OCHA centre for humdata

CENTRO PARA LOS DATOS HUMANITARIOS

SERIE DE NOTAS DE ORIENTACIÓN
RESPONSABILIDAD DE LOS DATOS EN LA ACCIÓN HUMANITARIA

GUÍA 8: ENFOQUES RESPONSABLES PARA EL INTERCAMBIO DE DATOS

CONCLUSIONES FUNDAMENTALES:

- El intercambio abierto de datos puntuales y precisos es esencial para una respuesta humanitaria eficaz y racional. El modo en que las organizaciones humanitarias abordan el intercambio de datos está directamente relacionado con la confianza y la cooperación en el sector.
- A medida que el ecosistema de datos humanitarios crece, las oportunidades y los riesgos de compartir datos se vuelven más evidentes, lo que lleva a las organizaciones a explorar métodos más limitados para compartir datos.
- Las organizaciones humanitarias reconocen ampliamente la sensibilidad de los datos personales: su exposición tiene una alta probabilidad de causar daños. La mayoría de los datos no personales son seguros para compartirlos abiertamente, aunque también pueden ser sensibles y deben manejarse con precaución.
- Las organizaciones humanitarias deben tener en cuenta cuatro factores a la hora de decidir si comparten datos no personales: (i) utilidad; (ii) sensibilidad; (iii) capacidad humana y técnica; y (iv) gobernanza.
- Las organizaciones humanitarias deben identificar y comparar todos los métodos disponibles para el intercambio de datos, considerando primero el enfoque más abierto y descendiendo a más limitados según sea necesario.

INTRODUCCIÓN

La utilización y el intercambio de datos se han convertido en funciones fundamentales de las organizaciones humanitarias. El personal tiene que decidir con regularidad si comparte los datos de su organización y de qué manera, incluso si su función no se centra principalmente en la gestión de datos o información. Más allá de las organizaciones individuales, también ha crecido el interés por compartir y utilizar los datos generados en la acción humanitaria. Por ello, el sector humanitario ha experimentado un aumento en la generación e intercambio de datos en los últimos años.

> "Los datos precisos son el alma de una buena política y de la toma de decisiones. Obtenerlos y compartirlos entre cientas de organizaciones en medio de una emergencia humanitaria es complicado y requiere mucho tiempo, pero es absolutamente crucial."
>
> -El Secretario General de las Naciones Unidas, António Guterres en la apertura del Centro de Datos Humanitarios de la OCHA en La Haya en diciembre de 2017.

El intercambio abierto de datos puntuales y precisos es esencial para una respuesta humanitaria eficaz y racional y debe seguir siendo un objetivo fundamental para el sector. Por ejemplo, los datos epidemiológicos de COVID-19[1] recopilados y compartidos diariamente por el Centro de Ciencia e Ingeniería de Sistemas de la Universidad Johns Hopkins se han integrado en una serie de paneles de información e informes sobre la situación para los responsables de la toma de decisiones en todo el sector humanitario desde el inicio de la pandemia. En diciembre de 2020, este conjunto de datos se había descargado más de 320 000 veces de la plataforma de Intercambio de Datos Humanitarios (HDX, por sus siglas en inglés) desde que se publicó por primera vez en enero de ese año. La utilidad de los datos abiertos para los profesionales de la ayuda humanitaria se ve reforzada por el hecho de que el uso del HDX en los países que cuentan con un Plan de Respuesta Humanitaria (HRP) ha crecido mucho más rápido que en otros lugares.[2]

El modo en que las organizaciones humanitarias abordan el intercambio de datos está directamente relacionado con la confianza y la cooperación en el sector. Mantener la confianza dentro del ecosistema de datos es fundamental para la sostenibilidad del intercambio de datos y está relacionado con cuestiones como la calidad de los datos, el nivel de seguridad de los datos después de compartirlos y el uso responsable de los datos por parte del receptor. Como los datos en el sector humanitario suelen estar relacionados con las poblaciones de mayor riesgo, la gestión y el intercambio de los mismos exigen prudencia.

Muchas organizaciones humanitarias han desarrollado o actualizado sus orientaciones, gobernanza y prácticas para apoyar diferentes aspectos de la responsabilidad de los datos: la gestión segura, ética y eficaz de los datos. El sector también ha visto un aumento de los esfuerzos de colaboración para mejorar la responsabilidad de los datos más allá de las organizaciones individuales.[3] Aun así, a medida que el sistema humanitario conoce mejor los riesgos asociados al intercambio de datos, las organizaciones se enfrentan a retos más complejos a la hora de compartir estos datos de forma responsable.[4]

Esta nota orientativa tiene como objetivo apoyar la toma de decisiones en torno al intercambio de datos no personales en situaciones humanitarias. Explica la sensibilidad de los datos, ofrece ejemplos comunes de datos sensibles no personales y explica un enfoque para la clasificación de la información y la sensibilidad de los datos en situaciones humanitarias. También ofrece un marco que las organizaciones pueden utilizar para sopesar cuatro factores que ayudan a determinar si los datos pueden ser compartidos, y explica los enfoques comunes para hacerlo de manera responsable.

Opciones para compartir datos en el Intercambio de Datos Humanitarios

Cuando se lanzó el Intercambio de Datos Humanitarios (HDX) en 2014, contaba con casi 900 conjuntos de datos, compartidos por un puñado de organizaciones "pioneras". A finales de 2020, ese número había aumentado a más de 18 000 conjuntos de datos. Sólo las organizaciones autorizadas pueden compartir datos en la plataforma. Pueden hacer que los datos estén disponibles públicamente para cualquier persona que visite el sitio o de manera privada sólo para los miembros de sus organizaciones.

En 2017, el equipo de HDX añadió otra opción para compartir datos: HDX Connect. Esta característica permite a las organizaciones publicar sólo los metadatos, con los datos subyacentes disponibles bajo petición. En el caso de contar con autorización, los datos se comparten bilateralmente sin pasar por la plataforma HDX. Por ejemplo, Ground Truth Solutions utiliza HDX Connect para proporcionar acceso a los datos de percepción comunitaria sobre COVID-19 recogidos en Irak.

[1] Acceda a **datos de los nuevos casos de coronavirus (COVID-19) en HDX**.

[2] "Desde agosto de 2016 hasta agosto de 2020 (el periodo para el que se dispone de datos), el crecimiento de los usuarios mensuales de los países que cuentan con un HRP fue del 943%, en comparación con el 566% de la resta de países". Resultados del **estudio del caso HDX**, septiembre de 2020.

[3] Entre ellas se encuentran, por ejemplo, el Subgrupo del IASC sobre Responsabilidad con los Datos en el Contexto Humanitario, y las iniciativas de Protection Information Management y Responsible Data for Children, entre otras.

[4] Para comprender mejor el reto al que se enfrentan las organizaciones humanitarias a la hora de compartir datos, concretamente en crisis humanitarias prolongadas, véase **ALNAP, "Uso de recopilación de datos en crisis humanitarias prolongadas"** (junio de 2020).

Como parte de su proceso de garantía de calidad, el equipo de HDX también realiza una evaluación del riesgo de divulgación de cualquier recurso añadido a la plataforma que contenga microdatos. La razón de ello es porque puede ser posible volver a identificar a los individuos o exponer información confidencial incluso después de que se hayan eliminado los identificadores directos de los microdatos.[5]

Algunas organizaciones en HDX se han orientado más hacia el acceso controlado a sus datos, ya sea debido a la naturaleza sensible de los mismos, a la mayor presión para hacer un seguimiento e informar sobre cómo se utilizan los datos, o a las limitaciones de recursos relacionados con la sostenibilidad operativa. El HDX siempre apoyará diferentes formas de compartir los datos; sin embargo, el acceso abierto sigue siendo la mejor opción para la mayoría de los datos que se generan para la respuesta humanitaria.

COMPRENSIÓN DE LA SENSIBILIDAD DE LOS DATOS

Las organizaciones humanitarias reconocen ampliamente la sensibilidad de los datos personales[6]: la divulgación de datos tiene una alta probabilidad de causar daños. Sin embargo, esta idea todavía no está ampliamente reconocida para los datos no personales, que suelen abarcar las tres categorías siguientes en entornos humanitarios:

1. Datos sobre el contexto en el que tiene lugar la respuesta (por ejemplo, marcos jurídicos, condiciones políticas, sociales y económicas, infraestructuras, etc.) y la situación humanitaria (por ejemplo, incidentes de seguridad, riesgos de protección, impulsores de la situación o crisis).
2. Datos sobre las personas afectadas por la situación que incluyan sus necesidades, las amenazas y las vulnerabilidades a las que se enfrentan, así como sus capacidades.
3. Datos sobre los actores humanitarios y sus actividades (por ejemplo, a través de tácticas 3W/4W/5W).

La mayoría de estos datos se pueden compartir abiertamente. Sin embargo, los datos no personales también pueden ser sensibles. Algunos ejemplos de datos sensibles no personales incluyen los datos sobre grupos que sufren violencia de género o la localización de minorías étnicas en situaciones de conflicto. Estos datos se consideran sensibles porque permiten la identificación de grupos de individuos por factores demográficos, como la etnia, el sexo, la edad, la ocupación, la religión o el lugar de origen. Los datos no personales también pueden crear riesgos de otras maneras, por ejemplo, exponiendo la ubicación de las instalaciones médicas en áreas donde son propensas a los ataques. A medida que aumenta la sensibilización sobre el riesgo que conlleva compartir estos datos, algunas organizaciones están pasando de centrarse en la divulgación pública de la información a compartirla de forma más restringida.

Muchas organizaciones cuentan con clasificaciones de la sensibilidad de la información y los datos (véase la figura 1) que definen qué datos corresponden a cada categoría de sensibilidad para facilitar la gestión responsable de estos. Estas clasificaciones también pueden desarrollarse como un ejercicio colectivo para ayudar a las organizaciones a alinearse en torno a lo que constituye datos sensibles en su contexto e identificar los métodos de divulgación o difusión adecuados para los diferentes tipos de datos en función de su sensibilidad.

[5] Obtenga más información sobre el proceso de mitigación de riesgos del Centro para los microdatos, el "Control de Divulgación Estadística" (SDC, por sus siglas en inglés) en la **Trayectoria de Aprendizaje sobre el tema**.

[6] Los datos personales no deben compartirse abiertamente, y la gestión de los datos personales debe cumplir siempre con las leyes nacionales y regionales de protección de datos, o con las políticas internas de protección de datos en el caso de las organizaciones cubiertas por privilegios e inmunidades.

Clasificación de la sensibilidad de los datos e información		
Sensibilidad	Definición	Clasificación de la sensibilidad de los datos e información
Baja o nula	Si la información o datos se divulgan o acceden sin la debida autorización, es poco probable que la información o datos causen daños o impactos negativos a las personas y/o agentes humanitarios.	**Pública**
Moderada	Si la información o datos se divulgan o acceden sin la debida autorización, es probable que puedan causar daños menores o impactos negativos y/o ser desventajoso para las personas afectadas y/o agentes humanitarios.	**Restringida**
Alta	Si la información o datos se divulgan o acceden sin la debida autorización, es probable que causen daños graves o impactos negativos a los afectados, personas y/o agentes humanitarios y/o daño a una respuesta.	**Confidencial**
Extrema	Si la información o datos se divulgan o acceden sin la debida autorización, es probable que causen daño severo o impactos negativos y/o daños a las personas afectadas y/o agentes humanitarios y/o impedir la realización del trabajo de una respuesta.	**Estrictamente confidencial**

Figura 1. Ejemplo de la clasificación de la sensibilidad de los datos e información[7]

Las políticas de la organización y los instrumentos de gobernanza colectiva, como los protocolos de intercambio de información (ISPs, por sus siglas en inglés), suelen incluir una clasificación de sensibilidad y deberían ser los principales puntos de referencia para determinar cómo gestionar los datos sensibles. Sin embargo, estos documentos tienden a dejar margen para poder decidir qué y cómo se pueden compartir. Esto significa que el intercambio de datos puede estar influenciado por las preferencias y habilidades personales y puede variar entre las organizaciones. Si adoptan un enfoque más coherente a la hora de compartir los datos y garantizan las debidas medidas de seguridad para los datos sensibles, las organizaciones pueden generar confianza y contribuir a una respuesta humanitaria más eficiente y eficaz.

[7] UNOCHA (2019), Proyecto de las Pautas de Responsabilidad con los datos.

CUATRO FACTORES PARA DETERMINAR LA POSIBILIDAD DE COMPARTIR LOS DATOS NO PERSONALES

Existen cuatro factores que las organizaciones humanitarias deben tener en cuenta a la hora de decidir si comparten datos no personales.

1. **¿Cuál es la utilidad de los datos para otras partes interesadas?**
   La utilidad de los datos depende del nivel de detalle, del número de personas o de la zona geográfica cubierta, de su actualidad y de su relevancia para el análisis y la toma de decisiones en la respuesta humanitaria. Realizar una evaluación del impacto de los datos (DIA, por sus siglas en inglés) para ayudar a determinar la utilidad de datos específicos.[8]

2. **¿Cual es el grado de sensibilidad de los datos?**
   La sensibilidad de los datos se basa en el riesgo asociado a su exposición en un contexto concreto.[9] En algunos contextos de respuesta, las organizaciones, los grupos/sectores y las estructuras de coordinación de todo el sistema también han establecido clasificaciones de sensibilidad de los datos y la información (véase más arriba) que pueden informar sobre esta determinación. La realización de una DIA también puede ayudar a determinar la sensibilidad de los datos. Para los resultados de las encuestas y otras formas de microdatos, la sensibilidad está estrechamente relacionada con el riesgo de reidentificación, que puede determinarse aplicando una evaluación del riesgo de divulgación.

3. **¿Qué capacidad humana y técnica tienen las organizaciones que comparten y utilizan los datos?**
   Tanto la organización que comparte los datos como la(s) organización(es) que los recibe(n) y los utiliza(n) deben tener suficiente capacidad humana y técnica para la gestión responsable de los datos. Esto incluye la disponibilidad del personal, los conocimientos de los datos, la infraestructura técnica y los recursos relacionados. En entornos con poca conectividad, los métodos de intercambio de datos con mayor ancho de banda pueden no ser apropiados. En contextos con riesgos de seguridad identificados, los datos deberían compartirse normalmente a través de métodos más limitados.

4. **¿Qué instrumentos de gobernanza se aplican?**
   Entre los instrumentos de gobernanza de datos más comunes se encuentran los ISPs, los acuerdos de intercambio de datos bilaterales y las licencias o condiciones de uso para el intercambio de datos públicos.[11] TEstos instrumentos deben informar sobre cómo se comparten los datos de forma segura, ética y eficaz. A veces, será necesario desarrollar una gobernanza para el enfoque de intercambio de datos concretos. Los instrumentos de gobernanza pueden abordar una serie de temas y disposiciones específicas, pero siempre deben incluir los siguientes elementos: (a) un propósito de la divulgación; (b) las limitaciones de la gestión de los datos después de que estos se hayan compartido; (c) funciones y responsabilidades a lo largo del proceso de intercambio; y (d) procedimientos para la gestión de incidentes con datos.[12]

[8] Véase la **Nota Orientativa sobre la Evaluación del Impacto de los Datos (DIA)**.

[9] Para la gestión de datos en el sector humanitario, el riesgo puede definirse como la probabilidad y el impacto del daño resultante de la gestión de datos.

[10] El Foro Económico Mundial, junto con el Centro de **Seguridad de la Información y Ciberseguridad de la Universidad de Washington**, la **Red de Soluciones para el Desarrollo Sostenible TReNDS** y el **GovLab de la Universidad de Nueva York**, han comenzado a crear un repositorio de acuerdos de intercambio de datos para apoyar la profesionalización de esta práctica a través de sus proyecto de **Contratos para la Colaboración de Datos** (C4DC).

[11] Las licencias recomendadas para compartir datos a través de HDX se encuentran aquí: **https://data.humdata.org/about/license**.

[12] Para más información sobre la gestión de incidentes con datos en la respuesta humanitaria, consulte nuestra **Nota de Orientación sobre la Gestión de Incidentes con Datos**.

IDENTIFICAR Y COMPARAR ENFOQUES

Las organizaciones deben determinar el mejor enfoque para el intercambio de datos basándose en los cuatro factores anteriores. Estos enfoques van desde el acceso abierto para maximizar el beneficio de los datos, hasta enfoques más privados, como la divulgación bilateral de datos o la divulgación de los resultados de los análisis de datos. La siguiente tabla contiene una visión general de los diferentes métodos de la divulgación de datos y ofrece ejemplos de algunas herramientas y plataformas comúnmente utilizadas.

Enfoques, herramientas y plataformas para compartir datos en la respuesta humanitaria [13]

Enfoques para el intercambio de datos	**Acceso abierto** Compartir los datos públicamente es el enfoque más abierto, permitiendo el acceso libre a cualquier persona.	**Acceso restringido** La restricción del acceso a los datos sigue permitiendo a determinados socios utilizarlos siempre que cumplan ciertos requisitos.	**Intercambio bilateral** El intercambio bilateral es la forma más limitada de compartir datos, efectuada de manera directa con	**No se puede compartir** Los datos que no deberían compartirse en absoluto pueden seguir ofreciendo valor a los socios, siempre que se les permita consultar los datos a distancia o beneficiarse de ellos indirectamente.
Herramientas y plataformas comunes	Plataformas de datos de la organización HDX Open Listservs	HDX Private UNHCR Microdata Library[14] IFRC GO[15] Compartir clústeres/ sectores Listas de correo cerradas	HDX Connect Correo electrónic[16] Dropbox	OPAL[17] Aircloak[18] Cifrado homomórfico[19] Computación multipartita[20]

Al comparar estos diferentes enfoques, el enfoque más abierto debe considerarse siempre como primera opción, descendiendo así a enfoques más limitados según sea necesario. Los diferentes tipos de datos requerirán diferentes formas de compartirlos. Por ejemplo, los archivos de datos de gran tamaño requerirán una infraestructura especializada y las interfaces de programación de aplicaciones (API) son adecuadas para los datos que se publican en el mismo formato de forma regular. Dado que la sensibilidad de los datos y la información están en constante cambio, las organizaciones deben revisar y comparar periódicamente los enfoques disponibles para la divulgación de datos.

[13] No todas las herramientas y plataformas de este resumen han sido examinadas por la Secretaría de las Naciones Unidas. Consulte siempre a los asesores informáticos pertinentes antes de utilizar una nueva herramienta.

[14] **UNHCR's MicroData Library**.

[15] **IFRC's GO Platform**.

[16] En el contexto de las respuestas humanitarias, una de las formas más comunes de compartir datos es a través de archivos adjuntos al correo electrónico. Al compartir datos por correo electrónico, tome siempre las precauciones de seguridad necesarias. Esta forma de compartir es apropiada en algunos casos, pero a menudo hay formas más adecuadas de compartir los datos. Para obtener información sobre cómo cifrar el correo electrónico, consulte la siguiente página: **https://www.cloudwards.net/how-to-encrypt-your-emails/**.

[17] Plataforma **OPAL**.

[18] **Aircloak Insights**.

[19] Para saber más sobre el cifrado homomórfico como forma de compartir el valor de los datos sensibles, consulte aquí: **https://www.microsoft.com/en-us/research/project/homomorphic-encryption/** and here: **https://www.wired.com/story/google-private-join-compute-database-encryption/**.

[20] Para saber más sobre la computación multipartita, consulte aquí: **https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/secure-multi-party-computation/**.

Extracción del valor de los datos sin necesidad de compartir: el Método de la Consulta

Un sistema relativamente nuevo para utilizar los datos sin transferirlos es a través de la "consulta". La consulta permite a terceros formular preguntas específicas acerca de los datos sin tener acceso directo a ellos. El propietario de los datos puede comprobar la sensibilidad de los datos resultantes o cualquier otro problema. Este enfoque evita las transferencias de datos que pueden causar problemas legales y éticos, a la vez que da acceso a conocimientos valiosos para el bien público.

Al usar este enfoque, es fundamental establecer una gobernanza con instrucciones y límites con respecto a las consultas que pueden enviarse, a fin de evitar la recuperación de información sensible mediante el planteamiento de una combinación de preguntas.[21] La verificación de los usuarios, así como de sus preguntas, debe ser siempre un paso clave en el proceso en torno a este tipo de procedimiento.

Una de las soluciones comerciales para establecer enfoques de consulta es el Aircloak Insights, que actúa como "proxy entre los analistas y los datos sensibles con los que necesitan trabajar". También existe una plataforma llamada **Open Algorithms** (OPAL). Esta herramienta se ha desarrollado específicamente para los sectores humanitario y desarrollo y actualmente se encuentra en fase de prueba en Colombia.

Métodos de intercambio de datos en el Servicio conjunto interinstitucional de elaboración de perfiles de desplazados internos (JIPS)
En 2019, el **Servicio conjunto interinstitucional de elaboración de perfiles de desplazados internos** (JIPS) recibió una subvención del Fondo de Innovación de ACNUR para investigar métodos avanzados de ciencia de datos para anonimizar los datos. JIPS estudió métodos como la computación multipartita y la encriptación homomórfica, y trabajó con expertos técnicos del Laboratorio de Física Aplicada de la Universidad Johns Hopkins, Flowminder y la Oficina Nacional de Estadística del Gobierno de Colombia.

En estrecha colaboración con Flowminder y aprovechando su herramienta **Flowkit**, JIPS ha desarrollado un prototipo de método de consulta que permite a los agentes humanitarios y de desarrollo acceder y consultar de forma segura datos sensibles a nivel individual sin necesidad de que sean compartidos. El equipo desarrolló un flujo de trabajo técnico para demostrar la viabilidad de este enfoque con un solo proveedor de datos y trazó los problemas y limitaciones en caso de múltiples proveedores de datos.

Animamos a que las organizaciones compartan su experiencia en la fomentación del intercambio responsable de datos con el Centro de Datos Humanitarios a través de **centrehumdata@un.org**.

COLABORADORES: **SERVICIO CONJUNTO INTERINSTITUCIONAL DE ELABORACIÓN DE PERFILES DE DESPLAZADOS INTERNOS (JIPS).**

El **Centro Para Los Datos Humanitarios** ('El Centro'), en cooperación con asociados principales, está publicando una serie de ocho notas de orientación sobre la responsabilidad con los datos en el contexto humanitario a lo largo de 2019 y 2020. La serie de Notas de Orientación son la continuación del **proyecto de las Pautas de Responsabilidad con los Datos de OCHA** publicado en marzo de 2019. A través de esta guía, el Centro pretende ofrecer orientación adicional sobre cuestiones, procesos y herramientas específicas para la responsabilidad con los datos en la práctica. Esta serie ha sido posible gracias al generoso apoyo de la Dirección General de Protección Civil y Operaciones de Ayuda Humanitaria Europeas (DG ECHO).

El presente documento hace referencia a las actividades de ayuda humanitaria realizadas con la ayuda financiera de la Unión Europea. Los puntos de vista expresados en este documento no deben considerarse, en modo alguno, como la opinión oficial de la Unión Europea, y la Comisión Europea no es responsable del uso que pueda hacerse de la información que contiene.

Este proyecto está cofinanciado por la Unión Europea

[21] For an explanation of this risk, see for example: **https://www.usenix.org/conference/usenixsecurity19/presentation/gadotti**.