gestión responsable de los datos. Tal como se indica en la hoja de orientación 2, en la sección sobre bases jurídicas (véase las casillas 12 y 13, páginas 20 y 21), el uso del consentimiento como base jurídica para la recopilación y tratamiento de datos está siendo cuestionado. Sin embargo, independientemente de la base jurídica para la recopilación y el tratamiento de datos, deberá ser capaz de explicar a las comunidades afectadas, de una manera transparente y culturalmente apropiada, quién ordena la recopilación de estos datos, cómo comunicarse con ellos, por qué se están recopilando y procesando los datos, con quién comunicarse en caso de tener preguntas sobre el tratamiento de los datos y con quién se intercambiarán estos datos, en especial, si se van a compartir con las autoridades, entidades gubernamentales como organismos del orden público, o entidades en otro territorio o jurisdicción.

CASILLA 16: ¿QUÉ DEBEN SABER LAS PERSONAS AFECTADAS ANTES DE PROPORCIONAR SUS DATOS?

La política del CICR exige que se proporcione la siguiente información a las personas afectadas cuando la base jurídica sea el Consentimiento:

- la identidad y los datos de contacto de la organización que ha ordenado y que controla la recopilación y el tratamiento de los datos (el "controlador de datos");
- el propósito específico del procesamiento de datos personales;
- una explicación de los posibles riesgos y beneficios del procesamiento de datos;
- que el controlador de datos podría procesar los datos para otros fines similares (deben indicarse cuáles podrían ser esos propósitos);
- que puede retirar su consentimiento en cualquier momento;
- las circunstancias en las cuales podría no ser posible tratar los datos personales de manera confidencial;
- derecho a objetar al tratamiento de sus datos; derecho a acceder, corregir y eliminar los datos personales;
- cómo ejercer los derechos relacionados con sus datos y las posibles restricciones sobre el ejercicio de esos derechos;
- a qué terceros países u organizaciones internacionales podrían ser transferidos sus datos para cumplir con el propósito de la recopilación inicial y del tratamiento adicional;
- por cuánto tiempo se mantendrán los datos personales (o los criterios que se utilizarán para determinar cuánto tiempo se mantendrán) y las medidas tomadas para garantizar que los registros sean precisos y que se mantengan actualizados;
- con qué otras organizaciones, como autoridades del país donde se recopilan los datos, podrían intercambiarse los datos;
- una indicación de las medidas de seguridad implementadas por el controlador de los datos respecto al tratamiento de datos.[36]

36 ICRC Data Protection Handbook (2020) (Manual de protección de datos).

Será necesario simplificar toda comunicación respecto al modo en que los datos serán procesados y almacenados en un lenguaje claro y accesible, y que sea comprensible por las personas y comunidades afectadas. Puede ser útil proporcionar dibujos, vídeos y audios de los procesos de consentimiento. Tenga en cuenta que, de acuerdo con la cultura, el consentimiento y la privacidad individuales son conceptos que se traducen de distintas maneras. Algunos miembros del personal que trabaja en los PTM han criticado el enfoque legal de Europa al consentimiento y la privacidad por tener características del Norte y percibirse como paternalista, siendo con frecuencia poco útil y no valorado. Cuando se busca la transparencia en la recopilación y el tratamiento de datos, lo más importante es asegurarse que la población afectada comprenda todo el proceso, en lugar de simplemente realizar un ejercicio de lista de comprobación.

Asegúrese de incluir en todos los PTM, información sobre la recopilación de datos, los derechos sobre los datos y los mecanismos de reclamación en sus procesos generales de retroalimentación y rendición de cuentas. Esto incluye información sobre los metadatos (véase la definición en la página 26) que serán recopilados a través de la programación digital de los PTM o la recopilación de datos digital.

Esta guía práctica puede ayudarle a diseñar un plan de comunicación y alcance de datos para su respuesta.

Si está ofreciendo un mecanismo de reclamación —algo que debería hacer— asegúrese de haber previsto personal, capacidad de los sistemas y presupuesto para su ejecución. Por ejemplo, si una persona quiere eliminar sus datos del sistema, ¿es capaz de encontrarlo en su sistema, verificar su identidad y atender su petición?

Para obtener más información sobre los consentimientos, véase la **hoja de consentimiento informado** de World Vision.

Consulte el manual del CICR, **"Data Protection Handbook"** (Manual de protección de datos) para obtener más ideas sobre cómo gestionar el consentimiento informado y otras bases jurídicas, junto con plantillas y lenguaje para adaptarse a su situación. El Capítulo 9 del manual ofrece una orientación detallada sobre los PTM y también sobre la protección de datos.

Conozca más sobre los **Mecanismos de reclamación basados en la comunidad entre agencias**.

HOJA DE ORIENTACIÓN 4

TRANSMISIÓN Y ALMACENAMIENTO DE DATOS

Cada vez que se pasan datos entre un lugar y otro ocurre una transmisión de datos, por ejemplo, cuando los empleados de su organización se pasan datos o archivos entre sí, a otra organización, o a un gobierno, u otra entidad. A veces la transmisión de datos es un proceso activo, por ejemplo, cuando un encuestador presiona "enviar" para que los datos de la encuesta se muevan a través de la red móvil desde un teléfono móvil hacia el servidor de la organización, o a la nube. En otros casos ocurre tras bastidores, porque un dispositivo móvil, una aplicación, un sitio web o un software central, transmiten datos automáticamente a medida que una persona los utiliza, por ejemplo, cuando datos de ubicación se transmiten a un operador de redes móviles porque un teléfono móvil se conecta a una torre de telefonía celular cercana. Por lo general, los datos se almacenan en un dispositivo (como un teléfono móvil, una computadora portátil), en un servidor o en la nube.

Los datos recopilados durante las distintas fases de una respuesta de PTM (evaluación de necesidades, focalización, inscripción y registro, entrega/distribución, retroalimentación y MEAL) serán transmitidos y almacenados de distintas maneras, dependiendo del modo en que esté diseñado su proceso de recopilación de datos. Los datos pueden estar en peligro durante la transmisión y el almacenamiento por varias razones, por lo que es importante transmitir y almacenar los datos de una manera segura, que restrinja quién puede acceder a ellos. Los profesionales de PTM suelen trabajar con socios y aplicaciones de terceros, por lo que se debe garantizar que los datos recopilados de las poblaciones afectadas no sean vulnerables a un acceso no autorizado, alteraciones, eliminaciones o intercambio de datos que pueda que creen un potencial daño. Los acuerdos de transferencia de datos pueden ayudar a formalizar la transferencia de los datos entre los implementadores de los PTM.

En la hoja de orientación 4 exploramos el modo de minimizar los riesgos asociados con la transmisión y el almacenamiento de datos.

SIGA LAS RECOMENDACIONES BÁSICAS DE SEGURIDAD DE DATOS PARA LA TRANSMISIÓN Y EL ALMACENAMIENTO DE DATOS

Toda persona que recopile, transmita o almacene datos debe utilizar protocolos básicos de seguridad de datos. Los profesionales en materia de los PTM deben consultar, en primer lugar, sus políticas y directrices institucionales sobre seguridad de datos, y garantizar que se cumplan, además de otros estándares legales, reglamentarias y buenas prácticas.

CASILLA 17: MODOS DE PROTEGER LOS DATOS CUANDO SE UTILIZAN HERRAMIENTAS Y APLICACIONES DIGITALES

- Evite desarrollar nuevas herramientas y aplicaciones hechas a medida, ya que podrían requerir recursos adicionales para garantizar la seguridad, para gestionar y mantener la seguridad y para descubrir posibles defectos.
- No utilice un sistema o una herramienta simplemente porque un socio, otra organización o un donante lo solicite. Trabaje en primer lugar con su equipo de seguridad informática y con el responsable de privacidad, para asegurar que el sistema o la herramienta sean seguros.
- Planifique suficiente tiempo y recursos para realizar evaluaciones de seguridad de las herramientas y plataformas.
- Utilice únicamente redes de Wi-Fi seguras y privadas o conéctese vía una red privada virtual (VPN, por sus siglas en inglés).
- Encripte los dispositivos y la transmisión de datos, y utilice aplicaciones de mensajería encriptada, como, por ejemplo, Signal.
- Utilice sistemas de contraseñas con doble autenticación.
- Solamente visite sitios web seguros (los que utilicen https —no solo http— en su dirección).
- Utilice contraseñas robustas y no las comparta ni utilice un solo nombre de usuario y contraseña para varias personas.
- Utilice sistemas organizativos aprobados para la transferencia cifrada y el almacenamiento de datos (por ejemplo, Microsoft SharePoint para la transferencia de archivos, en lugar de programas de transferencia de archivos de terceros).
- Utilice navegadores y motores de búsqueda que respeten la privacidad (Firefox y DuckDuckGo).
- Mantenga actualizados el software y protección contra virus.

Su equipo de informática le podrá orientar respecto a los modos más seguros de transmitir y almacenar datos. Es posible que deba trabajar con los equipos de informática en sede central para identificar algunos de los retos contextuales, con el fin de hacer contrapartidas informadas en el caso de que la seguridad de los datos entre en conflicto con la facilidad de las operaciones, haciendo más probable que las personas pasen por alto la seguridad para facilitar las prácticas de trabajo. Este es un aspecto clave a describir en su EIPD o RBA (véase la hoja de orientación 2). Posiblemente, la seguridad de los datos no sea la prioridad del personal y de los encuestadores, en especial en situaciones de estrés elevado y conflicto. Las medidas de seguridad más técnicas tienden a ralentizar los sistemas y procesos, y el personal podría verse obligado a buscar otra forma de agilizar su labor. Es vital que su organización haga énfasis en la importancia de cumplir con las medidas de seguridad estipuladas, y abra el diálogo con el personal y los encuestadores para diseñar medidas de seguridad que sean cumplidas y que no sobrecarguen innecesariamente su trabajo.

En situaciones de conflicto, incluso las mejores medidas de seguridad podrían ser fallidas porque los encuestadores o el personal reciben amenazas físicas de quienes quieren acceder a los datos de la población beneficiaria de los PTM, o a otros datos. Los riesgos al personal y a las poblaciones afectadas pueden reducirse buscando formas de almacenar cantidades limitadas de datos en dispositivos y minimizando la recopilación de datos sensibles. Muchas herramientas de recopilación de datos móviles permiten que los datos sean transmitidos de inmediato a la nube al presionar "enviar", de modo que los datos no se almacenan en un dispositivo, y esto puede ayudar a proteger a los encuestadores y al personal de primera línea. En ciertos contextos volátiles, las organizaciones se han visto obligadas a mantener escondidos los criterios de necesidades y vulnerabilidad a los encuestadores como otro mecanismo de protección. Se considera que la toma de decisiones sobre la elegibilidad realizadas fuera del país protege al personal de primera línea de la coerción y las amenazas provenientes de grupos que desean interferir con la programación de los PTM o acceder a datos sobre las poblaciones afectadas.

Además de los beneficios antes mencionados, almacenar en la nube permite a las organizaciones acceder a altos niveles de potencia informática, flexibilidad en cuanto a la ubicación y al flujo de datos, y ahorro en costes. Sin embargo, es importante señalar que el almacenamiento en la nube presenta desventajas en términos de privacidad y seguridad. El CICR identifica dos retos principales que presentan los servicios de almacenamiento en la nube: la falta de control sobre los datos y la falta de transparencia respecto a cómo los servicios de almacenamiento en la nube procesan los datos. El CICR recomienda que los actores humanitarios presten especial atención a los riesgos relacionados con: el acceso a los servicios en la nube desde ubicaciones desprotegidas o inseguras; intercepción de información sensible; autentificación deficiente; filtraciones de datos del proveedor de servicio de almacenamiento en la nube y el acceso de autoridades gubernamentales y policiales. Estos problemas deberán ser evaluados y abordados por los equipos de seguridad y privacidad para determinar la mejor manera de gestionar los datos de forma responsable. Un reto adicional a tener en cuenta es que algunos países prohíben que los datos de sus ciudadanos se transmitan fuera del país, incluso a servidores en la nube alojados fuera del país.

Puede encontrar recursos más detallados sobre la seguridad de los datos organizativos y aplicaciones que protegen la privacidad en **esta lista de comprobación de seguridad** y en la **hoja de orientación sobre encriptación** de ELAN.

El "Centre for Humanitarian Data" ofrece una **guía sobre las transferencias de datos** y **la seguridad en las operaciones organizativas**.

El CICR ofrece un **resumen de los tipos de datos que se recopilan automáticamente** cuando se utilizan aplicaciones y software digitales. Esto debe tomarse en cuenta al realizar una EIPD, PIA o RBA.

Si piensa almacenar datos en la nube, no olvide revisar las leyes nacionales de datos y asegurarse de que los datos en la nube estén protegidos por medio de acuerdos de intercambio de datos con los proveedores de servicios en la nube. Consejo: Véase el Capítulo 10 del manual de CICR, **"Data Protection Handbook"** (Manual de protección de datos) donde encontrará un resumen completo del uso del almacenamiento en nube.

UTILIZAR Y MANTENER NIVELES DE ACCESO BASADOS EN ROLES

Otra manera de mostrar responsabilidad en la gestión de datos es asegurándose de que únicamente las personas autorizadas puedan acceder a los datos. Por ejemplo, una organización puede no permitir que los gerentes a nivel distrital accedan a datos de nivel global. También es posible que los encuestadores no puedan acceder a ningún dato de un sistema, y únicamente se les permita subir datos al sistema. Los socios de un programa de PTM de gran escala podría acceder únicamente a los datos que ellos han subido al sistema y no a los datos que han sido cargados al sistema por las otras organizaciones. Estos permisos basados en roles/perfiles de usuario, reflejarán la autoridad y la responsabilidad con relación a los datos en cuestión, por ejemplo, deben permitir únicamente el acceso a los datos que cada individuo realmente necesite para desempeñar su función, ni más ni menos. Se deben realizar revisiones regulares para supervisar los niveles de acceso a datos de las personas, a medida que pasan a distintas posiciones dentro de la organización o salen de ella, así como el acceso de consultores y terceros.

Se pueden configurar autorizaciones incorporadas a los sistemas de gestión de datos que se accionan cuando se solicite acceso a ciertos datos restringidos. Este tipo de mecanismo de seguridad incluye las fechas, las solicitudes de descargas, el rastreo de vistas y otros tipos de rastreo de quién hace qué en una base de datos. Esto ayuda al equipo de informática o al gerente de sistemas a supervisar de manera continua la seguridad de la base de datos y el acceso a los datos. También es útil para determinar si la integridad de los datos se ha visto en peligro o si se está realizando algún tipo de fraude o filtración. En algunos casos, puede ser más seguro alojar los datos en la nube, pues permite que las computadoras portátiles y otros aparatos susceptibles al robo o a la piratería no contengan datos personales o sensibles.

Los niveles de acceso autorizados reducen la posibilidad de alteraciones no autorizadas de datos, filtraciones y fuga de datos, no obstante, puede ser frustrante para las organizaciones que alimentan los datos en un sistema más grande no poder tener un panorama global visualizando la totalidad de los datos. Esto puede dar la impresión de que las agencias más grandes controlan los datos y el poder de la respuesta, porque tienen acceso a todos los datos de todos los socios y por tanto, tienen un mayor conocimiento sobre las tendencias, lo que puede ser útil para solicitar fondos y para otras alianzas. Sería buena idea conversar sobre este tipo de situación con el consorcio o el Grupo de Trabajo de Transferencias Monetarias para encontrar una solución viable.

En el plano interno, las organizaciones deben dar instrucciones a sus equipos de recursos humanos para elaborar acuerdos de protección de datos y de confidencialidad para ser firmados por las personas con acceso a datos, con el fin de hacerles rendir cuentas sobre el intercambio, la eliminación o el mal uso no autorizado de los datos.

HOJA DE ORIENTACIÓN 5

ANÁLISIS Y USO DE DATOS

Una vez se disponga de los datos, ya sean datos nuevos recopilados para la respuesta de PTM o datos de fuentes existentes, se debe revisar su calidad y utilidad. Es conveniente revisar los procesos de análisis de datos para garantizar que los datos sean inclusivos, y que el análisis de estos no conduzca a la exclusión de ciertas personas o grupos a recibir los beneficios a los que tienen derecho. Si utiliza los datos para tomar decisiones automatizadas, es importante que cuente con criterios claros y transparentes para los procesos de toma de decisión, de modo que puedan ser revisados por terceros en busca de sesgos; si estos tienen sospechas o reclamos de una asignación injusta de los beneficios. Además, los datos deben utilizarse únicamente para los fines previstos para los cuales fueron recopilados y para los que exista un consentimiento u otra base jurídica para su uso.

La hoja de orientación 5 abarca aspectos a tener en cuenta para analizar y utilizar datos de manera responsable en los PTM.

UTILIZAR ÚNICAMENTE LOS DATOS PARA LOS FINES PARA LOS QUE FUERON RECOPILADOS, SALVO QUE OBTENGA NUEVOS PERMISOS

Según se ha señalado en la hoja de orientación 2 (véase las casillas 12 y 13 sobre la base jurídica), debe existir una base jurídica y un propósito legítimo para el tratamiento de datos. Antes de empezar a analizar o a utilizar datos, debe revisar la base jurídica con arreglo a la cual fueron recopilados los datos inicialmente (junto con el equipo legal y el oficial de protección de datos) y determinar si se pueden procesar, desde el punto de vista legal.

Las organizaciones humanitarias con frecuencia reciben listas de los participantes de un programa de transferencias monetarias o referencias de otros grupos (por ejemplo, socios locales, agencias homólogas, entidades de la ONU o gobiernos). Si los datos fueron recopilados con arreglo a la base de interés legítimo/función pública/interés público, es apropiado procesarlos si el segundo tratamiento se ajusta a lo explicado originalmente a las personas sobre cómo se utilizarían sus datos. Si los datos fueron recopilados sobre la base de un consentimiento, es probable que deba obtener un nuevo consentimiento antes de utilizarlos para un segundo propósito. Es importante involucrar al responsable de la privacidad o equipo legal de su organización para garantizar que no se esté violando la ley cuando se reutilicen los datos.

Los PSF, los MNO u otras entidades del sector privado querrán cotejar las listas de personas beneficiarias o retener metadatos para fines legales, que podrían ser admisibles con arreglo a los requisitos de cumplimiento jurídico. Es posible que quieran trazar un perfil de la población beneficiaria para conocer su solvencia, lo cual sería incompatible con el propósito original de la recopilación de datos

(realización de los PTM) y requiere una nueva base jurídica, y posiblemente una nueva relación con los destinatarios, con consentimientos nuevos o adicionales, u otros permisos. Por ejemplo, proceder con este tipo de tratamiento sería ilegal conforme al RGPD. Las organizaciones humanitarias deben revisar todo tratamiento de datos adicional por parte de los MNO o PSF en busca de posibles perjuicios a corto o largo plazo para las poblaciones afectadas (por ejemplo, futura inhabilidad para acceder a crédito o la comercialización de productos de servicios financieros explotadores). Este uso de los datos también podría ir en contra de los principios humanitarios de neutralidad, imparcialidad e independencia.

DEPURAR Y VERIFICAR LA CALIDAD DE LOS DATOS

Los datos desordenados arrojarán resultados sesgados o inválidos. Sin importar si los datos los recopila directamente su organización o si utiliza conjuntos o listas de datos intercambiadas por otros, es necesario depurar los datos para garantizar su utilidad. Durante la depuración de los datos se pueden buscar datos duplicados, comprobar que los participantes cumplan con los requisitos y verificar una parte de la lista. Además, puede eliminarse todo dato que pueda ser utilizado para identificar a individuos en el conjunto de datos, salvo que este dato sea necesario para la ejecución del programa. Asegúrese de documentar toda brecha, error y restricción que encuentre en el conjunto de datos.

Observación: Es necesario tener cuidado de no exponer inadvertidamente datos o información humanitaria sensible durante o después del análisis y/o visualización. El análisis de datos humanitarios sensibles sólo debe realizarse en un entorno seguro y por personas autorizadas a acceder a los datos.

Consejo: IMPACT Initiatives ofrece un **Procedimiento operativo estándar** para depurar datos que puede utilizar como guía en su propio proceso.

ELIMINAR O ANONIMIZAR DATOS PERSONALES Y SENSIBLES DE LOS CONJUNTOS DE DATOS SIEMPRE QUE SEA POSIBLE

Según se estableció en la hoja de orientación 3, la minimización de datos es un principio básico de la responsabilidad en la gestión de datos. Una manera de minimizar la cantidad de datos personales o sensibles es de anonimizarlos. En otras palabras, eliminar información que sirva para identificar a una persona, de modo que los datos se vuelvan "anónimos". Cuando los datos se anonimizan, se elimina la asociación entre los datos y las personas, de modo que no es posible identificar a una persona en los datos. Esto se logra eliminando tanto los "identificadores directos" como los "identificadores indirectos", por ejemplo, eliminado el número de identidad nacional o la fecha de nacimiento. Este proceso hace que los datos sean más privados y que las personas corran menos riesgos, porque ha eliminado la información identificativa o ha agregado un nivel en el que las personas no pueden ser identificadas.

Es importante recordar que incluso los datos anonimizados o agregados pueden poner en riesgo a grupos completos de personas; por ejemplo, si la ubicación de un grupo étnico o religioso puede utilizarse para atacar a esos grupos. Si se divulga información sobre dónde va a realizarse o se ha realizado una distribución de PTM, esto podría resultar a que grupos no deseados interfieran o perjudiquen a las personas que reciben transferencias monetarias, o a las organizaciones que las proporcionan. Aparte de planificar, en primer lugar, el modo de anonimizar los datos individuales también querrá considerar cómo proteger datos no personales. Ciertos datos únicamente deben intercambiarse o divulgarse a quienes los necesitan para fines aprobados y en entornos de datos adecuadamente protegidos con controles técnicos y organizativos adecuados.

Dado que la tecnología y los análisis de datos se vuelven cada vez más sofisticados, es probable que necesite el respaldo de su equipo de datos o de informática para anonimizar los datos.

Los datos anónimos son más seguros, pero si son demasiado generalizados, se vuelven inútiles para la implementación de los PTM. Es necesario encontrar maneras de minimizar los datos y también lograr los objetivos de los PTM.

Incluso cuando se han anonimizado los datos a nivel individual, es posible volver a identificar a las personas a través del emparejamiento (estadístico) con otros conjuntos de datos o dentro de resultados de encuestas individuales. Con frecuencia se combinan y fusionan listas de los PTM, tanto dentro de organizaciones individuales como después de compartir conjuntos de datos. Si este es el caso, se hace más fácil identificar a individuos dentro de conjuntos de datos. El control de divulgación estadística es un método para evaluar el riesgo de volver a identificar a personas y de reducir este riesgo antes de intercambiar datos. OCHA **ofrece orientación** sobre este método.

Cuando se colabora con socios comerciales en lugares donde exista preocupación por la privacidad de los datos, una opción podría ser establecer un acuerdo con un PSF para utilizar subcuentas, por lo que la diligencia debida o el KYC se completa únicamente en la agencia implementadora como tenedora de la cuenta principal y no en quienes acceden a las subcuentas. Se puede acceder a las subcuentas a través de tarjetas inteligentes (por ejemplo, tarjetas prepago o cajeros automáticos) que únicamente tienen números de referencia anexos y que incluyen detalles personales. Luego, se les permite a los destinatarios retirar efectivo sin proporcionarle al PSF sus datos personales. Únicamente la agencia implementadora tiene la información que vincula la tarjeta o la cuenta con el destinatario de efectivo.

TOMA DE DECISIONES AUTOMATIZADA

El Relator especial de la ONU sobre pobreza extrema y derechos humanos advirtió en 2019, que las reformas de bienestar facilitadas, justificadas y amparadas por las nuevas tecnologías digitales pueden reflejar valores y presunciones que no están alineados con los principios de derechos humanos.[37] Por ejemplo, cuando las decisiones las toman programas informáticos automatizados, es posible excluir por error, a personas que deberían recibir beneficios. Además, las personas pueden ser señaladas o categorizadas de manera permanente, lo que puede conducir a una discriminación en el futuro; por ejemplo, alguien que recibió asistencia debido a la condición de refugiado durante una fase específica de su vida, podría ser categorizada por los algoritmos que toman decisiones como riesgo crediticio. A medida que los PTM se vuelven cada vez más digitales, es importante que los valores humanitarios permanezcan a la delantera y que los datos que perjudican y excluyen a las personas no sean exacerbados por herramientas y tecnologías digitales que los agentes de transferencias monetarias incorporen a sus programas. La toma de decisiones automatizada sobre la base de los datos podrá permitir una mayor escala y una toma de decisiones más ágil, pero todavía se encuentra en las etapas iniciales y podría conducir a la exclusión o a daños futuros.

El RGPD también contiene artículos específicos que protegen a las personas cuyos datos son objeto de toma de decisiones automatizadas que tienen efectos legales o de importancia similar sobre ellas. Por ejemplo, el RGPD ordena que cuando se realice este tipo de toma de decisiones, las personas deben tener información sobre el tratamiento; deben existir maneras simples para que soliciten la intervención humana o impugnen una decisión y se deben verificar de manera regular los sistemas con el fin de garantizar que estén trabajando del modo previsto.

Aunque la mayoría de las organizaciones no está utilizando la toma de decisiones automatizada en sus programas, está siendo cada vez más utilizado en el sector comercial para transacciones financieras, como aprobaciones de crédito. En el contexto de los PTM, algunas organizaciones están estudiando el modo de utilizar registros de llamadas para identificar a posibles personas receptoras de PTM.

En el caso de utilizar la toma decisiones automatizada, esta debe respaldar —no reemplazar— la toma de decisiones humana. Las organizaciones que operan los PTM deben garantizar que toda toma de decisiones automatizada utilizada para focalizar, inscribir o registrar a personas beneficiarias se realice con algoritmos abiertos y transparentes, supervisión humana, investigaciones comparativas y exámenes para verificar posibles sesgos, y mecanismos claros de quejas y rectificaciones, en el caso de que una decisión fuese errónea o conduzca a daños futuros.

Véase el **estudio de caso en focalización remota usando data no tradicional** de CaLP, donde encontrará más debate sobre este tema.

37 P. Alston (2019), Rapport du Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté. Assemblée générale des Nations Unies.

HOJA DE ORIENTACIÓN 6

INTERCAMBIO DE DATOS

Las organizaciones implementadoras de los PTM trabajan en una amplia variedad de contextos, incluidos conflictos activos, crisis de refugiados, poblaciones de desplazados internos y bloqueos. El intercambio de datos es necesario en los PTM, y a medida que los grupos de trabajo de transferencias monetarias y los consorcios se alinean y colaboran, se establecen alianzas con los PSF y los MNO, y se realizan vínculos con los sistemas de protección social; el intercambio de datos es cada vez más frecuente por razones de coordinación y otros motivos.

Los donantes y actores humanitarios respaldan cada vez más el desarrollo de registros únicos o sociales para programas de asistencia social y una mayor interoperabilidad e intercambio de información, alejándose de sistemas de gestión de la información separados e inconexos. Algunas agencias de la ONU, por ejemplo, el PMA, ACNUR, Unicef y OCHA, están presionando a favor de enfoques comunes a los PTM humanitarios y a una colaboración entre agencias.[38] No obstante, con frecuencia, los beneficios de los intercambios de datos se definen en términos de avances en la eficiencia, haciendo poca referencia a la protección y a otras ventajas y compensaciones.[39]

La hoja de orientación 6 ofrece lineamientos sobre el intercambio responsable de datos, aunque reconoce que este es un ámbito polémico que debe resolverse caso a caso, dependiendo del contexto y de los agentes involucrados.

DETERMINAR QUÉ INFORMACIÓN DEBE SER COMPARTIDA, CON QUIÉN Y POR QUÉ

Según se especifica en la hoja de orientación 2, casilla 10, sobre los controladores de datos y los procesadores de datos, los controladores de datos toman decisiones sobre el modo en que se recopilan y procesan los datos. También toman decisiones sobre el intercambio de datos. Los procesadores de datos no deben tomar decisiones sobre con quién intercambiar los datos, ni por qué intercambiarlos, éste debe ser el mandato del controlador de datos.[40]

Antes de intercambiar cualquier dato, debe determinar los siguientes parámetros:

- **Propósito:** ¿Por qué se comparten los datos? ¿Qué datos está compartiendo? ¿Necesita compartir todos los datos para lograr el propósito, o puede compartir solo una parte o ciertos campos?
- **Legalidad:** Desde el punto de vista legal, ¿tiene la capacidad de compartir estos datos o de decidir qué debe compartirse? ¿Tiene permiso o se les ha informado a las personas afectadas que los datos serán compartidos?

38 Véase esta declaración sobre el Sistema común de asistencia en efectivo.
39 R. Goodman et al. (2020) "Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises" (Revisión y análisis de los sistemas de identificación y registro en crisis prolongadas y recurrentes).
40 Oficina del Comisionado de Información del Reino Unido (2018) "Controllers and Processors" (Controladores y procesadores).

- **Mecanismos:** ¿Cómo se compartirán los datos? ¿Cómo se almacenarán los datos? ¿Ha investigado a la organización con la que compartirá los datos para garantizar que ésta pueda mantener los datos seguros y privados? (Véase la hoja de orientación 4 sobre transmisión y almacenamiento de datos).
- **Descripción:** ¿Ha proporcionado suficiente descripción sobre los datos y el contexto en el que fueron recopilados, cuándo fueron recopilados, y otra información clave con el fin de que los datos no sean utilizados fuera de contexto?[41]

Probablemente sea necesario crear versiones diferentes de conjuntos de datos para diferentes usos y socios. Los datos personales y sensibles deben compartirse únicamente si es absolutamente necesario y después de que haya un acuerdo formal de intercambio de datos.

Antes de compartir cualquier tipo de dato, es vital asegurarse de que las personas reflejadas en los datos comprendan lo que pasará con sus datos y que han dado su consentimiento informado para su uso o, de lo contrario, que se haya establecido otra base jurídica para el tratamiento e intercambio de datos. Esto significa que los participantes han dado su permiso para el intercambio de los datos, con pleno conocimiento de las posibles consecuencias (véase la hoja de orientación 2 y las casillas 12 y 13).

El acceso a datos personales y sensibles debe realizarse según la "necesidad de conocer", no por defecto.

Considere qué tipo de acceso necesitan realmente los socios y, si es posible, configure permisos de acceso y rastreadores de bases de datos para controlar quién puede visualizar, agregar, alterar, descargar o eliminar datos.

EVALUAR LOS RIESGOS Y BENEFICIOS ANTES DE COMPARTIR DATOS CON GOBIERNOS

Una suposición muy común es que los sistemas centralizados de los PTM humanitarios formarán la base de los sistemas de protección social a más largo plazo, o de sistemas dirigidos por el gobierno. Estas presunciones deben valorarse con aspectos relacionados con la privacidad y la protección de datos debido a los posibles efectos sobre los derechos básicos de los receptores.[42] En algunos casos, la opción correcta podría ser un sistema unitario y en otros casos, el contexto del país y la respuesta podrían hacer que ésta no sea la opción ideal. En cualquier contexto, las organizaciones deben intentar evaluar esto conjuntamente para encontrar la mejor solución para las poblaciones afectadas por la crisis.

Dependiendo del contexto, intercambiar datos con los gobiernos puede conllevar altos riesgos para las poblaciones vulnerables; por ejemplo, si se compartieran datos de migrantes irregulares con gobiernos que no acogen a migrantes, o si grupos armados locales accedieran a datos de refugiados o de poblaciones de desplazados internos a quienes quisieran hacer daño. Además del intercambio de datos legal (aunque posiblemente perjudicial), el intercambio de datos forzado ocurre en varios niveles de una respuesta, incluyendo a nivel local cuando los encuestadores reciben amenazas y son acosados, y en niveles más altos donde las agencias son presionadas a compartir datos para que se les permita operar en un país o en una zona específica del país. Es importante recordar que los datos compartidos con una sección del gobierno podrían ser intercambiados más adelante con otra sección del gobierno, y que los datos que se comparten con entidades que tienen mandatos de compartir con los gobiernos, podrían tener la obligación de compartirlos más adelante.

Recuerde que los gobiernos cambian, por tanto, un intercambio de datos que hoy luzca libre de problemas, podría ser problemático el año siguiente. Por este motivo, la mejor práctica es la minimización de datos y el intercambio limitado de estos, como se indica en la hoja de orientación 2, donde abordamos el tema de la gobernanza de datos. Un cambio de gobierno podría actuar como desencadenante para la revisión y posiblemente actualización de su EIPD.

Véase el **Estudio de caso sobre el intercambio de datos con los gobiernos** del CaLP.

EVALUAR LOS RIESGOS Y BENEFICIOS DEL INTERCAMBIO DE DATOS Y LA COLABORACIÓN CON UN CONSORCIO O UN GTM

El intercambio de datos y el uso de sistemas interoperables y comunes pueden facilitar el proceso de aplicación de los PTM y reducir la duplicación y el fraude cuando son bien realizados y se presta suficiente atención a la protección de datos. En la IASC "Operational Guidance on Data Responsibility" (Orientación operativa sobre responsabilidad en la gestión de los datos del Comité Permanente Inter Agencial) se recomienda, por ejemplo, establecer Protocolos de intercambio de información a nivel de respuesta (vía el Mecanismo de coordinación inter-cluster ICCM, por sus siglas en inglés) o el Equipo humanitario de país HCT, por sus siglas en inglés). También se recomienda establecer un Protocolo de intercambio de información específico para los GTM en aquellos contextos donde esto sea útil. A la vez, porque los datos significan poder, con frecuencia surgen desafíos dentro de los consorcios o de los GTM al determinar qué sistema utilizar y quién accede y gestiona los datos en el sistema. Además, los sistemas únicos y el aumento de intercambio de datos pueden exponer los datos de la población beneficiaria de los PTM a violaciones de la privacidad y causar daños directos, si los datos se filtran o se intercambian con agentes que los usen de manera indebida.

41 A. Doornbos (2020) Data Sharing with Partners (Intercambio de datos con los socios).
42 R. Goodman et al. (2020) Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises (Revisión y análisis de los sistemas de identificación y registro en crisis prolongadas y recurrentes).

Los miembros de consorcios o de los GTM con frecuencia enfrentan retos al colaborar e intercambiar datos. Como se señala en la hoja de orientación 1 sobre el contexto y las capacidades, el proceso de determinar quién dirige una respuesta y quién intercambia los datos con quién, está plagado de tensiones relacionadas con el poder y el control de una respuesta, el acceso actual y futuro a la financiación de los donantes y los diferentes enfoques e inquietudes respecto a la privacidad de los receptores de los PTM. Algunas organizaciones expresan reservas respecto a la cantidad de datos que se capturan de los destinatarios de los PTM, si esto incluye datos biométricos y si los sistemas de datos gestionados por otros agentes son lo suficientemente seguros. Por otra parte, aquellos socios de ejecución que reciban fondos de la ONU quizás tengan que compartir datos con las agencias de la ONU para poder participar en una respuesta. Obviamente, surgen tensiones cuando la provisión de fondos depende de acuerdos de intercambio de datos, pues, el suministro, el acceso y el control de los datos es político e implica dinámicas de poder.

Si bien cada organización contará con sus propios sistemas, si el intercambio de datos forma parte de la respuesta de PTM, los datos tendrán que ser interoperables de modo que puedan alimentar el mismo sistema de gestión de información. Este es otro aspecto desafiante en el intercambio de datos: ponerse de acuerdo sobre qué datos recopilar y cómo estructurarlos para que puedan ser utilizados con eficacia.

Algunos agentes de PTM, consorcios y GTM, están innovando en los modos de intercambiar datos en el marco de acuerdos de intercambio de datos establecidos. Por ejemplo, si las organizaciones no han celebrado acuerdos de intercambio de datos entre sí, pero cada una tiene un acuerdo de intercambio de datos con una tercera agencia, podrían decidir cada una intercambiar datos con la tercera agencia, que a su vez puede servir de enlace, sin dejar de cumplir los acuerdos legales y de intercambio de datos. Otros miembros de GTM experimentan con distintas maneras de intercambiar datos de manera anónima, por ejemplo, a través de un algoritmo de control seguro o utilizando tecnología de cadena de bloques. El programa "Emergency Social Safety Net" (Red de protección social de emergencia) de Turquía ha creado una arquitectura de intercambio de información para datos entre socios, y con el fin de alinear los sistemas de información sin compartir los datos con todos los actores. Los actores de los PTM también pueden establecer Protocolos de intercambio de información o Procedimientos operativos estándar que guíen el modo en que pueden compartir los datos entre agencias.

Las leyes sobre la protección de datos pueden utilizarse para la toma de decisiones futura sobre la gestión de datos. Los controladores de datos serán responsables de las filtraciones de datos o las violaciones a la privacidad y el controlador es responsable de manejar cualquier solicitud de las poblaciones afectadas relacionada con la rendición de cuentas. Al establecer quién es el controlador de datos y quién es el procesador de datos, o si habrá controladores conjuntos, las organizaciones podrán encontrar un terreno neutral donde establecer una conversación abierta con respecto al poder y a la rendición de cuentas (véase la hoja de orientación 2, casillas 10 y 11 sobre los controladores de datos y los procesadores de datos).

REVISAR LAS POLÍTICAS SOBRE DATOS DE LOS PSF Y TERCEROS ANTES DE ACEPTAR UN INTERCAMBIO DE DATOS

A medida que las modalidades de transferencias monetarias cambian para incluir más PSF y MNO, los actores de los PTM con frecuencia intercambian los datos personales de los participantes con los PSF y con los gobiernos del país anfitrión para cumplir con los requisitos de KYC, entre otros. Estos datos podrían incluir nombres, números de teléfono o números de identidad, así como, cada vez más, datos biométricos. Con frecuencia, los PSF mantienen registros de transacciones, además de datos personales. Estos registros mantienen información de dónde y cuándo las personas realizan compras, y de sus ahorros y gastos. Estos datos sobre transacciones deben estar protegidos contra el uso indebido. Es importante que los actores de los PTM tengan una imagen clara de lo que los PSF recopilarán sobre la población beneficiaria del programa mientras les proporcionan sus servicios, y que evalúen, durante el proceso de EIPD o RBA, los posibles riesgos que esto supone a las poblaciones afectadas. Todo contrato debe incluir condiciones explícitas respecto al intercambio de datos, así como estipulaciones relacionadas con la responsabilidad ante todo tipo de fuga o filtración de datos.

Cuando establezca acuerdos para compartir datos con socios del sector privado, incluidos los PSF y los MNO, asegúrese de revisar las políticas de intercambio de datos, y sus términos y condiciones, e incluir condiciones robustas en su propio acuerdo a fin de garantizar un estándar adecuado de protección de datos y de responsabilidad en la gestión de datos de una manera más general, incluyendo restricciones sobre el intercambio, el uso, la retención y la eliminación. Algunos acuerdos pueden incluir una cláusula predeterminada en sus contratos, que permite el "intercambio con terceros", lo que significa que pueden intercambiar cualquier dato con cualquier persona en el futuro. Es probable que estos proveedores además tengan una cláusula que indique que, en el caso de ser adquiridos o vendidos, todo dato que posean será parte clave de los activos que se incluirán en la venta o adquisición.

Si no se siente cómodo con este escenario, asegúrese de plantear la cuestión antes de compartir los datos o de acordar una asociación. Es perfectamente razonable rechazar una política de intercambio de datos predeterminada y hacer que el acceso a los datos del PTM sea más adaptado a las necesidades particulares de la tercera parte.

Realice evaluaciones de debida diligencia a los socios del sector privado, antes de intercambiar datos con los mismos.

Los PSF y otros terceros pueden oponerse a las restricciones relacionadas con el intercambio de datos y su uso posterior. En algunos casos, puede que tengan razones legítimas (por ejemplo, si necesitan proporcionar KYC u otros datos a gobiernos, desde el punto de vista legal). En otros, quizás tengan un modelo comercial basado en la obtención de ganancias a partir de los datos, y esto podría ser incompatible con la misión de la organización humanitaria. Si bien los requisitos legales como el KYC no son negociables, es posible agregar cláusulas que prohíban el uso de datos de los receptores de PTM para fines comerciales, o estipular que los PSF deben ser transparentes y notificar a las organizaciones cuando haya una solicitud de intercambio de datos con autoridades gubernamentales.

Las agencias homólogas quizás no sean conscientes de los riesgos que plantea el compartir datos, por tanto, es importante conversar sobre este tema antes de firmar acuerdos de intercambio de datos.

ESTABLECER ACUERDOS DE INTERCAMBIO DE DATOS ANTES DE COMPARTIR DATOS

Antes de compartir datos, es importante indicar de manera explícita, lo que se puede y lo que no se puede hacer con los datos. Esto, por lo general, se hace a través de un acuerdo de intercambio de datos. Los acuerdos de intercambio de datos no contienen necesariamente información específica a los datos del programa que se recopilarán. En cambio, podrían expresar lo que se puede y lo que no se puede hacer al compartir los datos. Deben incluir los estándares mínimos de seguridad y privacidad de datos y establecer responsabilidades y obligaciones para las violaciones a la privacidad de datos y de seguridad o el uso indebido de datos, o el intercambio futuro sin autorización.

Establecer un acuerdo de intercambio de datos puede tomar varios meses, incluso si existen términos de referencia para la colaboración entre organizaciones y agencias. Esto se debe, en parte, a que toma tiempo establecer estándares de interoperabilidad. También se debe a que, por lo general, las organizaciones y agencias necesitan involucrar a sus equipos legales, de protección de datos y de informática, lo que podría requerir un compromiso tanto a nivel nacional, como global, para las organizaciones internacionales. Se ha dado una tendencia de intercambiar datos sin tener un acuerdo formal previo. No obstante, debe señalarse que, con arreglo al RGPD, se requiere por ley celebrar Acuerdos de intercambio de datos y Acuerdos de transferencia de datos y otras regulaciones de privacidad de datos. En algunos casos, negociar acuerdos de intercambio de datos se ha convertido en un ejercicio de poder de las organizaciones más grandes sobre las más pequeñas.

La información sobre el intercambio de datos debe incluirse en las solicitudes de consentimiento u otra información que se proporcione a las poblaciones afectadas para que tengan claro a qué están dando su consentimiento o qué ocurrirá con sus datos. Incluso si no utiliza el "consentimiento" como base jurídica para la recopilación de datos, debe informar de manera transparente a las personas sobre con quiénes se pudieran intercambiar sus datos.

En los casos en que sea necesario realizar una respuesta urgente y todavía no se haya preparado un acuerdo de intercambio de datos, quizás sea necesario intercambiar una cantidad limitada de datos con arreglo a un memorando de entendimiento específico y de duración limitada con el fin de proceder con la respuesta. Esta es una solución intermedia que puede tomar en cuenta. ¿Es mejor compartir datos con el fin de que la respuesta pueda proceder o es demasiado alto el riesgo? En estos casos, quizás quiera optar por un diseño de PTM con la menor carga de datos que pueda manejar.

Los acuerdos de intercambio de datos son una herramienta importante para la gestión responsable de los mismos. No obstante, en la práctica, quizás sea difícil implementar los mecanismos de rendición de cuentas de estos acuerdos, lo que significa que hay poco control sobre cómo se utilizan o se comparten. Por esta razón, es importante respetar los principios de minimización de datos al determinar exactamente qué datos deben compartirse y con quién.

El intercambio de datos entre los miembros de los GTM y los consorcios, con los gobiernos y los PSF, debe ser un aspecto clave para evaluar cuándo realizar su EIPD, PIA o RBA en las evaluaciones de capacidades y contexto iniciales y durante el diseño y la planificación de programas. También debe realizar investigación de antecedentes para cerciorarse de los niveles de protección de datos que funcionaban durante respuestas pasadas y sistemas de datos que se proponen para una respuesta conjunta.

El ACNUR y el PMA han creado un Memorando de entendimiento sobre el intercambio de datos disponible **en este enlace**.

La **"Data Responsibility Guide"** (Guía de responsabilidad en la gestión de datos) de la OCHA abarca el tema del intercambio de datos.

CREAR ESTRATEGIAS Y ENSAYAR LA PREVENCIÓN Y RESPUESTA AL "INTERCAMBIO FORZADO DE DATOS" Y A OTROS INCIDENTES CRÍTICOS DE DATOS

Además del intercambio de datos acordado, en muchos contextos de los PTM, el "intercambio forzado de datos" es una realidad. Es posible que su personal y sus socios locales puedan verse coaccionados por diversos medios para compartir datos con grupos que se benefician del acceso y el control de los datos. También existe la preocupación de que algunas entidades compartan datos que no deberían compartirse, como cuando las organizaciones no están dispuestas a compartir datos con los gobiernos, pero los datos se obtienen a través de los PSF o de otra agencia asociada. Es importante identificar las posibles áreas de riesgo de compartir datos de forma forzada y ensayar cómo podrían responder usted y su personal.

Véase la hoja de orientación 2, Diseño y planificación, donde encontrará más información sobre los incidentes de datos críticos.

CaLP motiva a los Grupos de trabajo de transferencias monetarias y a los consorcios a colaborar y crear estrategias conjuntas sobre el modo de responder a los incidentes de datos comunes en sus contextos y a contribuir con un registro de estos incidentes con el fin de poder realizar mayor investigación y aprendizaje sobre las buenas prácticas. Véase la CaLP **"Critical Data Incident Management initiative"** (Iniciativa de gestión de incidentes de datos críticos de CaLP) donde encontrará más información.

PONER EN ACCIÓN LOS ACUERDOS DE INTERCAMBIO DE DATOS

Una cosa es redactar un acuerdo de intercambio de datos y otra es garantizar su aplicación. Las organizaciones deben asegurarse de que su personal y sus socios sean conscientes del contenido de los acuerdos de intercambio de datos y de otros acuerdos sobre datos relacionados con donantes, gobiernos y PSF, para que las organizaciones no compartan o gestionen los datos fuera de estos acuerdos; y con el fin de que los socios respeten lo que ha sido convenido.

Toma mucho tiempo y esfuerzo elaborar un acuerdo de intercambio de datos y puede ser difícil de prepararlo. Requiere la aprobación de los equipos legales y de las oficinas de protección de datos, lo que podría implicar etapas de revisión considerables. Es importante que una de las primeras tareas de la respuesta sea crear acuerdos de intercambio de datos y que se asignen recursos a este proceso, para contar desde el inicio con el personal y el tiempo necesarios.

Establezca un tiempo para revisar los acuerdos con los socios y converse sobre las expectativas en la gestión de datos y las restricciones para compartir los datos en las etapas iniciales del proceso. Si es necesario, ofrezca capacitación. Posiblemente sea necesario ofrecer apoyo a la capacidad o a otros recursos de los socios si requieren mejorar las destrezas, los conocimientos o los sistemas para un intercambio de datos seguro y responsable.

HOJA DE ORIENTACIÓN 7

MANTENIMIENTO, RETENCIÓN Y ELIMINACIÓN DE DATOS

A través del ciclo del programa, los datos que recopile deben almacenarse y mantenerse de manera segura, según se indica en la hoja de orientación 4. Cuando se completa una respuesta, los datos deben retenerse o destruirse, dependiendo de la situación.

Su organización debe retener datos personales y sensibles únicamente por el tiempo que sea necesario. En general, es mejor cuanto antes se puedan anonimizar los datos personales. Una vez los datos ya no sean requeridos para fines legales u otros propósitos legítimos, deben destruirse de manera segura.

DESDE EL INICIO PLANIFICAR Y PRESUPUESTAR EL MANTENIMIENTO, LA RETENCIÓN Y LA ELIMINACIÓN DE LOS DATOS

Si bien la retención y eliminación de datos ocurren al final del programa o al final del ciclo de vida de los datos, es necesario haberlo incluido en sus planes desde las etapas iniciales de diseño y planificación para garantizar un presupuesto suficiente. Una falta de planificación puede poner en riesgo a los participantes del programa o provocar que almacene los datos más tiempo de lo necesario. Para planificar correctamente, debe comprender las necesidades de todas las partes interesadas. Incluso dentro del mismo programa, los distintos equipos podrían tener diferentes necesidades para retener datos. Por ejemplo, el personal de finanzas y de control quizás deban tener acceso a los datos para una auditoría del donante, años después de finalizado el programa. En cambio, el personal de programas quizás ya no necesite los datos una vez el programa ha finalizado. Para cumplir con las necesidades relacionadas con los datos de todos los equipos, es importante llegar a un entendimiento compartido de las necesidades de retención de datos de cada equipo antes de finalizar el programa y asegurarse de que los sistemas utilizados para recopilar y almacenar datos de programas estén coordinados sin problemas de inicio a fin.

ÚNICAMENTE RETENER LOS DATOS QUE NECESITE, AL NIVEL DE DETALLE QUE NECESITE, Y DESTRUIR EL RESTO

Los PTM recopilan muchos datos. Dependiendo del tipo de programa y de la estructura de financiación, quizás deba retener datos relevantes para justificar la toma de decisiones, para fines de auditoría o para fines de seguimiento, evaluación y aprendizaje. Quizás a los gestores de programas les preocupe eliminar datos por temor a eliminar algo importante. Y aunque esto puede ser un riesgo, mantener los datos por demasiado tiempo también lo es.

La hoja de orientación 7 ofrece orientación sobre la responsabilidad en la retención y la eliminación de datos.

(La hoja de orientación 4 sobre la transmisión y el almacenamiento ofrece más información sobre cómo asegurar los datos para una respuesta activa).

Cuantos más datos personales y sensibles se mantengan, mayor será la responsabilidad y el riesgo que asuma una organización, y mayor será el riesgo para los receptores de los PTM de que sus datos puedan filtrarse o de que tengan acceso a ellos personas que podrían darles un uso indebido o causarles daño. Además, a medida que transcurre el tiempo y cambia el personal, resulta más difícil que los datos sean precisos, que el nuevo personal sea consciente de las limitaciones que se han establecido sobre un cierto conjunto de datos, y que se pueda rastrear con precisión una fuente de datos, y los permisos asociados a los mismos. Por otro lado, una organización que mantiene datos es responsable de los mismos y debe poder responder a las solicitudes de los participantes para acceder a sus datos personales. Mientras más datos mantenga una organización, más complejo será esto.

Quizás su organización ya tenga una política general de retención de datos, y que esta incluye los datos de sus PTM. Si trabaja en un consorcio más amplio, los miembros deben acordar una política de retención de datos. El Grupo de trabajo de transferencias monetarias podría ser un buen lugar para debatir en qué momento del ciclo del programa de transferencia monetaria deben anonimizarse ciertos datos y cuáles son los debidos plazos para destruir determinados tipos de datos. Establezca términos claros para la retención y eliminación de datos en sus diferentes documentos de orientación, memorando de entendimiento, acuerdos de transferencia de datos y acuerdos de intercambio de datos; entre otros.

Aunque se sienta tentado a guardar listas de receptores de los PTM por periodos prolongados, recuerde que estas listas podrían perder relevancia después de un tiempo y ya no ser útiles para identificar población beneficiaria de PTM, o para distribuir efectivo, si éstas no han sido mantenidas y actualizadas.

A veces los planes de retención de datos se denominan planes de retención, archivo y eliminación (RAD, siglas en inglés para "Retention, Archival and Destruction"). Véase la **"Data Starter Kit"** (Guía práctica de inicio sobre datos) de ELAN donde encontrará más orientación y ejemplos de RAD.

www.calpnetwork.org

Marzo de 2021