IASC Inter-Agency Standing Committee

Directriz Operacional

MANEJO RESPONSABLE DE DATOS EN LA RESPUESTA HUMANITARIA

Resultados Grupo 1 en la respuesta operacional

Febrero 2021

Aprobado por el IASC Operational Policy and Advocacy Group (OPAG)

DIRECTRICESOPERACIONALES

MANEJO RESPONSABLE DE DATOS EN LA RESPUESTA HUMANITARIA

Comité Permanente entre Organismos
Resultados Grupos 1 en la respuesta operacional

Febrero 2021

Tabla de Contenidos

Prólogo

El manejo responsable de datos es primordial, ya que el sistema humanitario recopila y comparte más datos que nunca. Al igual que la pandemia de COVID-19 ha agravado las crisis humanitarias existentes, también ha aumentado nuestra dependencia de las tecnologías digitales y de los datos actualizados.

Cuando hablamos de datos en contextos humanitarios, hablamos de las personas más vulnerables del mundo: un récord de 235 millones de personas necesitan asistencia y protección humanitaria en 2021. Las nuevas tecnologías y las fuentes de datos nos ayudan a tomar decisiones más rápidas e informadas y cada año conseguimos asistir a más personas. Sin embargo, las formas en que los datos son recogidos, compartidos y utilizados por las organizaciones individuales y en todo el sistema humanitario pueden presentar desafíos para la privacidad y la seguridad de las personas afectadas. Para proteger a las personas a las que tratamos de ayudar, debemos ser capaces de sortear los problemas técnicos y éticos que conlleva la gestión de los distintos tipos de datos. Los datos pueden exponer a las personas, ya de por sí vulnerables, a un mayor riesgo de daño o explotación, cuando no se manejan de una forma responsable.

En los últimos años hemos presenciado el desarrollo de principios, políticas y estrategias para la gestión responsable de los datos en la acción humanitaria, pero siguen existiendo lagunas entre los marcos globales y su aplicación práctica en las operaciones sobre el terreno.

La Directriz Operacional del Comité Permanente entre Organismos sobre el Manejo Responsable de Datos en la Acción Humanitaria es un paso bienvenido y oportuno para abordar colectivamente los desafíos y las oportunidades en esta área. Llega en medio de un creciente reconocimiento mundial de la importancia de la responsabilidad de los datos.

Esta Directriz Operacional para todo el sistema, que es una primicia, garantizará medidas concretas para la responsabilidad de los datos en todas las fases de la acción humanitaria. Es el resultado de un proceso inclusivo y participativo en el que han intervenido más de 250 partes interesadas del sector humanitario. Los socios de todo el sistema aplicarán estas directrices de acuerdo con sus respectivos mandatos y las decisiones de sus órganos de gobierno.

Exhorto a los miembros del IASC y a la comunidad humanitaria en general a que apoyen el uso responsable de los datos mediante la aplicación de esta Directriz Operacional.

Mark Lowcock
Secretario General Adjunto de Asuntos Humanitarios y Coordinador del Socorro de Emergencia, Naciones Unidas

Resumen Ejecutivo

La responsabilidad de los datos en la acción humanitaria es la gestión segura, ética y eficaz de los datos personales y no personales para la respuesta operativa. Se trata de una cuestión crítica para el sistema humanitario y es mucho lo que está en juego.

Garantizar el "no hacer daño" al tiempo que se maximizan los beneficios de los datos requiere una acción colectiva que se extiende a todos los niveles del sistema humanitario. El personal humanitario debe tener cuidado al manejar los datos para evitar poner en mayor riesgo a personas y comunidades ya vulnerables. Esto es especialmente importante en contextos en los que la urgencia de las necesidades humanitarias impulsa la presión por soluciones de datos rápidas, a veces no probadas, y la politización de los datos puede tener consecuencias más extremas para las personas. Por ejemplo, revelar la ubicación o la identidad o afiliación particular de una persona o comunidad podría dar lugar a ataques selectivos, exclusión social y/o estigmatización, entre otros daños potenciales. Además de evitar los daños, la gestión segura, ética y eficaz de los datos tiene una serie de beneficios: puede conducir a una toma de decisiones más informada y transparente, a una respuesta humanitaria más eficiente y a un aumento de la confianza entre los actores humanitarios y con las personas a las que tratan de servir.

La implementación de la responsabilidad de los datos en la práctica es a menudo incoherente dentro y entre los contextos de respuesta humanitaria. Esto es así a pesar de los principios, las normas y los estándares profesionales establecidos en relación con el respeto de los derechos de las poblaciones afectadas; la gama de recursos sobre la responsabilidad de los datos disponibles en la comunidad internacional de datos más amplia; así como los esfuerzos significativos de muchas organizaciones humanitarias para desarrollar y actualizar sus políticas y orientaciones en este ámbito. Sin embargo, dado que el ecosistema de datos humanitarios está intrínsecamente interconectado, ninguna organización individual puede abordar todos estos retos por sí sola. Si bien cada organización es responsable de sus propios datos, los trabajadores humanitarios del Comité Permanente entre Organismos (IASC) -que reúne a entidades de las Naciones Unidas (ONU), consorcios de organizaciones no gubernamentales (ONG) y el Movimiento Internacional de la CruzRoja y de la Media Luna Roja- necesitan una orientación normativa común para todo el sistema que sirva de base para la acción individual y colectiva y para mantener un alto nivel de responsabilidad en materia de datos en diferentes entornos operativos.

En vista de ello, el Grupo de Resultados 1 del IASC creó un Subgrupo [1] sobre Responsabilidad de los Datos en enero de 2020 para desarrollar conjuntamente esta **Directriz Operacional sobre el Manejo Responsable de Datos en la Respuesta Humanitaria**, que abarca todo el sistema.

[1] El Subgrupo estaba codirigido por la Organización Internacional para las Migraciones (OIM), el Centro de Datos Humanitarios de la OCHA y el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), y estaba compuesto por veinte organizaciones miembros que representaban a diferentes partes interesadas del sistema humanitario. El Subgrupo incluía representantes de CARE, CRS, DRC, CICR, IFRC, IRC, OIM, JIPS, Mercy Corps, MSF, NRC, OCHA, OACNUDH, Oxfam, Save the Children, FNUAP, ACNUR, UNICEF, PAM y OMS. Véase el Anexo D para más información sobre el proceso que siguió el Subgrupo para desarrollar esta Directriz Operacional.

La Directriz Operacional está dividida en cuatro secciones:

- La primera sección describe la **justificación y el enfoque** de la Directriz, ofrece una **visión general de la responsabilidad de los datos en la acción humanitaria** y aclara la **audiencia y el alcance** del documento.
- La segunda sección presenta un conjunto de **Principios para la Responsabilidad de los Datos en la Acción Humanitaria**.
- La tercera sección describe las **acciones clave para la responsabilidad de los datos** que deben tomarse en los diferentes niveles de la respuesta humanitaria, incluyendo las **funciones y responsabilidades** específicas para la realización de estas acciones.
- La cuarta sección es un conjunto de **anexos** que ofrecen **definiciones clave, ejemplos de plantillas y herramientas para la responsabilidad de los datos, recursos y referencias, e información de fondo sobre el desarrollo de la Directriz Operacional.**

Dada la naturaleza dinámica y cambiante de los retos y oportunidades de la responsabilidad de los datos en la acción humanitaria, esta Directriz Operacional se revisará y actualizará mediante un proceso de colaboración y consulta cada dos años.

Definir el manejo responsable de datos

La responsabilidad de los datos en la acción humanitaria es la **gestión segura, ética y eficaz de los datos personales y no personales para la respuesta operativa**, de acuerdo con los marcos establecidos de protección de datos personales.[2]

- **Segura** | Las actividades de gestión de datos garantizan la seguridad de los datos en todo momento, respetan y defienden los derechos humanos y otras obligaciones legales, y no causan daños.
- **Ética** | Las actividades de gestión de datos se ajustan a los marcos y normas establecidos para la ética humanitaria[3] y la ética de los datos.
- **Efectiva** | Las actividades de gestión de datos logran el objetivo para el que fueron realizadas.

La responsabilidad de los datos requiere la aplicación de acciones basadas en principios en todos los niveles de una respuesta humanitaria. Esto incluye, por ejemplo, acciones para garantizar la protección y la seguridad de los datos, así como estrategias para mitigar los riesgos y maximizar los beneficios en todos los pasos de la gestión operativa de los datos, como se define a continuación.

Si bien la responsabilidad de los datos está relacionada con la protección y la seguridad de los datos, estos términos son diferentes. La "protección de datos" se refiere a la aplicación sistemática de un conjunto de salvaguardias institucionales, técnicas y físicas que preservan el derecho a la intimidad con respecto al tratamiento de datos personales. La "seguridad de los datos", aplicable tanto a los datos personales como a los no personales, se refiere a las medidas técnicas y organizativas destinadas a preservar la confidencialidad, la disponibilidad y la integridad de los datos.

Los siguientes términos clave deben guiar la lectura de esta Directriz Operacional:

Gestión de datos operativos: El diseño de las actividades de gestión de datos y la subsiguiente recopilación o recepción, almacenamiento, procesamiento, análisis, intercambio, uso y retención y destrucción de datos e información por parte de los actores humanitarios. Dichas actividades se llevan a cabo como parte de la acción humanitaria a lo largo del ciclo de planificación y respuesta en todos los clústeres/sectores e incluyen, entre otras, el análisis de la situación, la evaluación de las necesidades, la gestión de los datos de la población, el registro y la inscripción, la gestión de los casos, la comunicación con las poblaciones afectadas, el seguimiento de la protección y el seguimiento y la evaluación de la respuesta

Datos personales: Toda información relativa a una persona física identificada o identificable ("interesado"). Una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la

[2] A efectos de esta Directriz Operacional, "de acuerdo con los marcos establecidos para la protección de datos personales" significa que las actividades de gestión de datos se rigen por leyes nacionales y regionales de protección de datos o por políticas de protección de datos de la organización.

[3] La ética humanitaria se ha desarrollado como una ética basada en los principios de humanidad, imparcialidad, neutralidad e independencia que guían la prestación de asistencia y protección humanitaria. Estos principios y las normas conexas están consagrados en diversos códigos de conducta que ahora se reconocen ampliamente como la base de la práctica humanitaria ética, entre ellos La Carta Humanitaria y las Normas Mínimas de Respuesta Humanitaria, incluidas las Normas Esenciales y los Principios de Protección, la Norma Humanitaria Esencial sobre Calidad y Responsabilidad, y el Código de Conducta del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja y de las Organizaciones No Gubernamentales (ONG) de Socorro en Casos de Desastre. Para obtener orientación adicional sobre la ética de los datos humanitarios, véase The Centre for Humanitarian Data, Guidance Note: Humanitarian Data Ethics (2019), disponible en: https://centre.humdata.org/guidance-note-humanitarian-data-ethics/.

identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.

Datos no personales: Cualquier información que no esté relacionada con una persona. Los datos no personales pueden clasificarse en función de su origen, a saber: los datos que nunca se han relacionado con un sujeto de datos, como los datos sobre el contexto en el que se desarrolla una respuesta y los datos sobre los agentes de la respuesta humanitaria y sus actividades; o los datos que inicialmente eran datos personales pero que posteriormente se hicieron anónimos, como los datos sobre las personas afectadas por la situación humanitaria y sus necesidades, las amenazas y vulnerabilidades a las que se enfrentan y sus capacidades. Los datos no personales incluyen la Información Demográfica Identificable, es decir, los datos que permiten la identificación de grupos de individuos por factores demográficos definitorios, como el origen étnico, el género, la edad, la ocupación, la religión o la ubicación.

Datos sensibles: Los datos clasificados como sensibles se basan en la probabilidad y gravedad del daño potencial que puede materializarse como resultado de su exposición en un contexto particular. Tanto los datos personales como los no personales pueden ser sensibles. Muchas organizaciones tienen sistemas de clasificación específicos sobre lo que constituye datos sensibles para facilitar las prácticas de gestión de datos.

Nota: La lista completa de definiciones está disponible en el Anexo.

Antecedentes, justificación y alcance

Esta Directriz Operacional pretende ayudar al personal humanitario, a las organizaciones y a sus socios a practicar la responsabilidad de los datos en diferentes contextos de respuesta. La responsabilidad de los datos se define como la gestión segura, ética y eficaz de los datos personales y no personales para la respuesta operativa.

Esta Directriz Operacional ofrece un conjunto de principios y acciones que las entidades del sistema, los clústeres y/o los sectores, y las organizaciones pueden aplicar para la responsabilidad de los datos en la acción humanitaria. No pretende sustituir o reemplazar las políticas y orientaciones oficiales de las organizaciones,[4] ni tiene en cuenta los mandatos específicos de las organizaciones o las leyes nacionales o regionales pertinentes.

Manejo responsable de datos en la respuesta humanitaria

La responsabilidad de los datos es una cuestión fundamental que debe abordar el sector humanitario. Para garantizar que se minimizan los riesgos y se maximizan los beneficios de la gestión de datos en los entornos humanitarios, es necesario un cambio continuo en las prácticas y una acción colectiva que se extienda a través de las organizaciones humanitarias y más allá de ellas.

La implementación de la responsabilidad de los datos en la práctica es a menudo incoherente dentro y entre los contextos de respuesta humanitaria. Esto es así a pesar de los principios, normas y estándares profesionales establecidos en relación con el respeto de los derechos de las poblaciones afectadas y la gama de recursos disponibles sobre la responsabilidad de los datos.

En los últimos años, muchas organizaciones humanitarias han desarrollado o actualizado sus políticas, orientaciones y prácticas para apoyar diferentes aspectos de la responsabilidad de los datos. El sector también ha visto un número creciente de esfuerzos de colaboración para mejorar la responsabilidad de los datos más allá de las organizaciones individuales.

Sin embargo, incluso en las organizaciones con marcos políticos sólidos o en las que se han adoptado principios firmes, los problemas de gobernanza, capacidad y recursos sostenibles pueden dar lugar a actividades y prácticas incompatibles con la responsabilidad de los datos. Dado que el ecosistema de datos humanitarios está intrínsecamente interconectado, ninguna organización individual puede hacer frente a todos estos retos por sí sola. Si bien cada organización es responsable de sus propios datos, el personal humanitario del Comité Permanente entre Organismos -que reúne a las entidades de las Naciones Unidas, los consorcios de ONG y el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja- necesita una orientación normativa común para todo el sistema, a fin de informar la acción individual y colectiva y mantener un alto nivel de responsabilidad en materia de datos en diferentes entornos operativos. Esta orientación operativa complementa y se basa en las orientaciones existentes[5] sobre la responsabilidad de los datos, tanto de los actores del desarrollo como de la comunidad humanitaria en general.

4 En el caso de la protección de datos, se incluyen, por ejemplo, los Principios de Privacidad y Protección de Datos de las Naciones Unidas, las políticas y leyes de protección de datos que se aplican a los organismos de las Naciones Unidas y las ONG, y los marcos de protección de datos como el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (ETS 108), Estrasburgo (1981), el Reglamento General de Protección de Datos (RGPD), o documentos equivalentes, incluidos los de carácter no vinculante.

5 Esto incluye, por ejemplo, la Directriz Operacional del IASC sobre las Responsabilidades de los Líderes de Grupos Sectoriales/ Inter-Sectoriales, las Normas Profesionales para el Trabajo de Protección, el Marco de Gestión de la Información de Protección (PIM), los Datos Responsables para Niños initiative, and the Signal Code: A Human Rights Approach to Information During Crisis, entre otros (véase anexo 3 parareferencias adicionales).

Desafíos y oportunidades de la responsabilidad de los datos en la acción humanitaria

La experiencia adquirida en diferentes contextos de respuesta humanitaria ha dado lugar a un conjunto de retos y oportunidades comunes que constituyen la base de la acción colectiva en el ámbito de la responsabilidad de los datos.

Desafíos:

- Falta de **definiciones comunes e incoherencias relacionadas con la comprensión y el uso de la terminología** entre las organizaciones humanitarias sobre la responsabilidad de los datos.
- **Brechas en las orientaciones y normas existentes**, especialmente en lo que se refiere a la gestión responsable de datos sensibles, la evaluación de los riesgos asociados a los diferentes tipos de datos en diferentes contextos, y los desafíos específicos y complejos de la responsabilidad de los datos en entornos humanitarios.
- Aplicabilidad variada de los **diferentes marcos jurídicos y regulatorios** entre las Organizaciones Internacionales (OI), las ONG y las entidades de la ONU.
- I**ncertidumbre y falta de coordinación** en el desarrollo de nuevas tecnologías y normas y prácticas de gestión de datos humanitarios, que a menudo evolucionan más rápido que los instrumentos políticos que rigen su uso.
- P**rioridad a las prácticas internas de protección de datos de las organizaciones** en lugar de invertir en el apoyo a esta labor dentro del sector de forma más amplia.
- **Ausencia de instrumentos y procesos compartidos y aprobados** para aplicar la responsabilidad de los datos en la práctica.
- **Falta de capacidad** para la gestión responsable de datos entre muchas organizaciones humanitarias y su personal.
- **Infrarrepresentación** de las organizaciones locales, las organizaciones de la sociedad civil y las estructuras comunitarias en las actividades de gestión de datos.

Oportunidades:

- **Mayor inversión por parte de las organizaciones humanitarias y de desarrollo, donantes y gobiernos anfitriones en la responsabilidad de los datos** como parte de una estrategia para promover los derechos de las poblaciones afectadas y contribuir a los resultados humanitarios y a los objetivos de desarrollo más amplios.
- **Mejora de la capacidad institucional** en cuestiones relacionadas con la gestión responsable de datos (especialmente la protección de datos personales).
- **Ampliación de las oportunidades de colaboración en la gestión de datos, con la consiguiente eficiencia**, incluso mediante evaluaciones coordinadas, prestación conjunta de asistencia y otras actividades similares.
- **Mayor interés y apoyo a la creación de una base de evidencia práctica** sobre "lo que funciona" y "lo que no funciona" para la responsabilidad de los datos.
- **Aumento de la transparencia y la responsabilidad** de las organizaciones humanitarias en cuanto a la forma de gestionar los datos en apoyo de las diferentes actividades de respuesta.
- **Economías de escala** a través de esfuerzos conjuntos para producir orientación y herramientas para la aplicación de medidas específicas para la responsabilidad de los datos.

Ámbito de aplicación y público objetivo

La Directriz Operacional se aplica a diferentes tipos de datos operativos (tanto personales como no personales) generados o utilizados en entornos de respuesta humanitaria, a saber[6]:

- **Datos sobre el contexto** en el que tiene lugar la respuesta (por ejemplo, marcos legales, condiciones políticas, sociales y económicas, infraestructuras, etc.) y la situación humanitaria en la que se centra (por ejemplo, incidentes de seguridad, riesgos de protección, impulsores y causas/factores subyacentes de la situación o crisis).
- **Datos sobre las personas afectadas por la situación** y sus necesidades, las amenazas y vulnerabilidades a las que se enfrentan y sus capacidades.
- **Datos sobre los actores de la respuesta humanitaria y sus actividades** (por ejemplo, como se informa en 3W/4W/5W).

Esta Directriz Operacional no abarca los datos "corporativos", como los relacionados con la gestión financiera interna, los recursos humanos y el personal, la gestión de la cadena de suministro y la logística, y otras funciones administrativas de las organizaciones humanitarias.

La Directriz Operacional es relevante para todas las formas de gestión de datos operativos que tienen lugar en todos los contextos de respuesta humanitaria. La gestión de datos operativos incluye el diseño de las actividades de gestión de datos y la posterior recopilación o recepción, almacenamiento, procesamiento, análisis, intercambio, uso y retención y destrucción de datos e información por parte de los actores humanitarios. Dichas actividades se llevan a cabo como parte de la acción humanitaria a lo largo del ciclo de planificación y respuesta en todos los clústeres o sectores, e incluyen, entre otras, el análisis de la situación, la evaluación de las necesidades, la gestión de los datos de la población, el registro y la inscripción, la gestión de los casos, la comunicación con las poblaciones afectadas, el seguimiento de la protección y el seguimiento y la evaluación de la respuesta. Dado que las organizaciones humanitarias tienen una variedad de ciclos y procesos[7], esta Directriz Operacional no presenta un conjunto único o armonizado de pasos para la gestión de datos. Más bien, los principios y las acciones de esta directriz son pertinentes para todos los pasos que intervienen en la gestión de datosoperativos para la acción humanitaria.

Esta Guía Operativa apoya a todos los actores humanitarios, incluidas las entidades de la ONU, otras OI, ONG internacionales y nacionales, y otras partes interesadas que participan en la acción humanitaria.

Se dirige específicamente a las siguientes estructuras de coordinación como foros para promover y supervisar la aplicación de la responsabilidad de los datos en diferentes niveles de una respuesta: el Equipo Humanitario de País (HCT); el Grupo de Coordinación Interclúster (ICCG), el Mecanismo de Coordinación Interclúster (ICCM), el Grupo de Trabajo Intersectorial (ISWG), y/o el Grupo de Trabajo de Gestión de la Información (IMWG); y los clústeres, las Áreas de Responsabilidad (AoR), los Grupos de Trabajo, y/o los sectores.

6 Esto puede incluir tipos de datos nuevos o no tradicionales, como registros detallados de llamadas (CDR), datos de res sociales, etc. Las organizaciones humanitarias deben aplicar la misma norma para la gestión de estos datos que para otras formas de datos. . .

7 Una revisión bibliográfica de 55 documentos dio como resultado 18 procesos y ciclos diferentes, cada uno de los cuales varía en longitud y contiene diferentes pasos. La lista de documentos revisados está disponible en el Anexo C.

También se dirige a diferentes papeles y funciones a nivel de todo el sistema, de los grupos sectoriales y de las organizaciones. Entre ellos se encuentran los Coordinadores Residentes/Coordinadores Humanitarios, los Jefes de Oficina/Representantes de País, los Gestores y Oficiales de Programa[8], los Coordinadores o Líderes de Clúster/Sector, los Comités Directivos de Clúster/Sector y los Grupos de Asesoramiento Estratégico (SAG), y el Personal Técnico.[9]

En última instancia, la responsabilidad de los datos requiere la aceptación y la participación de todas las funciones de cada organización, clúster o sector, y del sistema humanitario en general.

8 Esto incluye, por ejemplo, oficiales de programa, expertos sectoriales/técnicos, oficiales de asuntos humanitarios y funciones similares.

9 Esto incluye, por ejemplo, oficiales de gestión de datos e información, analistas de datos y científicos, estadísticos, oficiales de protección de datos/puntos focales, personal de tecnología de la información, oficiales de registro, operadores de mecanismos de retroalimentación y respuesta de la comunidad, oficiales de seguimiento y evaluación, encuestadores y funciones similares.

Principios del Manejo Responsable de Datos en la Respuesta Humanitaria

Los siguientes Principios para la Responsabilidad de los Datos en la Acción Humanitaria (en adelante "los Principios") están diseñados para informar sobre la gestión segura, ética y eficaz de los datos operativos dentro de las organizaciones, los grupos sectoriales y el sistema humanitario más amplio en un contexto de respuesta determinado. Deben servir como guía normativa para los actores que implementan las acciones recomendadas para la responsabilidad de los datos que se describen en esta Directriz Operacional. Los Principios no representan una norma de cumplimiento.

Estos Principios se basan en una revisión de los principios existentes para la gestión de datos (incluida la protección de datos) en los sectores humanitario y de desarrollo[10]. La revisión reveló deficiencias en la orientación para la gestión de datos operativos a nivel de todo el sistema y de los grupos sectoriales, así como deficiencias en la orientación para la gestión de datos no personales en todos los niveles de la respuesta humanitaria. Los Principios contribuyen a colmar estas lagunas y a garantizar una gestión de datos segura, ética y eficaz. De este modo, refuerzan el compromiso general de los trabajadores humanitarios de no hacer daño, al tiempo que **maximizan los beneficios** de los datos en la acción humanitaria[11]. Los Principios también reafirman la importancia de las personas afectadas y sus derechos y bienestar en la acción humanitaria.

La gestión de los **datos personales** debe basarse en el Principio de Protección de Datos Personales[12], mientras que la gestión de los **datos no personales** debe basarse en los demás principios. Los Principios se presentan en orden alfabético, y no se pretende establecer una jerarquía.

Cuando estos Principios entren en conflicto en su interpretación o aplicación, deberán equilibrarse entre sí en función de la dinámica particular del contexto de la respuesta[13]. En caso de que los Principios entren en conflicto con las políticas internas o las obligaciones legales aplicables, estas últimas tendrán prioridad.

---

10 Esto incluye los principios humanitarios y las normas ampliamente aceptadas articuladas, por ejemplo, en Esfera, la Norma Humanitaria Esencial y el Código de Conducta para el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja y las Organizaciones No Gubernamentales (ONG) en el Socorro en Casos de Desastre, la Estrategia de Datos de las Naciones Unidas y los Principios de Protección de Datos Personales y Privacidad de las Naciones Unidas. Además, incluye orientaciones más específicas o temáticas sobre distintos aspectos de la gestión de datos, como las Normas profesionales para el trabajo de protección, el Marco de gestión de la información sobre protección (PIM) y el Manual del ICRC sobre protección de datos en la acción humanitaria, entre otros. Por último, los Principios se basan en las orientaciones existentes del IASC, incluidas lasDirectrices Operacionales del IASC sobre las Responsabilidades de los Líderes de los Grupos Sectoriales y la OCHA en la Gestión de la Información, y las Directrices Operacionales del IASC para las Evaluaciones Coordinadas en las Crisis Humanitarias. La lista completa de los documentos analizados por el Subgrupo sobre Responsabilidad de los Datos está disponible en el Anexo C. 11 Ampliamente reconocido en todo el sector humanitario, el concepto de "no hacer daño" tiene sus raíces en la práctica médica, a partir de la cual se convirtió en un axioma de la respuesta humanitaria en Mary B. Anderson, Do No Harm: How Aid Can Support Peace - Or War, (1999). A efectos de este documento, el término se utiliza de la siguiente manera: No hacer daño" implica que la gestión de datos en la respuesta humanitaria no debe causar o exacerbar el riesgo para las personas y comunidades afectadas, lascomunidades de acogida, el personal humanitario u otras partes interesadas, a través de acciones u omisiones. El daño se define como "las implicaciones negativas de una actividad de gestión de datos sobre los derechos de un sujeto de datos, o de un grupo desujetos de datos, incluyendo, pero sin limitarse a ello, el daño físico y psicológico, la discriminación y la denegación de acceso a losservicios". Maximizar los beneficios" de la gestión de datos humanitarios implica que los datos se compartan cuando un propósito lorequiera, de forma adecuada y segura, manteniendo los requisitos necesarios de protección de datos. También implica que los datos se gestionen de forma que aumenten las probabilidades de que tengan un impacto positivo para las personas afectadas.

12 Esto incluye los Principios de Protección de Datos Personales y Privacidad de la ONU.

13 Véase en el Anexo B ejemplos de principios en la práctica.

Principios para el Manejo Responsable de Datos en la Respuesta Humanitaria

Rendición de cuentas .

De acuerdo con las normas aplicables pertinentes, las organizaciones humanitarias tienen la obligación de rendir cuentas y aceptar la responsabilidad de sus actividades de gestión de datos. Las organizaciones humanitarias deben rendir cuentas a las personas afectadas por la crisis, a las estructuras de gobernanza interna, a los socios humanitarios nacionales e internacionales y, si procede, a los gobiernos nacionales y a los organismos reguladores. Para cumplir con sus compromisos de rendición de cuentas, las organizaciones humanitarias deben establecer todas las medidas necesarias para mantener y supervisar el cumplimiento de estos Principios. Esto incluye el establecimiento de políticas y mecanismos adecuados y la garantía de la disponibilidad de competencias y capacidades suficientes, incluyendo, pero sin limitarse a ello, la capacidad de personal, recursos e infraestructuras.[14]

Confidencialidad

Las organizaciones humanitarias deben aplicar las salvaguardias y los procedimientos organizativos adecuados para mantener la confidencialidad de los datos sensibles en todo momento. Las medidas deben estar en consonancia con las normas generales de confidencialidad, así como con las normas específicas del sector humanitario[15] y con las políticas organizativas y los requisitos legales aplicables, teniendo en cuenta al mismo tiempo el contexto y los riesgos asociados.

Coordinación y Colaboración

Una gestión de datos coordinada y colaborativa implica la inclusión significativa de los socios humanitarios, las autoridades nacionales y locales, las personas afectadas por la crisis y otras partes interesadas en las actividades de gestión de datos, todo ello cuando sea apropiado y sin comprometer los principios humanitarios[16] o estos Principios. La coordinación y la colaboración también deben tener como objetivo garantizar que se establezcan conexiones adecuadas entre las actividades de gestión de datos operativos humanitarios y los procesos de datos orientados al desarrollo a más largo plazo y las inversiones en datos. La capacidad local y nacional debe reforzarse siempre que sea posible, y no debe socavarse.

Seguridad de los datos .

Las organizaciones humanitarias deben implementar salvaguardas, procedimientos y sistemas organizativos y técnicos adecuados para prevenir, mitigar, informar y responder a las violaciones de la seguridad. Estas medidas deben ser suficientes para proteger contra las violaciones externas, así como contra el acceso o la manipulación interna no autorizada o inapropiada, la divulgación accidental, el daño, la alteración, la pérdida y otros riesgos relacionados con la gestión de datos. Las medidas deben ajustarse en función de la sensibilidad de los datos gestionados y actualizarse a medida que se desarrollen las mejores prácticas de seguridad de los datos, tanto para los datos digitales como para los analógicos.

14 Esto incluye la defensa del IASC, Compromisos sobre la rendición de cuentas a las personas afectadas y la protección contra la explotación y el abuso sexual (2017), disponible en: https://interagencystandingcommittee.org/accountability-affected-populations-including-protection-sexual-exploitation-and-abuse/documents-56.

15 El Manual de protección de datos en la acción humanitaria del ICRC (2020) y la Política de protección en la acción humanitaria del IASC (2016) ofrecen orientación sobre la confidencialidad. Estas normas deben interpretarse en consonancia con las políticas y directrices organizativas existentes.

16 Para más información sobre los principios humanitarios, véase OCHA on Message: Principios humanitarios, disponible en: https://www.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf.

Propósito definido, necesidad y proporcionalidad .

La gestión de datos humanitarios y sus actividades relacionadas deben tener un propósito claramente definido. El diseño de los procesos y sistemas de gestión de datos debe contribuir a mejorar los resultados humanitarios, ser coherente con los mandatos pertinentes y los derechos y libertades correspondientes, y equilibrarlos cuidadosamente cuando sea necesario. En consonancia con el concepto de minimización de datos, la gestión de datos en la respuesta humanitaria debe ser pertinente, limitada y proporcionada -en términos de inversión necesaria así como de riesgo identificado- a los fines especificados.

Equidad y legitimidad -

Las organizaciones humanitarias deben gestionar los datos de manera justa y legítima, de acuerdo con sus mandatos, el contexto de la respuesta, los instrumentos de gobierno y las normas y estándares mundiales, incluidos los Principios Humanitarios. Los motivos legítimos para la gestión de los datos incluyen, por ejemplo: el interés superior de las personas afectadas por la crisis, de acuerdo con el mandato de la organización; el interés público en la promoción del mandato de la organización; los intereses vitales de las comunidades y los individuos que no pueden tomar una decisión sobre la gestión de los datos por sí mismos; y cualquier otro motivo legítimo específicamente identificado por el marco normativo de la organización o las leyes aplicables.

Enfoque basado en los derechos humanos .

La gestión de datos debe diseñarse y aplicarse de forma que respete, proteja y promueva el cumplimiento de los derechos humanos, incluidas las libertades fundamentales y los principios de igualdad y no discriminación definidos en los marcos de derechos humanos, así como el derecho más específico a la privacidad y otros derechos relacionados con los datos, y los derechos específicos de los datos promulgados en la legislación de protección de datos aplicable y en otras normativasaplicables.

Centrado en las personas e inclusivo .

Siempre que el contexto operativo lo permita, las poblaciones afectadas deben tener la oportunidad de ser incluidas, representadas y capacitadas para ejercer su capacidad de acción en la gestión de datos. Deben hacerse esfuerzos especiales para apoyar la participación y el compromiso de las personas que no están bien representadas y que pueden estar marginadas en la actividad de gestión de datos en cuestión (por ejemplo, debido a la edad, el género y otros factores de diversidad como la discapacidad, elorigen étnico, la religión, la orientación sexual u otras características), o que son "invisibles" por otros motivos, en consonancia con los compromisos de no dejar a nadie atrás. Un enfoque inclusivo y centradoen las personas es especialmente importante en el desarrollo de normas y estándares específicos para la gestión de datos.

Protección de datos personales .

Las organizaciones humanitarias tienen la obligación de adherirse a (i) las leyes nacionales y regionales de protección de datos aplicables, o (ii) si gozan de privilegios e inmunidades tales que las leyes nacionales y regionales no se les aplican, a sus propias políticas de protección de datos [17]. Estas leyes y políticas contienen la lista de bases legítimas para el tratamiento de datos personales, incluyendo, pero

[17] Con respecto a las organizaciones del sistema de las Naciones Unidas, el Comité de Alto Nivel sobre Gestión (CANG) ha adoptado los Principios de protección de los datos personales y de la intimidad, que deberían servir de marco fundamental para el tratamiento de los datos personales por parte de las entidades de las Naciones Unidas. En el caso de las organizaciones que no gozan de prerrogativas e inmunidades, debe hacerse referencia a la legislación aplicable en materia de protección de datos, así como a los conjuntos de principios y otras orientaciones a las que están sujetas dichas organizaciones.

no limitándose al consentimiento [10]. Al diseñar los sistemas de gestión de datos, las organizaciones humanitarias deben cumplir las normas de privacidad y protección de datos por diseño y por defecto. Las organizaciones humanitarias deben tener en cuenta la protección de los datos personales a la hora de desarrollar marcos de datos abiertos. En consonancia con su compromiso con la inclusión y el respeto de los derechos humanos, deben garantizar los derechos de los interesados a ser informados sobre el tratamiento de sus datos personales y a poder acceder, corregir, eliminar u oponerse al tratamiento de sus datos personales.

Calidad

La calidad de los datos debe mantenerse de manera que los usuarios y las principales partes interesadas puedan confiar en la gestión de los datos operativos y sus productos resultantes. La calidad de los datos implica que éstos sean pertinentes, precisos, oportunos, completos, actualizados e interpretables, en consonancia con el uso previsto y según convenga en el contexto dado. Siempre que sea posible y apropiado, y sin comprometer estos Principios, las organizaciones deben esforzarse por recoger yanalizar los datos desglosados por edad, sexo y discapacidad, así como por otras características de la diversidad que sean relevantes para los fines definidos de una actividad.

Retención y Destrucción .

Los datos sensibles sólo deben conservarse durante el tiempo que sea necesario para la finalidad especificada para la que se gestionan o según lo exija la legislación aplicable o las normas de auditoría de los donantes. Cuando se requiera su conservación, debe garantizarse un almacenamiento seguropara evitar que los datos sensibles se utilicen indebidamente o se expongan de forma irresponsable. Todos los demás datos pueden conservarse indefinidamente, siempre que se reevalúe su nivel de sensibilidad en los momentos oportunos, que puedan establecerse derechos de acceso y -en el caso de los datos anonimizados o agregados- que se realice una evaluación de reidentificación. Independientemente del nivel de sensibilidad, un esquema de conservación debe indicar cuándo deben destruirse los datos y cómo hacerlo de manera que resulte imposible su recuperación. Siempre que sea posible, deben definirse períodos específicos de conservación y, cuando no sea así, deben establecerse períodos específicos de revisión de la necesidad.

Transparencia

La gestión de datos en la respuesta humanitaria debe llevarse a cabo de forma que ofrezca una transparencia significativa a las partes interesadas, especialmente a las poblaciones afectadas. Esto debería incluir la provisión de información sobre la actividad de gestión de datos y sus resultados, así como la puesta en común de los datos de manera que se promueva una verdadera comprensión de la actividad de gestión de datos, su propósito, su uso previsto y su puesta en común, así como las limitaciones y los riesgos asociados.

18 Para más información sobre el tratamiento de datos personales y el uso del "consentimiento" como base legítima en la respuesta humanitaria, véase el Manual del ICRC sobre protección de datos en la acción humanitaria (2ª edición, 2020).

Acciones Recomendadas para la Responsabilidad de los datos en Contextos de Respuesta Humanitaria

La siguiente sección presenta las acciones recomendadas para la responsabilidad de los datos a nivel de todo el sistema (1), a nivel de grupo/sector (2) y a nivel de organización (3). Estas acciones representan los mayores puntos de apalancamiento para el impacto colectivo y organizativo con respecto a la responsabilidad de los datos. También representan un conjunto básico de acciones recomendadas para la responsabilidad de los datos en la práctica que la comunidad humanitaria debería tratar de mantener.

Estas acciones son aplicables en todos los contextos de respuesta humanitaria. Dado que la adopción de la responsabilidad de los datos varía dentro de los contextos de respuesta y entre ellos, estas acciones pretenden servir de referencia común para su adaptación y aplicación en el contexto. Su aplicación variará en función de los entornos y requerirá una adaptación basada en la naturaleza de una crisis concreta. Aunque algunas de las acciones pueden ser nuevas a nivel de sistema, grupo/sector yorganización en diferentes entornos, todas las acciones están diseñadas para aprovechar ycomplementar las prácticas, los procesos y las herramientas existentes.

Las acciones se presentan en una secuencia lógica en cada nivel para que sirvan de hoja de ruta para la acción y la mejora progresivas. Los actores humanitarios y sus socios deberán identificar los puntos de entrada apropiados para implementar estas acciones en función del estado de la responsabilidad de los datos en su contexto.

La siguiente tabla ofrece una **descripción de cada acción** y su importancia para la **responsabilidad de los datos**. Las secciones siguientes, correspondientes a los niveles de sistema, grupo/sector y organización, describen cómo **deben adaptarse y aplicarse las acciones en cada nivel y quién debe participar en ellas.** Estas secciones también incluyen referencias a modelos de plantillas y herramientas (disponibles en el Anexo B) para apoyar la implementación de las diferentes acciones.

Acciones para la Responsabilidad de los datos en Contextos de Respuesta Humanitaria		
Acciones	**Descripción**	**Importancia**
Diagnóstico de la responsabilidad de los datos	Un diagnóstico de la responsabilidad de los datos implica la identificación y revisión de las leyes, normas, políticas y estándares existentes en el contexto; los procesos y procedimientos; y las herramientas técnicas para la gestión de datos.	Este diagnóstico ayuda a identificar las oportunidades y los retos comunes para la gestión responsable de los datos e informa sobre la priorización de las acciones para la responsabilidad de los datos en los diferentes niveles de una respuesta.
Mapa del Ecosistema de datos y registro de activos de datos	Un mapa del ecosistema de datos proporciona un resumen de las principales actividades de gestión de datos, incluyendo la escala, el alcance y los tipos de datos que se procesan, las partes interesadas, los flujos de datos entre los diferentes	El mapa del ecosistema y el registro de activos de datos ayudan a identificar las lagunas de datos y las posibles duplicaciones, y apoyan la complementariedad y la convergencia (incluso con los procesos orientados al desarrollo a largo plazo), facilitar la

	actores, y los procesos y plataformas en uso. Un registro de activos de datos proporciona un resumen de los principales conjuntos de datos que generan y gestionan los diferentes actores en un contexto.	colaboración y permitir el establecimiento de prioridades y la toma de decisiones estratégicas sobre la gestión responsable de los datos.
Evaluación del impacto de los datos[19]	La realización de una evaluación del impacto de los datos ayuda a determinar los riesgos, daños y beneficios previstos, así como las repercusiones sobre la privacidad, la protección de datos y/o los derechos humanos de una actividad de gestión de datos.	Una evaluación informa el diseño y la implementación de las actividades de gestión de datos de manera que se maximicen los beneficios y se minimicen los riesgos.
Diseño para la responsabilidad de los datos	El diseño de la responsabilidad de los datos implica tener en cuenta los Principios para la Responsabilidad de los Datos en la Acción Humanitaria desde el inicio de una actividad de gestión de datos (incluso en la fase de diseño y planificación) y supervisar la adhesión a estos Principios a lo largo del proceso.	Incluir consideraciones sobre la responsabilidad de los datos en el diseño, la ejecución, el seguimiento y la evaluación de las actividades de gestión de datos ayuda a minimizar los riesgos y maximizar los beneficios.
Protocolo de intercambio de información y clasificación de la sensibilidad de los datos y la información	Un Protocolo de Intercambio de Información (ISP) debe incluir una clasificación de la sensibilidad de los datos y la información en función del contexto[20], articular acciones comunes para la responsabilidad de los datos, contener cláusulas sobre la protección de los datos personales, si procede, y especificar cómo tratar las infracciones del protocolo.	Un ISP sirve de base para un enfoque colectivo del intercambio responsable de datos e información. Aunque normalmente se establece a nivel de todo el sistema, los ISP también pueden establecerse a nivel de clúster/sector y de organización, según sea necesario.
Acuerdo de intercambio de datos	Un acuerdo de intercambio de datos establece los términos y condiciones que rigen el intercambio de datos personales o datos sensibles no personales. Se utiliza principalmente para compartir datos entre dos partes y suele establecerse a nivel nacional. De acuerdo con los marcos de protección de datos, es necesario firmar un Acuerdo de intercambio de datos para compartir datos personales.	Este tipo de acuerdo es esencial para mantener los requisitos legales, políticos y normativos relacionados con el intercambio de datos personales y, en algunos casos, de datos sensibles no personales.
Gestión de incidencias de datos [21]	La gestión, el seguimiento y la comunicación de los incidentes de datos requieren procedimientos operativos estándar para la gestión de incidentes y un	La gestión de incidentes con datos ayuda a reducir el riesgo de que se produzcan, apoya el desarrollo de una base de conocimientos y fomenta enfoques más

19 'La "evaluación del impacto de los datos" es un término genérico que hace referencia a múltiples tipos de evaluaciones, tal y como se define en el Anexo A. Tenga en cuenta que una evaluación del impacto de la protección de datos (DPIA) es la herramienta y el proceso establecido en la ley de protección de datos que debe utilizarse (específicamente) para evaluar los riesgos de la protección de datos personales.

20 La clasificación de la sensibilidad de los datos y la información indica el nivel de sensibilidad de los diferentes tipos de datos e información para un contexto determinado. Debe elaborarse mediante un ejercicio colectivo en el que las distintas partes interesadas se pongan de acuerdo sobre lo que constituye un dato sensible en su contexto.

21 Para más información sobre la gestión de incidentes de datos, véase: Centro de Datos Humanitarios de la OCHA, Nota de orientación: Gestión de incidentes de datos (2019), disponible en: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf

	registro o bitácora central que capture los detalles clave sobre la naturaleza, la gravedad y la resolución de cada incidente.	coordinados para la gestión de incidentes a lo largo del tiempo.
Coordinación y toma de decisiones sobre la acción colectiva para la responsabilidad de los datos	Los mecanismos existentes pueden utilizarse para coordinar y tomar decisiones sobre la acción colectiva para la responsabilidad de los datos en diferentes niveles de una respuesta. Esto incluye el Equipo Humanitario de País, el Mecanismo de Coordinación Interclúster, y los clústeres/sectores, entre otros.	La coordinación y la acción colectiva ayudan a la comunidad de respuesta a supervisar el progreso y los desafíos, y a identificar las oportunidades para mejorar la responsabilidad de los datos. También ayudan a fomentar la responsabilidad y la inversión conjunta en la aplicación de las demás acciones de esta Directriz Operacional.

Nivel 1: Acciones a nivel de todo el sistema para la responsabilidad de los datos

Apoyar la responsabilidad de los datos a nivel de todo el sistema de una respuesta requiere una acción colectiva en una serie de áreas. La Oficina del Coordinador Residente/Coordinador de Asuntos Humanitarios, el Equipo Humanitario de País, la OCHA o el ACNUR[22], y varias estructuras de coordinación como la ICCM/ICCG/ISCG, el IMWG y el Foro de ONG tienen importantes funciones que desempeñar en el apoyo a estas acciones.

Debido a que los niveles de responsabilidad de los datos varían dentro y a través de los entornos de respuesta, estas acciones pretenden servir como una referencia común para la adaptación y aplicación en el contexto. Si bien algunas de las acciones pueden ser nuevas a nivel de todo el sistema en determinados entornos, todas las acciones están diseñadas para aprovechar y complementar las prácticas, los procesos y las herramientas existentes dentro del sistema humanitario. En el cuadro siguiente se definen las funciones y responsabilidades específicas para la aplicación de cada acción.

En todas estas acciones, las organizaciones humanitarias deben garantizar un compromiso significativo con las organizaciones y autoridades nacionales, según el contexto específico.[23] Esto puede fortalecer la capacidad de respuesta de los actores nacionales, generar confianza y crear un espacio para la colaboración productiva y la gestión de cuestiones relacionadas con los datos.

Acciones a nivel de sistema para responsabilidad de los datos		
Acciones	**Enfoque recomendado**	**Funciones y responsabilidades**
Realizar un diagnóstico de la responsabilidad de los datos en todo el sistema. **[Anexo B: Plantilla de diagnóstico de la responsabilidad de los datos]**	El diagnóstico de la responsabilidad de los datos en todo el sistema proporciona una visión general de las medidas de responsabilidad de los datos entre organismos, grupos y sectores. Apoya la toma de decisiones conjunta sobre cómo enfocar y priorizar la acción colectiva en materia de responsabilidad de datos. Si no existe un mapa del ecosistema de datos a nivel de todo el sistema, lo ideal es que se realice conjuntamente.	**El mecanismo o mecanismos interinstitucionales pertinentes** (tanto el **ICCM/ICCG/ISCG** como el **IMWG**), con el apoyo de la **OCHA**, deberían completar este diagnóstico anualmente. El diagnóstico deberá presentarse al **Equipo Humanitario en el País** para que sirva de referencia y como herramienta para supervisar los avances en las cuestiones clave del fortalecimiento de la responsabilidad de los datos.
Generar y mantener un sistema de datos a nivel de todo el sistema.	El mapa del ecosistema de datos de todo el sistema proporciona un resumen de las principales actividades de gestión de datos realizadas en la respuesta global. Requiere aportaciones de los clústeres/sectores y otros organismos interinstitucionales, así como de organizaciones individuales cuyas actividades no estarían cubiertas por el mapa de clústeres/ sectores. El mapa del ecosistema de datos de	El ejercicio de mapeo del ecosistema de datos debe ser completado anualmente por el **mecanismo o mecanismos interinstitucionales pertinentes** (tanto el **ICCM/ICCG/ISCG** como el **IMWG**) y

[22] La Directriz Operacional propone funciones y responsabilidades en consonancia con las estructuras de coordinación introducidas a través del enfoque de grupos temáticos. Reconoce la responsabilidad general de las autoridades nacionales, a las que trata de apoyar promoviendo una acción coordinada para la responsabilidad de los datos. En las situaciones relacionadas con los refugiados y otras personas bajo su mandato, el ACNUR es responsable de coordinar todos los aspectos de la respuesta humanitaria.

[23] Este compromiso debe alinearse con la Directriz Operacional del IASC para Agencias Líderes de Clústeres sobre el Trabajo con Autoridades Nacionales (2011), disponible en: https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, en función del papel que las autoridades nacionales asuman en la respuesta.

[Anexo B: Plantilla del mapa del ecosistema de datos]	todo el sistema proporciona un resumen de las principales actividades de gestión de datos realizadas en la respuesta global. Requiere aportaciones de los clústeres/sectores y otros organismos interinstitucionales, así como de organizaciones individuales cuyas actividades no estarían cubiertas por el mapa de clústeres/ sectores.	presentado al **Equipo Humanitario en el País** para su referencia.
Desarrollar y mantener un protocolo de intercambio de información en todo el sistema. **[Anexo B: Modelo de protocolo de intercambio de información]**	El Protocolo de Intercambio de Información de todo el sistema es el principal documento de referencia que rige el intercambio de datos e información en la respuesta. Debe incluir una clasificación de la sensibilidad de los datos y de la información en función del contexto, que describa la sensibilidad y el protocolo de divulgación correspondiente para los tipos de datos clave de la respuesta.	El protocolo de intercambio de información (ISP) debe desarrollarse a través de un ejercicio colectivo dirigido por el **mecanismo o mecanismos interinstitucionales pertinentes** (tanto el I**CCM/ICCG/ISCG** como el **IMWG**) con el apoyo de la **OCHA**. Una vez redactado, el ISP deberá presentarse al **Equipo Humanitario en el País** para su revisión y aprobación. Todas las partes implicadas en la gestión de datos deben conocer el PSI y sus respectivas obligaciones.
Seguimiento y comunicación de los incidentes de datos.	A nivel de todo el sistema, el seguimiento y la comunicación de los incidentes de datos debe incluir un registro central que capture detalles clave sobre la naturaleza, la gravedad y la resolución de los diferentes incidentes. Cuando sea apropiado, esto puede vincularse conotros procesos y herramientas de seguimiento de incidentes a nivel de todo el sistema, por ejemplo, sistemas de seguimiento de la seguridad y el acceso.Al establecer este registro, deben tomarse medidas de confidencialidad y protección de datos sensibles.	El **ICCM y el IMWG** son responsables de establecer y mantener el registro central de incidentes y de proporcionar actualizaciones periódicas al Equipo Humanitario en el País. Este registro debe completarse con las aportaciones de los clústeres/ sectores y de las organizaciones individuales. El **Equipo Humanitario en el País**, con el apoyo de la OCHA, es responsable de supervisar los datos de los incidentes a nivel de todo el sistema
Apoyar la coordinación y la toma de decisiones sobre la acción colectiva relacionada con la responsabilidad de los datos a través de los mecanismos interinstitucionales existentes.	Las estructuras interinstitucionales e interclústeres/sectoriales deberían proporcionar un foro o plataforma común para la coordinación y la toma de decisiones sobre la responsabilidad de los datos a nivel de todo el sistema. Estos grupos también deberían supervisar el progreso colectivo y/o los retos y oportunidades de laresponsabilidad de los datos en el contexto.	El Equipo Humanitario en el País es responsable de supervisar las cuestiones relacionadas con la responsabilidad de los datos según sea necesario o de forma ad hoc. El ICCM y el IMWG son responsables de proporcionar actualizaciones periódicas al Equipo Humanitario en el País sobre sus respectivas áreas de interés en relación con la responsabilidad de los datos.

Nivel 2: Acciones a nivel clúster/sector para la responsabilidad de los datos Apoyar la responsabilidad de los datos a nivel de clúster/sector requiere una acción colectiva en una serie de áreas que complementarán las acciones articuladas a nivel de todo el sistema y de la organización. Estas acciones deben implementarse en línea con otras orientaciones globales existentes del IASC y de los clústeres/sectores individuales.

Dado que los niveles de responsabilidad de los datos varían dentro de los entornos de respuesta y entre ellos, estas acciones pretenden servir de referencia común para la adaptación y la aplicación en el contexto. Si bien algunas de las acciones pueden ser nuevas a nivel de clúster/sector en determinados entornos, todas las acciones están diseñadas para aprovechar y complementar las prácticas, los procesos y las herramientas existentes dentro del sistema humanitario más amplio. Dependiendo de la naturaleza del entorno de la respuesta, estas acciones pueden ser completadas tanto a nivel nacional como subnacional por las agencias líderes y colíderes del clúster/sector y sus socios.

Los Organismos Líderes y Colíderes del Clúster/Sector son responsables de garantizar que las acciones se lleven a cabo en el ámbito de una respuesta determinada del clúster/sector (es decir, acciones de los Organismos Líderes o Co-Líderes, y de cualquiera de sus organizaciones asociadas que actúen en nombre del clúster/sector en general). Esto incluye los esfuerzos para promover la adhesión a las leyes de protección de datos globales y nacionales (cuando sea aplicable), normas, políticas y estándares.

A través de estas acciones, los clústeres/sectores deben garantizar un compromiso significativo[24] con las organizaciones y autoridades nacionales y locales, así como con otras partes interesadas pertinentes. Este compromiso puede reforzar la capacidad de respuesta de los actores nacionales, generar confianzay crear un espacio para la colaboración productiva y la gestión de las cuestiones relacionadas con los datos.

Acciones a nivel de clúster/sector para la responsabilidad de los datos		
Acciones	**Enfoque recomendado**	**Funciones y responsabilidades**
Realización de un diagnóstico de responsabilidad de datos a nivel de clúster/sector. **[Anexo B: Plantilla de diagnóstico de la responsabilidad de los datos]**	El diagnóstico de responsabilidad de datos a nivel de clúster/sector proporciona una visión general de las medidas de responsabilidad de datos dentro del clúster/sector. Sirve de base para la toma de decisiones conjunta sobre cómo enfocar y priorizar las acciones y el apoyo del clúster/sector en materia de responsabilidad de datos en el contexto. Complementa (alimenta y/o se basa en) el diagnóstico de todo el sistema	Este diagnóstico debe ser completado/actualizado anualmente (o con mayor frecuencia si el entorno de la respuesta cambia significativamente) por el l**íder del clúster/sector y las agencias co-líderes** en colaboración con sus **socios**.
Crear y mantener un mapa del	El mapa del ecosistema de datos del clúster/ sector debe capturar todas las actividades	El ejercicio de mapeo del ecosistema de datos del clúster/sector y el

[24] Este compromiso debe estar alineado con la Guía Operativa del IASC para Agencias Líderes de Clústeres sobre el Trabajo con Autoridades Nacionales (2011), disponible en: https://www.alnap.org/help-library/iasc-operational-guidance-for-cluster-lead-agencies-on-working-with-national, en función del papel que las autoridades nacionales estén asumiendo en la respuesta, y llevarse a cabo en coordinación con los mecanismos inter-clúster/inter-sectoriales pertinentes.

cosistema de datos del clúster/ sector y un registro de activos de datos. **[Anexo B: Plantilla del mapa del ecosistema de datos]**	existentes de gestión de datos relevantes para las intervenciones de respuesta clave dentro del clúster/sector. El registro de activos de datos del clúster/sector debe capturar todos los activos de datos relacionados con las actividades identificadas en el mapa. Juntas, estas dos acciones ayudan a evitar la duplicación de esfuerzos y apoyan el intercambio de datos dentro del clúster/sector y en toda la respuesta en general. También informan de las aportaciones del clúster/sector al ejercicio de mapeo del ecosistema de datos de todo el sistema.	desarrollo del registro de activos de datos deben ser completados y posteriormente actualizados anualmente por el **líder del clúster/sector y las agencias co-líderes** en colaboración con sus **socios**.
Desarrollar y mantener un protocolo de intercambio de información específico para cada clúster/ sector. **[Anexo B: Plantilla del Protocolo de intercambio de datos]**	En los casos en los que un clúster/sector identifique problemas comunes que son específicos de la gestión de datos dentro de su clúster/sector y que no se abordan suficientemente en el ISP de todo el sistema, se debe desarrollar un ISP adicional para atender estas necesidades y ser aprobado por todos los miembros del clúster/sector. *El ISP específico del clúster/sector debe alinearse con el ISP de todo el sistema y complementarlo, así como con las leyes, normas, políticas y estándares aplicables en el contexto.* *Nota: Si los miembros del clúster/sector planean compartir datos personales entre sí, deben establecer acuerdos de intercambio de datos para este fin (ver más en el Nivel 3: Acciones a nivel de organización para la responsabilidad de los datos, más adelante).*	El ISP debe desarrollarse a través de un ejercicio colectivo dirigido por el clúster/sector l**íder y las agencias co-líderes** en colaboración con sus **socios**. Una vez redactado, el ISP debe ser aprobado por todos los socios del clúster/sector y presentado al mecanismo(s) interinstitucional(es) pertinente(s) para su referencia
Ofrecer apoyo técnico y de asesoramiento a los miembros del clúster/sector sobre la responsabilidad de los datos	Los recursos humanos y financieros para la responsabilidad de los datos a nivel de clúster/ sector son esenciales para fortalecer la responsabilidad de los datos dentro del propio clúster/sector y entre sus miembros. Esto es especialmente importante cuando los miembros emprenden o participan en actividades conjuntas de gestión de datos en nombre o en beneficio del clúster/sector en general. El contenido sobre la responsabilidad de los datos (por ejemplo, cómo realizar evaluaciones del impacto de los datos y transferir de forma segura los datos sensibles) debe incorporarse a las actividades de desarrollo de capacidades a nivel de clúster/sector.	El **líder del clúster/sector y las agencias co-líderes** tienen la responsabilidad de abogar por los recursos necesarios y promover las actividades de desarrollo de capacidades pertinentes.

Diseñar la responsabilidad de los datos en las actividades de gestión de datos dirigidas por el clúster/ sector.	Modelar diferentes enfoques para la gestión responsable de datos a través de actividades conjuntas o comunes (por ejemplo, evaluaciones conjuntas de necesidades) como una forma de exponer a los miembros del clúster/sector a diferentes medidas y estrategias para una gestión de datos segura, ética y eficaz. Los clústeres/sectores también pueden querer desarrollar y apoyar el uso de normas y herramientas comunes para las actividades de gestión de datos dirigidas por el clúster/sector para fomentar un enfoque coherente entre los miembros.	El l**íder del clúster/sector y las agencias co-líderes** deben tratar de diseñar actividades de gestión de datos dirigidas por el clúster en línea con esta Directriz Operacional. Esto podría hacerse, por ejemplo, incluyendo la responsabilidad de los datos en las estrategias de los clústeres.
Seguimiento y comunicación de los incidentes de datos dentro del clúster/sector.	El seguimiento y la comunicación de los incidentes dentro del clúster/sector ayudan a reducir el riesgo de que los incidentes se repitan. Un clúster/sector debe alimentar el seguimiento de los incidentes de datos a nivel de todo el sistema para compartir aprendizajes y buenas prácticas para mitigar los riesgos dentro de la comunidad más amplia. A nivel de clúster/sector, esto puede incluir un registro central que capture detalles clave sobre la naturaleza, la gravedad y la resolución de los incidentes. Cualquier registro de este tipo debe garantizar medidas adecuadas de confidencialidad y protección de los datos sensibles.	El l**íder del clúster/sector y las agencias co-líderes** tienen la responsabilidad de establecer y mantener un registro de los incidentes de datos que ocurren dentro de las actividades de gestión de datos dirigidas por el clúster/ sector. También deben garantizar que estos incidentes y las correspondientes lecciones aprendidas se compartan con los organismos y foros pertinentes de todo el sistema.

Nivel 3: Acciones a nivel de organización para la responsabilidad de los datos.

El mantenimiento de la responsabilidad de los datos a nivel de la organización en un determinado entorno de respuesta es fundamental para el éxito de las acciones de responsabilidad de los datos tanto a nivel de todo el sistema como del clúster o del sector. Las acciones de la siguiente tabla deben aplicarse de acuerdo con las políticas y directrices oficiales de la organización. No afectan ni sustituyen en modo alguno las obligaciones contenidas en las políticas organizativas o los marcos legales y reglamentarios aplicables. Las acciones recomendadas están diseñadas para ser aplicadas por las oficinas y/o equipos de la organización en un entorno de respuesta determinado (por ejemplo, oficinas y equipos de país o de área).

Dado que los niveles de responsabilidad de los datos varían dentro y entre los entornos de respuesta, estas acciones pretenden servir de referencia común para su adaptación y aplicación en el contexto. Si bien algunas de las acciones pueden ser nuevas para las organizaciones en un determinado entorno, todas las acciones están diseñadas para aprovechar y complementar la práctica, los procesos y las herramientas existentes dentro del sistema humanitario más amplio.

Dada la variedad de funciones y capacidades de las organizaciones humanitarias, esta Directriz Operacional no asigna funciones y responsabilidades específicas para la responsabilidad de los datos a nivel de la organización. Siempre que sea posible, las organizaciones deben integrar las acciones que se describen a continuación en los roles y responsabilidades de los equipos y funciones existentes que participan en la gestión de datos operativos en diferentes entornos de respuesta.

Acciones a nivel de organización para la responsabilidad de los datos	
Acciones	**Enfoque recomendado**
Realizar un diagnóstico de la responsabilidad de los datos a nivel de la organización. **[Anexo B: Plantilla de diagnóstico de la responsabilidad de los datos]**	El diagnóstico de la responsabilidad de los datos a nivel de la organización proporciona una visión general de las medidas de responsabilidad de los datos existentes en la oficina de una organización en un entorno humanitario determinado. Apoya la priorización de las acciones para la responsabilidad de los datos por parte de la organización en un contexto particular. También ayuda a la organización a identificar las oportunidades de colaboración y de acción colectiva en materia de responsabilidad de datos dentro de los clústeres/sectores (y otros foros interinstitucionales) de los que la organización es miembro. Este diagnóstico debe completarse anualmente o cuando las circunstancias de una respuesta y/o las propias políticas y/o prácticas de gestión de datos de una organización cambien significativamente.
Crear y mantener un registro de activos de datos a nivel de la organización y contribuir a los ejercicios de mapeo del ecosistema de datos	Las organizaciones deben hacer un seguimiento de todas las actividades de gestión de datos (por ejemplo, evaluaciones, supervisión de la respuesta y análisis de la situación) que dirigen o en las que participan en un registro central de activos de datos. El registro de activos de datos a nivel de organización también puede revelar lagunas en los datos de una organización. Las organizaciones deben consultar este registro cuando realicen aportaciones a los mapas del ecosistema de datos del clúster/sector y de todo el sistema, cuando sea pertinente, y antes de emprender cualquier actividad de de datos de todo el sistema, cuando sea pertinente, y antes de emprender cualquier nueva recopilación de datos.

	El registro debe actualizarse de forma continua y compartirse ampliamente dentro de una organización determinada como referencia institucional.
Realizar una evaluación de impacto de los datos para las actividades de gestión de datos dirigidas por la organización. **[Anexo B: Plantilla de evaluación del impacto de los datos]**	Las evaluaciones del impacto de los datos deben llevarse a cabo antes y durantelas actividades de gestión de datos con el fin de informar sobre la planificación, el diseño, la implementación y los ajustes/revisiones del proyecto. Las evaluaciones del impacto de los datos deben llevarse a cabo de forma inclusiva, con la participación de las poblaciones afectadas cuando sea posible. Una actividad de gestión de datos debe ser rediseñada o cancelada si sus riesgos previsibles superan los beneficios previstos, a pesar de las medidas de prevención y mitigación. Los resultados de una DIA deben compartirse internamente y, en algunos casos, externamente con los actores clave que participan en la actividad de gestión de datos y/ o planifican una actividad similar en el contexto. Esto apoya la coherencia en la evaluación, el seguimiento y la mitigación de los riesgos relacionados con los datos a lo largo del tiempo. *Nota: Muchas organizaciones tienen políticas, requisitos y directrices específicas sobre cómo deben realizarse las DIA. Para los que no lo hacen, la plantilla puede servir de referencia útil (véase el anexo B).*
Diseño para la responsabilidad de los datos en las actividades de gestión de datos dirigidas por la organización.	Las organizaciones deben incorporar la responsabilidad de los datos en las actividades de gestión de datos por diseño como parte de la etapa de planificación de un ejercicio concreto. Esto incluye, por ejemplo, los siguientes pasos y consideraciones: - Abordar las preocupaciones identificadas en la Evaluación del Impacto de los Datos para una actividad determinada a través de medidas de prevención y mitigación apropiadas, factibles y sólidas para todos los riesgos principales identificados. - A la hora de seleccionar herramientas para la gestión de datos, fomentar la complementariedad, la interoperabilidad (cuando proceda) y la armonización (también en lo que respecta a la estructura de los datos). - Apoyar las medidas para la gestión segura de los datos (por ejemplo, la aplicación del Control de Divulgación Estadística25 para los microdatos de las encuestas o evaluaciones, la provisión de un almacenamiento seguro, etc.) - Adherirse a las orientaciones y protocolos pertinentes sobre la responsabilidad de los datos y los procesos y procedimientos conexos, incluidos los ISP a nivel de todo el sistema y/o de los grupos o sectores pertinentes. Esto incluye garantizar que todos los datos que deban compartirse para un fin específico se pongan a disposición a través de los canales adecuados de manera segura, ética y eficaz, con las salvaguardias necesarias para los datos personales y de conformidad con los marcos de protección de datos aplicablesal data and in compliance with applicable data protection frameworks. - Las organizaciones deben establecer y comunicar claramente cómo los individuos pueden acceder, verficar, rectificar y/o eliminar los datos sobre ellos mismos.
Establecer acuerdos de	Las organizaciones deben establecer acuerdos de intercambio de datos siempre que transfieran datos personales o datos sensibles no personales a otras organizaciones,

[25] El Control de Divulgación Estadística (SDC) es una técnica utilizada en estadística para evaluar y reducir el riesgo de que una persona u organización sea reidentificada a partir de los resultados de un análisis de datos administrativos o de encuestas, o en la publicación de microdatos. Para más información, véase The Centre for Humanitarian Data, Guidance Note: Statistical Disclosure Control (2019), disponible en: https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

intercambio de datos para regular la transferencia de datos personales y datos sensibles. **[Anexo B: Creador del Acuerdo de Intercambio de Datos]**	consonancia con los requisitos institucionales, legales y reglamentarios pertinentes, así como con los Principios de Responsabilidad de los Datos en la Acción Humanitaria. Nota: Aunque las circunstancias del intercambio de datos difieren demasiado como para ofrecer una plantilla única para los acuerdos de intercambio de datos, el Constructor de Acuerdos de Intercambio de Datos del Anexo B ofrece una serie de puntos a tener en cuenta en la elaboración de dichos acuerdos, en caso de que no existan ya plantillas y modelos (por práctica o política) en la organización.
Establecer un procedimiento operativo estándar para la gestión de incidentes de datos. **[Anexo B: SOP para la gestión de incedentes con datos]**	Las organizaciones deben desarrollar y aplicar procedimientos operativos estándar (SOPs) para gestionar los incidentes de datos. Esto debería incluir un proceso de notificación, clasificación, tratamiento y cierre del incidente. También deben incluir un registro de los incidentes en la base de conocimientos de su organización (por ejemplo, utilizando un registro que capture los detalles clave sobre la naturaleza, la gravedad y la resolución de cada incidente). También deben incluirse en los SOPs los canales apropiados para la rectificación y reparación de los individuos afectados por un incidente de datos. Las organizaciones deben compartir su experiencia en la gestión y mitigación de incidentes de datos con otros actores, es decir, a nivel de grupo/sector y de todo el sistema.

Anexo A: Definiciones

Datos agregados: Datos acumulados adquiridos mediante la combinación de datos a nivel individual. Se refiere a los datos que (1) se recogen de múltiples fuentes y/o sobre múltiples medidas, variables o individuos y (2) se compilan en resúmenes de datos o informes resumidos, normalmente con fines de información públicao análisis estadístico.

Anonimización: Proceso por el cual los datos personales se alteran de forma irreversible, ya sea eliminando o modificando las variables de identificación, de tal manera que un sujeto de datos ya no puede ser identificado directa o indirectamente.[26]

Consentimiento: El consentimiento es la base jurídica más utilizada y a menudo la preferida para el tratamiento de datos personales. Sin embargo, dada la vulnerabilidad de la mayoría de los beneficiarios y la naturaleza de las emergencias humanitarias, muchas organizaciones humanitarias no estarán en condiciones de confiar en el consentimiento para la mayor parte de su tratamiento de datos personales.[27]

Datos: Representación reinterpretable de la información de manera formalizada y adecuada para su comunicación, interpretación o procesamiento.[28]

Activo de datos: Los activos de datos son un conjunto de datos o información, definidos y gestionados como una sola unidad para que puedan ser comprendidos, compartidos, protegidos y explotados eficazmente.[29]

Registro de activos de datos: Un registro de activos de datos proporciona un resumen de los conjuntos de datos clave que están siendo generados y gestionados por diferentes actores en un contexto.

Mapa del ecosistema de datos: Un mapa del ecosistema de datos proporciona un resumen de las principales actividades de gestión de datos, incluyendo la escala, el alcance y los tipos de datos que se procesan, las partes interesadas, los flujos de datos entre los diferentes actores y los procesos y plataformas en uso.

Evaluación del impacto de los datos: Una evaluación del impacto de los datos es un término genérico para referirse a una variedad de herramientas que se utilizan para determinar las consecuencias positivas y negativas de una actividad de gestión de datos. Entre ellas se encuentran herramientas de uso común -y a veces obligatorias por ley- como las evaluaciones de impacto sobre la protección de datos y las evaluaciones de impacto sobre la privacidad.

I**ncidentes de datos**: Acontecimientos relacionados con la gestión de datos, como la pérdida, destrucción, alteración, adquisición o divulgación de datos e información, causados con fines accidentales o intencionados, ilícitos o no autorizados, que han causado daños o tienen el potencial de causarlos.[30]

Minimización de los datos: El objetivo de garantizar que sólo se procese la cantidad mínima de datos para lograr el objetivo y los fines para los que se recogieron los datos.[31]

Calidad de los datos: Conjunto de características que hacen que los datos sean adecuados para el fin para el que se procesan. La calidad de los datos incluye componentes como la exactitud, la pertinencia, la suficiencia, la integridad, la exhaustividad, la facilidad de uso, la validez, la coherencia, la puntualidad, la accesibilidad, la comparabilidad y la actualidad.[32]

---

[26] *Centro de Datos Humanitarios de la OCHA, Glosario*: https://centre.humdata.org/glossary/.

[27] ACNUR, Orientación sobre la protección de los datos personales de las personas de interés para el ACNUR (2018), https://www.refworld.org/docid/5b360f4d4.html.

[28] ONU, Estrategia de datos del Secretario General para la acción de todos, en todas partes, con conocimiento, impacto e integridad, 2020-22 (2020), https://www.un.org/en/content/datastrategy/index.shtml.

[29] Adaptado de los Archivos Nacionales del Reino Unido Achives, *Information Asset Fact Sheet* (2017), https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.

[30] Centro de Datos Humanitarios, *Guidance Note: Data Incident Management* (2019), https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

[31] ICRC, *Handbook on Data Protection in Humanitarian Action* (2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

[32] ONU OCHA, *Directrices de responsabilidad de datos de la OCHA ((Borrador)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

Protección de datos: La aplicación sistemática de un conjunto de garantías institucionales, técnicas y físicas que preservan el derecho a la intimidad respecto al tratamiento de datos personales.[33]

Evaluación del impacto de la protección de datos: Una herramienta y un proceso para evaluar los impactos de protección en los sujetos de datos en el tratamiento de sus datos personales y para identificar las acciones correctivas necesarias para evitar o minimizar dichos impactos.[34]

Responsabilidad de los datos: Un conjunto de principios, procesos y herramientas que apoyan la gestión segura, ética y eficaz de los datos en la respuesta humanitaria.[35]

Seguridad de los datos: Conjunto de medidas físicas, tecnológicas y de procedimiento que salvaguardan la confidencialidad, la integridad y la disponibilidad de los datos y evitan su pérdida, destrucción, alteración, adquisición o divulgación accidental o intencionada, ilícita o no autorizada.[36]

Sensibilidad de los datos: Clasificación de los datos en función de la probabilidad y gravedad del daño potencial que puede materializarse como resultado de su exposición en un contexto determinado.[37]

Acuerdo de intercambio de datos: Acuerdo que establece los términos y condiciones que rigen el intercambio de datos personales o datos sensibles no personales. Se utiliza principalmente para compartir datos entre dos partes y suele establecerse a nivel nacional. De acuerdo con los marcos de protección de datos, se requiere la firma de un acuerdo de intercambio de datos para compartir datos personales.

Sujeto de los datos: Persona física (es decir, un individuo) cuyos datos personales son objeto de tratamiento y que puede ser identificada, directa o indirectamente, por referencia a estos datos y a medidas razonablemente probables. La designación como interesado está vinculada a un conjunto de derechosespecíficos del interesado a los que esta persona física tiene derecho con respecto a sus datos personales, incluso cuando estos datos son recogidos, recopilados o tratados de otro modo por otros.[38]

Daño: Consecuencias negativas de una iniciativa de tratamiento de datos sobre los derechos de un sujeto de datos, o de un grupo de sujetos de datos, incluidos, entre otros, los daños físicos y psicológicos, la discriminación y la denegación de acceso a los servicios.[39]

Producto de información: Producto derivado de datos brutos que se organiza de manera que transmita la información prevista a los usuarios (por ejemplo, infografías, gráficos, mapas, informes de situación, etc**).**

Microdatos: Datos de observación sobre las características de las unidades estadísticas de una población, como los individuos, los hogares o los establecimientos, recopilados a través de ejercicios como las encuestas de hogares, la evaluación de las necesidades o las actividades de seguimiento.[40]

Datos no personales: Cualquier información que no se relaciones con un sujeto de datos. Los datos no personales pueden clasificarse en función de su origen, a saber: los datos que nunca se han relacionado con un sujeto de datos, como los datos sobre el contexto en el que se desarrolla una respuesta y los datos sobre los agentes de la respuesta humanitaria y sus actividades; o lo datos que inicialmente eran datos personales pero que posteriormente se hicieron anónimos, como los datos sobre las personas afectadas por la situación humanitaria y sus necesidades, las amenazas y vulnerabilidades a las que se enfrentan y sus capacidades. Los datos no personales incluyen la Información Demográficamente Identificable, es decir, los datos que

[33] Definición elaborada por el Grupo de Política de Privacidad de la ONU (2017).
[34] ACNUR, Política de protección de los datos personales de las personas de interés para el ACNUR(2015), https://www.refworld.org/pdfid/55643c1d4.pdf.
[35] ONU OCHA, *OCHA Data Responsibility Guidelines (Borrador)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[36] *El Centro de Datos Humanitarios, Glosario*: https://centre.humdata.org/glossary/.
[37] El Centro de Datos Humanitarios, Glosario: https://centre.humdata.org/glossary/.
[38] ONU OCHA, *OCHA Data Responsibility Guidelines (Borrador* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.
[39] ibid.
[40] *El Centro de Datos Humanitarios, Nota de orientación: Control de la divulgación de estadísticas* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

permiten la identificación de grupos de individuos por factores demográficos definitorios, como el origen étnico, el género, la edad, la ocupación, la religión o la ubicación.

Gestión de datos operativos: El diseño de las actividades de gestión de datos y la posterior recopilación o recepción, almacenamiento, procesamiento, análisis, intercambio, uso y retención y destrucción de datos e información por parte de los actores humanitarios. Dichas actividades se llevan a cabo como parte de la acción humanitaria a lo largo del ciclo de planificación y respuesta en todos los grupos sectoriales/ sectores e incluyen, entre otras, el análisis de la situación, la evaluación de las necesidades, la gestión de los datos de la población, el registro y la inscripción, la gestión de los casos, la comunicación con las poblaciones afectadas, el seguimiento de la protección y el seguimiento y la evaluación de la respuesta.

Datos personales: Cualquier información relativa a una persona física identificada o identificable ("sujeto de datos"). Una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.[41]

Datos primarios: Datos que han sido generados por el propio investigador, encuestas, entrevistas, experimentos, especialmente diseñados para comprender y resolver el problema de investigación planteado.[42]

Privacidad: Nadie podrá ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[43]

Reidentificación: Proceso por el cual los datos desidentificados (anonimizados) pueden ser rastreados o vinculados a un individuo o grupo de individuos a través de medios razonablemente disponibles en elmomento de la reidentificación de los datos.[44]

Datos secundarios: Datos que se recogieron originalmente con un propósito de investigación específico o, alternativamente, sin un propósito de investigación específico (por ejemplo, un censo nacional), y que ahora son utilizados por otros investigadores para un propósito diferente.

Datos sensibles: Datos clasificados como sensibles en función de la probabilidad y gravedad del daño potencial que puede materializarse como resultado de su exposición en un contexto particular. Tanto los datos personales como los no personales pueden ser sensibles. Muchas organizaciones tienen sistemas de clasificación específicos sobre lo que constituye datos sensibles para facilitar las prácticas de gestión de datos.[45]

Control de divulgación estadística: Técnica utilizada en estadística para evaluar y reducir el riesgo de que una persona u organización sea reidentificada a partir de los resultados de un análisis de datos administrativos o de encuestas, o en la publicación de microdatos.[46]

---

[41] ONU OCHA, *OCHA Data Responsibility Guidelines (Borrador)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[42] *Guía de investigación en salud pública, definiciones de datos primarios y secundarios:* https://researchguides.ben.edu/c.php?g=282050&p=4036581.

[43] Asamblea General de la ONU, Pacto Internacional de Derechos Civiles y Políticos (1976), https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[44] ONU OCHA, *OCHA Data Responsibility Guidelines (Borrador)* (2019), https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

[45] El Centro de Datos Humanitarios, Glosario, https://centre.humdata.org/glossary/.

[46] El Centro de Datos Humanitarios, *Guidance Note on Statistical Disclosure Control* (2019), https://centre.humdata.org/guidance-note-statistical-disclosure-control/.

Anexo B: Plantillas y herramientas para la responsabilidad de los datos

Las siguientes plantillas y herramientas están diseñadas para apoyar la implementación de las acciones recomendadas para la responsabilidad de los datos presentadas en esta Guía Operativa.

Estas plantillas y herramientas no son obligatorias. Más bien, se proporcionan como ejemplos para ayudar a las organizaciones a poner en práctica las acciones presentadas en esta Directriz Operacional. No sustituyen a las plantillas o herramientas existentes cuando éstas ya existen en una organización, ya sea por la práctica o por la política.

Estas plantillas y herramientas se actualizarán en función de los comentarios recibidos y las lecciones aprendidas sobre su uso a lo largo del tiempo. Cada plantilla y herramienta incluye una sección introductoria en la que se describe el propósito de la herramienta, su(s) fuente(s) y su uso hasta la fecha (cuando sea pertinente), y las instrucciones para su adaptación y uso.

- **Ejemplos de los Principios en la práctica**
- **Herramienta de Diagnóstico de Responsabilidad de Datos**
- **Mapa del Ecosistema de datos y plantilla del registro de activos**
- **Plantilla del Protocolo de Intercambio de Información (incluyendo una clasificación de la sensibilidad de los datos)**
- **Creador del acuerdo de Intercambio de Datos**
- **Plantilla de evaluación del impacto de los datos**
- **Procedimiento operativo estándar para la gestión de incidentes con datos**

Anexo C: Recursos y Referencias

Los siguientes documentos se incluyeron en la revisión bibliográfica que sirvió de base para la redacción de esta Directriz Operacional.

Brussels Privacy Hub (VUB) and International Committee of the Red Cross (ICRC), 2020. Handbook on Data Protection in Humanitarian Action (2nd edition): https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

CARE (Kelly Church) and Linda Raftree, 2019. Responsible Data Maturity Model: https://careinternational.sharepoint.com/:b:/t/Digital/EeATyuHMQSFIoiBzgKHVFKwBuRgwhvQ8mHgTfloFglS1WQ?e=x0yEvz.

Catholic Relief Services, 2019. Responsible Data Values & Principles: https://www.crs.org/about/compliance/crs-responsible-data-values-principles.

CHS Alliance, Group URD and the Sphere Project, 2014. The Core Humanitarian Standard on Quality and Accountability: https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf.

Commission Nationale Informatique & Libertés (CNIL). DPIA/PIA Guides and open source PIA software: https://www.cnil.fr/en/privacy-impact-assessment-pia.

DLA Piper, 2020. Data Protection Laws of the World: https://www.dlapiperdataprotection.com/.

ELAN/Cash Learning Partnership, 2018. Data Starter Kit for Humanitarian Field Staff: https://elan.cashlearning.org/.

European Union, 2018. General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/law-topic/data-protection_en and https://gdpr-info.eu/.

Foreign, Commonwealth & Development Office (FCDO). Personal Information Charter: https://www.gov.uk/government/organisations/foreign-commonwealth-development-office/about/personal-information-charter.

Grand Bargain Working Group on Workstream 5, co-convened by ECHO and OCHA, 2019: https://interagencystandingcommittee.org/grand-bargain/workstream-5-improve-joint-and-impartial-needs-assessments-january-2020-update.

Grand Bargain, 2019. Principles for Coordinated Needs Assessment Ethos: https://interagencystandingcommittee.org/system/files/ws5_-_collaborative_needs_assessment_ethos.pd.

Harvard Humanitarian Initiative (HHI), 2017. The Signal Code: A Human Rights Approach to Information During Crisis: https://hhi.harvard.edu/publications/signal-code-human-rights-approach-information-during-crisis.

Harvard Humanitarian Initiative (HHI), 2018. Signal Code: Ethical Obligations for Humanitarian Information Activities: https://hhi.harvard.edu/publications/signal-code-ethical-obligations-humanitarian-information-activities.

ICRC-led Advisory Group incl. DRC on "Professional Standards", 2018. Professional Standards for Protection Work; Chapter 6: Managing Data and Information for Protection Outcomes: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights.

Inter-Agency Standing Committee (IASC), 2008. Operational Guidance On Responsibilities Of Cluster/Sector Leads & OCHA In Information Management: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/IASC_operational_guidance_on_information_management.pdf.

Inter-Agency Standing Committee (IASC), 2016. Policy on Protection in Humanitarian Action: https://interagencystandingcommittee.org/protection-priority-global-protection-cluster/documents/iasc-policy-protection-humanitarian-action.

International Conference on Data Protection and Privacy Commissioners, 2009. Madrid Resolution: International Standards on the Protection of Personal Data and Privacy: http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf.

International Organization for Migration (IOM), 2010. Data Protection Manual: https://publications.iom.int/books/iom-data-protection-manual.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Do No Harm Checklist and Guiding Questions for DTM and Partners: https://displacement.iom.int/dtm-partners-toolkit/field-companion-sectoral-questions-location-assessment.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: Enhancing Responsible Data Sharing: https://displacement.iom.int/dtm-partners-toolkit/enhancing-responsible-data-sharing.

International Organization for Migration (IOM), 2018. DTM & Partners Toolkit: DTM Data Sharing Forms: https://displacement.iom.int/dtm-partners-toolkit/dtm-data-sharing-forms.

International Red Cross and Red Crescent Movement, 1994. Code of Conduct for the International Red Cross and Red Crescent Movement and Non-Governmental Organizations (NGOs) in Disaster Relief: https://www.icrc.org/en/doc/resources/documents/publication/p1067.htm.

International Rescue Committee (IRC), 2018. Obtaining meaningful informed consent: https://www.rescue.org/resource/obtaining-meaningful-informed-consent.

Médecins Sans Frontières, 2013. Data Sharing Policy: https://fieldresearch.msf.org/bitstream/handle/10144/306501/MSF+data+sharing+policy+final+061213.pdf;jsessionid=E85DF92F1427CE9A46DA5A06D8D6AED5?sequence=1.

MERL Tech/various. Responsible Data Hackpad: https://paper.dropbox.com/doc/Responsible-Data-Hackpad-SA6kouQ4PL3SOVa8GnMEY.

Office of the Australian Information Commissioner. Undertaking a Privacy Impact Assessment (Training): https://www.oaic.gov.au/s/elearning/pia/welcome.html.

Oxfam, 2015. Responsible Data Program Policy: https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950.

Oxfam, 2017. Responsible Data Management Training Pack: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management.

Principles for Digital Development, 2017: https://digitalprinciples.org.

Protection Information Management (PIM) Initiative, 2015. PIM Principles: http://pim.guide/guidance-and-products/product/principles-protection-information-management-may-2015/.

Protection Information Management (PIM) Initiative, 2017. PIM Quick Reference Flyer (PIM Process, Matrix & Principles): http://pim.guide/essential/principles-matrix-process-quick-reference-flyer/.

Protection Information Management (PIM) Initiative, 2017. PIM Principles in Action: http://pim.guide/guidance-and-products/product/pim-principles-action/.

Protection Information Management (PIM) Initiative, 2018. PIM Framework for Data Sharing in Practice: http://pim.guide/essential/a-framework-for-data-sharing-in-practice/.

Terre des Hommes and CartONG, 2017. Data Protection Starter Kit: https://www.mdc-toolkit.org/data-protection-starter-kit/.

The Engine Room: Responsible Data Program, 2016. Responsible Data in Development Toolkit: https://responsibledata.io/resources/handbook/.

The Sphere Project, 2018. The Humanitarian Charter and Minimum Standards in Humanitarian Response (Sphere): https://handbook.spherestandards.org/en/sphere/#ch001.

UN, 2020. Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf.

UN Global Pulse, 2020. Risks, Harms and Benefits Assessment: https://www.unglobalpulse.org/policy/risk-assessment/.

UN Office for the Coordination of Humanitarian Affairs (UN OCHA), 2019. Working Draft Data Responsibility Guidelines: https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

UN Office of Human Rights (OHCHR), 2010. Manual on Human Rights Monitoring (with updated chapters): http://www.ohchr.org/EN/PublicationsResources/Pages/MethodologicalMaterials.aspx.

UN Office of Human Rights (OHCHR), 2018. A Human-Rights Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

UNICEF, 2015. Procedures for Ethical Standards in Research, Evaluation, Data Collection and Analysis: https://www.unicef.org/media/54796/file.

UNICEF, 2018. Industry Toolkit: Children's Online Privacy and Freedom of Expression: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf.

UNICEF/GovLab, 2019. Responsible Data for Children Synthesis report: https://rd4c.org/files/rd4c-report-final.pdf.

UNHCR, 2015. Policy on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/pdfid/55643c1d4.pdf.

UNHCR, 2018. Guidance on the Protection of Personal Data of Persons of Concern to UNHCR: https://www.refworld.org/docid/5b360f4d4.html.

UN Conference on Trade and Development (UNCTAD), 2020. Data Protection and Privacy Legislation Worldwide: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

UN Development Group (UNDG). Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda: https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda.

UN General Assembly, 1945. Charter of the United Nations: https://www.un.org/en/charter-united-nations/.

UN General Assembly, 1948. Universal Declaration of Human Rights: https://www.un.org/en/universal-declaration-human-rights/.

UN General Assembly, 1990. General Assembly Resolution on Guidelines for the Regulation of Personalized Data Files, A/RES/45/95: http://www.refworld.org/pdfid/3ddcafaac.pdf.

UN General Assembly, 1991. General Assembly Resolution 46/182 December 19, 1991: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/GA%20Resolution%2046-182.pdf.

UN High-Level Committee on Management (HLCM), 2018. Privacy and Data Protection Principles: https://www.unsystem.org/personal-data-protection-and-privacy-principles.

UN International Civil Service Commission, 2013. Standards of Conduct for the International Civil Service: https://icsc.un.org/Resources/General/Publications/standardsE.pdf.

UN Secretariat, 2004. Secretary-General's Bulletin on the Use of Information and Communications Technology Resources and Data, ST/SGB/2004/15: https://popp.undp.org/UNDP_POPP_DOCUMENT_LIBRARY/Public/United%20Nations%20Secretary-Generals%20Bulletin%20on%20Use%20of%20ICT%20Resources%20and%20Data%20ST_SGB_2004_15%20%E2%80%93%20Amended.docx.

UN Secretariat, 2010. UN Information Sensitivity Toolkit: https://archives.un.org/sites/archives.un.org/files/RM-Guidelines/information_sensitivity_toolkit_2010.pdf.

UN Secretariat, 2017. Secretary-General's Bulletin on Information Sensitivity, Classification and Handling, ST/SGB/2007/6: http://undocs.org/ST/SGB/2007/6.

UN Secretariat, 2007. Secretary-General's Bulletin on Record-Keeping and the Management of United Nations Archives, ST/SGB/2007/5: http://www.wgarm.net/ccarm/docs-repository/doc/doc462548.PDF.

USAID, 2019. Considerations for Using Data Responsibly at USAID: https://www.usaid.gov/responsibledata.

World Health Organization (WHO), 2007. WHO Ethical and safety recommendations for researching, documenting and monitoring sexual violence in emergencies: https://www.who.int/gender/documents/OMS_Ethics&Safety10Aug07.pdf.

Anexo D: Antecedentes a la elaboración de la Directriz Operacional

El Grupo de Resultados 1 del Comité Permanente entre Organismos creó el Subgrupo sobre Responsabilidad de los Datos en enero de 2020 para dirigir el desarrollo de una directriz operacional conjunta para todo el sistema sobre la responsabilidad de los datos en la acción humanitaria. El Subgrupo fue codirigido por la Organización Internacional para las Migraciones, el Centro de Datos Humanitarios de la OCHA y el Alto Comisionado de las Naciones Unidas para los Refugiados, y estaba compuesto por veinte organizaciones miembros[47] que representaban a diferentes partes interesadas dentro del sistema humanitario.

El Subgrupo elaboró estas Orientaciones Operativas mediante un proceso de colaboración y consulta con los miembros del IASC y la comunidad humanitaria en general, las ONG, los organismos de las Naciones Unidas, otras organizaciones internacionales y los donantes a nivel mundial, regional y nacional. El desarrollo de la Guía Operativa se basó en una serie de actividades, entre ellas:

- Revisión bibliográfica[48]
- Encuesta pública[49]
- Una serie de consultas específicas con diferentes partes interesadas de todo el sistema humanitario, incluyendo organizaciones, clústeres/sectores y estructuras de todo el sistema
- Un período abierto de comentarios en el que 250 compañeros de 30 organizaciones diferentes hicieron aportaciones y comentarios sobre el proyecto de orientación operativa,
- Tres rondas de revisión estructurada y organizativa del proyecto de Directriz Operacional en diferentes etapas de desarrollo.

Esta Directriz Operacional complementa y se basa en las orientaciones existentes sobre la responsabilidad de los datos, tanto de los actores del desarrollo como de la comunidad humanitaria en general. Se ha diseñado para aprovechar la experiencia existente en materia de responsabilidad de los datos, reforzar los esfuerzos y las iniciativas, y ayudar a incorporar las mejores prácticas. Está en consonancia con otras orientaciones e iniciativas clave del sector sobre diferentes temas relacionados con la gestión responsable de los datos. En el Anexo C se incluye una lista completa de recursos revisados como parte del proceso de redacción de esta Directriz Operacional.

Dada la naturaleza dinámica y cambiante de los retos y las oportunidades de la responsabilidad de los datos en la acción humanitaria, esta Directriz Operacional se revisará y actualizará[50] de forma colaborativa y consultiva cada dos años.

[47] El Subgrupo incluía representantes de: CARE, CRS, DRC, ICRC, IFRC, IRC, IOM, JIPS, Mercy Corps, MSF, NRC, OCHA OHCHR, Oxfam, Save the Children, UNFPA, UNHCR, UNICEF, WFP y WHO.

[48] El Subgrupo llevó a cabo la revisión de la literatura de las orientaciones pertinentes existentes sobre la responsabilidad de los datos con el apoyo de la Universidad Técnica de Delft. La lista de documentos revisados está disponible en el Anexo C.

[49] La encuesta pública se realizó en línea desde el 27 de febrero hasta el 18 de marzo de 2020. Los resultados de la encuesta están disponibles aquí: https://centre.humdata.org/survey-results-on-priorities-for-data-responsibility-in-humanitarian-action/.

[50] OCHA será responsable de iniciar el proceso de revisión y actualización de esta Directriz Operacional.