Guía práctica para la protección de datos en los Programas de Transferencias Monetarias (PTM)

Suplemento de la caja de herramientas para «PTM en emergencias»

Enero del 2021

IFRC

TABLA DE CONTENIDO

I. Introducción

Puesto que el Movimiento Internacional de la Cruz Roja y la Medialuna Roja aumenta su compromiso con la ampliación de las transferencias monetarias, también aumenta la recolección y tratamiento de datos personales, en particular, los de aquellas comunidades vulnerables a las que se asiste. La protección de datos no solo es una cuestión de buena gobernanza, sino de crear confianza. En tiempos de crisis, los beneficiarios piensan más en las prioridades urgentes más necesarias para su supervivencia y seguridad que en los riesgos derivados del intercambio de sus datos personales con organizaciones de ayuda humanitaria. Razón de más para que los profesionales que gestionan los programas de transferencias monetarias respeten y sean responsables de la protección de datos de los beneficiarios. Asimismo, otras partes interesadas como donantes, entidades del gobierno y otros asociados depositarán una mayor confianza en nuestros programas de transferencias monetarias (PTM) si se prueban buenas prácticas y normas para la protección de datos.

Población destinataria y objetivo del documento

Esta guía práctica está dirigida a los profesionales que gestionan el dinero en efectivo o programas para integrar los principios de protección de datos en la ejecución de transferencias monetarias. Existen muchas referencias útiles sobre la protección de datos para el personal humanitario, como el Manual sobre Protección de Datos en la Acción Humanitaria y las respectivas políticas de protección de datos del IFRC y del CICR. Si bien estas referencias son de una naturaleza más genérica o sólo abordan algunas de las cuestiones a las que se enfrentan los responsables de la gestión del programa de transferencias monetarias a gran escala, este documento pretende traducir los principios generales de protección de datos en una orientación práctica y específica para las actividades clave del proceso de PTM. Esta guía presentará consideraciones sobre la protección de datos y guiará a los profesionales del manejo de transferencias monetarias en la toma de decisiones y su aplicación.

Este documento hace referencia a los procesos de la Caja de herramientas en casos de emergencia y complementará la caja de herramientas hasta que se revise para incluir directamente las consideraciones de protección de datos presentes en este documento.

IMPORTANTE:
Las Sociedades Nacionales deben contextualizar esta guía para que cumpla con los requisitos propios de las mismas; en particular, la adhesión a sus leyes nacionales de protección de datos y políticas que podrían ser más estrictas que las normas de protección de datos expuestas aquí.

Estructura del documento

El próximo apartado ofrecerá una visión general de la protección de datos para presentar a los lectores los principios clave y terminologías que se emplearán en esta guía. A continuación, le seguirán unos capítulos para cada uno de los cinco procesos claves en los PTM.

Antes de desarrollar esta guía, se llevó a cabo un análisis de la caja de herramientas para programas de transferencias monetarias (PTM) para identificar los procesos en los que se recopila y procesa datos personales de los beneficiarios. Seguidamente, se priorizaron los procesos según el nivel de tratamiento de datos personales y posibles riesgos. Esta guía se centrará en 5 de esos procesos prioritarios:[1]

1 Este pretende ser un documento abierto y una guía práctica para otras áreas de la caja de herramientas para PTM que puedan desarrollarse en revisiones posteriores a medida que nuestra experiencia en la protección de datos va en aumento.

1. Focalización
2. Registro de los beneficiarios
3. Uso de proveedores de servicios financieros.
4. Intercambio de los datos con gobiernos, otras organizaciones humanitarias y donantes.
5. Seguimiento posterior a la distribución

Cada capítulo incluye una visión general que describe cómo se utilizan o procesan los datos personales con ejemplos extraídos de consultas con Sociedades Nacionales. A continuación, se expondrán un conjunto de consideraciones sobre la protección de datos basadas en cuestiones claves del proyecto.

Cada consideración comienza con un recuadro que resalta una cuestión clave del proyecto. El símbolo 🔔de una campana indica los principios de la protección de datos relevantes para la consideración. A continuación, se proporciona un recuadro con la cuestión relevante del proyecto para incorporar la consideración de protección de datos. Las mismas se explican con mayor detalle y van acompañadas por ejemplos simplificados para demostrar cómo se deben aplicar.

El último capítulo se centra en las consideraciones generales aplicables para el ciclo completo del PTM.

II. Visión general de la protección de datos

Tratamiento de datos personales

¿Qué son exactamente los datos personales? Los datos personales son cualquier información relativa a una persona viva identificada (el interesado). Estos datos pueden ser personales incluso si a primera vista no parecen estar directamente relacionados con una persona, pero podría llevar a su identificación indirecta con información adicional. Esto puede sonar complicado, pero básicamente significa que la protección de datos cubre una amplia cantidad de información, y que el término “datos personales” no puede interpretarse de forma restrictiva. En el contexto de las transferencias monetarias, la mayoría de los datos de beneficiarios recogidos se calificarán como datos personales, por ejemplo:

- Nombres y detalles de contacto.
- Número de identificación
- Número de cuenta bancaria
- Detalles sobre empleo
- Situación familiar
- Estado de salud
- Dirección o ubicación

Al contrario, los datos recopilados para analizar la situación en un **nivel abstracto** (p. ej. información económica de la región, etc.) no se califican, por lo general, como datos personales. Estos datos son anónimos ya que no tratan la información de las personas en absoluto, o bien la información está en forma agregada.

Los datos agregados son los datos resultantes de resumir y poner en común datos individualizados. Los individuos no son identificables (ni directa, ni indirectamente). Los datos agregados suelen ofrecer una visión general mediante gráficos, tablas, estadísticas e información general sobre grupos de personas, no individuos. Los ejemplos incluyen estadísticas de tipos de medios de vida, tamaño o ingresos medios de los hogares, los porcentajes de los daños a los refugios en una zona, o el cálculo de la canasta básica de gastos mínimos (MEB).

El **tratamiento** de datos personales se refiere a todo lo que se haga con los datos, como: recolectarlos, almacenarlos, compartirlos, evaluarlos, modificarlos, publicarlos, registrarlos, utilizarlos, corregirlos e incluso eliminarlos.

Base legítima

Todo tratamiento de datos personales requiere una base legítima (o legal). Una que se emplea con frecuencia es el consentimiento. Sin embargo, existen otros motivos para legitimar el tratamiento de los datos personales, entre los que se incluyen:

- Cumplimiento de una obligación legal.
- Cumplimiento de un contrato con el interesado.
- Una tarea de interés público.
- Interés(es) vital(es) de una persona (amenazas a corto plazo para su salud mental o física)
- Interés legítimo de la entidad (p.ej., IFRC, CICR, una Sociedad Nacional) que está tramitando la información personal.

En ocasiones, decidir la base legítima en la que apoyarse puede ser complicado. Encontrará más detalles sobre la definición y diferencias de estas bases legítimas en la Política de la IFRC sobre protección de datos personales , el Manual sobre Protección de Datos en la Acción Humanitaria de la CRIC y en el Brussels Privacy Hub.

En las transferencias monetarias es bastante habitual apoyarse en el consentimiento. Muchos de los profesionales que gestionan un programa de transferencias monetarias incluyen un apartado de consentimiento al principio de la encuesta o del formulario de recogida de datos. Sin embargo, esta no es necesariamente la mejor opción en caso de emergencias. Esto se explica con mayor detalle en el capítulo sobre el registro de beneficiarios con un árbol de decisión, que ayuda a evaluar si una o más bases legítimas puede ser lo más apropiado en estas circunstancias.

Principios fundamentales de protección de datos

Hay muchos principios de protección de datos que se deben tener en cuenta al procesar información personal. Aunque puedan cambiar los nombres según la política o instrumento internacional, por lo general los principios principales de la protección de datos aceptados son: (1.) legitimidad, equidad y transparencia; (2.) limitación de los fines; (3.) minimización de los datos; (4.) precisión; (5.) limitación del almacenamiento; y (6.) integridad y confidencialidad (seguridad). Puede encontrar más detalles sobre éstos en la Política de la IFRC sobre protección de datos personales y en el Manual sobre Protección de Datos en la Acción Humanitaria.

No obstante, para los fines de esta guía, nos centraremos en los principios más relevantes en las transferencias monetarias (teniendo en cuenta que el principio de legitimidad, o “base legítima” ya se ha comentado anteriormente). En general, los principios se debatirán conjuntamente cuando sea necesario para realizar el análisis pertinente de la protección de datos, aunque en sentido estricto se consideren principios distintos. Por ejemplo, en el próximo apartado se analizarán conjuntamente dos principios distintos “minimización de datos” y “limitación de los fines”, ya que no es posible analizar los datos necesarios sin una evaluación de los fines de la recogida y tramitación de los datos.

Minimización de datos, necesidad y limitación de los fines

El principio de minimización de datos consiste en “recoger lo menos posible y SÓLO aquello que sea necesario”. Para definir lo que es necesario, es importante identificar con claridad la finalidad para la que se van a utilizar los respectivos datos. En el caso de los PTM, el tratamiento de datos personales puede servir para varios fines (p. ej. comprobar los criterios de selección, verificar la identidad, facilitar

las transferencias monetarias, detectar o evitar el fraude, y hacer un seguimiento del impacto del programa). El tratamiento de datos personales debe ser necesario para lograr la finalidad correspondiente. Antes de recopilar información, es crucial saber que datos se necesitan en el contexto específico. Si no está seguro de por qué recoge una serie de datos, cree que éstos podrían ser de utilidad más tarde sin una justificación específica, o simplemente piensa que entre más datos de los beneficiarios recoja mejor, entonces seguramente vaya a recoger más de los estrictamente necesarios. Para identificar con claridad los datos necesarios, se recomienda revisar los principios de minimización de datos, necesidad y limitación de los fines.

Estas cuestiones son fundamentales para la protección de los datos y aparecerán a menudo en esta guía. En el capítulo "selección" encontrará más detalles y ejemplos pertinentes.

Además, los datos personales recogidos para una finalidad no pueden usarse sin más para cualquier otra. Es evidente que un conjunto de datos existentes puede emplearse para fines futuros bajo ciertas circunstancias. Sin embargo, éstas deben ser generalmente "compatibles" con el original. Dicha compatibilidad existe cuando los fines están estrechamente relacionados, y cabe suponer que el interesado no se sorprenderá de este uso secundario. Por ejemplo, cuando finaliza un programa de transferencias monetarias se dispone de fondos adicionales que no se esperaban anteriormente. La revisión de los datos de beneficiarios previamente recogidos, para determinar quiénes deben recibir de nuevo asistencia se consideraría compatible con el objetivo y base jurídica sobre la que se recogieron datos personales anteriormente.

De lo contrario, sería preciso determinar una base jurídica apropiada y los interesados podrían tener que recibir información actualizada sobre el futuro uso previsto (véase el próximo principio de transparencia).

Transparencia

La transparencia va de la mano con la equidad. La idea consiste en ser abiertos y honestos sobre el tratamiento de los datos personales. Bajo el principio de transparencia, los interesados deben recibir siempre cierta información esencial sobre lo que ocurre con sus datos, entre la que se incluye:

- El hecho de que se están procesando sus datos personales y las bases de dicho procedimiento
- Quien tratará los datos
- Para que finalidad se tratan los datos
- Cómo se almacenan los datos y durante cuánto tiempo.
- Si se pretende compartir sus datos con otra entidad
- Los derechos que tienen con relación al tratamiento, como el derecho de rectificación y supresión
- Datos de contacto o alguien a quien dirigirse en caso de que los interesados tengan dudas o quejas.

La manera en la que se proporciona esta información depende del contexto. A lo largo de la guía se darán ejemplos concretos.

Seguridad de datos (Confidencialidad, integridad, limitación de almacenamiento[2])

Los datos personales deben ser tratados con confidencialidad y seguridad. Esto podría resultar obvio, pero no siempre queda claro lo que es necesario para asegurar la confidencialidad. La ley de protección de datos (o política, cuando sea aplicable) requiere la implementación de varias medidas de seguridad, como restricciones al acceso y prevención de la pérdida de información. El objetivo final es evitar la violación de datos, es decir, el acceso no autorizado, destrucción, pérdida, alteración o divulgación de los datos personales.

2 Normalmente la limitación de almacenamiento se considera un principio independiente.

III. Focalización

Uso de datos personales

La focalización en las transferencias monetarias se basa en los objetivos del programa según las necesidades evaluadas. Esta orienta las actividades del programa a beneficiarios específicos mediante criterios de selección definidos, que suelen incluir indicadores socioeconómicos y de vulnerabilidad. Véase la sección M3_3 de la caja de herramientas para PTM para más detalles.

Gráfico 1: Etapas en el proceso de selección

Las etapas principales en el proceso de selección se muestran en el gráfico *1.* Este proceso puede respaldarse con datos previamente recogidos para informar sobre la fijación de criterios y acelerar la creación de lista preliminar de beneficiarios aptos para transferencias monetarias.

Los pasos del 1 al 3 abarcan las decisiones clave de la focalización en función de los objetivos del programa. Dichas decisiones incluyen:

- ¿Qué zonas geográficas se seleccionarán para la intervención?
- ¿Distribuciones generales o específicas?
- ¿Se debe dirigir a los núcleos familiares o a los individuos?
- ¿Qué criterio de selección elegir en función de la vulnerabilidad, aspecto socioeconómico, o aportaciones específicas del contexto?
- ¿Qué mecanismo de selección elegir (mecanismo de selección categórico, propio o comunitario)?

En general, los datos personales no juegan un papel significativo en estos tres primeros pasos. Las decisiones se basan en la información general o datos agregados de las áreas afectadas y en la población en su conjunto. En este caso, la situación individual de los posibles beneficiarios no resulta todavía de interés, sino la situación general del territorio y objetivos del programa.

Las etapas 4 y 5, sin embargo, si se ocupan de los datos personales ya que se analizan y verifican a los posibles beneficiarios según los criterios que se han establecido. Luego, se crea una lista preliminar de beneficiarios antes del proceso formal de registro de estos. La lista contendrá, como mínimo, los nombres de los beneficiarios; y el proceso de análisis o verificación puede involucrar información detallada de los mismos.

En el paso 4, la lista preliminar se suele crear en base al mecanismo de selección elegido en el paso 3:

- **Selección comunitaria** – hogares vulnerables identificados por líderes y miembros comunitarios en función de los criterios acordados; resultados triangulados y verificados por la Sociedad Nacional. P. ej. Se pidió a los líderes comunitarios que identificaran los núcleos familiares con viviendas totalmente destruidas.
- **Autoselección** - se solicitó a los individuos que aportaran información personal y detalles relacionados con los criterios acordados. P. ej. El equipo del programa busca adultos sanos en situación de inseguridad alimentaria que estén dispuestos a participar en un proyecto de Dinero por trabajo.
- **Selección categórica** – la elegibilidad se basa en categorías específicas de vulnerabilidad (p. ej.

hogares liderados por niños) y, potencialmente, en un buen registro civil para decidir a qué miembros pertenecientes a una categoría específica seleccionar. P.ej., se pide a los funcionarios de gobiernos locales que compartan una lista de miembros de la comunidad bajo pobreza extrema).

Independientemente del mecanismo de selección empleado, esta etapa se basa en la información recolectada de diferentes fuentes (p. ej. gobierno, comunidades locales, otras organizaciones o individuos). Aunque se puede obtener esta lista por otra fuente, hacer uso de esta se califica como uso de datos personales. Si no hay una lista inicial disponible, la Sociedad Nacional puede optar por ir de puerta en puerta por las comunidades afectadas para elaborar una, solicitando datos personales.

En la etapa 5, se verifica la elegibilidad de todas las personas nombradas en la lista preliminar. Este proceso podría involucrar a representantes comunitarios o líderes locales que tengan un conocimiento actual de la población o que han recopilado información mediante otros datos o sistemas (p. ej. registro civil o listas de protección social). En algunos casos, la Sociedad Nacional puede ir de puerta en puerta para corroborar directamente con los beneficiarios y verificar que son realmente elegibles según los datos personales que aporten. El proceso de esta verificación puerta por puerta puede hacerse en paralelo a la creación de la lista inicial de la etapa 4. Este procedimiento puede ser similar al proceso de registro de los beneficiarios y utilizar formularios de encuestas y una base de datos para recopilar y gestionar datos personales estructurados, o puede simplemente ser ah hoc con papel y lápiz para marcar los criterios con los que cumple el beneficiario (a esto también se le considera datos personales).

Al final del proceso de selección, se puede compartir y publicar en la comunidad la lista de beneficiarios verificados (p. ej. la lista en formato papel se publicará en un espacio público para que la comunidad pueda comprobar quien forma parte de la intervención). La publicación de esta lista se califica como uso (tratamiento) de datos personales, ya que permite que los datos que están bajo su control sean accesibles para otras personas (para todos los miembros de la comunidad, para que puedan evaluarla).

Consideraciones para la protección de datos

El proceso de selección implicará el tratamiento de datos personales al elaborar y verificar la lista preliminar de beneficiarios. Este apartado examinará las decisiones claves del proyecto en el proceso de selección y las consideraciones relacionadas con la protección de datos. El principio más relevante que tratará este apartado es la minimización y necesidad de datos. Todos los demás principios están relacionados con el tratamiento de los datos recogidos, mientras que la minimización y la necesidad tiene como objetivo limitar la recopilación de estos desde un principio. No recopilar datos que realmente no son necesarios para el proyecto es la forma más efectiva de aumentar el nivel de protección de los mismos. Por consiguiente, al establecer el programa y antes de recoger cualquier información de los beneficiarios, es fundamental pensar en el ciclo de vida del proyecto y decidir, de antemano, que datos serán necesarios durante su ejecución.

Resolución 1 del proyecto: ¿Debo usar los datos de los beneficiarios recogidos por una fuente externa?

Minimización, Necesidad y Seguridad de los datos

Resolución del proyecto reformulada: ¿Necesito los datos recogidos por una fuente externa?, ¿cómo puedo asegurarme de que los datos de los beneficiarios han sido recogidos adecuadamente?

Al crear la lista inicial de beneficiarios, es habitual usar los datos recogidos por fuentes externas como otras organizaciones o el gobierno. De modo que la pregunta de la decisión del proyecto puede parecer

obvia y necesaria. Sin embargo, la pregunta sobre la resolución reformulada del proyecto recomienda a los profesionales que gestionan las transferencias monetarias adoptar un enfoque matizado a la hora de pedir y usar datos de fuentes externas que tengan en cuenta los principios de minimización y seguridad Estos son los principales aspectos que hay que tener en cuenta cuando se piensa usar datos de beneficiarios recogidos por fuentes externas (otras ONG, gobierno, etc.)

- **¿Esta organización es fiable?, ¿puedo fiarme de estos datos?**

  Si la organización que ofrece los datos no es muy conocida, podría querer preguntar o investigar sobre cómo se han recogido esos datos, y, ¿consideraría esto fiable? No sólo preocupa que la información pueda estar incompleta o que sea incorrecta, sino que también se puedan haber obtenido los datos de forma inapropiada (p. ej. No tener una base jurídica clara o que no se informara a los beneficiarios sobre cómo se compartirían sus datos con otros, especialmente si fueran muy sensibles). En función del contexto, podría ser de ayuda preguntar a los líderes comunitarios y otras organizaciones activas en el área, si conocen y se fían de esta organización. También sería aconsejable preguntar a dicha organización sobre algunos aspectos de cómo se recopiló la información. Es importante saber si los beneficiarios están al tanto de que sus datos podrían compartirse con usted. Si duda que las cosas no se hayan hecho debidamente, este podría ser un indicador de que quizás debería considerar otras fuentes de datos.

- **¿Qué datos debo solicitar y aceptar?**
  El hecho de que otra entidad haya recogido una determinada cantidad o tipo de datos no implica que deba solicitarlos todos o su mayoría. Una vez más, conviene reflexionar sobre el principio de minimización y necesidad. Los datos que debe solicitar o aceptar dependerán del proyecto. Si la entidad le proporciona más datos de los necesarios, sería aconsejable pedir solo los imprescindibles, y, si le facilitaran información extra, eliminarla e informar a la entidad correspondiente para que estén al tanto sobre la información seleccionada. Se recomienda tener precaución si el conjunto de datos contiene categorías muy sensibles, como información sanitaria, sexual o religiosa, especialmente si estos datos no tienen una relevancia directa para las necesidades del proyecto. Que una entidad facilite libremente este tipo de información con o sin acuerdos formales de intercambio de datos puede ser un indicador de que tienen unas normas de protección de datos deficientes o inexistentes. Además, la información proporcionada por externos debe ser tratada con responsabilidad.

  El panorama descrito anteriormente no afecta a los acuerdos de intercambio de datos entre las partes y, por lo tanto, el control de datos adquiere gran relevancia. En el caso de los PTM en los que la Sociedad Nacional es socia ejecutora de otro organismo, debe acordarse el intercambio de datos entre las partes involucradas, externas o no. Estas consideraciones se pueden analizar al negociar el acuerdo de intercambio de datos. Si en el marco de los programas de transferencia de transferencias monetarias siente preocupación por la protección de los datos con relación al intercambio de estos con externos, comunique sus inquietudes a su gerente o equipo jurídico de su Sociedad Nacional y anote los riesgos/inquietudes en la matriz de riesgos de transferencias monetarias.

Ejemplos:

El criterio de selección es "núcleos familiares con niños que han perdidos sus hogares durante la inundación"

El equipo de la Sociedad Nacional solicita al gobierno local que le proporcione:

- *"Información de interés" sobre los residentes de la zona. Esta solicitud es muy amplia y es bastante probable que el gobierno facilite más información de la necesaria, por lo que se debe limitar la solicitud.*
- *"nombres y situación familiar de todos los residentes de las zonas afectadas". Esta solicitud es más específica, pero sigue siendo demasiado amplia. Las personas sin hijos no son el objetivo, por lo que es poco probable que sus nombres sean necesarios.*
- *"solo los nombres de los residentes con hijos de las zonas afectadas". Posiblemente esto es suficiente y lo necesario.*

Tras un terremoto, la Sociedad Nacional intenta identificar a las personas que han perdido sus hogares. Una asociación del pueblo más afectado se ofrece a compartir una lista de las personas que actualmente no tienen un refugio debido al terremoto. La Sociedad Nacional considera esta oferta minuciosamente. Se ponen en contacto con el alcalde del poblado y le preguntan acerca de la reputación de la asociación. Además, se ponen en contacto con la asociación para conocer su procedimiento de recogida de datos. La asociación explica que ha informado a la población sobre la protección de datos y la intención de intercambiarlos con otras organizaciones de ayuda. Los datos recogidos por la asociación incluyen: nombres, tamaño de la familia, edad de los niños y número de teléfono. La Sociedad Nacional programa una distribución general para todos los núcleos familiares que han perdido sus hogares. Por lo tanto, deciden que para su intervención solo se necesitan los nombres de los beneficiarios y sus números de teléfono para contactar con ellos. El equipo se asegura de recibir únicamente estos datos.

Resolución 2 del proyecto: ¿Cómo verifico la elegibilidad de los beneficiarios?

Minimización de datos, necesidad, confidencialidad

Resolución del proyecto reformulada: ¿Qué datos necesito realmente para verificar la elegibilidad de los beneficiarios?

El objetivo de la verificación o "comprobación de la elegibilidad" es averiguar si una persona (o núcleo familiar) reúne realmente los criterios de selección. Esto se hace normalmente en la etapa 5 del proceso de selección nombrado anteriormente, en el que puede ser necesario reunir o analizar los datos relacionados con el beneficiario. Al llevar a cabo esta verificación, es importante no recoger o procesar más datos de los que se necesitan para completar la tarea (principio de minimización de datos y necesidad). Con el fin de comprobar la elegibilidad se pueden emplear diferentes métodos que

podrían requerir o procesar los datos personales de otro modo.

- **Verificación con miembros de la comunidad.** Con este método, es posible que no se consulte directamente con los propios beneficiarios. En su lugar, miembros de la comunidad con conocimientos sobre la situación o detalles personales de estos podrían elaborar una lista preliminar de posibles destinatarios. Esto podría complementarse con un control de verificación formal durante el proceso de registro. Cuando se emplea este método es importante proteger su privacidad, especialmente si se realiza en un entorno público (p. ej. con otros miembros de la comunidad) dado que no pueden oponerse a intercambiar información que otros ya conocen sobre ellos. Las preguntas dirigidas a los líderes de la comunidad sobre los beneficiarios deben ser pocas y evitar las preguntas delicadas en un entorno público. Si se requiere información para el programa que pudiera considerarse delicada, hay que tratar de recogerla en un entorno privado, como, por ejemplo, la verificación puerta por puerta.

- **Verificar puerta por puerta**. Antes de visitar los hogares beneficiarios para comprobar su elegibilidad, es importante saber que datos son completamente necesarios para esta finalidad, respetando de nuevo el principio de minimización de datos y necesidad. Debido a que el esfuerzo de ir puerta por puerta es mayor, puede haber una tendencia a preguntar más información de la que es estrictamente necesaria, para así evitar tener que repetir la visita. Si no está seguro de qué información debe pedir, hágase la siguiente pregunta: ¿qué impacto tendrá la información en mi decisión de seleccionar a un beneficiario? Si no lo tiene claro, podría no ser necesaria.

- **Publicar la lista preliminar de beneficiarios**. Como parte de la etapa 4 o tras la etapa 5 en el proceso de selección mostrado anteriormente, la lista preliminar de beneficiarios se suele compartir y publicar en un espacio público (p. ej. un salón comunitario). Esto se hace con el fin de ser transparentes e informar a la comunidad los beneficiarios seleccionados y los criterios de selección acordados. También, ofrece la oportunidad que se incluyan aquellos que no están en lista, pero reúnen los criterios de selección. Dicha lista incluirá datos personales, por lo que será importante minimizar lo que se comparte públicamente. Normalmente, los nombres y direcciones son suficientes, no siendo necesarios otros detalles o datos empleados en la verificación de la selección. Sin embargo, puesto que la lista de nombres está vinculada a algunos criterios definidos (aunque los detalles de esos criterios puedan cumplirse o no), revela información sobre los individuos que aparecen en ella al público general, lo que podría ser problemático para su privacidad. Depende del contexto que esto pueda ser problemático desde el punto de vista de la protección de datos. En un poblado pequeño en el que las condiciones de vida de todos los residentes son conocidas igualmente (es decir, que reúnen o no las características que corresponden con el criterio de selección), la publicación de esta lista no es tan problemática en cuanto a la privacidad. Por el contrario, en un contexto en el que los beneficiarios viven en relativo anonimato, su publicación podría ser un problema.

  La divulgación de información antes desconocida públicamente podría oponerse al principio de confidencialidad. Por lo tanto, sería aconsejable considerar detenidamente el contexto antes de decidir si publicar o no la lista.

Además, tras el proceso de verificación o de comprobación de la elegibilidad, los datos de los que no se consideraron aptos deben tratarse con responsabilidad (p. ej., si existen derechos de auditoría se archivan de forma segura, se mantiene una lista simplificada para evitar una nueva verificación o se eliminan si ya no son necesarios). Puede encontrar más detalles al respecto en el apartado de Orientación General.

Ejemplos de necesidad y minimización durante la verificación de admisión:

En el marco de un programa, el criterio de selección es "núcleos familiares al cargo del cuidado de personas con discapacidad". Para comprobar la elegibilidad es necesario saber si realmente hay miembros con discapacidad viviendo en el mismo núcleo familiar. Podría ser relevante conocer la naturaleza de la enfermedad que sufren. Esto se contrastará, por ejemplo, durante la visita al hogar para verificar los hechos. Sin embargo, lo más probable es que no sea necesario consultar el historial médico para verificar la discapacidad y hacerlo podría revelar información personal considerada sensible y no relevante para el proyecto.

Los líderes de la comunidad sugieren seleccionar a madres solteras sin ingresos con al menos tres hijos como las más vulnerables y se crea una lista preliminar en base a este criterio. La información proporcionada por los líderes comunitarios se verifica durante las visitas a hogares, donde se identifica y pregunta a la beneficiaria por la edad de todos los miembros del núcleo familiar. Para comprobar los ingresos, podría ser necesario preguntar por las fuentes de ingreso de la beneficiaria. No obstante, lo más probable es que no sea necesaria información adicional como su edad o afiliación religiosa, ya que esto no influirá sobre la decisión de selección. Tampoco es necesario preguntar sobre anteriores trabajos o pedir un extracto bancario para determinar el nivel de ingresos.

En el marco de la lucha contra el hambre, el criterio de selección para el programa de transferencias monetarias es "la inseguridad alimenticia en núcleos familiares a cargo de niños". Resulta poco probable que haya que preguntar sobre el nivel de educación de los niños durante el proceso de selección, ya que este no influye en el control de admisibilidad ni en la cantidad de la subvención monetaria.

Nota: Durante la recolección de datos y en cualquier tratamiento posterior de estos, es importante recordar que deben tratarse de forma segura. Tanto si los datos se recolectan en papel, una aplicación móvil u otros medios, asegúrese de que sólo tengan acceso a estos aquellos que verdaderamente lo necesiten. La protección de datos debe tenerse en cuenta en todas las etapas, incluyendo su eliminación, para garantizar que no se puedan recuperar. En el capítulo de Orientaciones Generales podrá encontrar más información al respecto.

Resolución 3 del proyecto: ¿Debo informar a los beneficiarios sobre el tratamiento de sus datos en esta fase?

Transparencia

Resolución del proyecto reformulada: ¿Cómo puedo asegurarme de que los beneficiarios tengan acceso a información relacionada con el tratamiento de sus datos?

La transparencia es un principio importante de la protección de datos. En el contexto de control de admisibilidad, la recolección de información puede ser menos formal que el registro de beneficiarios. No obstante, es importante que los beneficiarios sepan que ocurre con la información que le han

facilitado. En el capítulo Registro de Beneficiarios se ofrecen más detalles sobre cómo informar a los beneficiarios. Sin embargo, estaría bien echar un vistazo a estas normas durante las comprobaciones o controles de admisibilidad.

Algunos aspectos sobre los que hay que informar al beneficiario:

- La proveniencia de la información principal sobre ellos (p. ej., a través de miembros de la comunidad, listas del gobierno, otras organizaciones).
- Motivos por los que se lleva a cabo el control de admisibilidad.
- Posibilidad de que los datos incorrectos sean subsanados en cualquier momento.
- La posibilidad de intercambiar los datos proporcionados con otras instituciones y con qué fin (si ese es el caso).

IV. Registro de los beneficiarios

Uso de datos personales

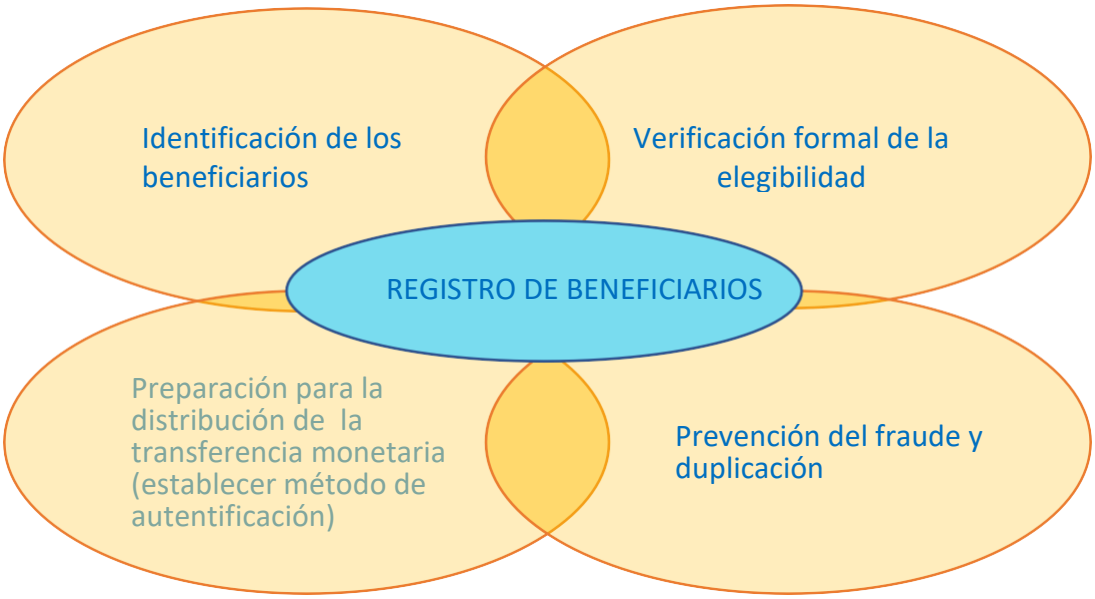

Gráfico 2: fines para llevar a cabo el control de admisibilidad

El proceso de registro formal de los beneficiarios suele producirse tras crearse una lista con los beneficiarios elegibles (véase sección M4_4 de la caja de herramientas para PTM en emergencias para más detalles). Esto implica la recopilación y gestión de datos personales para la distribución y supervisión del programa.
En el gráfico 2 se muestra los fines habituales del registro de beneficiarios y los ejemplos a continuación explican el uso de datos personales.

- **Identificación.** Al comenzar el procedimiento de registro, se suele solicitar al cabeza de familia que muestre un documento de identidad (p. ej., el permiso de conducir, la identificación fiscal o electoral) para asegurarse de que esa persona es la que está incluida en la lista de beneficiarios. El documento de identidad deberá incluir su nombre, fecha de nacimiento y otros datos personales que pueden recogerse en el registro. Es posible que se pida al beneficiario que proporcione datos biométricos (como una huella dactilar) para una autenticación sólida y asegurarse de que no se

registraron varias veces. Los datos biométricos se consideran datos personales y podrían ser sensibles.

- **Verificación formal de la elegibilidad.** Se hacen preguntas al beneficiario relacionadas con los criterios de selección en el caso de que el proceso de verificación no se haya realizado formalmente antes, y si existe la posibilidad de que los datos hayan cambiado desde que se realizó la selección, para garantizar que el beneficiario siga siendo apto antes del desembolso de la transferencia monetaria.
- **Preparación para la distribución de la transferencia monetaria.** Cuando proceda, se solicita al beneficiario la medida antifraude Conoce a Tu Cliente (KYC en inglés) u otra información que requiera el proveedor del servicio financiero para poder ingresar dinero (p. ej., número de teléfono para el dinero móvil o detalles de cuenta bancaria)
- **Establecer método de autentificación.** Se proporciona al beneficiario una tarjeta de beneficiario de la Cruz Roja con su foto e identificador único que pueden mostrar al proveedor de servicios financieros como prueba de que son aptos y que han sido registrados. Esto es especialmente útil cuando no posee identificaciones oficiales.
- **Prevención del fraude y la duplicación:** Para evitar el fraude y la duplicación, se puede pedir al beneficiario que de datos personales relacionados con miembros de su familia o datos biométricos.

Consideraciones para la protección de datos

El proceso de registro de beneficiarios implicará la recogida y tratamiento de datos personales en función de los fines comunes descritos anteriormente. En esta sección se examinarán las decisiones claves del proyecto en el proceso de registro y las consideraciones relacionadas con la protección de datos.

Resolución 1 del proyecto: ¿Cómo se debe verificar la identidad de un beneficiario?

Minimización y necesidad de datos

Resolución reformulada del proyecto: ¿Cuál es el mecanismo de verificación más efectivo y que interfiere lo menos posible en los intereses de los beneficiarios (incluida la privacidad)?

Para verificar la identidad de las personas que se presentan al registro, se requiere un identificador único. Los identificadores únicos pueden estar papel (permiso- de conducir, documento nacional de identidad, etc.) o ser biométricos (huellas dactilares, escaneo del iris, etc.) A la hora de considerar cuál de estas opciones usar, deben tenerse en cuenta los aspectos operacionales y de la protección de datos. En algunas situaciones, solicitar el DNI cuando la mayoría de la población carece de estos documentos no resulta demasiado útil. En otras, la recopilación de datos biométricos parece ser la forma más eficiente y única de evitar el fraude. Desde un punto de vista de la protección de datos, es importante tener en cuenta que algunos datos son más sensibles que otros. En la medida de lo posible, la finalidad es recoger la menor cantidad de datos confidenciales.

Identificación en formato físico

En muchas zonas, la forma más sencilla y común es solicitar un documento de identidad, como los documentos nacionales de identidad (DNI) expedidos por el gobierno o los pasaportes. Solicitar estas identificaciones no suponen un gran riesgo desde el punto de vista de la protección de datos puesto que tienen como fin identificar a su titular. Si es necesario escanear o copiar y archivar el documento de identidad de cada beneficiario ya es una cuestión aparte. Para la identificación, suele bastar con pedir al beneficiario que muestre su ID en el registro y anotar el número de su documento único de identidad (NUI). Puede marcar la casilla indicando que la identidad ha sido verificada sin quedarse con una copia de esta. Se pueden aceptar documentos de identidad alternativos u otros documentos como el permiso de conducir, el certificado de nacimiento, las facturas de la luz en lugar del DNI si muchos dentro de la

comunidad no lo tienen. Cuando se recogen estos documentos para verificar la identidad, de nuevo, se recomienda recoger los menos posibles, ya que en marco de la protección de datos más no siempre es mejor. Además, se recomienda no solicitar documentos que contengan datos sensibles (p.ej., documentos relacionados con la salud). Así mismo, como se mencionó anteriormente, puede que no sea necesario conservar copias de dichos documentos.

Datos biométricos

Los datos biométricos son datos relacionados con las características fisiológicas o conductuales de una persona reconocidos por medios tecnológicos. Ejemplos típicos de estos son las huellas digitales, reconocimiento de iris, geometría de la mano, reconocimiento facial o por voz. Estos datos se consideran muy sensibles, ya que son altamente personales y no se pueden sustituir si se vieran comprometidos, por lo que requieren un nivel de protección mayor. En algunos casos, los datos biométricos están sujetos a restricciones legales, incluyendo su limitación o prohibición de uso. Su potencial uso indebido es la causa principal de esto:

- **Aplicación de la ley o seguridad.** Los datos biométricos pueden ser muy interesantes para la aplicación de la ley o agentes de seguridad, ya que no pueden ser modificados. Al recoger estos datos en el contexto de un proyecto, se puede estar expuesto a la presión de otras partes para que se divulguen esos datos con otros fines.
- **Robo de identidad.** Los datos biométricos son más susceptibles de ser pirateados para el robo de identidad puesto que son únicos y no se pueden modificar.
- **Fuente de datos en el futuro.** Es posible que los datos biométricos recogidos hoy puedan emplearse en un futuro para saber más sobre un individuo de lo que se puede actualmente. Las nuevas soluciones tecnológicas podrían ser capaces de descifrar otra información, como detalles genéticos.

Por consiguiente, la recolección de datos biométricos[3] plantea un riesgo mayor y debería ser considerado como último recurso. Se debe evaluar su recolección para determinar si son verdaderamente necesarios o si en su lugar se puede utilizar una solución alternativa. Así mismo, se debe considerar el contexto del proyecto, así como la responsabilidad y habilidad de la organización para proteger cuidadosamente los datos. Aunque los datos biométricos puedan parecer la mejor forma de verificar la identidad de los beneficiarios y evitar el fraude, hay que sopesar los posibles riesgos para los mismos, especialmente si existe la posibilidad de que otras partes interesadas soliciten estos datos para sus propios fines (este riesgo podría superar las ventajas de esta clase de datos). Además, cuando se recolectan este tipo de datos, las consideraciones sobre el almacenamiento seguro son aún más importantes (véase el capítulo de Orientaciones Generales).

Además, recuerde el derecho de acceso a la información (transparencia). Dicha información debe presentarse de manera que resulte fácil de comprender para los individuos. La alfabetización general y/o el conocimiento sobre la biometría podrían ser insuficientes para que las personas comprendan los riesgos asociados a este tratamiento (hay que tener en cuenta que siempre se deben considerar alternativas al registro biométrico, véase la resolución 3 del proyecto más adelante).

Ejemplo:

3 Para más información, véase el capítulo sobre datos biométricos del Manual de Protección de Datos, así como la Política de datos biométricos del ICRC.

Varias áreas geográficas se han visto afectadas por una pandemia que ha provocado la pérdida de medios de vida. Se decidió prestar asistencia en efectivo a una comunidad urbana bien desarrollada y a una comunidad rural remota. Para el registro, se solicitó a los cabezas de familia de los hogares afectados en el entorno urbano que aportaran un tipo de documento de identidad de una lista de formularios y documentos válidos para demostrar su identidad. En la comunidad rural, se solicitó a los cabezas de familia que aportaran una certificación de los líderes/responsables del poblado por la falta de documentos de identidad oficiales. Luego, los beneficiarios de la zona rural recibieron una tarjeta de identificación temporal emitida por la Sociedad Nacional para que la presentaran ante el proveedor de servicios financieros al reclamar su dinero. En ambos casos, se evitó la recogida de datos biométricos para la identificación, y se emplearon otros medios de detección del fraude y la duplicación como comprobar los nombres y edades de los miembros del hogar. Además, se emitió un cupón de un solo uso con un código de barras único escaneado tras recibir el dinero para indicar que ya han ejercido sus derechos.

Resolución 2 del proyecto: ¿Qué otros datos del beneficiario debo recolectar durante su registro?

Minimización de datos, necesidad

Resolución reformulada del proyecto: ¿Qué otros datos de los beneficiarios son esenciales para el programa?

Además de la recolección de datos para la identificación, hay otro tipo de datos que se recogen durante el registro para los fines citados anteriormente. Para ello, es importante considerar que datos son absolutamente necesarios. Trate de preguntarse: ¿para qué necesito usar esta información? ¿Es vital para mi programa? Si no está seguro o piensa que podría cumplir el propósito con otros datos o de otra manera, entonces considere no recolectarlos. En ocasiones, se recogen más datos de los necesarios porque creemos que podrían ser de utilidad más adelante o porque siempre recopilamos esa información o la necesitamos para nuestra base de datos. La creación de una base de datos no es una razón válida para recoger información. Por el contrario, cada elemento de esta debe estar presente por una razón específica, para algo bien definido y crítico para el programa.

Uso de plantillas estándar

El uso de plantillas estándar para el registro es una práctica habitual que agiliza la recolección de datos puesto que se identifica el tipo de datos más utilizados. Sin embargo, estas plantillas suelen cubrir una amplia variedad de datos ya que están diseñadas para ser un cuestionario universal. En una emergencia, las plantillas podrían usarse tal y como vienen establecidas, en lugar de analizarse para definir cuales datos son relevantes y esenciales para el programa actual que se está ejecutando. Recoger las respuestas de preguntas irrelevantes se opondría al principio de minimización de datos y necesidad. Esto no significa que no deba utilizar estas plantillas, pero sí tomarse el tiempo de analizarlas y ajustarlas a cada intervención. Esta adaptación no consiste en volver a crear nuevos formularios cada vez, sino en utilizar el mismo, pero omitiendo las preguntas irrelevantes (p.ej., si el cuestionario se hace verbalmente). En

los archivos de Excel se pueden ocultar algunas columnas o filas; en las plantillas en formato papel se pueden redactar o tachar algunos apartados; y en formato digital se pueden marcar campos no necesarios[4]s u ocultarlos. Los miembros del equipo encargados de la recolección de los datos tienen que estar informados sobre el principio de minimización de datos para que comprendan por que se omiten deliberadamente algunas preguntas.

Ejemplos:

En un programa de transferencia monetaria dirigido a "núcleos familiares que han perdido sus medios de vida". El día del registro se pide a los beneficiarios que rellenen una plantilla estándar expedida por la Sociedad Nacional. El equipo ha analizado previamente la plantilla y ha decidido que los miembros de la familia conviviente deben responder a todas las preguntas de la plantilla relacionadas con su situación económica. Sin embargo, el equipo ha eliminado todas aquellas preguntas relacionadas con su estado de salud. Esta información no se debe dar ya que para este programa los núcleos familiares recibirán la misma asistencia, estén sanos o enfermos.

La Sociedad Nacional responde a una emergencia de sequía. También tienen un gran programa de donación de sangre. El equipo utiliza una plantilla estándar que incluye preguntas relacionadas con el tipo de sangre de los beneficiarios. Dado que esta información no es directamente relevante para la respuesta a la situación de emergencia en la que están trabajando, decidieron no solicitar esta información a los beneficiarios, y se informó de los motivos a los voluntarios encargados de la recogida de datos. Opcionalmente, se podría aclarar que los beneficiarios, por iniciativa propia, pueden dar información sobre su tipo sanguíneo si desearan participar en los esfuerzos de donación de sangre, pero esta participación no afectaría en el desembolso.

A continuación, se muestran distintas finalidades de recolección de datos y consideraciones claves de la protección de datos:

Verificación formal de la elegibilidad

Aunque sólo se invita a inscribirse a los beneficiarios que reúnen los requisitos, podría darse el caso de que la verificación realizada durante el proceso de selección no fuera lo suficientemente formal o que la situación haya cambiado, siendo necesario volver a verificar la elegibilidad durante el proceso de

4 Nótese aquí una distinción entre los campos señalados como "no necesarios" para que no se pregunten en caso de que se necesite una respuesta para poder continuar en un cuestionario digital, frente a "opcionales" en las que se siguen haciendo estas preguntas y es decisión del encuestado responderlas o no. Las preguntas opcionales deben reconsiderarse desde el punto de vista de la protección de datos. En primer lugar, no se debe recolectar información innecesaria e incluso cuando los datos se recogen de forma voluntaria se tiene que aplicar el principio de minimización de datos. En segundo lugar, los campos opcionales invitan a proporcionar esta información y podrían crear la impresión de que tienen más probabilidades de recibir la subvención si aportan más datos. Por último, si se proporciona información, aunque no sea directamente necesaria para el proyecto, habría que considerar si existe una base jurídica para el tratamiento de estos datos. Además, hay que recordar que se debe explicar con claridad al beneficiario cuando se está solicitando información opcional y aclarar que facilitar esta información no afectará en ninguna ayuda.

registro. En ese caso, habrá que recopilar datos relacionados con los criterios de selección acordados. Las consideraciones al respecto se tratan en el capítulo de focalización. Dichas consideraciones se tienen en cuenta durante el proceso de registro, en particular, la cuestión de si cierta información tiene un impacto en la decisión de seleccionar a una persona. Si es así, esta información se podría recolectar. En caso contrario, no habría razón para hacerlo.

Durante las distribuciones generales en las que no hay unos criterios de selección específicos dado que todas las personas afectadas de una zona necesitan ayuda, la recopilación de datos de elegibilidad puede no ser necesaria a menos que se necesite comprobar que pertenecen a la zona afectada o establecer la autenticación para recibir la ayuda. En este caso, el procedimiento de registro no requiere preguntas sobre indicadores de vulnerabilidad u otras preguntas que se hacen normalmente para determinar la elegibilidad. No son tampoco necesarias las preguntas para los típicos datos demográficos (p.ej., edad, sexo, tamaño del núcleo familiar), a menos de que tengan un propósito relevante ya que estos datos no se utilizan para seleccionar a los beneficiarios.

Distribución de efectivo

Los datos necesarios para facilitar la distribución de efectivo a beneficiarios dependerán del método de distribución seleccionado. En los pagos en efectivo, los datos necesarios se podrían limitar a información de identidad básica y autenticación empleada durante la distribución. Si se recurre a proveedores de servicios financieros (PSF), se necesitaría más información, incluidos los datos de Conoce a Tu Cliente (KYC) exigidos por ley para la distribución de efectivo. Los detalles sobre la recolección de datos para uso de los PSF se tratarán con mayor detalle en el próximo capítulo. Durante el registro es importante mantener una visión crítica sobre lo que es necesario y esencial para permitir la distribución de efectivo (p.ej., un número de teléfono para recibir dinero móvil).

Evitar el fraude y la duplicación

Con el fin de evitar el fraude y la duplicación de pagos, se podría requerir la recopilación de información adicional para triangular la información básica de las familias. Por ejemplo, recoger los nombres, edades y género de todos los miembros de la familia y efectuar una verificación en el caso de que alguno de estos haya intentado registrarse como hogar independiente. Además, en los programas cuya cuantía depende del número de miembros por núcleo familiar, se podría requerir una verificación detallada de este (p.ej., uso de tarjetas familiares expedidas por el gobierno). En estos casos, es importante reflexionar sobre el contexto real para evaluar el riesgo y, a continuación, asegurarse de que la recogida y tratamiento de datos es apropiado para el nivel de riesgo evaluado, en lugar de recolectar estos datos según el procedimiento normal.

Ejemplos:

Un PTM se ha puesto en marcha como respuesta a los incendios provocados en un pequeño poblado por el calor extremo. El criterio de selección (familias que han perdido sus viviendas) comprende a casi todos los hogares del poblado. Los líderes comunitarios han indicado y confirmado los nombres de los cabezas de familia. El día del registro, se les pide que se identifiquen. El equipo decide no recoger los datos relacionados con los miembros de la familia. El riesgo de fraude no es muy alto, ya que casi todos los hogares recibirán ayuda y se han identificado y puesto en una lista a los cabezas de familia con ayuda de la comunidad. Por consiguiente, es poco probable que otros miembros de la familia o gente de otros poblados puedan reclamar falsamente la ayuda.

Se ha puesto en marcha un PTM como respuesta a la inseguridad alimentaria en una pequeña comunidad destinado a madres de familia. La subvención destinada a cubrir las necesidades del hogar dependerá del tamaño de este. El equipo del programa identifica el tamaño de los hogares ya que es necesario para calcular el importe de la subvención, pero probablemente no será necesario recoger información adicional sobre los miembros de la familia por individual. Como la comunidad es pequeña es poco probable que sus miembros intenten indicar una cifra mayor al tamaño de sus hogares porque es probable que otros miembros de la comunidad los conozcan y denuncien la anomalía.

El mismo programa se ha extendido a comunidades más grandes y dispersas. Las subvenciones son mayores por el ajuste del costo de vida. En programas anteriores dirigidos por otras ONG se informó de un aumento excesivo del tamaño de los hogares. Los análisis del equipo del programa indicaron un riesgo potencial alto de fraude y se decidió recoger información adicional sobre los miembros de la familia (nombre, edad, género, grado de parentesco o pertenencia a la familia). Se utilizaron datos adicionales para cotejar los duplicados en la lista de beneficiarios.

Nota: En el caso de los programas con autoselección o auto inscripción, en los que los beneficiarios presentan su solicitud en base a los criterios de selección publicados, es importante dejar constancia de que también se recolectan los datos de aquellos que no cumplen con los requisitos. Se recomienda asegurarse de que cuando sea obvio que el solicitante no es apto, se eliminen o archiven sus datos para evitar intentos de reinscripción (si fuera necesario). Si se requiere una nueva verificación, almacene los datos por un tiempo limitado hasta que haya finalizado el proceso de verificación, y, en el caso de no cumplir los requisitos, se debe informar al solicitante y eliminar sus datos. Véase el Capítulo Consideraciones Generales para el almacenamiento de datos de los no beneficiarios. Así mismo, asegúrese de que los criterios de selección publicados estén limitados y detallados para limitar el número de solicitantes no aptos.

Resolución 3 del proyecto: ¿Qué debo comentar a los beneficiarios sobre el tratamiento de sus datos?

Transparencia

Resolución reformulada del proyecto: ¿Cómo debo cerciorarme sobre si los beneficiarios tienen acceso a información relacionada con el tratamiento de sus datos?

El principio de Transparencia de la protección de datos expone que los beneficiarios, como interesados, deben recibir directrices claras sobre la finalidad por la que se recogen sus datos y cómo se tratan; abarcando así desde la finalidad de su recogida, el almacenamiento, el posible intercambio de datos, los derechos de los interesados, etc. Informar sobre todo esto al beneficiario puede ser un reto, sobre todo en emergencias donde el tiempo es limitado. Es más, cuando los interesados tienen necesidades más urgentes e imperiosas que la protección de datos, es posible que no estén siquiera interesados en conocer estos detalles o entender sus implicaciones. Sin embargo, tienen el derecho a recibir esta información

Una buena estrategia es proporcionar a los beneficiarios **información básica** y un **contacto** al que acudir si desea saber más. Esto debe incluirse en el plan de Participación ciudadana y rendición de cuentas (CEA)

para el programa (véase el módulo M4_2 de la caja de herramientas en emergencias). La información básica podría proporcionarse en una reunión con las comunidades para explicar el programa y podría volver a comentarse durante el procedimiento de registro de los interesados. La Sociedad Nacional podría también preparar, imprimir y compartir un aviso de privacidad general (véase el modelo de Aviso de Privacidad en el apartado de referencias). Los interesados pueden consultar este documento y, si fuera necesario, pueden contactar con la Sociedad Nacional si así lo requirieran. Lo primordial es que puedan ponerse en contacto con alguien, ya sea a través de una línea telefónica para aquellos que tengan acceso a un teléfono o en persona.

Al facilitar información sobre el tratamiento de los datos, resulta útil ponerse en el lugar de los beneficiarios y preguntarse: ¿Qué información necesito saber antes de proporcionar mis datos personales? La información básica más común se enumera a continuación. Esta información debe presentarse de forma clara, que resulte fácil de entender y con el lenguaje adecuado.

- **Finalidad de la recogida de datos el día del registro.** Refiérase a los propósitos establecidos por su programa. Algunos de estos propósitos mencionados anteriormente incluyen: la necesidad de demostrar su identidad, verificar que reúnen los requisitos, ejecutar la distribución, o evitar el fraude y la duplicación. Los interesados tienen que conocer estos motivos y la necesidad de algunos datos para estos fines, lo que les ayuda a comprender lo que sucede.
- **Si has conseguido sus datos por terceros** (p.ej., otras ONG, líderes comunitarios, el gobierno). A menudo, se consigue información de los interesados por otras fuentes antes de contactar directamente con ellos. Es importante que los beneficiarios tengan constancia de la fuente de la que has extraído su información personal, para que se sientan seguros de que sus datos se utilizan de forma responsable.
- **Como rectificar los datos incorrectos.** Para los beneficiarios es tranquilizador saber que se pueden corregir los datos inexactos en cualquier momento. Los errores se producen, sobre todo, cuando se precipitan las acciones durante una emergencia, tanto por parte del equipo del programa que recoge los datos como por parte del beneficiario que aporta los datos iniciales. Si se descubre que la información es incorrecta, el interesado debería ser capaz de solicitar su corrección.
- **Cómo expresar las preocupaciones o presentar una hoja de reclamaciones:** Los beneficiarios deben saber que pueden expresar sus preocupaciones acerca del tratamiento de sus datos. Es importante que lo sepan ya que les aporta una sensación de control y es posible que quieran oponerse al procedimiento de los datos o quejarse de este. Si este fuera el caso, deben saber a dónde acudir y con quién pueden consultar sus preocupaciones y opciones. Esto debe formar parte del manejo de retroalimentación y quejas del programa (véase Modulo M4_2_5 de la caja de herramienta para emergencias)
- **La intención de intercambiar datos.** Si tiene constancia de que intercambiará los datos recogidos con otros grupos o instituciones (p.ej., otras ONG, PSF, el gobierno), los beneficiarios deberán estar al corriente de esto, además del motivo por el que se necesita intercambiar sus datos. Después de todo, el interesado le ha facilitado la información a usted únicamente y confía en que la mantenga a salvo. En algunos contextos, el interesado puede no querer que determinados tipos de información sean compartidos con otras entidades por motivos de sensibilidad o seguridad. Podría ser de utilidad crear la debida diligencia de dichas instituciones para poder mostrar su fiabilidad en términos del tratamiento de datos de los beneficiarios. Además, si los beneficiarios detectan un posible uso indebido de su información por haber sido compartida con entidades externas, se les debe alentar a informar a la Sociedad Nacional a través del servicio de asistencia o del contacto directo para estos asuntos.

Además de la información básica mencionada anteriormente, sería conveniente garantizar la preparación de detalles adicionales sobre el tratamiento de datos en el caso de que surjan nuevas

preguntas de los beneficiarios. Otra información que los beneficiarios deben recibir (en función del contexto) incluye:

- Almacenamiento de datos y medidas de seguridad.
- Periodo de retención de datos previsto.
- Base jurídica sobre la que se basa el tratamiento.
- Cualquier información adicional sobre la finalidad o el tratamiento posterior.
- Cualquier información adicional sobre el intercambio de datos.
- Otros derechos del interesado que pueden aplicarse, como el derecho de corrección, de oposición y de acceso a sus datos

Resolución 4 del Proyecto: ¿Debo solicitar el consentimiento de los beneficiarios?

Base legítima

Resolución reformulada del Proyecto: ¿En qué base legítima debo basarme?

La cuestión sobre si se debe pedir consentimiento al interesado para la recopilación y uso de sus datos tiene muchos matices. Se ha convertido en una práctica habitual comenzar el formulario de registro del beneficiario con una pregunta de consentimiento antes de continuar. A primera vista, parece lo correcto (pedir permiso es cortés y respetuoso). Sin embargo, en virtud de la ley de protección de datos, el tratamiento de datos personales puede basarse en otros campos además del consentimiento, lo que se analizará con más detalle a continuación.
Pero ¿no sería lo más apropiado pedir el consentimiento? No necesariamente. Puede parecer una señal de respeto solicitar la aprobación del beneficiario, pero entraña algunas dificultades que hay que considerar.

Problemas del consentimiento
El consentimiento debe darse libremente y con pleno conocimiento. En la práctica, esto significa que sólo es válido si hay una opción real de rechazo, ya que, de lo contrario, no se da "libremente". En el caso de emergencias, conseguir el consentimiento no es viable. Los beneficiarios se encuentran en una situación de vulnerabilidad y desesperación, en necesidad de ayuda inmediata. La protección de datos puede no ser su primera preocupación. Por esto, podrían dar su "consentimiento"[5] ya que no encuentran otra forma de conseguir ayuda y, en efecto, no se les puede ayudar sin no dan sus datos. Además, es posible que no estén en condiciones de comprender plenamente las consecuencias de que proporcionen sus datos o la forma en la que estos se procesan (p.ej., mediante la tecnología). No se puede aceptar sentidamente aquello que no comprendes (por lo que podría no considerarse como "plenamente informado").

Otra cuestión que se debe tener en cuenta es que el consentimiento se puede retirar en cualquier momento y sin ningún motivo (si se puede dar libremente, se puede retirar de la misma forma). Una vez revocado el consentimiento, se prohíbe cualquier otro tratamiento de los datos personales en cuestión (que se haya procesado sobre la base del consentimiento). Esto puede resultar muy problemático para el programa, dado que es importante tener un conjunto fiable de datos con los que trabajar. Una vez revocado el consentimiento, ya no es posible retroceder y emplear otra base legítima, como el interés vital o público. ¿Por qué? Porque su derecho a retirarse no sirve de nada si después no cambia nada para

5 El consentimiento va entre comillas porque, aunque el beneficiario marque una casilla o haga alguna otra indicación de que da su consentimiento, no sería correcto decir que se reconocería legalmente como consentimiento según las leyes y principios generales de protección de datos.

ellos, y también depende de si puede identificarse otra base legítima y de la información que ya se haya facilitado al beneficiario. Por todas estas razones, puede ser problemático utilizar el consentimiento como base legítima. Para el tratamiento de datos personales en el contexto de los programas de transferencias monetarias en situaciones de emergencia, se recomienda considerar otras opciones.

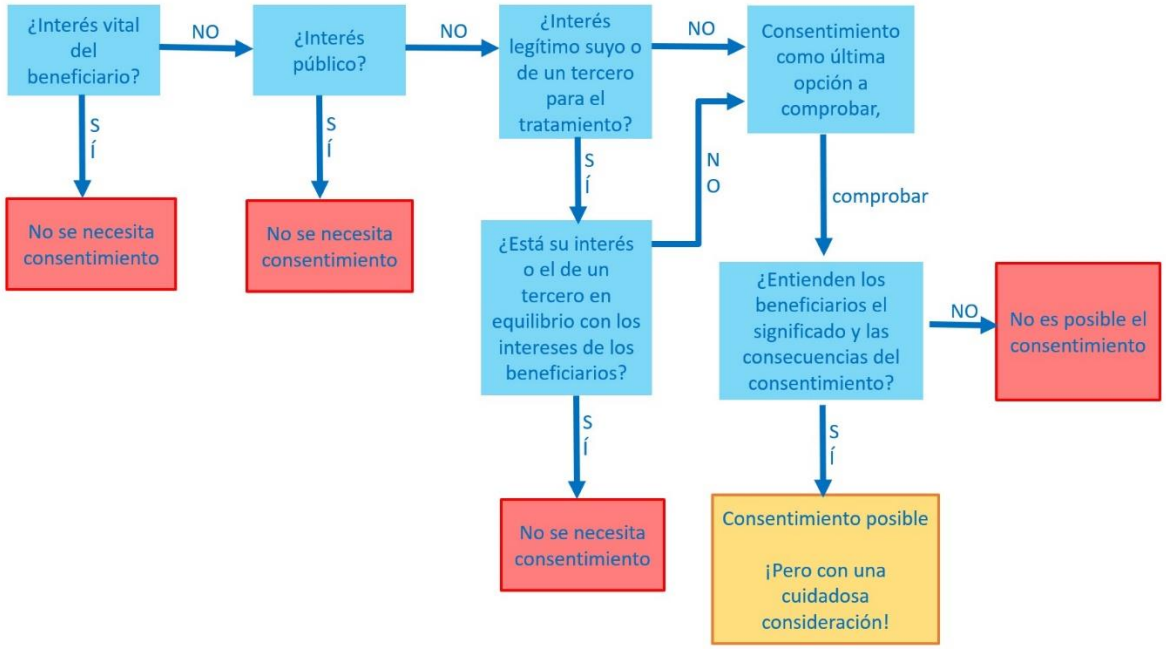

Gráfico 3: Árbol de decisión para determinar si el consentimiento es una base legítima adecuada

Otras opciones

El gráfico 3 muestra otras opciones para establecer una base legítima. Dos de estas opciones son el interés vital y el interés público. **El interés vital** significa que el tratamiento de los datos personales es esencial para la vida, integridad, salud, dignidad o seguridad de los beneficiarios. Los PTM diseñados para atender necesidades vitales o esenciales en situación de emergencia pueden cumplir este requisito; para otros PTM en contextos de no emergencia podría ser necesario considerar otras opciones. **El interés público** significa que el tratamiento de datos personales responde a una finalidad que interesa a todos. Las Sociedades Nacionales que prestan asistencia cumplen un mandato humanitario de interés público general. Por lo tanto, incluso cuando no se cumple el alto nivel de interés vital, la asistencia a través de PTM seguirá siendo normalmente de interés público.[6]

Para evitar malentendidos: participar o no en el programa sigue siendo decisión de los beneficiarios. No obstante, si deciden hacerlo, se puede tratar sus datos personales sin pedir explícitamente su consentimiento, siempre y cuando se les haya informado sobre el programa y tratamiento de los datos. Es de interés vital y/o de interés público. Lo importante es que sólo se utilicen los datos personales que sean absolutamente necesarios para el programa. Véase el apartado Programación de Transferencias Monetarias del manual de protección de datos para obtener más detalles sobre las bases legales de los PTM.

Intercambio de datos

El intercambio de datos con otras entidades (p.ej., otras ONG, gobierno, PSF) puede ser de interés vital

6 Tenga en cuenta que en algunas jurisdicciones basarse en el interés público puede requerir consideraciones adicionales o una aprobación oficial del gobierno. Está fuera del alcance de esta guía verificar esto para cada jurisdicción. Si tiene dudas sobre si puede invocar el interés público para su programa, no dude en comunicarlo a su gerente o equipo jurídico de su Sociedad Nacional.

para los beneficiarios o de interés público. Además, puede existir la obligación legal de compartir determinados datos[7] personales y, en ese caso, puede hacerse sin consentimiento. Cuando no existe obligación legal, puede ser del interés legítimo de la Sociedad Nacional compartir los datos personales. Dicho interés legítimo puede justificar el intercambio de datos sin consentimiento si los beneficiarios no presentan un interés opuesto general.

Es fundamental considerar las posibles consecuencias o riesgos a los que se exponen los beneficiarios si se intercambian sus datos. Esto se explica con mayor detalle en el Capítulo del intercambio de datos. En resumen, todo se reduce a la necesidad y confidencialidad.

Administración del programa

Algunas decisiones del proyecto relacionadas con el tratamiento de datos pueden no ser, directamente, de interés vital o público, pero siguen siendo razonables desde la perspectiva del programa (p.ej., tipo de almacenamiento, la inclusión de más miembros del equipo, etc.). De nuevo, entra en juego el interés legítimo de tu Sociedad Nacional para estructurar y organizar el programa de forma eficaz y eficiente.

¿Y entonces?

En la mayoría de los casos no es necesario solicitar consentimiento. Esto no implica que sus acciones estén menos justificadas (al contrario). Sin embargo, se deben considerar otros tres aspectos:

- Que no solicite el consentimiento no implica que no tenga el deber de informar a los beneficiarios. Independientemente de la base legítima que quiera emplear, se debe aplicar el principio de Transparencia. Como se indicó en la Resolución 3 del proyecto, facilitar información básica relacionada con el tratamiento de los datos personales y un contacto para futuras preguntas son buenas prácticas.
- Podría considerar la posibilidad de remplazar la preguntar de consentimiento por: "¿tiene alguna pregunta o preocupación antes de continuar?" o "¿reconoce haber recibido información básica sobre el programa, incluyendo dónde solicitar más detalles sobre el tratamiento de sus datos? Esto no es obligatorio, pero podría ser una forma alternativa de ser educado y cortés antes de pedir más datos personales.

- ¿Se debe evaluar la base legítima para cada una de las intervenciones de PTM que realice? No necesariamente. La mayoría de las intervenciones de PTM pueden emplear la misma base legítima, pero recuerde que no debe utilizar el consentimiento por defecto. Si la naturaleza de un nuevo PTM es única y las repercusiones en los datos de los beneficiarios no están claras, sería conveniente evaluar formalmente las bases legítimas antes de continuar. En este caso, también sería aconsejable realizar una Evaluación de Impacto en la Protección de los Datos Personales (EIPD). Véase el capítulo de Orientaciones Generales para obtener más detalles al respecto.

V. Uso de proveedores de servicios financieros

Uso de datos personales

Normalmente, la distribución de transferencias monetarias se realiza con el apoyo de proveedores de servicios, por lo que se establece un contrato con estos. En los programas de vales, los proveedores son los comerciantes de materias primas, vendedores locales, supermercados y mayoristas. En los PTM, estos son los proveedores de servicios financieros (PSF) como los bancos, operadores de redes móviles o agentes de remesa que respaldan el cobro. En este capítulo, nos centraremos en los PSF, pero tenga en cuenta que los principios de la protección de datos se deben considerar para todos los tipos de proveedores de servicios. Puede revisar el uso de proveedores de servicios en el Módulo M4_3 de la caja de herramientas para emergencias.

7 Tenga en cuenta que el cumplimiento de una obligación legal es una base legítima generalmente reconocida en muchas leyes de protección de datos.

Consideraciones sobre la protección de datos

El uso de PSF puede requerir el intercambio de datos personales de beneficiarios para posibilitar la transferencia monetaria. En este apartado se examinarán las decisiones claves del proyecto cuando se trabaja con PSF y las consideraciones relacionadas con la protección de datos. Los riesgos relacionados con la protección de datos y los PSF deben incluirse en la Matriz de Riesgos de la PTM, desarrollada a partir de las fases de Evaluación y Análisis de respuesta de su programa. Véase módulo M2_4 Evaluación y Módulo m3_1_4 Análisis de respuesta en la caja de herramientas para PTM en emergencias.

Resolución 1 del proyecto: ¿Debo usar proveedores de servicios financieros?

Minimización, necesidad y seguridad de datos

Resolución reformulada del proyecto: ¿Podría el PSF utilizar los datos del beneficiario de forma que fuera perjudicial para estos?

A la hora de considerar si debe usar un PSF en su proyecto, es importante analizar cuáles datos necesitarán para poder prestar su servicio, lo que puede implicar solicitar información adicional a los beneficiarios para ello y evaluar minuciosamente las posibles consecuencias a las que se exponen cuando se comparten estos datos[8].

Conoce a tu cliente (KYC) y proyección de lista de vigilancia

Muchos PSF están sujetos a la regulación KYC, que les obliga a recopilar información sobre sus clientes para evitar el blanqueo de capitales, la financiación del terrorismo u otros delitos. La cantidad necesaria de información podría depender de la normativa local, ya que algunos países permiten una mayor flexibilidad en función de nivel de riesgo que consideran con las transacciones. Las agencias humanitarias que utilicen PSF tendrán que cumplir con estas normativas de KYC que exigen compartir algunos datos de los beneficiarios.

Estas son algunas consideraciones para garantizar el principio de minimización y necesidad de datos:

- Consulte las normativas KYC de su país y el contexto operacional. Determine los datos exigidos por ley y compárelos con los que solicita el PSF. Pueden existir políticas internas que expliquen por qué los PSF solicitan datos adicionales al margen de lo exigido por ley. Esto tiene que justificarse y negociarse para asegurar que solo se comparte lo estrictamente necesario para prestar la asistencia.
- En algunos casos, las organizaciones humanitarias pueden abogar por la simplificación o el ajuste de los requisitos KYC (p.ej., reducir los requisitos para aquellos que han perdido su documento de identidad, limitación de los importes que se pueden transferir a beneficiarios o terceros para el KYC, o permitir las transferencias de efectivo por tiempo limitado). Compruebe si en estos casos se pueden minimizar los datos compartidos con los PSF.
- Informar a los beneficiarios y explicarles los requisitos de KYC o por lo menos, incluirlos en el aviso de privacidad que puede consultarse en cualquier momento.

Los PSF pueden tener la obligación de comprobar la información de KYC e intercambiar los datos con terceros (como reguladores y autoridades) Estas comprobaciones pueden incluir el cotejo de listas de beneficiarios con listas de vigilancia, de sanciones o de personas señaladas por las autoridades locales que podrían estar involucradas en conflictos o violencia. Algunos PSF lo hacen de forma sistemática mientras que otros lo hacen por petición del gobierno. Este proceso marcará a aquellos individuos que podrían ser sospechosos de estar involucrados en ciertas actividades criminales (blanqueamiento de

8 En la sección de referencias de esta guía se puede encontrar un modelo de cuestionario para el PSF.

dinero, terrorismo, corrupción, etc.) y que, por lo tanto, no son aptos para recibir la ayuda. Si el nombre de un beneficiario coincide con alguna de esas listas, podría tener graves consecuencias. Por esto, es indispensable analizar el contexto del país y el programa. Estas son las típicas preguntas en las que hay que pensar:

- ¿Existen informes de persecuciones políticas, étnicas o religiosas por parte del gobierno?
- ¿Se consideran como opositores del régimen a parte de la población beneficiaria?
- ¿Pueden considerarse a los partidos políticos como grupos terroristas?
- ¿Está el PSF estrechamente vinculado con las autoridades estatales, como servicios de inteligencia o agencias de seguridad?
- Si los beneficiarios son refugiados, ¿dispone el PSF de una sucursal o centro de almacenamiento en el país de origen de los refugiados donde las autoridades puedan solicitar datos?
- ¿Se generaría gran preocupación o temor por parte de los beneficiarios si se tuviesen que compartir de alguna forma sus datos con el gobierno por dichas obligaciones?

Si sospecha que se podrían utilizar los datos de los beneficiarios de forma inapropiada, esto supone un grave riesgo para ellos. En estos casos, si no puede encontrar la forma de contratar un PSF sin intercambiar datos de los beneficiarios, se deben considerar otras opciones de distribución, como dinero en metálico, cupones o incluso pago en especie. Esto debe hacerse como parte de la evaluación de riesgos durante la fase de Respuesta y Análisis de su programa (Módulo 3 de la caja de herramientas para PTM en emergencias) y debe incluir un análisis sobre si la persecución, exclusión u otras sensibilidades pueden dar lugar a la recopilación e intercambio de información KYC en la selección de la mejor modalidad de transferencia. Otras referencias del CaLP: Know Your Customer Standards and Privacy Recommendations for Cash Transfers y KYC Regulations Tip Sheet.

Otros objetivos

Dado que los PSF suelen ser empresas con ánimo de lucro, estos podrían utilizar los datos de los beneficiarios para sus propios fines, entre los que se incluyen: intereses comerciales como la creación de perfiles con solvencia, la publicidad o marketing, y la comprobación de la admisibilidad para otros servicios financieros. Estos casos podrían parecer de relativo bajo riesgo para los beneficiarios, pero siguen considerándose ajenos al objetivo de la ayuda humanitaria de transferencias monetarias. Las leyes de protección de datos están concebidas para proteger a los ciudadanos de acciones indeseadas de instituciones públicas (como los correos basura).

Otra posible repercusión de la reutilización de datos del PSF podría ser la compensación de deudas (p.ej., un beneficiario debe un préstamo o dinero al banco, y este intenta quedarse con la ayuda económica recibida para recuperar lo prestado) o el intercambio de más datos con terceros, como cobradores.

En general, se debe llevar a cabo la debida diligencia sobre la reputación y desempeño del PSF durante la licitación o proceso de contratación.[9] Asimismo, los contratos con éstos deben restringir el tratamiento posterior de datos (durante e incluso después de la distribución de efectivo), e incluir ejemplos de acciones que deben evitarse si se conocen al momento del contrato (véase resolución 3 del proyecto). Durante la ejecución del programa, se debe pedir o solicitar a los beneficiarios que informen a la Sociedad Nacional de cualquier caso de uso posterior (o sospecha de uso indebido) de sus datos por parte de los PSF que sean ajenos al programa.

[9] En la sección de referencias de esta guía se puede encontrar un modelo de cuestionario para el PSF.

Resolución 2 del proyecto: ¿Qué tipo de cuenta debo escoger para la distribución de efectivo?

minimización, necesidad y seguridad de datos

Resolución reformulada del Proyecto: ¿Qué tipo de cuenta usada en las transferencias de efectivo protege mejor los datos de los beneficiarios?

Existen diferentes mecanismos de pago en efectivo que tener en cuenta, entre los que se incluyen el uso de bancos, agencias de remesas, proveedores de redes móviles y oficinas de correo. Desde el punto de vista de la protección de datos, es importante considerar como limitar el intercambio de datos personales, independientemente del mecanismo de pago elegido. Además, esto puede depender del tipo de cuenta empleada para la distribución de efectivo. Considere dos tipos de cuentas: uso de cuentas nominalizadas de beneficiarios individuales o tener una cuenta virtual gestionada por la Sociedad Nacional.

Cuentas nominativas

El programa puede optar por usar la cuenta del beneficiario con el proveedor de servicio o abrir una cuenta en su nombre. El uso de cuentas preexistentes interfiere menos con la protección de datos que abrir nuevas cuentas, puesto que existe una relación contractual entre el PSF y el beneficiario de la que se sirve su Sociedad Nacional para los fines del programa.

La creación de nuevas cuentas por parte de la Sociedad Nacional para los beneficiarios individuales (suponiendo que sea factible) debe analizarse con mayor detalle para determinar los posibles riesgos para la protección de datos. Por ejemplo, podría existir un motivo específico por el que el beneficiario no haya abierto su propia cuenta (p.ej., debido a algunas reticencias de KYC mencionadas en el apartado anterior). Abrir una cuenta en nombre de otra persona requiere cuidado en la recopilación e intercambio de datos con el PSF, así como la gestión de dicha cuenta tras el programa.

Cuentas virtuales

Las cuentas virtuales son propiedad y están gestionadas por organizaciones humanitarias. En estas se pueden crear subcuentas para los beneficiarios para que puedan recibir dinero. Con este tipo de cuentas, el KYC se realiza con la organización y no con los beneficiarios individuales. Ejemplos de uso de cuentas virtuales:

- Emisión de tarjetas de prepago para cajeros automáticos en las que cada tarjeta está vinculada a la cuenta de la Sociedad Nacional y que se entregan a los individuos que cumplen con los requisitos junto con un PIN para la retirada del efectivo.
- Emisión de cheques bancarios a personas para que puedan ser canjeados independientemente de si tienen una cuenta en ese banco.
- SIM móvil de uso limitado emitida por la organización para que los beneficiarios puedan recibir un SMS con códigos de transacción que podrían utilizar para canjear efectivo de agentes de dinero móvil.

En el momento del desembolso de efectivo, se podría requerir el intercambio de datos de beneficiarios con el PSF a efectos de la identificación, pero la cantidad de datos que hay que compartir con este suele ser inferior en comparación con la creación de cuentas nominativas, puesto que no se establece el KYC con los individuos. Desde el punto de vista de la protección de datos, esta opción resulta atractiva, pero también existen algunas consideraciones operacionales (p.ej., la capacidad de gestión de las subcuentas por parte del equipo del programa, la distribución de fichas como tarjetas de prepago para entregar efectivo a las personas adecuadas, la correcta vinculación de los números de subcuentas y la conciliación de las transacciones tras el desembolso). El riesgo de la gestión de las transacciones y fondos recae

principalmente en la agencia. Asimismo, cuando se utilizan cuentas virtuales, la SC tiene acceso a datos que revelan el uso que hacen los beneficiarios del dinero. Estos datos son sensibles. Para respetar su privacidad a este respecto, consulte el apartado sobre el seguimiento tras la distribución para obtener más detalles sobre la privacidad y seguimiento.

Resolución 3 del proyecto: ¿Qué debe incluir el contrato con un PSF?

Seguridad de datos

Resolución reformulada del Proyecto: ¿Qué disposiciones debo incluir en el contrato con el PSF para proteger los datos personales del beneficiario?

En primer lugar, es importante determinar qué datos son absolutamente necesarios para cumplir el servicio del PSF y negociar para minimizar el intercambio de datos. Entre estos se suelen incluir:

- Datos de identificación, como el nombre del beneficiario y un número de identificación válido.
- Datos requeridos por KYC que pueden variar según normativas nacionales.
- Y otros datos (si procede) necesarios para permitir la distribución de efecto, tales como: número de teléfono para las transferencias de dinero móvil, número de cuenta bancaria, nombre o identificación de la persona autorizada a recibir el dinero en nombre del beneficiario (representante)

También es importante saber los datos que podría crear y compartir con usted el PSF como parte de las transacciones realizadas con los beneficiarios. Por ejemplo, la fecha y el estado del cobro, la firma del beneficiario después de recibir el efectivo, el saldo actual si todavía no se ha retirado todo el efectivo de la cuenta, el lugar en el que se ha utilizado el efectivo (p.ej., el supermercado), etc.

En segundo lugar, se necesita crear un contrato o acuerdo de servicios. Este acuerdo debe incluir el marco de la provisión del servicio, alcance y elementos de la protección de datos. Se recomienda tener una plantilla preparada y compartida para este acuerdo como parte del proceso de licitación, y las consideraciones de la protección de datos evaluadas como parte de la selección del proveedor.

Algunas de las disposiciones claves a incluir en el contrato:

- **Los datos compartidos.** Sólo se utilizarán para los fines del programa (distribución de efectivo). No se permitirá ningún otro uso fuera del alcance del programa. Como se ha mencionado anteriormente, también podría ser de utilidad el ser explícito o enumerar con precisión los ejemplos de para qué no deben utilizarse los datos (por ejemplo, publicidad y marketing, fines crediticios). La lista debe estar marcada como "no exhaustiva".
- **Intercambio de datos con otros.** El PSF no compartirá los datos con otros si no lo aprueba la Sociedad Nacional. Además, en caso de que haya la obligación de hacerlo (p.ej., con autoridades) deberá informarse primero a la SN.
- **Seguridad de datos.** los datos se almacenarán de forma segura (p.ej., indicar controles de acceso, cifrado, copias de seguridad).
- **Confidencialidad.** Los datos compartidos se tratarán con confidencialidad.
- **No se recogen datos adicionales de los beneficiarios.** Los PSF no deben recoger más datos personales de los beneficiarios en el marco del programa. P.ej., puede que estos tengan que mostrar su documento de identidad al reclamar la asistencia de efectivo, pero el PSF no debe copiarlo o escanearlo y, por tanto, recoger datos adicionales del beneficiario.
- **Eliminación.** los datos compartidos se eliminarán de la base de datos del PSF una vez completado el programa o se archivarán fuera de línea y de forma segura para fines de autoría.
- **Consecuencias del incumplimiento por parte del PSF.** El contrato debe contener una declaración que indique que el PSF tiene constancia de que el incumplimiento de esos términos podría tener consecuencias legales, y que como mínimo, causará daños a la reputación de todas las partes

involucradas. Indique que se alienta a que beneficiarios informen a la Sociedad Nacional del uso de datos personales para acciones no relacionadas con el programa por el PSF.

En la sección de referencias encontrará un modelo de IFRC para la contratación de PSF, que contiene los puntos importantes en la protección de datos. Si cree que falta algo o quiere referirse a un asunto específico que haya surgido en el contexto de su programa, puede añadir estos aspectos en su plantilla.

En la práctica, el PSF a menudo prefiere usar su propia plantilla de contrato. En función de su poder de negociación, intente negociar utilizando la plantilla preparada por su Sociedad Nacional. Si se decide por la plantilla del PSF, es aconsejable examinar de cerca y comparar los elementos de protección de datos y solicitar que se modifiquen para garantizar una sólida protección de los datos de sus beneficiarios. Si la plantilla del PSF no contiene ninguna cláusula sobre la protección de datos, esta es su oportunidad de introducir los aspectos de protección de datos que considere importantes. Puede extraer algunas cláusulas de la plantilla de IFRC. Si el PSF no quiere aceptar aspectos sobre la protección de datos en el contrato, lo debería considerar como una señal de alarma o bien un motivo de descalificación del PSF del proceso de selección. Toda entidad respetable debe interesarse en unas normas mínimas de protección de datos.

Es habitual negociar un acuerdo marco con uno o varios PSF como parte de la preparación de efectivo para poder tener opciones según el contexto y las necesidades. Sin embargo, los nuevos programas pueden llevar a nuevas situaciones que no formen parte del acuerdo actual con el PSF. Si tiene la impresión de que la protección de datos no se haya abordado lo suficientemente bien en el marco del contrato, no dude en comunicárselo al PSF o a su gerente para tratar de negociar una modificación. La protección de datos ha cobrado importancia durante los últimos años y la concienciación no ha hecho más que empezar.

VI. Intercambio de datos con el gobierno, otras organizaciones humanitarias y donantes

Uso de datos personales

En las intervenciones de PTM se requiere la cooperación y coordinación con partes interesadas más amplias, como el gobierno nacional, otras organizaciones humanitarias (nacionales e internacionales) y donantes. En estas relaciones, es posible que se deban compartir los datos de beneficiarios de una Sociedad Nacional con externos (la Sociedad Nacional también puede recibir dichos datos). El intercambio podría hacerse de manera oficial mediante acuerdos de intercambio o de manera informal sin acuerdos establecidos, en particular, en situaciones de emergencia en las que la celeridad es clave.

En el apartado de selección, aparecen ejemplos sobre la recepción de datos de beneficiarios del gobierno y otras organizaciones que responden a la misma emergencia para establecer una lista preliminar de beneficiarios y verificar la admisibilidad de los que figuran en ella. Este nivel de intercambio de datos también es importante para la coordinación entre los diversos agentes para evitar la costosa duplicación de esfuerzos y asistencia. Por su parte, los donantes podrían tener la obligación de auditar, demostrar transparencia y responsabilidad garantizando que los beneficiarios que han recibido la asistencia son personas reales y aptas, y que recibieron la prestación

Consideraciones de la protección de datos

En este apartado se presentarán las principales consideraciones de la protección de datos cuando se intercambian con terceros. En general, al intercambiar datos con distintas partes, es importante asegurarse de que se transfieren de forma segura mediante medios seguros (p.ej., archivos cifrados,

almacenados en bases de datos de confianza) a los que sólo puede acceder el personal autorizado. Véase el apartado de orientación general.

Cuando se transfieren datos a otros países, es fundamental evaluar el nivel de protección de datos de los mismos. Si este es inferior a las normas de la SN, se debe reconsiderar la transferencia y si fuera inevitable, negociar un acuerdo de intercambio de datos sólido y detallado sobre los requisitos de la protección de datos.

Resolución 1 del proyecto: ¿Qué datos debo intercambiar con el gobierno?

Seguridad y necesidad de datos

Resolución reformulada del proyecto: ¿Es necesario y seguro intercambiar datos personales con el gobierno?

Aunque las Sociedades Nacionales actúan como auxiliares del gobierno de su país, tienen el deber de mantener su naturaleza neutral, imparcial e independiente en lo que refiere a la ayuda humanitaria. Sin embargo, también están sujetas a leyes nacionales [10] en las que podrían existir obligaciones legales y, por tanto, la obligación de compartir ciertos datos con el gobierno. Algunos de los riesgos de la protección de datos se mencionaron en el apartado KYC (relacionado con el uso de PSF) en cuanto a la denuncia de personas señaladas por las autoridades (listas de vigilancia y sanciones). También podría existir el riesgo de que las autoridades presionaran a la Sociedad Nacional para que intercambie datos personales para otros fines (p.ej., combatir el terrorismo). Por esto, se necesita realizar un análisis al diseñar la intervención de transferencia en efectivo (antes de recopilar los datos) y documentar los riesgos (utilizando una matriz de riesgo o un análisis más estructurado mediante un DPIA.

Además de leyes nacionales específicas, existen otros motivos por los que el gobierno puede necesitar los datos de la organización:

- **Comprender la intervención de las transferencias monetarias.** A menudo, el gobierno quiere estar al tanto de los programas humanitarios organizados bajo su jurisdicción, puesto que es el mayor responsable de la seguridad y bienestar de sus ciudadanos y habitantes de sus zonas. Además, si existen desacuerdos entre algunos de los miembros de la comunidad sobre el por qué no están incluidos en el programa, presentarán sus quejas frente a las autoridades. Por lo general, las autoridades desean conocer la finalidad, duración, grupos objetivo y criterios de selección acordados, escala financiera, requisitos de seguridad, recursos y el apoyo que necesitan de ellos. Para que el gobierno se haga una idea del programa, normalmente basta con proporcionar información general y datos agregados (criterios de selección, zonas, número de personas beneficiarias, porcentaje de ancianos/niños, cantidad de la subvención monetaria, etc.). En algunos casos, podrían estar interesados en ver la lista final de los beneficiarios que han sido seleccionados. Si esta lista no se ha hecho pública a través de la comunicación y sensibilización de la comunidad, sería apropiado entender por qué las autoridades necesitan dicha lista y puede ser necesaria una negociación para limitar los datos personales proporcionados.
- **Coordinación para evitar la duplicación de la asistencia.** En una emergencia, el gobierno dispone también de programas para dar apoyo a las comunidades afectadas. Si hay diferentes organismos prestando asistencia, las unidades gubernamentales pueden encargarse de la coordinación para garantizar que no se duplique la misma y apoyar a los organismos para que llegue lo antes posible. En algunos países y contextos, el gobierno puede solicitar los datos de beneficiarios de todas las organizaciones para comprobar si hay duplicados y, en algunos casos, se puede incluso necesitar la

10 La excepción es aquellos con privilegios e inmunidad

validación de la lista antes de que la organización pueda proceder con la distribución. La intención de evitar los duplicados puede ser razonable y requiere que el gobierno conozca los nombres de los beneficiarios. Otros datos personales, sin embargo, no necesitan ser compartidos para este fin. Además, por lo general no existe la necesidad de dar acceso al gobierno a su base de datos. Cuando sea posible, negocie para minimizar los datos que debe intercambiar con las autoridades para facilitar la coordinación y controles de duplicación.

- **Asociación para la implementación:** La Sociedad Nacional podría estar asociada con el gobierno para distribuir en su nombre. Los programas de protección social y las grandes distribuciones en las que el gobierno puede confiar en el alcance y capacidad de la Sociedad Nacional. En dichas asociaciones, normalmente se crean acuerdos formales. Al negociar dichos acuerdos, tenga en cuenta los principios de protección de datos y buenas prácticas.

Independientemente del propósito oficial, hay que tener en cuenta dos posibles problemas. En primer lugar, en determinados contextos, es concebible que los datos personales, una vez compartidos, puedan reutilizarse para otros fines. En segundo lugar, aunque sólo se comparta una cantidad muy limitada de datos personales, es posible que estos datos se puedan completar con otros que ya posee el gobierno. Las consecuencias que esto podría tener para los beneficiarios son difíciles de predecir. Para reducir estos dos riesgos, una opción podría ser presentar únicamente una copia impresa de la lista de beneficiarios. Los datos no digitalizados son más difíciles de reutilizar. Incluso, es mejor mostrar la lista sólo en una reunión y llevarse la copia impresa de inmediato. Depende del contexto si el gobierno aceptará este enfoque, pero la idea aquí es probar opciones para minimizar el intercambio de datos.
Cuando se deba proporcionar datos personales al gobierno recuerde:

- Ser claro sobre la finalidad del intercambio de datos y las posibles consecuencias o riesgos para los beneficiarios; minimícelos cuando sea posible e identifique una base legítima.
- Establezca un acuerdo de intercambio de datos, si es posible. Este acuerdo destacará la finalidad por la que se comparten datos personales y limitará el uso de los datos a esta. También requiere que el destinatario mantenga a salvo los datos personales y que no los almacene por más tiempo del necesario. Consulte el modelo de contrato[11] de PSF de IFRC para una orientación general. La Sociedad Nacional tiene el papel de auxiliar para el gobierno, que podría ser importante en la negociación de los acuerdos de intercambio de datos.
- Informe a los beneficiarios de que los datos se intercambiarán con el gobierno y explíqueles el por qué. También sea transparente con que unidades del gobierno se compartirán principalmente los datos, lo que podría disuadir a los beneficiarios de compartirlos. Esto debe ser abordado por el programa.

Resolución 2 del proyecto: ¿Qué datos debo compartir con otras ONG?

Minimización, necesidad y seguridad de datos

Resolución reformulada del proyecto: ¿Es necesario compartir información personal con otras ONG?, ¿Puede hacerse de forma segura?

En algunos contextos, podría ser necesario intercambiar información con otras ONG. Los siguientes son algunos ejemplos y consideraciones fundamentales para la protección de datos que deben incluir las siguientes preguntas:

11 La plantilla de un contrato con un PSF puede encontrarla en el apartado de referencias de esta guía

- ¿Le interesa a los beneficiarios compartir sus datos?
- ¿Los expondría esto a un riesgo?
- ¿Puedo estar segura de que los datos seguirán siendo confidenciales y que no se compartirá con terceros sin mi consentimiento?
- ¿Dispone la otra organización de normas suficientes para la protección de datos?

En cualquier caso, proporcionar más información que nombres y detalles de contacto será problemático. Los indicadores de vulnerabilidad suelen ser asuntos muy privados y, cuando sea posible, los beneficiarios deben tener la posibilidad de decidir por ellos mismos con los que quieren compartir esos datos.

Para la coordinación. El intercambio de datos juega un papel importante cuando diferentes actores humanitarios están proporcionando simultáneamente asistencia de ayuda en transferencias monetarias y es necesario trabajar de forma conjunta (p.ej., grupos de trabajo locales sobre transferencias monetarias). Con diferentes programas ejecutándose al mismo tiempo, es importante evitar las duplicaciones y asegurarse de que no se producen perjuicios por las acciones de diferentes actores. Algunos esfuerzos de coordinación buscan armonizar las cantidades de la ayuda monetaria, los criterios de selección y enfoques. A pesar de estas intenciones razonables, se recomienda ser críticos y considerar si realmente es necesario intercambiar datos personales (y hasta qué punto) para coordinar el trabajo. A menudo, es una buena alternativa compartir información general y datos agregados (criterios de selección, áreas geográficas seleccionadas, número de personas destinatarias, porcentaje de ancianos o niños, cantidad de la ayuda monetaria, etc.). Incluso cuando el objetivo es evitar la duplicación, no es automáticamente necesario comparar las listas de beneficiarios. En función del contexto, se puede evitar la duplicación designando diferentes áreas de actividad (poblado A/poblado B) o diferentes grupos objetivo (mujeres embarazadas/ancianos). Cuando llegue a la conclusión de que es inevitable intercambiar datos de los beneficiarios, la protección de datos exige que limite a mínimos la cantidad de datos compartidos. Por ejemplo, podría ser suficiente con comparar la lista en papel de beneficiarios en una junta con otras ONG. Esto supone un menor riesgo que permitir el acceso de otras ONG a su base de datos o enviar la lista por correo electrónico.

Aprovechar la experiencia y alcance en una comunidad. En algunas ocasiones, una ONG podría tener conocimientos especializados de un sector o grupos dentro de una comunidad (p.ej., grupos dirigidos a mujeres o niños vulnerables). En este caso, una Sociedad Nacional puede necesitar cooperar con dicha ONG para beneficiarse de su especialización y conocimientos de la comunidad. Muchas veces, otras ONG se apoyan en la Sociedad Nacional local por su presencia de base en muchas comunidades y, a veces, por ser el único actor humanitario allí presente.

También pueden darse situaciones en las que otras ONG quieran establecer su propio proyecto basado en su conjunto de datos de beneficiarios ya existentes, lo que es práctico y ahorra tiempo en la recogida de datos. Sin embargo, esto implica un mayor uso de datos personales que podría no ser compatible con el propósito original de la recogida de estos. Aunque esto parezca más conveniente desde el punto de vista de los beneficiarios porque pueden recibir más ayudas, el intercambio de datos en este caso sigue siendo una excepción, no la regla, y se recomienda ser cauteloso.

Asociación para la ejecución. El intercambio de datos también es importante en las asociaciones para la ejecución, en las que se puede contratar a una organización para prestar ayuda o servicios en el nombre de otra, o para compartir responsabilidades en la aplicación de la transferencia monetaria. P.ej., la agencia de refugiados de las NN. UU que trabaja con varias ONG prestando servicios a refugiados. En estas colaboraciones, el intercambio de datos se suele negociar e incluir en un contrato o acuerdo. Al

llevar a cabo estas negociaciones, es importante evaluar los riesgos a los que se exponen los beneficiarios cuando sus datos se comparten y los manejan socios, así como las funciones y responsabilidades de los socios, y las responsabilidades compartidas en lo que respecta la protección de datos. Es posible que la agencia líder dicte las normas de la protección de datos. No obstante, si encuentra vacíos en su evaluación de riesgos o si piensa que se deben reforzar ciertas disposiciones, no dude en comunicárselo a su gerente y/o al equipo legal de su SN para que estas cuestiones puedan ser abordadas en el proceso de negociación. Por ejemplo, si su SN recoge datos de beneficiarios, ¿debe entregar todos estos datos al socio líder? o, ¿puede reducirlos a lo esencial para cumplir con sus responsabilidades en la colaboración? Si dispone de PTM paralelos dirigidos a los mismos beneficiarios en el marco del acuerdo de asociación para la ejecución, ¿cómo garantiza la separación del acceso de los socios para cosas que están fuera del alcance del acuerdo?

Plataforma común. Existen algunas iniciativas para desarrollar una plataforma común en lo que respecta al intercambio de datos de beneficiarios y el posible uso del mismo mecanismo de pago por varias de las organizaciones participantes. Esto puede implicar disponer de una base de datos o de un mecanismo de interoperabilidad de los sistemas de datos propiedad de las agencias para intercambiar y exponer el conjunto de datos de beneficiarios acordado. Dicha plataforma está enfocada a mejorar la coordinación y colaboración entre actores humanitarios y puede estar respaldada por algunos donantes, ya que puede mejorar la eficiencia. Existen diferentes enfoques para disponer de estas plataformas comunes y la SN debería, una vez más, evaluar la necesidad y riesgos para los beneficiarios antes que los beneficios para las organizaciones. Algunas cuestiones que considerar:

- ¿Es absolutamente necesaria una plataforma de este tipo para la distribución de ayuda de transferencias monetarias de la SN? ¿Hay diferentes maneras de coordinar y colaborar con otras ONG que pueden no necesitar el acceso directo a los datos de beneficiarios?
- ¿Qué datos son necesarios para participar en la plataforma común? ¿se pueden minimizar?
- ¿Cómo se debe informar a los beneficiarios cuando sus datos son tratados por otras agencias? ¿Quién debe informarles?
- Una vez se compartan los datos mediante esta plataforma común (p.ej., las otras agencias que tengan acceso a sus datos) ¿cómo deben cerciorarse los socios de que se emplean los datos para los fines acordados?
- ¿Cuáles son las características de seguridad de la plataforma para garantizar que sólo el personal autorizado pueda acceder a los datos?
- ¿Cuál sería la gestión para el acceso a los datos por parte de las diferentes ONG? Cuantas más ONG se unan, más difícil será su gestión. Especialmente cuando una organización decide dejar de participar en la plataforma común, ¿cómo se utilizarían los datos que se comparten en adelante?
- ¿Dónde se almacenarán los datos? y ¿esta ubicación (p.ej., fuera del país destinatario) plantea problemas de cumplimiento de la protección de datos?

Si se decide intercambiar datos personales con otras ONG, en primer lugar, es importante tener un acuerdo en curso. Se debe identificar la base legítima para su tratamiento. Cuando el intercambio de datos se haga mediante una plataforma común, este acuerdo debe ser incluso más sólido, con normas firmes de protección de datos, alcance y definición de las funciones y responsabilidades de los socios participantes. Se recomienda involucrar a expertos en TIC y a peritos judiciales en la negociación del acuerdo de la plataforma común para asegurar un nivel de protección suficiente. En segundo lugar, se debe informar a los beneficiarios de que se compartirán sus datos con otras agencias. Si el intercambio de datos no estaba previsto en el momento de la recogida o registro, le resultará complicado informar a todas las personas. En este caso, debería ser responsabilidad de la otra ONG utilizar la información que se le ha facilitado para informar a los beneficiarios. Se recomienda dejar esto claro en el acuerdo de intercambio.

Resolución 3 del proyecto: ¿Qué datos debo compartir con los donantes?

Minimización de datos, necesidad y seguridad de datos.

Decisión reformulada del Proyecto: ¿Es necesario y seguro compartir los datos personales con los donantes?

Para los donantes es importante garantizar la responsabilidad y transparencia en sus actividades de financiación y, por tanto, podrían solicitar el intercambio de algunos datos de los beneficiarios. De nuevo, es importante pensar en los riesgos potenciales para la privacidad de los beneficiarios y considerar opciones para limitar la cantidad de datos compartidos.

Hay dos motivos principales por los que los donantes solicitan y usan datos de los beneficiarios:

- **Para conocer el programa y supervisar su estado.** El donante normalmente quiere conocer las circunstancias del sector y cómo responde el equipo del programa. En este caso, suele ser suficiente con facilitar información general y datos agregados (criterios de selección, zonas, número de personas beneficiarias, porcentaje de ancianos/niños, cantidad de la subvención monetaria, etc.) Compartir detalles sobre los nombres y otros datos personales no siempre es necesario. El donante podría estar también interesado en conocer cómo gastan los beneficiarios el dinero recibido[12]. De nuevo, debería bastar con los datos agregados (p.ej., porcentaje de personas que invirtieron la ayuda en comida y otros productos básicos, porcentaje de personas que conservaron el dinero durante más de una semana, etc.)

- **Para cumplir con los requisitos de auditoria.** A menudo, el donante necesita datos de los beneficiarios para poder cumplir con sus requisitos de auditoria. Deben asegurarse de que el dinero donado se invierte para el propósito previsto. Otras auditorías verifican si los beneficiarios son personas reales, si reúnen los criterios de selección acordados y si, efectivamente, recibieron la transferencia monetaria (comprobante o recibo). Para estas actividades relacionadas con la auditoría, existen diferentes opciones para proteger la privacidad de los beneficiarios.

Al **compartir una lista** para realizar las verificaciones, los datos incluidos podrían limitarse al mínimo necesario, y potencialmente, en lugar de mostrar los nombres de los beneficiarios se podría utilizar la referencia única del documento de identidad. Por ejemplo, como comprobante o recibo podría bastar con el nombre, fecha y firma indicando que han recibido la ayuda. En algunos casos, puede incluso no ser necesario el nombre mientras el beneficiario facilite un documento de identidad. Si las firmas se recogieron en papel y contienen más información de la necesaria, estas columnas se deben redactar, eliminar o tachar antes de enviarlas al donante para aumentar la protección de datos.

Otro enfoque consiste en conceder un **acceso de tiempo limitado o de solo lectura** a la base de datos o al documento para que los auditores puedan realizar sus comprobaciones de forma aleatoria. Los auditores de los donantes pueden verificar los datos o documentación pertinentes en persona junto con usted, sin descargar ni extraer datos. Puede consultar previamente con el donante la información necesaria y los métodos para realizar esas comprobaciones. El intercambio de datos con los donantes

12 Tenga en cuenta que este tipo de información no debe recogerse automáticamente. Debe existir una razón legítima para recoger información sobre las compras realizadas por los beneficiarios. Antes de recopilar este tipo de información, que puede revelar información sensible sobre los beneficiarios, realice una revisión de la protección de datos. Véase el capítulo de seguimiento posterior.

debe incluirse en el contrato o acuerdo.[13]

Se deben identificar las bases legítimas e informar a los beneficiarios sobre la intención de compartir datos con los donantes.

VII. Control posterior a la distribución

Uso de datos personales

Para saber si se están cumpliendo con los objetivos del PTM, se necesita un seguimiento y evaluación de las estrategias. Parte de esta consiste en determinar los indicadores necesarios para la identificación de la producción, resultados e impacto, así como la metodología para conseguir y analizar dichos indicadores. Existen varios tipos de seguimiento, entre los que se incluyen: seguimiento de mercado, seguimiento de la línea de base, seguimiento del cobro (normalmente mediante encuestas de salida) y supervisión posterior a la distribución. En este apartado, nos centraremos en este último aspecto. Para más información sobre el seguimiento y la evaluación, véase el Módulo M5_2 Programa de seguimiento de la caja de herramientas para PTM. El seguimiento posterior a la distribución (SPD) se realiza unas pocas semanas después de una distribución, para que los beneficiarios puedan utilizar la ayuda recibida. El SPD se utiliza para evaluar la calidad del programa y mejorar los futuros programas de transferencias monetarias, y lo más probable es que se utilicen datos personales. Dependiendo del programa, podrían hacerse múltiples visitas a beneficiarios para supervisar el progreso (p.ej., la construcción de refugios como parte de la recuperación) en las que habría que hacer un seguimiento de diferentes conjuntos de datos a lo largo del tiempo.

Consideraciones para la protección de datos

La palabra “supervisión” podría denotar que se está controlando a los beneficiarios de cierta manera, que se analiza su conducta. Pero en realidad, no se controla al beneficiario sino al programa y su efectividad. No obstante, esto no implica que el seguimiento (del programa) no tenga consecuencias para el beneficiario. Por esto, se debe considerar la privacidad de los beneficiarios.

Nota: En este capítulo, las resoluciones del proyecto se centrarán en el SPD. En el seguimiento de la línea de base y cobro los principios más importantes son: la minimización de datos y necesidad. Cuando se recoge información de beneficiarios, es importante reflexionar sobre los datos que son realmente necesarios en el contexto del seguimiento de su programa. Además, cuando se emplean formularios estandarizados hay que adaptarlos al contexto, eliminando aquellas preguntas innecesarias. Véase de nuevo el capítulo sobre la selección y registro de beneficiarios. Otro método recomendado para aumentar el nivel de la protección de datos en estos seguimientos consiste en eliminar la identificación de los beneficiarios (p.ej., nombres y documentos de identidad personales).

Resolución 1 del proyecto: ¿Qué datos personales se deben recolectar durante el proceso de s seguimiento?

Minimización de datos, necesidad

Resolución reformulada del proyecto: ¿Cómo puedo limitar el uso de datos personales durante el proceso de seguimiento?

13 Es importante tener en cuenta cuestiones como los requisitos de auditoría en la fase de negociación del contrato.

Según el contexto, el seguimiento se puede hacer de distintas maneras. En este caso, nos centraremos en el SPD para las transferencias condicionales e incondicionales y consideraciones de la protección de datos.

Condicionalidad y restricción

El PTM puede estar sujeto a ciertas condiciones (por ejemplo, que los beneficiarios reúnan unos requisitos previos antes de recibir la ayuda económica, como la asistencia escolar, la promoción de la salud, talleres sobre medios de vida) o restricciones (exige que los beneficiarios utilicen la ayuda para productos o servicios específicos o para que logren un resultado como reparar la vivienda o iniciar medios de vida). El objetivo del seguimiento es verificar si, a lo largo del tiempo, se siguen cumpliendo con las condiciones y respetando las restricciones. Una consideración fundamental es la privacidad de los beneficiarios, que se consigue reduciendo la cantidad de información recogida a la mínima esencial. Asimismo, resulta de utilidad establecer unos intervalos de tiempo razonables para el seguimiento y reducir el número de personas que participan en el seguimiento de los mismos beneficiarios. También, hay que limitar el acceso a datos desglosados, que podrían usar las distintas partes interesadas que ayudan o participan en este proceso.

Ejemplo:

En el contexto de un programa, los beneficiarios deben utilizar la ayuda para construir una vivienda tras un huracán devastador. El equipo del programa decide que visitará a cada beneficiario al cabo de una semana y de nuevo, al cabo de tres semanas para ver el progreso de la reconstrucción de la vivienda. El equipo preguntará por los materiales adquiridos con la ayuda monetaria y comprobará visualmente el estado de la vivienda. No pedirán al beneficiario que rellene largos formularios sobre sus condiciones generales de vida o que saquen una foto de la construcción. El equipo del programa decide también crear dos equipos diferentes de seguimiento que cubran diferentes zonas geográficas. Los mismos equipos supervisarán los mismos hogares al cabo de tres semanas para garantizar la coherencia de la supervisión, ya que, al no tomarse fotos, los mismos miembros del personal pueden verificar el progreso de la construcción.

Incondicional y sin restricciones

Cuando se entrega dinero en efectivo a los beneficiarios para que lo gasten en sus propias necesidades específicas y no en un producto o actividad previamente definidas, la supervisión podría ser diferente. Se seguirían necesitando datos de los beneficiarios para ver cómo (en términos generales, por ejemplo, por categoría) gastaron su subsidio y si se cumplieron los objetivos del programa. En este caso, el propósito no es supervisar al beneficiario individual, sino comprender la efectividad del programa. El comportamiento general de los beneficiarios participantes es un indicador importante para evaluar si los criterios de selección y la cantidad de efectivo entregado fueron los apropiados.

Un método habitual de seguimiento consiste en organizar debates de grupos focales con una muestra de beneficiarios y no beneficiarios de la comunidad. Con estas personas se crea un debate sobre el proyecto en general. Se les suele preguntar su opinión del proyecto (criterios de selección, efectos del proyecto, etc.). Asimismo, se les invita a compartir experiencias propias sobre cómo han empleado el dinero. Desde el punto de vista de la protección de datos, los debates orales ocasionan menos problemas que la recogida formal de información en papel o formato digital. Sin embargo, hay que tener muy en

cuenta como se graban estos debates de grupos focales. Las grabaciones en vídeo o audios pueden interferir mucho con la privacidad de los participantes. En general, es preferible levantar actas de las sesiones. Lo más probable es que esto facilite que los participantes expresen sus experiencias y opiniones. A la hora de tomar notas de la reunión, hay opciones para aumentar el nivel de privacidad.

Merece la pena considerar limitar las notas a:

- Puntos de discusión generales – en lugar de señalar a individuos y sus respectivos comentarios.
- Número de participantes y las características principales que les convierten en buenas muestras (edad, género, zona en la que viven) en lugar de recoger sus nombres completos.

Los comentarios pueden seguir sin ser completamente anónimos. Las personas que formaron parte del debate sabrán quién dijo qué. Sin embargo, para las personas que consulten las notas de la reunión será más difícil identificar a la persona que está detrás de cierto comentario. Evidentemente, depende del contexto que esta información limitada sea suficiente para la finalidad del seguimiento.

Otro método de seguimiento consiste en hacer entrevistas con una parte de los beneficiarios, lo que suele hacerse con modelos de cuestionarios. Será importante comprobar la identidad del beneficiario entrevistado para asegurarse de que es la persona correcta y de que, efectivamente, ha recibido la ayuda monetaria. Sin embargo, puede que no ser necesario almacenar información sobre su identidad, por lo que se puede mantener un cierto nivel de anonimato. El entrevistador conocerá la identidad del beneficiario, pero los datos recogidos tras rellenar el cuestionario estarán más protegidos frente a la consulta de los datos por otras personas.

Ejemplo:[14]

El equipo del programa solicita una muestra de los beneficiarios para que formen parte de un debate de grupos focales, para comprobar cómo se utilizó *la ayuda monetaria. El equipo comprueba el documento de identidad de los participantes, pero no anota sus nombres ni documento de identidad en el formulario de encuesta. En dicha encuesta, los beneficiarios se mostraron abiertos a manifestar su descontento en cuanto al cobro, ya que les exigía desplazarse a gran distancia para encontrar un agente monetario, había problemas de liquidez con este, y además indicaron que hubiera sido útil recibir ayuda en especie el lugar de efectivo. Debido al respeto de la privacidad, su honestidad permitió al equipo del programa aprender y ajustarse para el próximo desembolso de dinero, en lugar de decir que estaban aparentemente satisfechos por miedo a no recibir más ayudas.*

Cuando no sea posible mantener el anonimato de la identidad del beneficiario en los cuestionarios, es importante reducir las preguntas al mínimo necesario. Los formularios suelen incluir muchas preguntas que cubren diversos escenarios ("modelo único"). Como se explica en el capítulo de registro, estos formularios estandarizados deben adaptarse a las circunstancias específicas según sea necesario. Las preguntas innecesarias deben tacharse o eliminarse.

Trate de encontrar opciones para evitar el uso de datos personales. Si estos se utilizan con el fin de

[14] Por la imposibilidad de poner el pie de página en el recuadro azul, pongo la anotación justo antes de empezar el siguiente párrafo. Nota: los beneficiarios deben facilitar información de forma voluntaria, no pueden ser forzados. Se debe dejar aclarar que su participación no afectará en las distribuciones actuales o futuras y que son libres de negarse participar.

realizar un seguimiento, es importante identificar unas bases legítimas e informar a los beneficiarios sobre el tratamiento de sus datos.

Resolución 2 del proyecto: ¿qué datos puede proporcionarme el PSF sobre los beneficiarios para el seguimiento de mi programa?

Minimización de datos, necesidad y confidencialidad de datos

Resolución reformulada del proyecto: ¿Qué datos puede proporcionarme el PSF para fines de seguimiento sin invadir la privacidad de los beneficiarios?

Cuando en los programas de transferencias monetarias se utilizan PSF, dichos proveedores pueden tener datos de los beneficiarios que podrían ser de utilidad en el proceso de seguimiento. Dependiendo del PSF, algunos de los datos que pueden tener son: cuándo se retiró el dinero y desde dónde (p.ej, cajero automático o agentes monetarios), si el dinero se utilizó para comprar en ciertos establecimientos (p.ej., en una tienda de comestibles en lugar de una licorería), y firma en el comprobante de recibo. La obtención de estos datos puede ayudar a agilizar y obtener información precisa en el proceso de seguimiento. No obstante, desde el punto de vista de la protección de datos, este enfoque podría plantear ciertos riesgos. Los datos relacionados con pagos y compras pueden ser bastante sensibles. Recoger estos datos de fuentes externas en lugar de los propios beneficiarios podría considerarse como intromisión en su intimidad.

Cuentas personales de los beneficiarios

Cuando la distribución se hace mediante las cuentas personales (banco/móvil) de los beneficiarios, la Sociedad Nacional no tiene acceso a estas por defecto. Sin embargo, el PSF puede rastrear los movimientos de la cuenta y quizás esté dispuesto a compartir con usted la información de los pagos importantes. Por lo tanto, la cuestión es: ¿es esto relevante y necesario para el propósito del seguimiento? Es posible que quiera saber cuándo y cómo se ha utilizado el dinero. No obstante, el foco del seguimiento no está en el beneficiario individual sino en la actitud general de todos los beneficiarios. Por esto, normalmente bastaría con que reciba información agregada sobre los pagos. Por ejemplo, el PSF podría informarle de:

- El porcentaje de beneficiarios que se gastaron el dinero la primera semana.
- El porcentaje de beneficiarios que utilizaron el dinero en establecimientos específicos como supermercados o farmacias.
- El tiempo promedio que tardan los beneficiarios en gastarse todo el dinero.
- Las regiones en las que se gastó antes el dinero.
- Ubicación relativa de los agentes monetarios y cuáles han desembolsado más dinero que otros.

Dependiendo del contexto del programa, puede acordar con el PSF la información que deben facilitarle, teniendo en cuenta el principio de minimización de datos y necesidad.

Ejemplo:

Un PTM distribuye dinero con tarjetas de prepago que los beneficiarios pueden utilizar para comprar en tiendas y establecimientos que acepten MasterCard o pueden retirar el dinero de un cajero automático. La Sociedad Nacional podría querer saber para qué tipo de productos se ha utilizado el efectivo y comprueba con el PSF si se le puede facilitar esta información. El equipo del programa solicita explícitamente los datos agregados y ver si (1) la ayuda se retira de cajeros automáticos o si bien se utiliza para comprar en tiendas, (2) el porcentaje de beneficiarios que todavía no han utilizado la ayuda monetaria, y(3) las categorías de establecimientos en los que se utilizaron tarjetas de crédito (p.ej., comida, medicina, servicios) El PSF solamente facilita datos agregados y visualizaciones pertinentes en lugar de datos específicos sobre compras y sobre qué persona realizó la transacción, dónde y cuándo.

En la práctica, y si no se ha negociado previamente, el PSF podría no estar dispuesto a crear informes específicos o a facilitarle información demasiado específica puesto que les supondría un esfuerzo mayor. Si este es el caso, otra opción sería solicitar que no le envíe el conjunto completo de datos, sino solamente información transaccional muy limitada para proteger la privacidad del beneficiario. Se debe solicitar al PSF que elimine los nombres y números de tarjeta en cada una de las operaciones financieras.

Si la única opción es recibir por parte del PSF el conjunto completo de datos transaccionales sin procesar, se recomienda restringir el acceso a los datos completos y nombrar a una persona del equipo como custodio de la información. El PSF enviará exclusivamente los datos de pago a esta persona, de los que sólo podrá extraer la información necesaria para que la procese el resto del equipo del programa. Luego, el custodio podrá eliminar de forma segura los datos completos recibidos por parte del PSF, para evitar su uso inadvertido por alguien más. La información agregada abstracta ofrece un mayor nivel de protección de datos que, en muchos casos, podría ser suficiente.

Ejemplo:

Un programa de efectivo envía dinero mediante el monedero móvil de los beneficiarios. La Sociedad Nacional puede querer saber qué agentes de dinero móvil se utilizaron para el cobro, con el fin de poder informar a los proveedores en caso de que haya problemas de liquidez antes de la siguiente distribución. El PSF no solo es capaz de facilitar esta información, sino que está dispuesto a enviar el listado completo de las transacciones con las actividades financieras de cada uno de los beneficiarios y dónde están cobrando el dinero. El equipo del programa solicita al PSF que solo le remita estos datos al gestor IT apoyando el programa de efectivo, quien luego extraerá los datos necesarios para que el equipo del programa pueda procesarlos. Luego, el gestor IT eliminará el archivo tras extraer solamente los datos agregados pertinentes.

Cuenta virtual de la Sociedad Nacional

Cuando las distribuciones se realizan mediante cuentas virtuales de la Sociedad Nacional (véase el capítulo sobre PSF) el PSF puede no tener un vínculo directo entre los datos transaccionales y los beneficiarios reales, puesto que la Sociedad Nacional es quien gestiona las subcuentas. Por consiguiente, tener un acceso directo a las transacciones de los beneficiarios por ser el titular de la cuenta, podría

suponer riesgos en cuanto a la privacidad. Como se ha mencionado anteriormente, los datos sobre pagos individuales son sensibles y normalmente, a efectos de seguimiento, no suele ser necesario conocer los datos de beneficiarios individuales sino de lo grupo de beneficiarios en su conjunto.

De nuevo, una forma de proteger la privacidad de los beneficiarios es designar un custodio con acceso único a todas las transacciones disponibles en la plataforma. Si sólo una persona tiene acceso a la plataforma y transforma la información individual en abstracta, el riesgo derivado de la falta de protección de datos podría reducirse. Cuando no sea posible designar un custodio, es responsabilidad de todos los miembros del equipo con acceso a la plataforma y al conjunto completo de datos respetar la confidencialidad y privacidad de los beneficiarios, así como asegurarse de que los identificadores de las subcuentas no se vinculen a personas. Por esto es crucial que todos los miembros del equipo estén familiarizados con las prácticas y principios de la protección de datos. Siempre que reciba estos datos, es importante que se lo comunique al beneficiario y le comente cómo piensa proteger su privacidad.

Resolución 3 del Proyecto: ¿Qué datos del beneficiario puede proporcionarme el distribuidor en un programa de vales?

Minimización de datos, necesidad y seguridad de datos

Resolución reformulada de proyecto: ¿Qué datos puede proporcionarme el distribuidor para fines de supervisión sin invadir la privacidad del beneficiario?

En los programas de vales, se pueden emplear los datos de las transacciones de distribuidores para realizar el seguimiento. El distribuidor tiene registros de cuántos vales se han canjeado y en qué periodo de tiempo, así como los productos seleccionados a cambio de estos. Sin embargo, sigue siendo importante garantizar un alto nivel de protección de datos cuando se utiliza dicha información. Por lo general, basta con revisar los datos agregados del uso general de los vales y los productos básicos adquiridos. A efectos de supervisión, no es relevante conocer para qué utilizó el vale un solo beneficiario, sino conocer el comportamiento general de los beneficiarios participantes para evaluar la eficacia del programa. Por lo tanto, debe evitarse revisar los datos que permiten identificar cuándo y dónde un beneficiario individual compró un determinado producto. Esto se puede hacer solicitando al distribuidor que agregue los datos por usted. Si no es posible, solicite únicamente un conjunto limitado de datos sin identificadores. De lo contrario, al igual que en los apartados anteriores, trate de designar a un custodio en su equipo que reciba y extraiga solamente el conjunto de datos pertinentes y que elimine inmediatamente la lista completa de transacciones.

VIII. Orientación general

En esta sección se examinan las principales consideraciones en materia de protección de datos que se aplican en todo programa de transferencias monetarias.

Consideraciones para la protección de datos

Almacenamiento de datos

Cuando se recopilan datos personales de los beneficiarios, es de extremada importancia mantenerlos a salvo y protegidos. Esto se traduce en tomar suficientes medidas de seguridad para evitar la llamada violación de datos (pérdida, acceso no autorizado, etc.) (véase a continuación una orientación sobre lo que hacer en caso de violación de datos)

Las soluciones informáticas para la seguridad de los datos son muy técnicas y, a menudo, requieren

conocimientos especializados por lo que se recomienda desarrollar un programa de enfoque transversal coherente junto con su administración TI, si es posible. El concepto puede abordar los flujos de datos, los canales e interfaces para el intercambio, los niveles de encriptación en el almacenamiento y transferencia, las copias de seguridad o el almacenamiento redundante para evitar la pérdida de datos y los controles de acceso para garantizar que sólo las personas autorizadas tienen acceso a estos, etc.

En cualquier caso, se deben considerar minuciosamente los siguientes aspectos:

- En el caso de los datos digitales, es fundamental que cuando sea posible se utilicen bases de datos sólidas o una solución de gestión de datos. Se debe evitar en todo momento el almacenamiento de datos en repositorios de acceso público como Google o Dropbox. El uso de bases de datos presenta muchas ventajas, ya que proporcionan seguridad informática mediante el cifrado nativo, depósitos o carpetas protegidas por contraseña, rastreo de archivos del registro, copias de seguridad, etc. Las soluciones de gestión de datos (como RedRose y LMMS) pueden incorporarse a distintas herramientas de recolección de datos como ODK y Kobo, y a medios de pago como pagos móviles o bancos para las transferencias de efectivo. Es importante evaluar estas soluciones en términos de la protección de datos para asegurarse de que estos estén protegidos tanto en el tránsito (p.ej., cuando se recogen datos con el móvil con ODK y Kobo y tienen que transferirse desde el dispositivo móvil al servidor de bases de datos) como en su almacenamiento (cuando los datos están almacenados en el servidor de la nube). Se debe evaluar el lugar de almacenamiento físico en función de la legislación nacional (p.ej., algunos países prohíben, o ponen limitaciones a la transferencia de datos personales fuera de su jurisdicción).

- Cuando los datos deben almacenarse en portátiles o memorias USB, el riesgo de pérdida y robo es mayor que en una base de datos propiamente dicha. Para reducir este riesgo, se deben adoptar medidas de seguridad adicionales. Lo ideal sería proteger el disco duro con un cifrado (p.ej., Bitlocker de Microsoft). Además, se puede aumentar el nivel de protección cifrando o protegiendo con contraseña los documentos del disco duro. Los ordenadores portátiles y memorias USB también deberían estar protegidos físicamente con contraseñas y se deben guardar en un cajón cerrado con llave cuando no se estén utilizando.

- Al crear una contraseña, intente que esta sea fuerte y difícil de adivinar. Una buena técnica para esto consiste en alternar letras pequeñas y grandes, dígitos y caracteres especiales, además de cambiarla con frecuencia. Evite compartir cuentas y contraseñas. Si la cuenta es genérica (p.ej., cuentas de correo genéricas administradas por diferentes personas), es importante limitar el acceso. (véase a continuación Control de Acceso)

- Con los archivos en papel, se corre un riesgo aún mayor de extravío y acceso no autorizado. Si la única opción es tenerlos en este formato, archívelos en un depósito con cerradura. Al ser así, se evita la visualización por parte de terceros.

Para más consejos, véase el folleto sobre la protección de datos de IFRC (IFRC's IM Data Protection Flyer) en el que se indica lo que se debe hacer y lo que no en el almacenamiento y procesamiento, así como la política de seguridad de la información de IFRC (IFRC's information security policy).

Conservación y eliminación de datos

¿Qué ocurre con los datos personales de los beneficiarios una vez finalizado el programa? Lo ideal es no dejarlos en archivos de papel o en una base de datos durante un periodo de tiempo ilimitado. Una vez que los datos de un programa específico ya no son necesarios, deben ser eliminados o, como mínimo, agregados o anonimizados. Si se necesitan durante un periodo prolongado, pero no se requiere un

acceso regular (como en el caso de las auditorías), una opción podría ser archivarlos de forma segura y sin conexión.

Plazos de conservación

Se recomienda establecer previamente un periodo de tiempo de conservación que señale por cuánto tiempo deben almacenarse normalmente los datos. Una vez expirado este periodo, se eliminan los datos. Sólo si existen razones de peso que requieran la conservación de estos por un tiempo, se pueden conservar durante un periodo de tiempo mayor pero limitado. Estos plazos de conservación de datos pueden incorporarse en la base de datos para permitir la depuración automática. Si desea obtener más información sobre estas opciones, consulte con los compañeros de TI de su organización. Si no se pueden utilizar bases de datos o periodos de retención automatizados, otra opción es configurar recordatorios en el calendario. La finalidad consiste es reflexionar de forma activa, en intervalos regulares, sobre si conservar o eliminar los datos que ya no son necesarios. La duración de los plazos de retención depende del programa en sí, pero también podría estar dictada por las propias políticas de la organización. A la hora de concebir la intervención del PTM, se deben considerar unos plazos de retención apropiados para poder comunicárselos a los beneficiarios. Algunos aspectos que se tienen que considerar son:

- La duración del proyecto
- La sensibilidad de los datos
- La magnitud del seguimiento previsto
- La probabilidad de que se produzcan problemas de seguimiento.

Otros fines

Incluso cuando un programa ha finalizado y se ha realizado su seguimiento, podría parecer útil conservar algunos datos para otros fines. En primer lugar, se podrían utilizar para la creación de **informes y estadísticas** adicionales. Sin embargo, para esto no suele ser necesario conservar los datos que identifiquen directamente a las personas (p.ej., nombres, números de documentos de identidad), es suficiente con generar un conjunto condensado de datos agregados. En segundo lugar, es probable que los datos puedan ser útiles para la preparación general de futuros programas similares, sobre todo, en lugares propensos a los mismos peligros (p.ej. huracanes y tifones frecuentes). En estos casos, podría parecer razonable almacenar los datos sin más. No obstante, estos suelen tener una vida útil limitada. En el caso de los programas nuevos, es necesario actualizarlos y verificarlos. La gente se va o se traslada a la zona, sus condiciones de vida cambian, nacen niños o mueren miembros de la familia. Por esto, la retención de datos para posibles programas futuros no suele ser eficaz. Si se decide conservar los datos para programas futuros, es importante que se considere si la nueva finalidad es compatible con la original. Los asuntos humanitarios pueden ser compatibles, pero si la finalidad no lo es, es fundamental informar a los beneficiarios de su intención de reutilizar los datos para otros fines, además de identificar una nueva base legal para un nuevo tratamiento de datos (véase el apartado de base legítima en el capítulo de Registro). En tercer lugar, es posible que se tengan que almacenar datos para fines de auditoría. Si este es el caso, los requisitos de auditoría suelen identificar los periodos de almacenamiento necesarios. En caso contrario, a menudo se suele identificar un periodo de almacenamiento razonable teniendo en cuenta el marco temporal y/o el objetivo de la auditoría. Los datos recogidos para fines de auditoría deben archivarse por separado del resto de flujo de datos.

Datos de los no beneficiarios

Durante el proceso de selección, se recogen datos personales de personas que finalmente pueden no ser beneficiarios de la ayuda, puesto que no reúnen los requisitos de la elegibilidad (véase el capítulo Selección). Del mismo modo, durante el registro de beneficiarios es posible que se hayan recogido datos de personas que finalmente resultan no ser elegibles. El almacenamiento de datos de los no beneficiarios se debe considerar minuciosamente. Dado que no formarán parte del programa, sus datos dejan de ser

necesarios una vez se haya completado la verificación de elegibilidad. No obstante, podría ser de su interés e incluso del beneficiario, conservar la información personal durante un periodo de tiempo determinado, para así tener pruebas de las decisiones en caso de que el no beneficiario presente una denuncia contra la Sociedad Nacional por haber ser excluido del programa, por ejemplo. En este caso, puede ser muy útil poder ver como se tomó la decisión y que datos se utilizaron. Cuando sea posible, en este tipo de situaciones, almacene la respectiva información por separado del resto de los beneficiarios elegibles, para que estos datos dejen de forma parte del flujo de datos del programa en curso. Pero, si aparece una queja, se pueden recuperar.

Control de acceso

La información obtenida directamente de los beneficiarios u otras fuentes (gobierno, etc.) debe tratarse con confidencialidad. La confidencialidad está estrechamente relacionada con los principios de minimización de datos, necesidad y seguridad de datos, tal y como se explicó anteriormente.

En los programas de transferencias monetarias suelen participar diferentes partes interesadas: internas (p.ej., equipos del programa y en terreno, servicios de apoyo como compañeros de Finanzas, Logística, AI, TI, y gestores) y externos (p.ej., PSF, donantes, gobierno, otras ONG). Anteriormente, se ha mencionado el tratamiento de los datos personales con partes interesadas (véase el capítulo sobre PSF e intercambio de datos con externos). En el caso de las partes interesadas internas, es importante determinar el tipo y nivel de acceso necesario en relación con los datos de beneficiarios. Algunas organizaciones tienen una clasificación de la información. Por ejemplo, la política de seguridad de la información de IFRC (IFRC's information security policy) clasifica los datos de los beneficiarios como confidenciales o altamente confidenciales en función del contexto; lo que requiere el máximo nivel de protección de la seguridad, así como un acceso limitado según el principio de "la necesidad de conocimiento".

Algunas maneras de garantizar un control de acceso adecuado:

- Utilice el nombre de usuario y contraseña para acceder a la base de datos o plataforma de gestión de datos. Informe a los usuarios de que no deben compartir su usuario y contraseña con otras personas. Además, evite crear usuarios genéricos en los que varias personas puedan acceder como usuarios. Las acciones de cada usuario deben ser auditables y rastreables.
- Utilice el control de acceso basado en roles (RBAC) en el que cada usuario recibe un rol en específico que le permite el acceso a funciones específicas y datos del sistema. El acceso puede ser tan gradual como sea necesario (p.ej., acceso a la lista de beneficiarios, capacidad de descargar dicha lista, o tan sólo dar acceso a datos agregados como los cuadros de mando.) Se debe revocar el acceso si hay un problema de seguridad con un usuario.
- Disponer de un registro de acceso para dejar constancia de quien se ha conectado y accedido a determinadas páginas o datos, así como un registro de descarga para quienes descargan datos directamente del sistema (teniendo en cuenta que a esto se le considera recogida y tratamiento de datos personales y debe tratarse adecuadamente)
- Cuando descargue datos en una hoja de cálculo de Excel, protéjala con una contraseña o cifre el archivo.
- Si no se dispone de base de datos, los archivos deben estar protegidos con contraseña y sólo el personal autorizado debe tener acceso a estos. En el caso de los archivos en papel, solo el personal autorizado debe tener acceso directo y los archivos deben guardarse en un depósito cerrado con llave.

Ejemplos

El programa de transferencia monetaria cuenta con 10 miembros del personal y personal voluntario para su ejecución. Mientras que 3 son responsables de la selección y registro de los beneficiarios (equipo 1) los otros 7 se encargan de contactar con los proveedores de servicios financieros y la distribución (equipo 2). El equipo 2 no tiene por qué estar al tanto de la vulnerabilidad de los beneficiarios. Solo deben conocer los datos personales que son necesarios para la parte del proyecto relativa al efectivo (nombres, cuentas bancarias, KYC). Por esto, el equipo 1 crea para el equipo 2 una lista de beneficiarios con información limitada. El resto de la información se almacena en una base de datos protegida con contraseña que solo conoce el equipo 1. Además, solo 1 persona tiene el rol de administrador y puede acceder por completo a la base de datos (acceso de lectura y escritura), mientras que los otros dos miembros del equipo solo tienen acceso de lectura.

En el mismo escenario, el mecanismo de entrega es el de efectivo en mano. Se espera que el Equipo 2 tenga que justificar la elección de beneficiarios el día de la entrega. Si se da esta situación, es necesario que el Equipo 2 tenga acceso a información adicional. Por lo tanto, solicita esta información adicional al equipo 1, que la presenta de forma limitada.

Proceso de transmisión (intercambio de datos)

Cuando se intercambian datos, el proceso de transmisión puede aumentar el riesgo de pérdidas de información y de accesos no autorizados. Por lo tanto, cuando se transfieren datos personales, las medidas de seguridad adquieren un papel importante.

- Lo ideal es que se intercambien datos mediante herramientas seguras, como el FTP (protocolo de seguridad de datos) con nombre de usuario y contraseña, y un acceso limitado para descargar datos de una base de datos protegida o una plataforma de gestión de datos.
- Cuando sea necesario enviar información a los beneficiarios por correo electrónico, es importar recordar: (1) limitar el número de destinatarios, (2) proteger los archivos adjuntos con contraseña y (3) cifrar los correos electrónicos (cuando sea posible). Esto permite una cierta protección en el caso de que se pirateen los correos electrónicos o se envíe accidentalmente a la dirección incorrecta. El riesgo de exponer los datos del beneficiario a personas no autorizadas se reduce cuando se cifran los correos electrónicos y archivos. Si tiene dudas sobre cómo cifrar los archivos o correos, contacte con sus compañeros de TI. Enviar correos electrónicos a listas de difusión en lugar de a personas individuales, puede parecer conveniente, pero podría ser problemático si no sabes exactamente las personas que están incluidas en dicha lista. Lo mismo ocurre cuando se envían a direcciones de correo electrónicos genéricas en las que distintas personas pueden tener la contraseña de la cuenta o gestionarla. Tenga cuidado también cuando se reenvían correos electrónicos o cuando se crean cadenas de correo electrónico en las que se muestran las respuestas a mensajes. A medida que aumentan o cambian los receptores, asegúrese de que estos estén autorizados a ser informados de los datos personales del beneficiario.

Ejemplo:

La situación de determinados posibles beneficiarios se comenta por correo electrónico a líderes comunitarios para decidir si pueden acogerse al programa de ayuda en efectivo. Este correo electrónico puede enviarse al líder comunitario que ayuda en la toma de decisiones y a los compañeros que participan en la selección. Sin embargo, se debe evitar enviar este correo a cuentas de correo electrónico genéricas, como: info@comunidad o equipodeefectivo@

- Tenga cuidado si desea compartir archivos que contengan datos personales a través de aplicaciones de mensajería móvil, como WhatsApp. A menos de que confíe en la seguridad de la aplicación de mensajería (p.ej., Signal se considera mucho más segura que WhatsApp) no la utilice para enviar datos personales u otros datos sensibles (ya sean miembros del personal, voluntarios o beneficiarios)

Directrices en la violación de datos

A pesar de todas las medidas de seguridad, no existe la garantía de que se puedan prevenir las violaciones de datos en todas las situaciones. Tal y como se define al principio de esta guía, una violación de datos consiste en el acceso no autorizado, destrucción, pérdida, alteración o divulgación de datos personales. Una vez producida la violación de datos, es importante tomar las medidas adecuadas para remediar las consecuencias de esta. Se recomienda que tanto usted como su personal esté al tanto de estos pasos antes de que se produzca una violación. En cuanto tenga conocimiento de la vulneración, asegúrese de:

- **Informar sin retrasos indebidos** a su gerente o supervisor, así como al punto focal de protección de datos, el equipo legal u otra persona responsable de la protección de datos de la Sociedad Nacional. Si no conoce al responsable, comunique sus preocupaciones a los dirigentes de su organización.

Los siguientes pasos deben llevarse a cabo en colaboración de esos expertos:

- **Investigar el alcance de la violación:** tipo de violación, tipo de datos, cantidad de datos, duración de la vulneración, a cuántas personas se refieren los datos, quienes están expuestos a los datos.
- **(paralelamente) Adoptar medidas de mitigación** (dependiendo del tipo de mitigación, p.ej., interrumpa los sistemas informáticos, recuperar los datos de la copia de seguridad, contactar con la persona no autorizada para poner fin a la exposición de datos, cerrar las brechas, informar a los socios implicados y donantes potenciales.
- **Evaluar el nivel de riesgo para los sujetos de los datos y hacer esfuerzos razonables por informar a los sujetos de los datos si los riesgos son elevados** por cuestiones de transparencia.
- Según la legislación nacional, **considere la posibilidad de informar a las autoridades de la protección de datos de su país.**
- **Preparar el informe/la experiencia adquirida y eliminar las deficiencias organizativas o técnicas detectadas.**
- **Mejorar el plan de respuesta para una próxima incidencia, según sea necesario, basándose en la experiencia adquirida.**

Informar al personal y voluntariado

El primer paso hacia una protección de datos eficaz es la concienciación. Por lo tanto, es importante que el personal y los voluntarios conozcan los principios clave de la protección de datos y cómo abordarlos en el ciclo del PTM. Se recomienda celebrar sesiones de formación periódicas sobre protección de datos, especialmente para los nuevos miembros de la organización, como parte de su incorporación. El material de formación podría prepararse con antelación para una incorporación o como recordatorio para

aquellos que ya han sido formados. En esta formación, se debe resaltar la importancia de la protección de datos y explicar los principios fundamentales. Y, lo que es más importante, que consideraciones sobre la protección de datos deben abordarse en los procesos de PTM y las distintas responsabilidades del personal y voluntarios según su rol. También, se debería explicar la forma de actuar en casos de violación de datos

Análisis y seguimiento de los riesgos de la protección de datos

Para hacer de la protección de datos una verdadera salvaguardia de la privacidad de los beneficiarios en los programas, se recomienda encarecidamente que anote las diferentes consideraciones de la protección de datos que realice. ¿Por qué? Porque ayuda a establecer un enfoque estructurado y consistente para gestionar los riesgos y encontrar un equilibrio correcto. Además, documentar los riesgos y decisiones tomadas será importante en el caso de que una auditoría o investigación sean necesarios.

Existen algunas herramientas que pueden emplearse en el análisis y documentación de riesgos relacionados con la protección de datos:

Matriz de registro de riesgos. La caja de herramientas para PTM cubre el análisis de riesgos en la preparación (módulo M1_1 Preparar y Analizar), evaluación (módulo M2_4) y análisis de respuesta (Módulo M3_1_4). También se describen riesgos adicionales para la programación de dinero por trabajo y cupones. La misma matriz de registro de riesgos puede emplearse para asegurarse de que los elementos de protección de datos se revisen juntos con otros tipos de riesgos. Podría ser necesaria la creación de una nueva categoría para la protección de datos para clasificar los riesgos correctamente. Será importante analizar estos riesgos y generar medidas de mitigación. Asimismo, a medida que se ejecuta el programa, los riesgos deben revisarse y actualizarse según sea necesario.

Evaluación de Impacto en la Protección de los Datos Personales (EIPD) [15]se trata de una herramienta formal para documentar las consideraciones de la protección de datos para los riesgos identificados, así como medidas de mitigación previstas. Su preparación podría requerir una consulta externa o la inclusión de partes interesadas. La realización de una EIPD profunda no es necesaria en todos los casos, sobre todo, cuando se ejecutan PTM similares. Podría ser necesario cuando se emplean nuevos métodos y tecnologías y todavía no se conoce el impacto que podría tener en los beneficiarios. Asimismo, podría resultar también de utilidad, determinar cuáles son los riesgos reales y si pueden mitigarse, cuando existen posibles inquietudes de miembros de la comunidad respecto al tratamiento de sus datos.

15 Para más detalles, diríjase al Manual Sobre Protección de datos en la ayuda humanitaria. Encontrará también una plantilla de EIPD en el apartado de referencias de esta guía.

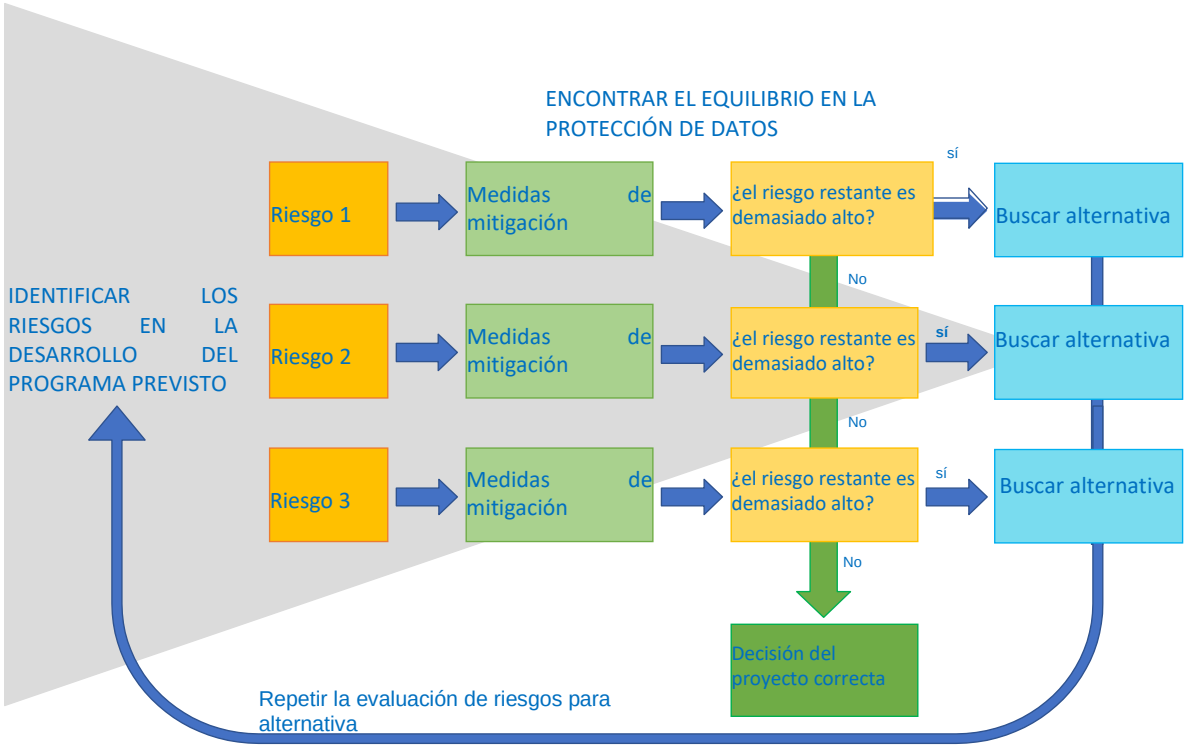

Gráfico 4: balance de riesgos y acciones relacionadas con la protección de datos

El gráfico 4 tiene como objetivo ayudar en el proceso de reflexión sobre la evaluación de riesgos de la protección de datos. Este incluye la identificación, anotación de los riesgos y medidas de mitigación posibles, determinando así el nivel de riesgo (basándose en el impacto y probabilidad) y buscando alternativas para tener en cuenta. Por ejemplo:
¿incluir al PSF?

> Riesgo 1: Uso de los datos para otros fines distintos a los acordados

> Medida de mitigación: prohibir en el contrato

> ¿Existe un riesgo restante alto? Sí, porque la reputación y fiabilidad del PSF son cuestionables.

> Alternativa: otro PSF, efectivo en mano o en especie.

> Repetir la evaluación de riesgos para una alternativa.

Si la evaluación inicial de riesgos revela que la configuración del programa presenta grandes riesgos para la protección de datos, se recomienda realizar la evaluación con un formato de EIPD. La obligación de realizar una EIPD formal recae en la organización que dirige el programa, en el caso de una asociación para la ejecución. La ejecución de esta evaluación formal debe ser considerada (y, en virtud de algunas leyes de protección de datos, puede ser obligatoria), por ejemplo, en las situaciones mencionadas a continuación. Tenga en cuenta que todas esas formas de tratamiento de datos están estrictamente sujetas al principio de minimización de datos y necesidad. Una EIPD no justifica el tratamiento innecesario de datos.

- Las nuevas tecnologías se emplean en recogida, gestión o almacenamiento de datos personales (almacenamiento en nube, geolocalización, redes sociales, etc.) El desconocimiento del funcionamiento de las nuevas tecnologías podría suponer un aumento del riesgo de acceso no

autorizado (piratería) y posibilidades abiertas a la vigilancia no autorizada.

- Las personas pueden ser objeto de la toma de decisiones automatizada o de la elaboración de perfiles. La toma de decisiones automatizada interfiere considerablemente con la protección de datos, puesto que las decisiones se toman fuera del control del individuo y sin la posibilidad de que este pueda retractarse y debatir la decisión. La elaboración de perfiles resulta problemática ya que crear el perfil de una persona es como encasillarla en ciertas categorías sin una interacción previa con este.
- Los datos personales podrían ser transferidos a un tercero (o país) sin unas normas de protección de datos similares. Como se ha mencionado anteriormente, el intercambio de datos puede dar lugar a que se pierda el control del uso de los mismos. Sólo debe hacerse cuando la otra parte disponga de una normativa de protección de datos adecuada. Si este no es el caso y se tienen que intercambiar los datos de todos modos, es importante evaluar detenidamente si esto supondría un riesgo demasiado elevado para los beneficiarios (tipo de datos, normas de protección, etc.)
- Los datos sensibles, como los relativos al estado de salud, orientación religiosa o datos biométricos deben procesarse a grandes rasgos (número de personas, variedad de datos, duración del tratamiento, extensión geográfica, etc.) Estos datos son altamente sensibles, ya que se refieren a aspectos muy personales y privados de la vida de alguien. Además, si este tipo de información acaba en manos equivocadas podría tener muchos riesgos para los beneficiarios.
- La vigilancia masiva podría formar parte del programa. Esta interfiere considerablemente con los derechos de todas las personas afectadas, puesto que un aspecto importante de la privacidad consiste en no estar sometidos al control constante de otros o de sistemas automatizados.
- Podría producirse la consolidación y el cruce de datos de diferentes fuentes. La combinación de varios conjuntos de datos sobre una persona aumenta el riesgo para la privacidad de esta.

Independientemente del formato, el análisis de riesgos debe llevarse a cabo previamente al comienzo del programa, junto con la evaluación general de riesgos para el programa, tal como se describe en la caja de herramientas para PTM.

Si tiene dudas o inquietudes relativas a la protección de datos, no dude en comunicárselas a su gerente y/o equipo legal. También puede enviar sus preguntas al Cash Hub, que es una amplia plataforma de PTM del Movimiento. El Cash Hub presta apoyo a los responsables que gestionan el programa de transferencias monetarias y ofrece materiales, incluidas las lecciones aprendidas de otras Sociedades Nacionales. Además, es posible que en el pasado haya analizado cuestiones similares de otros asociados del Movimiento.

Participación Comunitaria y rendición de cuentas a la comunidad (CEA)

Como se ha comentado en todos los capítulos, informar a los beneficiarios y contar con un servicio de asistencia y un mecanismo de retroalimentación son aspectos importantes para la aplicación de la protección de datos. Cuando la comunicación con los beneficiarios se realiza mediante un equipo independiente de Participación Comunitaria y rendición de cuentas a la comunidad (CEA), es importante que estén al tanto de las consideraciones para la protección de datos y asegurarse de que tienen la información necesaria para abordar cuestiones sobre la protección de datos o saben cómo remitir estas cuestiones a alguien que sepa responderlas.

IX. Referencias

Políticas y guías

- Manual sobre Protección de Datos en la Acción Humanitaria por CIRC y el Brussels Privacy Hub
- Política de la IFRC sobre protección de datos personales
- Política de la CIRC sobre el tratamiento de datos biométricos (Sólo disponible en inglés)
- Política de seguridad de la información de la IFCR
- IFRC's IM Data Protection Flyer (Sólo disponible en inglés)

Plantillas y material auxiliar

Las Sociedades Nacionales deben contextualizar los siguientes materiales para cumplir con los requisitos que les son propios; en particular, la adhesión a sus leyes y políticas nacionales de protección de datos, que podrían ser más estrictas que la norma de protección de datos aplicada al preparar estos documentos

- Modelo de contrato estándar para PSF (borrador, en inglés)
- Plantilla del cuestionario y diligencias pertinentes previas al contrato con el PSF (borrador, en inglés)
- Plantilla de EIPD (borrador, en inglés)
- Modelo de aviso de privacidad (borrador, en inglés)

Para poder acceder a los últimos 5 enlaces es necesario registrarse en IFRC.

X. Reconocimientos

La traducción de este documento ha sido posible gracias a las siguientes organizaciones