7 Prácticas Responsables y Protección de Datos

Índice de Contenidos del Módulo

Prácticas Responsables y Protección de Datos

Garantizar la protección y el uso responsable de los datos es una de las principales prioridades de la FICR y de todo el Movimiento. Con este módulo, esperamos proporcionarle información y ejercicios que exploren los problemas a los que podría enfrentarse y le ayuden a estar mejor preparado para comprender y resolver estos problemas en la práctica.

Como ocurre con cualquier contenido de carácter general, las orientaciones (y ejemplos) que figuran en el módulo sólo pretenden ser un punto de partida. Deberá realizar sus propias comprobaciones, en su caso con la ayuda de un asesor jurídico, para determinar cuáles son las obligaciones legales específicas (u otras consideraciones pertinentes) en su contexto operativo.

Cuestiones que explora este módulo:

- ¿Qué significan el uso responsable y la protección de datos para el personal humanitario y por qué son importantes estos conceptos?
- ¿Cuáles son las diferencias entre datos no personales, personales y sensibles y por qué es importante conocerlas?
- ¿Qué hace falta en la práctica para proteger y utilizar los datos de forma responsable?

Objetivos de Aprendizaje

- Comprender por qué el uso responsable y la protección de datos son importantes para la ejecución de la labor de la FICR y cómo se vinculan con los principios humanitarios;
- Desarrollar la confianza y los conocimientos necesarios para identificar y distinguir entre los distintos tipos de datos (por ejemplo, datos no personales, personales, sensibles y sensibles de grupos) y lo que ello significa para su uso responsable; y
- Explorar el impacto de los factores legales, éticos, prácticos y culturales sobre la protección de datos en la práctica en situaciones de emergencia complejas.

Temas del Módulo

- El uso responsable de los datos incluye su protección, pero también exige tener en cuenta responsabilidades humanitarias más amplias, como la de no hacer daño y la de imparcialidad.
- Distinguir entre los distintos tipos de datos puede facilitar la comprensión de qué datos deben protegerse. Los equipos humanitarios tienen el deber de proteger y utilizar de forma responsable la información que pueda servir para identificar a una persona o grupo vulnerable.
- Es importante trabajar con las comunidades locales para identificar posibles riesgos para ellas y, a continuación, tomar medidas para utilizar esos datos de forma responsable.

- El uso responsable y la protección de los datos deben tenerse en cuenta en cada etapa del workflow de un proyecto y es necesario reflexionar sobre ello antes de iniciar cualquier nueva actividad de recopilación de datos.
- La forma en que los datos deben protegerse y utilizarse de manera responsable en un contexto determinado depende en gran medida del mandato de la FICR o la SN para operar allí. Como trabajadores humanitarios, no siempre se necesita el consentimiento de las comunidades para utilizar sus datos, pero estos deben usarse siempre de forma responsable.
- Documentar las decisiones (y cómo se han tomado) sobre cómo se han protegido y utilizado los datos es una parte fundamental del uso responsable de los datos. Las evaluaciones de impacto sobre la protección de datos, los acuerdos de intercambio de datos y los formularios de consentimiento pueden ser útiles en este sentido.

Recetas

Proceso paso a paso sugerido para alcanzar los objetivos de aprendizaje

1. ¿Cómo podemos incorporar a nuestro trabajo buenas prácticas de protección y uso responsable de los datos? Con sus equipos, explore: **Las Personas antes que los Datos (folleto) (7 - 16)**, **¿Qué datos necesitamos realmente? (7 - 9)**, **¿Qué podemos hacer? vs. ¿Qué debemos hacer? (7 - 10)**, y
2. Los equipos humanitarios colaboran entre organizaciones. Compartir datos es importante para la respuesta humanitaria. Sin embargo, compartir datos debe hacerse con cuidado y guiándose por las prácticas de Protección de Datos y Uso Responsable de Datos. Comience con un breve debate. **¿Lo compartiría? (7 - 12)** A continuación, los equipos pueden trabajar con sus proyectos existentes revisando este folleto y la lista de comprobación asociada: **Acuerdos de Intercambio de Datos (parte 1) (7 - 1)** (parte 1 and parte 2).
3. ¿Cómo se alinea la protección de datos con nuestros valores y principios? **Valores Humanitarios y Protección de Datos (7 - 7)** (ejercicio) junto con **Valores Humanitarios y Protección de Datos (7 - 8)** (folleto) pueden guiar el intercambio de ideas.
4. **Seguimiento de la campaña de polio en Siria (7 - 17)**, **Simulación de Datos PMER (7 - 15)** "simulan" workflows de datos para varios temas. Los equipos deben utilizar estos casos hipotéticos junto con **Fortalecer Equipos y Proyectos de Datos (3)** (Módulo 3).

Ingredientes

Elija los ingredientes para crear su propia receta. ¿Tiene algún ingrediente que nos falte? Envíe un correo electrónico a data.literacy@ifrc.org

Ejercicios

Experiencias de aprendizaje social breves y concretas

- ¿Qué datos necesitamos realmente?
- ¿Qué debemos hacer vs. Qué podemos hacer?
- Responsabilidad en materia de datos (Caso)
- Protección de datos PMER (Caso)
- Control de la poliomielitis (Caso)

Planes de Sesión

Experiencias de aprendizaje social más prolongadas

- Club de Debate - Protección de Datos y Riesgos Digitales
- En sus zapatos
- Conciliar Valores Humanitarios y Principios de Protección de Datos
- Pesadillas en materia de protección de datos
- La Rueda del Infortunio

Presentaciones con Diapositivas

Presentaciones para usar y/o adaptar:

Contextualice el uso de los datos y su importancia dentro de la FICR

- Comprender e identificar distintos tipos de datos
- Comprender la "base legal"

Listas de Verificación/Folletos/Materiales

Para documentar los elementos esenciales de la experiencia de aprendizaje

- Acuerdos de Intercambio de Datos (Parte 1)
- Acuerdos de Intercambio de Datos (Parte 2)
- Principios de Conciliación (Folleto)

- Limpieza de Datos (lista de verificación)
- Personas antes que Datos (folleto)

Próximos Pasos

Módulos relacionados en el Data Playbook con contenido sugerido

- (Módulo 3: Fortalecer Equipos y Proyectos de Datos) y
  (Módulo 4: Obtener los Datos que Necesitamos)

Fuentes

- IFRC Data Protection guidance
- Handbook on Data Protection in Humanitarian Action, 2nd Edition (ICRC)
- IASC Operational Guidance on Data Responsibility in Humanitarian Action
- OCHA Data Responsibility Guidelines
- IFRC Digital Transformation Strategy
- Digital Dilemmas (interactive website)

Crédito

James De France, Tom Orrell, Heather Leson, colaboradores IFRC V1 Sprint and Data Playbook Beta

7 - 1 Acuerdos de Intercambio de Datos

parte 1

En nuestro trabajo, hay muchas preguntas sobre "intercambio de datos" y "acuerdos de intercambio de datos". Este folleto puede utilizarse antes del despliegue/sesión de planificación previa al proyecto como parte de la utilización responsable de datos y la protección de datos. También puede utilizarse sobre el terreno como herramienta de referencia rápida y lista de verificación para ayudar al personal a reflexionar sobre los requisitos del intercambio de datos.

Compartir datos es la práctica de conceder a otras personas u organizaciones acceso a los datos de los que uno es responsable. Compartir datos puede ser cualquier cosa, desde enviar una hoja de cálculo a un colega de otra organización humanitaria por correo electrónico, hasta proporcionar a los gobiernos un acceso limitado a los datos de la Cruz Roja y la Media Luna Roja. Este folleto es una explicación de los Acuerdos de Intercambio de Datos. En la Parte 2 encontrará un borrador de documento que podrá rellenar a medida que vaya desarrollando su labor de coordinación.

¿Qué son los Acuerdos de Intercambio de Datos?

En la labor de la Cruz Roja y la Media Luna Roja, los "acuerdos de intercambio de datos" (DSAs, por sus siglas en inglés) se refieren a una serie de documentos que abarcan la transferencia de datos dentro del Movimiento y entre éste y los socios gubernamentales y no gubernamentales. Los DSAs deben contemplar una serie de cuestiones y, cuando se refieren al intercambio de datos personales o sensibles, deben definir claramente cómo se protegerán esos datos y cómo se respetarán los derechos de las personas.

Como mínimo, los DSAs deben aportar claridad y un grado de certeza sobre qué datos se compartirán, cómo se compartirán, por qué se comparten, para qué se utilizarán, quién compartirá y quién recibirá los datos, cuándo y dónde se compartirán, y cómo garantizar que los datos estén protegidos y no se utilicen indebidamente después de compartirlos. Lo más adecuado sería que los DSAs también incluyeran condiciones acordadas sobre cómo se respetarán los derechos de propiedad intelectual, cómo y dónde se resolverán las disputas relacionadas con el acuerdo y cualquier otra consideración relevante.

En la Cruz Roja y la Media Luna Roja, los DSAs deben utilizarse siempre que se transfieran datos a, desde o entre las distintas organizaciones que componen el Movimiento.

¿Qué incluye un Acuerdo de Intercambio de Datos?

Contenido	Explicación
¿Qué datos se prevé compartir?	◉ Sea lo más específico posible sobre los conjuntos de datos que se van a compartir. Lo ideal es enumerarlos. ◉ Es sumamente importante que separe los conjuntos de datos "personales y sensibles" de los "no personales" y que se asegure de cumplir las leyes locales de protección de datos y privacidad aplicables, así como las orientaciones de la FICR sobre el intercambio de datos personales.
¿Quién envía los datos y quién los recibe?	◉ Enumere todos los nombres y datos de contacto de las organizaciones o personas que compartirán los datos, tanto las que los envían como las que los reciben. ◉ Si algunos o todos los datos que se van a compartir pertenecen a otra organización, asegúrese de que tiene permiso para compartirlos o inclúyalos también en el acuerdo si tienen control sobre los datos.

Contenido	Explicación
¿Cuándo comenzará y cuándo finalizará el intercambio de datos?	◉ Especifique las fechas de inicio y finalización del intercambio de datos. Especifique qué ocurrirá con los datos al final del acuerdo: se devolverán al proveedor de datos, se eliminarán, se archivarán, etc. ◉ Si no está seguro de cuándo finalizará el intercambio de datos, incluya una cláusula en el acuerdo por la que se comprometa a revisar el calendario en el momento oportuno (por ejemplo, podría acordar revisarlo dentro de un mes, tres meses o un año, en función de la naturaleza de sus necesidades en ese momento).
Si se trata de datos personales, ¿qué medidas son necesarias para garantizar que siguen estando protegidos durante y después de la transferencia (se facilita el acceso)?	◉ Revise el plan de intercambio de datos propuesto teniendo en cuenta todos los principios de protección de datos: es decir, la base jurídica, la minimización, la limitación de la finalidad, la seguridad de los datos, la transparencia, la proporcionalidad y los derechos del interesado.
¿Por qué se comparten los datos?	◉ Asegúrese de enumerar claramente las razones por las que se comparten los datos. ◉ Si se comparten datos personales o sensibles, asegúrese de documentar todas las bases legales legítimas sobre las que se comparten dichos datos.
¿Cómo se comparten los datos?	◉ El DSA debe especificar cómo se transferirán los datos; por ejemplo, por correo electrónico, concediendo acceso remoto a un servidor, a través de la nube, etc. ◉ Siempre que sea posible, el acuerdo debe especificar las normas y formatos que se aplican a los datos que se comparten.
¿Desde dónde se comparten los datos y hacia dónde van?	◉ Es importante aclarar desde dónde y hacia dónde se transfieren los datos, ya que esto podría afectar a las leyes que regulan el intercambio de datos. Por ejemplo, en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, existen normas especiales que deben cumplirse al realizar transferencias internacionales de datos. Cada organización y/o región/país puede tener sus propias obligaciones legales en materia de protección de datos. ◉ El acuerdo debe establecer qué leyes (jurisdicción) del país se aplican al acuerdo y garantizar que el DSA cumple esos requisitos. Esto podría requerir orientación jurídica. ◉ Para ello será necesario revisar la legislación nacional o regional aplicable en materia de protección de datos y privacidad.

Contenido	Explicación
Otras consideraciones	◉ ¿Quién poseerá los derechos de propiedad intelectual sobre los resultados obtenidos a partir de los datos compartidos? ◉ ¿Quién sufragará los costes asociados a la transferencia, el tratamiento o el análisis de los datos? ◉ ¿Cómo se utilizarán los logotipos y distintivos de la Cruz Roja/Media Luna Roja relacionados con los datos? ◉ ¿Qué sucederá con el acuerdo en caso de que alguna circunstancia imprevista lo interrumpa (fuerza mayor)? ◉ ¿Cómo acordarán usted y las demás partes del acuerdo compensarse mutuamente y protegerse financieramente en caso de pérdidas económicas (indemnización)? Si trabaja en una situación de emergencia de gran tensión y necesita compartir datos rápidamente con un socio de confianza, como un colega de otro organismo humanitario, en circunstancias excepcionales, recuerde tener en cuenta lo siguiente: ◉ Puede compartir datos no personales a menos que haya una buena razón para no hacerlo - NO comparta externamente ningún dato que pueda poner en peligro a personas o comunidades, comprometer la ejecución de programas u operaciones humanitarias o desacreditar al Movimiento. ◉ Si necesita compartir datos personales: — Piense qué datos concretos necesita compartir para satisfacer su necesidad urgente y cuál podría ser la mejor manera de compartirlos; — Acuerde cómo se utilizarán los datos, con quién deben o no volver a compartirse y qué medidas se tomarán para protegerlos; — Establezca un plazo para el uso de los datos compartidos y acuerde qué hará con ellos una vez utilizados. Acuerde el momento y el modo en que formalizará el intercambio de datos; — Considere la conveniencia de realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD). — Asegúrese de documentar sus decisiones de intercambio de datos y suscriba un acuerdo de intercambio de datos lo antes posible. Todo intercambio de datos personales o sensibles debe documentarse y registrarse.

Crédito

Tom Orrell, Consultor IFRC Data Playbook

7 - 2 Acuerdos de Intercambio de Datos

parte 2

En nuestro trabajo, hay muchas preguntas sobre "compartir datos" y "acuerdos para compartir datos". Este folleto puede utilizarse antes del despliegue o de la sesión de planificación del proyecto, como parte de la formación sobre el uso responsable y la protección de datos. También puede utilizarse en terreno como herramienta de referencia rápida y lista de verificación para ayudar al personal a reflexionar sobre los requisitos de la puesta en común de datos. La puesta en común de datos es la práctica de conceder a otras personas u organizaciones acceso a los datos de los que uno es responsable. Compartir datos puede ser cualquier cosa, desde enviar una hoja de cálculo a un colega de otra organización humanitaria por correo electrónico, hasta proporcionar a los gobiernos un acceso limitado a los datos de la Cruz Roja y la Media Luna Roja. Este folleto puede utilizarse con la parte 1 (explicaciones).

Coordinar su acuerdo de intercambio de datos:

Contenido	Descripción
¿Quién envía los datos y quién los recibe?	
¿Cuándo comenzará y cuándo finalizará el intercambio de datos?	
¿Qué datos se comparten?	
¿Por qué se comparten los datos?	
¿Cómo se comparten los datos?	
¿De dónde se comparten los datos y a dónde van?	
Otras Consideraciones ◉ ¿A quién pertenecerán los derechos de propiedad intelectual sobre los resultados obtenidos a partir de los datos compartidos? ◉ Si se trata de datos personales, ¿qué medidas son necesarias para garantizar que sigan protegidos durante y después de la transmisión (se facilita el acceso)? Revisar teniendo en cuenta todos los principios de protección de datos: es decir, base jurídica, minimización, limitación de la finalidad, seguridad de los datos, transparencia, proporcionalidad y derechos del interesado. ◉ ¿Quién sufragará los costes asociados a la transferencia, tratamiento o análisis de los datos? ◉ ¿Cómo se utilizarán los logotipos y emblemas de la Cruz Roja y de la Media Luna Roja relacionados con los datos? ◉ ¿Qué sucederá con el acuerdo en caso de que alguna circunstancia imprevista lo interrumpa (fuerza mayor)? ◉ ¿Cómo acordarán usted y las demás partes del acuerdo compensarse mutuamente y protegerse financieramente en caso de pérdidas económicas (indemnización)?	

Crédito

Tom Orrell, consultor IFRC Data Playbook

7 - 3 Debate Club de Debate - Protección de Datos y Riesgos Digitales

Las organizaciones y los individuos tienen muchas preguntas y preocupaciones sobre la protección de datos, la responsabilidad en materia de datos y el riesgo digital. En esta sesión interactiva, organizaremos un "club de debate informal". El objetivo es debatir abiertamente (con humor y juegos de rol) algunas de estas preguntas y preocupaciones. El resultado es una lista de preguntas/políticas y prácticas que necesitan más explicación/comprensión mutua.

Cada participante trabajará en pequeños grupos para redactar algunas " afirmaciones " informales que podrían debatirse en torno a temas de interés y actualidad. Por ejemplo: "Los beneficios de la IA superan cualquier riesgo de sesgo". Cada grupo/individuo manifestará su "acuerdo" o "desacuerdo" con las afirmaciones. Se recomienda discutir diferentes puntos de vista para suscitar el debate y resaltar los matices de los temas. Hay que animar a los participantes a debatir el tema en un animado juego de rol. Esta sesión está dirigida a todos los públicos para explorar las preocupaciones en torno al uso responsable de los datos, la protección de datos y los riesgos digitales. Invite a expertos en la materia a estar disponibles para la introducción y para el "debate posterior" durante esta sesión. Algunos ejemplos podrían ser un responsable de ciberseguridad, un abogado, un responsable de comunicación o un político.

- **Personas:** 5 a 30 personas
- **Tiempo:** 60 Minutos
- **Dificultad:** Fácil
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Ejercicio

Orientaciones para la sesión: Advierta a los participantes de que no se grabarán ni se citarán directamente las conversaciones. El objetivo es crear un espacio de diálogo abierto.

Parte 1: Preparar el escenario

- Dar la bienvenida a la sesión
- Presentar a expertos invitados.
- Comenzar la sesión con una breve introducción a los temas (algunas definiciones y políticas/prácticas en el lugar de trabajo) y ofrecer algunos ejemplos para que los asistentes reflexionen sobre el contexto de trabajo.
- Dependiendo del tamaño del grupo y del equipo, pida a los participantes que compartan 1 cosa que les preocupe sobre los datos y los riesgos digitales.
- Explicar el ejercicio (Partes 2 - 4)
- Demostrar cómo funcionaría la parte del "debate". Debatir con dos personas para representar el desarrollo de un "debate".

Algunos Ejemplos:

- Los beneficios de la IA superan cualquier riesgo de sesgo
- El gobierno protege a todos los ciudadanos vulnerables, por lo que debemos compartir los datos personales de los ciudadanos con el gobierno
- Debemos compartir los datos sobre el VIH de los beneficiarios con las organizaciones sanitarias de las administraciones locales
- Cuando una delegación/donante paga por un programa, debe tener derecho a todos los datos de los clientes (incluidos los datos personales).
- Debemos pagar el rescate en caso de un ciberataque de ransomware (malware de rescate)

- Mientras obtengamos el consentimiento, no tendremos problemas de protección de datos.

Cada "presentador" dirá si está de acuerdo o en desacuerdo con la afirmación. Promueva las respuestas divertidas.

- Opcional: Para una sesión virtual, también podría disponer de una serie de afirmaciones preparadas para que las personas piensen y participen explicando por qué están de acuerdo y en desacuerdo con la afirmación. Pida a los participantes que pongan sus iniciales en la frase y luego pídales que expliquen.

Parte 2: Grupos de discusión

En pequeños grupos de 2 a 4 personas, preséntense. Formulen hasta 5 "declaraciones" relacionadas con el tema de la sesión: "¿Cuáles son algunos ejemplos en torno a los datos responsables, la protección de datos y los riesgos digitales? "Las declaraciones deben inspirar el debate: polémicas y creativas. Tomen notas en el documento colaborativo o en notas adhesivas. Anoten también las preguntas que se plantearán en el futuro. Las utilizaremos en el "DEBATE" plenario. Elijan sus 2 mejores declaraciones para llevarlas al "club del debate".

Parte 3: Debatir en sesión plenaria

Cada equipo compartirá por turnos su "afirmación". Uno de los compañeros de equipo debe presentar el punto de vista de la declaración de "acuerdo" o "desacuerdo". Abra el debate para que los participantes compartan sus puntos de vista. Tome nota de los comentarios, ideas y preguntas.

Dependiendo del tiempo de la sesión y del tamaño del grupo, haga 3 - 4 rondas de afirmaciones.

Parte 4: Coordinar preguntas y opiniones

Pregunte a los participantes: ¿Cuáles son algunas de las cuestiones principales que han identificado? ¿Alguna idea? Anótelas en su documento colaborativo o en un rotafolio.

Bono Extra

Utilice este ejercicio para fomentar el debate en equipo antes de compartir las Políticas y Prácticas de Protección de Datos/Responsabilidad en materia de Datos de su organización.

Recursos

- IFRC Data Protection Guidance
- InterAgency Standing Committee Guidance on Data Responsibility
- Facilitation guidance (Aspiration, ejercicio Spectrogram)

Créditos

Aspiration, participantes IFRC Data and Digital Week

7 - 4 Comprender e identificar diferentes tipos de datos

Considere los datos que está utilizando para cualquier proyecto. Se trata de datos **no personales**, **personales**, **sensibles** o **datos sensibles de grupo**?

Identifique las **categorías** de los datos que está utilizando. A continuación, puede elaborar un plan para proteger y utilizar los datos de forma **responsable**.

Datos personales

Los Datos personales son cualquier dato que pueda utilizarse para identificar a una persona, ya sea por sí solo o en combinación con cualquier otro dato.

Ejemplos:

- Los nombres, direcciones, fechas de nacimiento y números de seguridad social de las personas pueden ser datos personales si se pueden utilizar para identificar a una persona.
- Los datos personales pueden incluir cosas como las coordenadas GPS de una persona (localización), su dirección IP o las cookies de su navegador de Internet.

Datos personales

El contexto importa:

- Recuerde que el contexto es importante. Por ejemplo, algunos nombres que pueden ser muy comunes en un país -y, por tanto, no constituyen datos personales por sí mismos- pueden ser considerados datos personales si aparecen en países donde son poco comunes -y, por tanto, es más probable que permitan identificar a una persona-.

Agregación (combinación) de conjuntos de datos:

- Algunos datos que PUEDEN no ser personales por sí solos, pueden convertirse en personales si se combinan con otros.
  - **Ejemplo:** los datos GPS de un vehículo de la FICR en el terreno por sí solos probablemente no sean datos personales, pero si se combinan con los datos de un registro de conductores autorizados de la FICR, podrían convertirse en datos personales, ya que es probable que el conductor del vehículo pudiera ser identificado como individuo si ambos puntos de datos estuvieran disponibles para la misma persona.

Datos no personales

Los datos no personales son simplemente datos que no pueden utilizarse para identificar a ningún individuo o grupo vulnerable en particular.

Los datos no personales no suelen estar sujetos a requisitos legales estrictos de protección de datos. Sin embargo, **estos datos pueden seguir siendo confidenciales o sensibles** y PUEDEN seguir necesitando ser almacenados de forma segura, mantenidos y actualizados periódicamente y utilizados de forma responsable.

Ejemplo: Datos no personales

- Datos logísticos, como inventarios de suministros médicos o el número de vehículos de la FICR registrados en un país determinado.

Datos sensibles

Los datos sensibles son datos personales que, si se revelan, podrían utilizarse para discriminar a alguien o causarle daños (psíquicos o físicos).

- Los datos confidenciales son **específicos del contexto** y los datos que no son confidenciales en un país, pueden serlo en otro dependiendo de las normas sociales y culturales locales.
- En muchos países, los datos sensibles requieren un grado muy alto de protección y/o no deben recolectarse, utilizarse o compartirse a menos que sea absolutamente necesario.

Ejemplo:

- Historial médico de las personas, estatus respecto al VIH, datos biométricos o ADN, creencias religiosas o políticas, origen étnico y nacionalidad, u orientación sexual e identidad de género.
- Un nombre, por ejemplo, no suele considerarse sensible. Sin embargo, en algunos lugares, ciertos apellidos pueden revelar la religión o la etnia.

Datos sensibles de grupo

Los datos sensibles de grupo son datos que no pueden utilizarse para identificar a personas, pero sí a **grupos vulnerables**, ya sea por sí solos o combinados con otros datos.

Los datos sensibles de grupo son **específicos de cada contexto**, pero es muy importante protegerlos en situaciones de emergencia. Lo ideal sería que los datos sensibles de grupo que se recolecten o utilicen estuvieran sujetos a las mismas normas que los datos sensibles.

Ejemplo: ▶ Fotografía aérea que muestra la ubicación de una tribu indígena no contactada. Aunque no se puede identificar a ningún individuo, la imagen muestra claramente una comunidad vulnerable en numerosos aspectos y, si cayera en las manos equivocadas, podría causar daños a la comunidad.

Gracias

Créditos: Thomas Orrell, James de France, Heather Leson

7 - 5 Comprender la “base legal” al recolectar y usar datos

¿Qué es una “base legal” para la recolección de datos?

Si tiene previsto recolectar datos personales o sensibles, es importante que piense si está autorizado a hacerlo.

Hay un número limitado de razones por las que se pueden recolectar y utilizar datos personales y sensibles (a veces se denomina “base legítima”).

¿Cuáles son las bases legales generalmente aceptadas para la recolección de datos?

Entre las bases legales de la recolección y el uso de datos figuran las siguientes:

- Consentimiento plenamente informado y libremente otorgado.
- Interés público.
- Interés legítimo.
- Interés vital.
- Contrato.
- Obligación legal.

Consentimiento plenamente informado y libremente otorgado

El consentimiento plenamente informado y libremente otorgado es el procedimiento que otorga a las personas más derechos y poder para decidir si se utilizan y comparten sus datos..

En contextos humanitarios, el consentimiento puede no ser la base legal adecuada, ya que las personas pueden sentir que no tienen más remedio que facilitar sus datos (por tanto, no se facilitan libremente). Además, basarse en el consentimiento como única base jurídica puede plantear problemas administrativos adicionales, especialmente en situaciones de emergencia. También hay que tener en cuenta que las personas pueden retirar su consentimiento en cualquier momento.

El consentimiento es más adecuado para recolectar datos no esenciales y en entornos que no son de emergencia.

Véanse ejemplos en la Guía Práctica para la Protección de Datos en Asistencia en Efectivo y Vales.

Consentimiento plenamente informado y libremente otorgado (continuación)

Para que el consentimiento sea “plenamente informado”, el recolector de datos debe comunicar claramente a la persona de/sobre la que se recolectan los datos lo siguiente: cómo y por qué se tratarán sus datos, cómo se protegerán, si se compartirán, cuánto tiempo se conservarán, las consecuencias de no facilitar los datos y cómo resolver cualquier duda que él/ella pueda tener.

Para que el consentimiento para el tratamiento de datos personales sea “libremente otorgado”, la persona que recolecta los datos debe estar razonablemente segura de que la persona que facilita la información no ha sido coaccionada o forzada a darla; que realmente tiene la opción de facilitar la información sin consecuencias negativas.

Interés público

En ocasiones, los datos personales o sensibles pueden recolectarse y utilizarse sobre la base de que dicho tratamiento es de “interés público”.

Ejemplo: emergencia de salud pública

- El Gobierno puede pedir (no exigir) a una Sociedad Nacional que apoye la recolección de datos para la emergencia. En muchos países, lo que se considera de interés público debe basarse en la legislación vigente. Sin embargo, existe una tendencia a considerar la acción humanitaria como de interés público. Lo mejor es revisar los requisitos legales nacionales cuando se pretenda invocar este fundamento.

Interés legítimo

El interés legítimo es una actividad que respalda el(los) mandato(s) subyacente(s) de la organización. Por ejemplo, la recaudación de fondos es necesaria para brindar apoyo a las operaciones en curso. La organización tiene un interés legítimo en recolectar los datos personales de los donantes para recibir las donaciones y poder comunicarse con ellos en el futuro. Cuando utilice el interés legítimo como base legal, deberá evaluar si los derechos del interesado pueden prevalecer sobre los intereses de la organización. Otro ejemplo podría ser la recogida de datos personales durante una auditoría de un proyecto para determinar si ha tenido éxito, si se puede mejorar y cómo hacerlo.

Cumplimiento contractual

Los datos personales y confidenciales a menudo se recolectan para cumplir con un acuerdo.

Ejemplo:

- Es posible que se solicite al personal que brinde detalles sobre su dirección, familias y parientes más cercanos, nacionalidad y detalles financieros al unirse al movimiento como empleados.

  - Es necesario recolectar ciertos datos para garantizar que el personal reciba el pago de su salario, cumpliendo así una de las obligaciones contractuales de la FICR para con un miembro del personal.
  - Otros datos sobre los miembros de la familia pueden ser necesarios para calcular correctamente las prestaciones debidas en el marco del contrato de trabajo.

Obligación legal

A veces, una obligación legal exige que se recolecten y traten determinados datos.

Ejemplo:

- En el caso del personal que se traslada a un nuevo país para asumir sus funciones, la FICR debe recolectar ciertos datos y facilitarlos al gobierno para poder obtener el permiso de residencia (o visado) adecuado. El gobierno ha impuesto esta obligación para obtener el permiso.

Interés vital

A veces puede ser absolutamente necesario recolectar datos personales para ayudar a alguien. La recolección y el uso de datos personales sobre la base de un interés vital suele considerarse apropiada cuando existe una amenaza relativamente inmediata, ya sea física o mental.

Ejemplo:

- Si alguien sufre una lesión grave, podría recolectar todos los datos necesarios (como datos sanitarios) para ayudar a esa persona basándose en la protección de sus intereses vitales. Una vez que la situación de emergencia haya pasado, y la persona se encuentre física y mentalmente estable, usted podrá basarse en otras bases legales para el tratamiento de sus datos personales.

¿Cómo sé qué base legal utilizar?

- No es fácil saber cuál es la base legal correcta. Siempre hay que evaluar las situaciones individualmente para determinar cuál es la correcta.
- Recuerde, si las personas necesitan ayuda, el consentimiento no puede utilizarse si la ayuda está condicionada a la recepción de datos. Eso no se da libremente.
- Asimismo, con independencia de la base legal en la que se fundamente, siempre deberá facilitarse a los interesados, de forma comprensible y accesible, al menos la siguiente información:
  - por qué está siendo recolectada la información,
  - para qué se utilizará,
  - con quién se compartirá,
  - cuánto tiempo se conservará y
  - a quién pueden dirigirse si tienen preguntas.
- En caso de duda, consulte a su Departamento Legal.

Preguntas para el debate

- ¿Cuáles son algunos de los retos que cree que pueden surgir al intentar recolectar y utilizar datos sobre la base de un “consentimiento plenamente informado y libremente otorgado” en un contexto de emergencia? ¿Cuándo sería apropiado que la FICR o una Sociedad Nacional utilizaran el consentimiento? ¿Cuándo podría ser inapropiado?
- ¿Qué responsabilidades adicionales cree que debe tener en cuenta la red de la FICR a la hora de recolectar y utilizar datos sobre una base distinta al consentimiento?
- Si tuviera que recolectar datos personales o sensibles sobre la base de un interés legítimo o público, ¿qué tipo de información se esforzaría por facilitar a las personas de las que está recolectando esos datos?

¡Gracias!

Créditos: Thomas Orrell, James de France, Heather Leson

7 - 6 En sus zapatos

Utilizar el "consentimiento" como base para la recolección y el uso de datos en un entorno humanitario requiere una serie de juicios de valor. En una situación ideal, el personal y los voluntarios de la FICR podrían obtener los datos personales de todos y cada uno de los individuos que necesitan sobre la base de un consentimiento plenamente informado y libremente otorgado. En la realidad, la urgencia y la complejidad de las situaciones de emergencia hacen que sea extremadamente difícil hacerlo. Si bien la FICR y las Sociedades Nacionales a menudo están autorizadas a utilizar datos personales o sensibles sin haber obtenido necesariamente el consentimiento de las personas, cuando lo hacen deben reflexionar sobre la forma en que esos datos deben utilizarse de manera responsable y en consonancia con las buenas prácticas en materia de protección de datos.

Este ejercicio de juego de roles basado en un caso está diseñado para poner de manifiesto algunas de las complejidades que plantea la recolección y el uso de datos sobre la base del consentimiento. También aborda la obligación de ser abiertos y transparentes con respecto a los datos que la FICR recolecta y utiliza, así como las responsabilidades que tiene la FICR de ser un administrador de datos ético y responsable. El ejercicio está dirigido a un público intermedio y avanzado que ya conoce las bases sobre las que se pueden recolectar y utilizar los datos, y las formas en que los valores humanitarios y los principios de protección de datos se solapan.

- **Personas:** 5 a 20 personas
- **Tiempo:** 60 – 90 Minutos
- **Dificultad:** Intermedia
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Ejercicio: Juego de Roles (Role Playing)

Una Sociedad Nacional se prepara para recibir a un numeroso grupo de personas que han tenido que evacuar sus tierras y hogares debido a graves inundaciones. La comunidad internacional y el país anfitrión han reconocido la crisis y han emitido mandatos -tanto a escala internacional como dentro del país anfitrión- para apoyar a las comunidades que se han visto afectadas. Se está movilizando personal para establecer puntos de encuentro en los que se realizará una evaluación rápida de las familias que están llegando y se las registrará para recibir ayuda (ayuda prevista: alimentos, alojamiento, asistencia básica en efectivo mediante un vale, psicosocial y médica). Las personas que llegan están muy traumatizadas, ya que han perdido sus hogares y medios de subsistencia, así como a familiares y amigos. A menudo se encuentran en la más absoluta pobreza, agotadas y en estado de shock.

Roles:

- Coordinador de la respuesta de la Sociedad Nacional: responsable de la planificación y el establecimiento de los puntos de encuentro, incluidos los procesos de recolección de datos.
- Recolector de datos: miembro del personal sobre el terreno o voluntario que recogerá los datos.
- Adulto muy traumatizado que busca ayuda
- Menor muy traumatizado que viaja solo en busca de ayuda
- ¿Alguno más que sea necesario?

Parte 1: planificación - debate en grupo

- ¿Qué procesos debe poner en marcha el coordinador de la respuesta para recolectar datos?
- ¿Qué datos hay que recolectar?
- ¿Cómo debe enfocar el recolector de datos la recolección de datos en la práctica?

Parte 2: recolección de datos - simulación

- Simule una interacción inicial entre el recolector de datos y las personas afectadas. ¿Qué tipo de preguntas se harían? ¿Cómo serían probablemente las respuestas?
- Si el recolector de datos intentara obtener el "consentimiento plenamente informado y libremente otorgado" de las personas afectadas, ¿qué implicaría esto? ¿Cómo sería probablemente esa conversación?
- ¿Qué otra vía podría ser más adecuada en este caso para recolectar datos?
- ¿Qué consideraciones adicionales hay que tener en cuenta al entrevistar al menor no acompañado?

Parte 3: uso de datos - debate en grupo

- Una vez recolectados los datos, dada la vulnerabilidad de estos colectivos, ¿qué responsabilidades tiene la Sociedad Nacional para utilizarlos de forma responsable y mantenerlos a salvo?
- ¿Qué información debe proporcionarse a los colectivos afectados sobre cómo se utilizarán sus datos? ¿Cuál sería el mejor momento para facilitarles esta información dado su estado de shock y trauma?
- Revisando ahora la situación, ¿sería el consentimiento una base adecuada para recolectar datos en este caso? En caso afirmativo, ¿por qué? En caso negativo, ¿por qué no?

Bono Extra

Presente la política de protección de datos de su organización y discuta los próximos pasos y ejemplos de aplicación de las lecciones en su trabajo. Consulte las orientaciones de la FICR en materia de Protección de Datos

Crédito

Tom Orrell, James De France, Heather Leson

7 - 7 Valores Humanitarios y Protección de Datos

El uso responsable y la protección de datos pueden ser temas difíciles de tratar con participantes que no están familiarizados con los datos y con algunos de los riesgos potenciales de las tecnologías digitales. Este ejercicio sólo requiere una comprensión básica de los valores humanitarios y de lo que son los datos personales. El objetivo del ejercicio es relacionar los principios humanitarios con el trabajo con datos e introducir conceptos clave de uso responsable y protección de datos desde un punto de vista de valores en lugar de legal. Los participantes pueden ganar confianza en su capacidad para entender los términos y conceptos relativos a la protección de datos.

- **Personas:** 2 a 12 personas
- **Tiempo:** 30 – 60 Minutos
- **Dificultad:** Fácil
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Ejercicio

Parte 1: Explorar

En pequeños grupos (preferentemente en parejas), debatir:

1. ¿Qué cree que significa "proteger la información" en el ámbito humanitario?
2. ¿Qué significa hacer un uso "responsable" de los datos?

Tome nota de cualquier idea o pregunta en un documento compartido.

Parte 2: Revisar

Discutan las respuestas en grupo y pida a cada grupo que comparta un aspecto destacado de su discusión.

Parte 3: Debatir

Comparta los Principios de Concordancia (Folleto). En pequeños grupos, debatan sobre las siguientes cuestiones:

- ¿Cómo afecta nuestra independencia al modo en que recolectamos, utilizamos y compartimos los datos?
- ¿Debemos ser abiertos y transparentes sobre la información que recogemos de las comunidades y cómo se utiliza?
- ¿Debemos recopilar tantos datos como podamos de las comunidades a las que servimos o necesitamos recopilar los menos posibles? ¿Cómo encontrar un equilibrio?
- Tome nota de cualquier idea o pregunta en un documento compartido.

Parte 4: Reflexionar

En sesión plenaria, solicite reflexiones y preguntas. Comparta más detalles sobre la política de protección de datos de la organización.

Bono Extra

Este ejercicio también podría incluir un caso para la parte 2. Un recurso de aprendizaje basado en un caso puede relacionar los conceptos con situaciones reales a las que se enfrenten los participantes y en las que tengan que reflexionar sobre lo que significaría utilizar los datos de forma responsable y protegerlos.

Ejemplos:

- Una ONG local asociada comparte datos con una Sociedad Nacional, pero se niega a revelar cómo se recolectaron los datos, lo que plantea dudas sobre su calidad. ¿Qué problemas plantea esta situación? ¿Cómo gestionaría usted la situación?
- Ha recolectado datos de un pueblo sobre sus necesidades médicas. Al recolectar los datos, obtuvo su consentimiento para utilizarlos únicamente en sus propias actividades logísticas. Ahora quiere compartir esos datos con las autoridades sanitarias locales. ¿Puede compartir estos datos? ¿Qué información debe revelar a la población sobre sus planes?
- Está recolectando datos en una zona de conflicto sumamente delicada. Las comunidades locales son reacias a facilitarte información porque les preocupan las repercusiones si cayera en malas manos. ¿Qué medidas puede tomar para asegurarse de que se tienen en cuenta sus preocupaciones?

Facilitadores: puede dividir a los grupos en parejas para que discutan la situación entre ellos antes de plantear un debate en grupo sobre los temas clave.
Este ejercicio puede durar entre 30 y 45 minutos por situación, en función del número de participantes.

Consideraciones:

Al repasar los ejercicios y las actividades de los bonos extra, tenga en cuenta que 1) todo tratamiento de datos debe ajustarse a los principios de protección de datos (es decir, tener una o más bases jurídicas, datos exactos y minimizados, comunicación transparente sobre el tratamiento, datos utilizados únicamente para fines compatibles, garantizar la seguridad de los datos y respetar los derechos de los interesados), y 2) nuestras acciones, aunque ayudemos a un gobierno, deben seguir ajustándose a los principios fundamentales, en particular aquí la independencia y la neutralidad. Nuestro objetivo debe ser servir a un fin humanitario, no sólo para ayudar a una entidad gubernamental o bajo su dirección.

Crédito

Tom Orrell, Arturo Garcia, Dirk Slater, Heather Leson, Melissa el Hamouch, James De France

7 - 8 Valores Humanitarios y Protección de Datos

La acción humanitaria tiene sus fundamentos en la empatía y la solidaridad humanas. Su objetivo es proteger la vida y socorrer a los más vulnerables. Dentro de la comunidad humanitaria, el valor más elevado es la idea de que los actores humanitarios deben "no hacer daño" en sus acciones. Cada vez más, esto también se aplica a la forma en que las organizaciones humanitarias utilizan las herramientas digitales y los datos.

Sin embargo, ¿qué significa "no hacer daño" cuando se recolectan, analizan, utilizan o comparten datos de comunidades e individuos? Un buen punto de partida es reflexionar y discutir en profundidad sobre cómo los valores y principios humanitarios y los principios de protección de datos se solapan y refuerzan mutuamente. De este modo, es posible empezar a encontrar respuestas a preguntas como qué significa "proteger" y utilizar los datos de forma "responsable". Este folleto relacionará los Principios Fundamentales del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja con una visión general de algunos principios clave de la protección de datos.

Principios Fundamentales del Movimiento:

- Humanidad –necesidad de actuar para prevenir y aliviar el sufrimiento humano
- Imparcialidad – no discriminar a ninguna persona
- Neutralidad – no tomar partido en los conflictos
- Independencia – ser autónomo y resistir cualquier injerencia
- Voluntariado –deseo de ayudar a los demás, no motivado por el afán de beneficio propio
- Unidad – sólo puede haber una sociedad de la CRMLR en cada país
- Universalidad – La FICR es mundial y tiene una responsabilidad colectiva ante todos

Principios de la Protección de Datos:

- No recopile datos personales que no necesite: sólo recopile datos que puedan identificar a una persona ("datos personales") si realmente los necesita.
- Mantenga sus conjuntos de datos actualizados y en buen estado, como cualquier otro activo: los datos personales recopilados deben ser exactos, completos y mantenerse actualizados.
- Explique claramente y documente las razones por las que recopila los datos: es necesario exponer claramente las razones por las que se recopilan los datos personales y sólo deben recopilarse los datos personales necesarios para esas razones.
- Utilice los datos personales únicamente por motivos o para actividades concretas que ya haya planificado: los datos personales recogidos para un fin determinado sólo deben utilizarse para ese fin.
- Asegúrese de que sus conjuntos de datos son seguros y están bajo su control: los datos personales deben estar protegidos contra el acceso, la destrucción, el uso, la modificación o la divulgación/publicación no autorizados.
- Sea abierto sobre los datos que tiene y lo que hace con ellos: la información sobre qué datos personales se recogen y cómo se utilizan debe estar a disposición de los interesados.
- Respete el derecho de las personas a decidir cómo se muestran y utilizan sus datos: las personas tienen derecho a preguntar qué información se ha recopilado sobre ellas, para qué se utiliza y tienen derecho a que se modifique y, en ocasiones, a que se elimine (si los datos se recopilaron con su consentimiento).

- La FICR es responsable ante las comunidades a las que sirve, lo que incluye la forma en que utiliza sus datos: quienes recopilan y utilizan datos personales deben ser responsables ante las personas cuyos datos están utilizando y cumplir la legislación internacional o local aplicable.

Referencias

IFRC Data Protection Policy

7 - 9 ¿Qué datos necesitamos realmente?

Este ejercicio aborda los principios que rigen el uso responsable y la protección de datos a partir de un caso. Dos conceptos clave abordados en el caso son: la "minimización de datos" y la "privacidad desde el diseño".

¿Cuál es la "necesidad" a lo largo del ciclo de vida de los datos? Qué datos hay que recolectar, qué información hay que facilitar a los interesados (y a sus comunidades), quién debe tener acceso a los datos, qué hay que hacer para protegerlos si hay que compartirlos y cuánto tiempo hay que conservarlos antes de borrarlos.

- **Personas:** 4 a 20 personas
- **Tiempo:** 60 Minutos
- **Dificultad:** Intermedia
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

EJERCICIO

Parte 1: Explorar

En sesión plenaria, presente el ciclo de vida de los datos y resuma el objetivo del caso: debatir "¿cuáles son los datos que realmente necesitamos?".

Parte 2: Revisar

Los casos resultan más eficaces en pequeños grupos de discusión. En los grupos, los participantes deben presentarse y designar a una persona que tome notas. Revisar el caso:

Recolección de Datos Periódica/en Curso

Su SN gestiona un centro de salud local. Con el fin de prever mejor las necesidades de la comunidad, planificar los recursos necesarios y evaluar el grado de satisfacción con los servicios, usted recolecta habitualmente datos de las personas que visitan la clínica. Ha explicado a las familias de la comunidad los motivos de la recolección de datos. También les informó de que, si no querían facilitar parte de la información, podían seguir accediendo a los servicios sanitarios. Así pues, el consentimiento fue la base jurídica en la que se basó la recolección de datos, al menos con respecto a los pacientes que no tenían urgencias médicas.

- ¿Qué datos necesitaría recabar en el supuesto anterior (teniendo en cuenta que no somos expertos en medicina ni en aprovisionamiento)?
- Una vez evaluadas las necesidades, ¿qué hacer con los datos recogidos?

Justo antes de comenzar a recolectar datos, recibe una llamada de sus colegas, que le informan de que se está planificando una actuación con dinero en efectivo dirigida a la misma comunidad. Quieren que haga algunas preguntas más para no tener que volver a visitar a las familias en el futuro.

- ¿Qué información adicional se necesitaría para la entrega de efectivo?

- ¿Qué información adicional, en su caso, debe facilitar a los beneficiarios sobre los datos que desea recolectar en relación con el programa de dinero en efectivo?

Una ONG local se entera de su trabajo y quiere acceder a sus datos para basar en ellos sus propias intervenciones.

- ¿Es necesario compartir los datos?
- ¿Qué información debe compartirse si decide hacerlo?
- ¿Qué información adicional (u opciones) debe proporcionar a las personas antes de compartirla?

Un nuevo miembro del personal de TI le notifica que la base de datos de datos personales está disponible para el acceso de cualquier persona en la SN, y además está alojada en un servidor en la nube desprotegido.

- ¿Quién necesita acceder a los datos?
- ¿Qué hay que hacer para garantizar que se almacena de forma segura?

En un giro favorable de los acontecimientos, el gobierno local ha terminado un nuevo hospital y ha conseguido financiación para proporcionar asistencia sanitaria a largo plazo a la comunidad. Su SN puede cerrar la clínica y centrarse en otras iniciativas.

- ¿Qué datos hay que conservar?
- ¿Cuánto tiempo y de qué forma debe conservarse?
- ¿Podemos utilizar esos datos para otros fines?

Parte 3: Debatir

En sesión plenaria, invite a reflexionar y formular preguntas. Comparta más detalles sobre la política de Protección de Datos de la organización. Véase IFRC Data Protection policy.

Bono Extra

Se trata de un breve ejercicio para debatir conceptos relevantes. Si el equipo dispone de más tiempo, pida a los participantes que compartan ejemplos directamente de su trabajo relacionados con los dos conceptos "minimización de datos" y "privacidad desde el diseño".

Crédito

Tom Orrell, James De France

7 - 10 ¿Qué *podemos* hacer? vs. ¿Qué *debemos* hacer?

Parte de la comprensión de lo que significan el uso responsable y la protección de datos en un entorno humanitario consiste en ser capaz de reconocer la diferencia entre los dilemas éticos (buenas prácticas de uso responsable de datos) y las cuestiones jurídicas (protección de datos). Este ejercicio está diseñado para analizar estos conceptos desde un punto de vista más comprensible, replanteando los requisitos de protección de datos frente a los dilemas éticos como "qué PODEMOS hacer" (requisitos de protección de datos) frente a "qué DEBERÍAMOS hacer" (prácticas responsables de datos).

Este ejercicio está dirigido principalmente a los participantes que tienen un conocimiento y una comprensión limitados de la responsabilidad en materia de datos y la protección de datos y desean ampliar sus conocimientos. Al final del ejercicio, los participantes deberán ser capaces de identificar las diferencias entre los requisitos de protección de datos y las buenas prácticas de responsabilidad en materia de datos, y lo que esto significa para el modo en que deben abordar situaciones concretas.

- **Personas:** 4 a 16 personas
- **Tiempo:** 60 Minutos
- **Dificultad:** Fácil
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Ejercicio

Parte 1:

En pequeños grupos (preferiblemente en parejas), discuta: ¿qué significan para usted la protección de datos y el uso responsable de los mismos? ¿Cómo se aplican a nuestro trabajo?

Anote las ideas o preguntas en un documento compartido.

Parte 2:

Revise los supuestos y debata: "¿Qué ***podemos*** hacer? vs. ¿Qué ***debemos*** hacer? Cada grupo debe intentar realizar 2 supuestos.

Supuesto 1: Un amigo que trabaja en una organización asociada le pide algunos datos que sus colegas han recopilado recientemente sobre casos de VIH en una localidad concreta. Planean ofrecer apoyo médico/psicosocial adicional a la comunidad y necesitan saber dónde centrar sus actividades.

¿Puede compartir los datos? ¿Cumpliría el compartir los datos con los requisitos de protección de datos? En caso afirmativo, ¿debería compartir los datos? ¿Por qué sí o por qué no? Si decide compartirlos, ¿qué consideraciones debe tener en cuenta antes de facilitar la información? ¿Qué pasaría si en la comunidad hubiera un peligro concreto de violencia o estigma contra las personas seropositivas? ¿Y si su amigo trabajara en el gobierno? Y, aunque eliminemos los datos identificativos, ¿sigue habiendo riesgos al compartir la información?

- ¿Adónde acudiría para saber qué podría hacer?
- ¿Qué debemos hacer? Aunque las normas lo permitan, ¿hay otras razones para no compartir?
- ¿Qué no deberíamos hacer? ¿Y por qué?

Supuesto 2: Recientemente ha recolectado algunos datos de una comunidad local en una emergencia que contienen nombres, direcciones y otra información identificable. Su tableta/portátil se estaba quedando sin batería, así que hizo una copia de seguridad rápida

en un pendrive sin proteger los datos de ninguna manera (sin contraseña ni cifrado). Al volver a la oficina se da cuenta de que ha perdido el pendrive. ¿Qué hace? ¿Qué medidas podría tomar antes de ir a recolectar los datos para asegurarse de que, aunque perdiera la unidad donde haga una copia de seguridad, los datos seguirían estando a salvo?

- ¿Qué podemos hacer?
- ¿Qué debemos hacer?
- ¿Qué no deberíamos hacer?

Supuesto 3: Una gran empresa de tecnología se pone en contacto con su oficina y le ofrece ayuda gratuita para gestionar los datos de la oficina en caso de emergencia. ¿Debería aceptar esta oferta?

(Opciones: La empresa tecnológica #1 tiene un largo y reconocido historial de contribución a emergencias humanitarias y de trabajo con fines benéficos; la empresa tecnológica #2 tiene grandes contratos con gobiernos y otras empresas que podría considerarse que no respetan la privacidad u otros derechos humanos).

- ¿Qué podemos hacer?
- ¿Qué debemos hacer?
- ¿Qué no deberíamos hacer?

Parte 3:

Discuta los resultados en sesión plenaria. Pregunte qué otros dilemas éticos deberían considerar.

Bono extra

Revise la política de protección de datos de su organización con los participantes. Invite a su punto focal de TI o a su Responsable de Seguridad a compartir información sobre los riesgos digitales y de datos después del ejercicio de simulación. Esto podría proporcionar un contexto real para el trabajo de sus Sociedades Nacionales.

Recursos

Digital Dilemmas

IFRC Data Protection Policy

Crédito

Tom Orrell, Heather Leson

7 - 11 Pesadillas en materia de protección de datos

¿Cuál de estas situaciones podría quitarle el sueño?

- **Personas:** 4 a 12 personas
- **Tiempo:** 60 Minutos
- **Dificultad:** Fácil
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Instrucciones:

Divida a los participantes en pequeños grupos y pídales que piensen si alguno de los siguientes puntos podría quitarles el sueño. Una vez identificadas las posibles pesadillas, reúnalos de nuevo en el gran grupo para hablar de las políticas de protección de datos de sus organizaciones.

Ejercicio

Parte 1: Explorar

Divida a las personas en pequeños grupos y pídales que piensen si alguna de las siguientes situaciones les quita el sueño:

1. No obtuvimos el consentimiento
2. No disponemos de procedimientos adecuados de almacenamiento de datos.
3. De vez en cuando desaparece uno de nuestros portátiles/dispositivos.
4. No realizamos copias de seguridad de nuestros datos críticos
5. No detectamos el sesgo en nuestros datos
6. Podríamos tener acceso no autorizado a los datos
7. No tenemos claro qué datos pueden ser sensibles
8. Hemos estado compartiendo/publicando datos personales (información identificable) y no nos hemos dado cuenta
9. Las personas han optado por que no se utilicen sus datos, pero los hemos utilizado de todos modos
10. Nuestras políticas de datos no son lo suficientemente sólidas

Pregunte: ¿Hay alguna otra situación que le quite el sueño?

Parte 2: Debatir

Una vez que hayan identificado las posibles pesadillas, reúnalos de nuevo en gran grupo para hablar de las políticas de protección de datos de sus organizaciones. Comparta la política de de datos de su organización. Aborde con su equipo cualquier cuestión pendiente que pueda necesitar resolución. Esto también puede utilizarse con la planificación de la Transformación Digital para identificar las necesidades de la organización y del equipo. Véase - digital.ifrc.org.

Crédito

Dirk Slater

7 - 12 ¿Lo compartiría?

El intercambio responsable de datos puede ser difícil de poner en práctica. Aunque el intercambio de información es de vital importancia para el trabajo humanitario y de emergencia, a menudo hay dudas e incertidumbre sobre lo que debe o no debe compartirse, teniendo en cuenta las necesidades de protección de datos. Este ejercicio está diseñado para ayudar a los participantes a comprender mejor los fundamentos de la protección y el intercambio de datos y cómo se interrelacionan. La sesión se inspiró en el trabajo realizado por una Sociedad Nacional para formar al personal de la Unidad de Respuesta de Emergencia (ERU) antes de su despliegue.

La primera parte del ejercicio pretende brindar a los participantes una comprensión más fundamentada del uso responsable, la protección y la puesta en común de datos, partiendo de las percepciones de los propios participantes sobre qué información sobre sí mismos se sentirían o no cómodos compartiendo. La segunda fase plantea discusiones de grupo basadas en supuestos que reproducen ejemplos reales del ámbito humanitario en los que se plantean cuestiones de intercambio de datos. Estos supuestos pueden ser planteados por los propios participantes como parte del ejercicio, o presentados por el facilitador si hay una cuestión específica que deba abordarse.

- **Pesonas:** 4 a 12 personas
- **Tiempo:** 60 Minutos
- **Dificultad:** Intermedia
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores

Ejercicio

Parte 1: ¿Lo compartiría? 30mins

Divida a los participantes en pequeños grupos de no más de cuatro y pídales que discutan y respondan a cada una de las afirmaciones (a continuación). Cada individuo debe responder a las afirmaciones y las respuestas deben basarse en las preferencias personales. Esta parte del ejercicio debería durar unos 10 minutos. El contenido podría colocarse en una tabla o diagrama (dependiendo de si el evento es virtual o presencial.) Anime a los participantes a compartir ejemplos de su vida personal y ejemplos de trabajo. Tome nota de cualquier idea o pregunta en un documento compartido. A efectos de este ejercicio, céntrese en los datos personales (es decir, datos que solos o con otros datos pueden utilizarse para identificar a una persona física).

Afirmación:	Respuestas:
Es útil compartir este tipo de datos:	
Quiero compartir este tipo de datos:	
No quiero compartir (o no compartiré) este tipo de datos:	
No quiero compartir (o no compartiré) este tipo de datos:	
No tengo otra opción que compartir estos datos:	

Cuando se reúna todo el grupo, pida a los participantes que revisen las respuestas de los demás y que comenten las similitudes/diferencias. Puede preguntar a los participantes cómo cambiarían sus respuestas si vivieran en una situación de conflicto o desastre. Esta parte del ejercicio durará probablemente unos 20 minutos.

Parte 2: Aprendizaje basado en Supuestos (45-60 mins)

Para esta parte de la sesión, hay una serie de escenarios preparados (más abajo). También puede crear su propio supuesto específico para su organización. Se recomienda hacerlo con antelación con un compañero de equipo.

Caso 1: Datos de la Filial

Como parte de un programa de ayuda anterior, su filial de la SN recopiló datos sobre los beneficiarios que solicitaron atención médica por una enfermedad infecciosa. Los datos recopilados se almacenan en un archivo Excel que contiene los siguientes campos: Número de identificación (que no es una identificación oficial, sino un número asignado por su filial de la SN), afección médica, edad, región y localidad, número de hijos en el hogar, nivel de estudios y número de teléfono (si la persona tenía). El departamento de sanidad de la administración local le ha pedido que facilite los datos de las personas. ¿Qué tipo de datos compartiría o no compartiría? ¿Por qué? ¿Cuáles son las ventajas (o los riesgos) de compartir estos datos?

Caso 2: Datos sobre Ayudas en Efectivo y Vales

Tras un terremoto, una Sociedad Nacional intenta identificar a las personas que han perdido sus hogares, ya que pueden optar a una ayuda en efectivo o en forma de vales. Una asociación de la localidad más afectada se ofrece a compartir una lista de las personas que actualmente no tienen vivienda debido al terremoto. ¿Qué información pediría a la asociación que compartiera con usted? ¿Qué tipo de problemas cree que podrían surgir, por ejemplo, cómo ha recopilado los datos la propia asociación, hasta qué punto serán fiables, etc.? ¿Qué medidas podría tomar para mitigar estos problemas?

La sesión debe comenzar con el grupo definiendo una lista típica de tipos de datos que podrían compartirse durante el escenario. También deben hacer una lista de los tipos de datos que no deben compartirse. De este modo, se garantiza que los participantes compartan el mismo itinerario a medida que avanzan por los casos hipotéticos. (Nota: Puede que no todas las preguntas sean aplicables o que falte alguna información). Tome nota de cualquier idea o pregunta en un documento compartido.

Pregunta	Respuesta
¿Quién necesita los datos? ¿Cuál es su función? ¿Cuál es el objetivo de compartirlos?	
¿De dónde proceden los datos? ¿Quién tiene acceso a ellos? ¿Es posible publicar abiertamente los datos?	

Pregunta	Respuesta
¿Quién puede compartir los datos?	
¿Existe un registro de datos compartidos en el sistema y/o para la organización?	
¿Existe un acuerdo de intercambio de datos/MoU con la parte con la que se compartieron los datos?	
Si se comparten datos personales, ¿qué otros aspectos hay que tener en cuenta? ¿Se pueden agregar, seudonimizar o anonimizar los datos? ¿Puede/debe eliminar determinados campos?	
¿Existen condiciones de servicio y licencia para los datos?	
¿Qué funcionalidades de importación, exportación e intercambio de datos se necesitan y en qué formato?	

Bono Extra

Opcional: Creación de un nuevo supuesto: Los equipos pueden crear su propio caso para este ejercicio. Se recomienda hacerlo con suficiente antelación a la sesión con los compañeros de equipo.

- Conseguir que la gente hable de problemas reales relacionados con el intercambio de datos. El método utiliza supuestos como ejemplos, ya sean reales o hipotéticos. El componente interactivo permite visualizar los pasos y acciones para "simular" la toma de decisiones. Proporcióneles un ejemplo. A menudo, lo mejor es que alguien del equipo lo prepare antes de la sesión.
- O/ Impulsar una conversación sobre los "pasos para la realización" y los "requisitos" para compartir datos.

Crédito

Dirk Slater, Heather Leson, Arturo Garcia, Melissa el Hamouch, Tom Orrell, James De France

7 - 13 Lista de verificación de Limpieza de Datos

Estas son las categorías de datos que deben tenerse en cuenta al evaluar las necesidades de protección de datos.

Categorías de Datos	Notas
Información básica sobre la identidad, como nombre, ubicación (dirección, comunidad, etc.) y números de identificación.	
Datos web como ubicación, dirección IP, datos de cookies y etiquetas RFID	
Datos sobre la salud y genéticos	
Datos biométricos	
Datos raciales o étnicos	
Opiniones políticas	
Orientación sexual	

La segunda parte de este análisis consiste en asociar las categorías de datos a los siguientes términos formales:

Categorías de datos	Conjunto de datos	Notas
Datos no personales	Por ejemplo, datos logísticos como el número de vehículos de que dispone una sociedad nacional.	
	Etc	
Datos personales	Por ejemplo, nombres y direcciones de las familias que reciben ayuda en la comunidad.	
	Etc	
Datos sensibles	E.G. Datos biométricos, datos médicos, datos raciales o étnicos	
	Etc	
Datos sensibles de grupo	Por ejemplo, fotografías o imágenes de satélite que permitan identificar grupos vulnerables de personas, como campos de refugiados o pueblos indígenas	

7 - 14 La Rueda del Infortunio de los Datos

La Rueda del Infortunio de los Datos puede ayudar a suscitar el debate al tiempo que pone de relieve cuestiones relacionadas con la protección de datos y la alfabetización en materia de datos. Utilícela como introducción interactiva a la política de protección de datos de la organización.

- **Personas:** 2 a 24 personas
- **Tiempo:** 30 Minutos
- **Dificultad:** Media

Construir la rueda

Tiempo de realización: No más de 2 horas

Materiales

- hojas grandes de cartulina de 8 colores
- Tijeras
- Pegamento en barra
- Soporte para girar

Medidas: 50 × 50cm

17 secciones, unas 3-4 por cuarto

Identificación

Identifique 17 categorías. Las 17 que figuran a continuación se ofrecen a modo de ejemplo; siéntase libre de elegirlas y adaptarlas al contexto de sus participantes.

1. Consentimiento
2. Almacenamiento de datos
3. Pérdida de datos
4. portátil/dispositivo robado
5. Copias de seguridad
6. Sesgo de los datos
7. Plan de archivo
8. Acceso no autorizado a los datos
9. Comprender qué datos son sensibles
10. Fatiga de las encuestas
11. ¿Existen normas externas (por ejemplo, la IATI) que deberíamos adoptar?
12. Datos personales (información identificable)
13. Seguimiento de personas a través de los datos
14. La persona afectada opta por no utilizar los datos o se opone a ello
15. Datos erróneos/falsos
16. Ausencia de datos
17. Solicitud gubernamental de datos

Ejercicio

- Tener todas las categorías seleccionadas
- En la sesión, abra el debate haciendo que alguien gire la ruleta para elegir el tema. Pregunte a los participantes si tienen alguna anécdota o pregunta al respecto. (Haga unas cuantas rondas para iniciar el debate y, a continuación, pase a otros temas clave que consideren que faltan o que son prioritarios, desde carencias hasta oportunidades).

Después de la sesión, déjelo en el pasillo (o en versión digital) con algunas notas en las que pida a los participantes que compartan de forma anónima sus historias sobre datos o cuestiones relacionadas con la responsabilidad en materia de datos que consideren prioritarias.

Recursos:

- How to Build a Wheel of Fortune Wheel (with Pictures) – wikiHow
- How To Make Pinwheels – Paper Source
- How We Made Wheel of Fortune From Cardboard – PLAYTIVITIES

Crédito

Heather Leson

7 – 15 Simulación de Datos PMER

En esta sesión, utilizaremos un ejemplo de emergencia para guiar las conversaciones sobre riesgos, roles, decisiones, lagunas y necesidades de evidencia para nuestro trabajo. Se utilizará con Fortalecer Equipos y Proyectos de Datos (3) (Módulo 3).

Caso: Deportación masiva de trabajadores inmigrantes de Randowsa

El país Randowsa cuenta con trabajadores migrantes regulares e irregulares. El gobierno de Randowsa aplica políticas para impedir la migración irregular y que los trabajadores trabajen sin la documentación necesaria.

Debido a la reciente inestabilidad política, el gobierno de Randowsa está aplicando sus políticas relativas a los trabajadores migrantes irregulares, lo que ha provocado el temor de los trabajadores migrantes a ser detenidos o deportados. En los últimos siete días, más de 400.000 personas han abandonado el país atemorizadas, muchas voluntariamente, otras deportadas, y las empresas están siendo multadas con elevadas sumas si se descubre que han empleado a trabajadores irregulares. Muchos de los migrantes han cruzado la frontera de Dakandka. Se está formando un campamento cada vez mayor y la CRMLR está intensificando sus actividades para dar apoyo a los complejos mandatos.

PMER ha sido contratado para brindar apoyo a los esfuerzos de los distintos sectores en el diseño de encuestas junto con las Sociedades Nacionales, así como para planificar el proceso de recolección de datos móviles. Usted dirige un proyecto de recolección de datos móviles en el que participan varias Sociedades Nacionales. El procesamiento de los datos se lleva a cabo en el país, así como mediante ayuda a distancia a través de los equipos de apoyo a la gestión de la información (equipos SIMS) en las Sociedades Nacionales, así como de un procesador externo (un grupo de investigación). Se realizan encuestas periódicas sobre salud, alojamiento, aseo y Prevención de la explotación y los abusos sexuales (PSEA, por sus siglas en inglés) para recopilar información exhaustiva con entrevistas a informantes clave. Cada una de las encuestas es diferente y está a cargo de distintas Sociedades Nacionales. Recientemente se ha completado una revisión de todas las encuestas.
El informe ha suscitado mucho interés. La mayoría de los socios están preocupados por el empeoramiento de la situación, aunque algunos se muestran escépticos ante las cifras. El Gobierno es especialmente crítico con las cifras.

Ejercicio

Cada equipo de 3 a 4 personas dispone de 30 minutos para tomar decisiones y abordar las cuestiones clave.

Cuestiones clave

- ¿Cuáles son algunos de los riesgos, carencias y necesidades? Cómo salvaguardará los workflows de datos para proteger a los más vulnerables?
- ¿Cuáles son algunos de los pasos, roles y decisiones de esta iniciativa?
- ¿Cuál es el conjunto mínimo de datos que puede compartirse y con quién? ¿Por qué?

Your Decision Points

Ha recibido una solicitud de los datos de la última realización de la encuesta por parte de los siguientes actores. ¿Deberíamos compartir los datos con este actor? ¿Y en qué fase del proceso lo haría? ¿Cómo gestionará/compartirá los datos con proveedores externos?

1. La unidad PMER de la FICR quiere examinar los datos para ver si pueden hacer un gráfico convincente a partir de ellos para acompañar un comunicado de prensa que se hará sobre el empeoramiento de la situación. Han solicitado el conjunto completo de datos.
2. La Oficina del Gobernador y las regiones más afectadas identificadas en la última encuesta dicen que les gustaría tomar medidas y necesitan los datos.
3. El responsable de proyectos de los donantes desea ver los datos.
4. Uno de los informantes clave/miembros de la comunidad que participó en la encuesta y cree que su informe no refleja con exactitud el problema en su zona.

Crédito

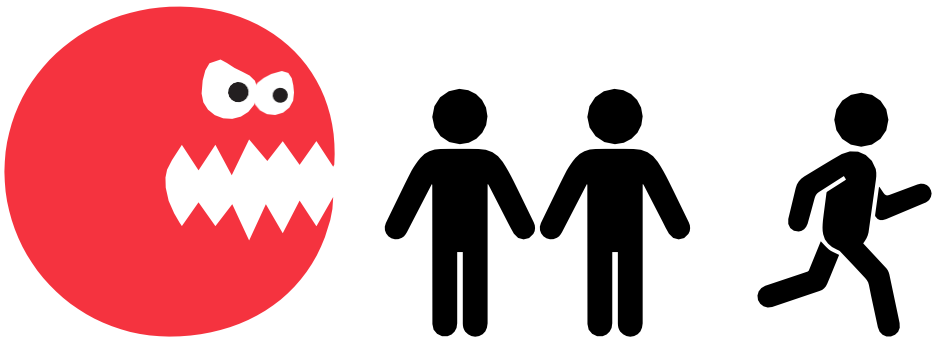
Equipo de Migración de la FICR, Heather Leson, Miki Tsukamoto

7 - 16 Las Personas antes que los Datos (folleto)

Crédito

Jennifer Chan

El Pasado



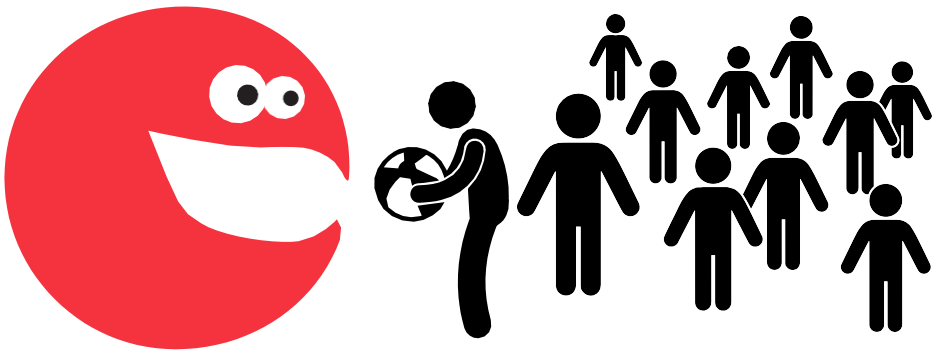
Recolección de Datos

Tal vez ahora

Medición de datos

Las personas y los datos aprenden a dialogar

El Futuro



Medición de datos

Las personas aprovechan los datos con un propósito y un significado

7 - 17 Seguimiento de la campaña de polio en Siria

Caso

La Media Luna Roja de Qatar realiza el monitoreo por parte de terceros de una campaña contra la poliomielitis en Siria. Cuenta con el apoyo de la Organización Mundial de la Salud (OMS).

Cuando revise el caso que se expone a continuación, considere las siguientes cuestiones relativas a qué medidas de protección de datos (en particular, suministro de información) y de responsabilidad en materia de datos deben tenerse en cuenta a lo largo de la campaña.

- ¿Cuáles son algunos de los riesgos, carencias y necesidades relacionados con el apoyo a la campaña? ¿Cómo salvaguardará los workflows de datos para proteger a los más vulnerables?
- ¿Cuáles son algunos de los pasos, roles y decisiones de esta campaña?
- ¿Cuál es el conjunto mínimo de datos que puede compartirse y con quién? ¿Por qué y qué cuestiones deben tenerse en cuenta antes de compartirlos?
- ¿Debemos basarnos en el consentimiento para la recolección de datos y, en caso afirmativo, cómo se obtendrá?
- ¿Cómo deben almacenarse y, en su caso, transmitirse los datos?
- ¿Algún otro aspecto relacionado con la protección o responsabilidad en materia de datos?

El workflow del equipo es el siguiente:

1. Prepare formularios de recolección de datos en papel. (Nota: asegúrese de definir claramente qué datos pueden y deben recolectarse. Cumpla las directrices aplicables sobre protección de datos (leyes y/o políticas).
2. Introduzca los campos de datos en la plataforma de recolección de datos (DHIS2).
3. Un controlador recolecta los datos de los centros y las comunidades.
4. Un supervisor, responsable de dirigir un equipo de controladores en un área de notificación definida, proporciona actualizaciones al supervisor de distrito.
5. El supervisor de distrito puede proporcionar informes consolidados sobre la campaña.
6. Los encargados de realizar los reportes analizan los datos recolectados y extraen informes previamente definidos para mostrar los indicadores de vacunación que luego se comparten con la OMS y el Grupo de Trabajo de inmunización.

El monitoreo por parte de terceros se desarrolla en tres fases principales durante la campaña:

1. Pre-campaña (visitas a los centros y comprobación de la preparación de los centros, las vacunas y el equipo de vacunación).
2. Intra-campaña (durante la campaña, los controladores comprueban el progreso de la vacunación en los centros y visitan los hogares y los mercados para controlar la cobertura de la campaña de vacunación).
3. Pos-campaña (después de la campaña, los monitores visitan los hogares y los mercados para recopilar datos sobre la cobertura de la campaña).

Solemos visitar los centros de vacunación uno o dos días antes de la campaña para comprobar la preparación del centro y del equipo, y asegurarnos de que todo marcha según lo previsto.

Además, elegimos a personas al azar en los mercados y les preguntamos si saben algo de la campaña y de la vacuna y dónde se han enterado.

Antecedentes

En marzo de 2016, en la fase previa a la campaña, un organismo independiente de la zona asediada de Homs analizó los datos y detectó algún problema en los viales de la vacuna. Enviamos fotos de los viales a la OMS, y decidieron suspender la campaña hasta que tuvieran una nueva vacuna.

La importancia de la fase de precampaña no es solo comprobar la vacuna y el equipo de vacunación, sino también recopilar información de un lugar específico para medir el conocimiento de la población sobre la campaña y la vacuna.

En agosto de 2017, los indicadores de precampaña mostraron una disminución del conocimiento sobre la campaña. El 40% de las personas no sabían nada de la campaña, que debía comenzar al día siguiente. Por lo tanto, la campaña se pospuso una semana más.

Crédito

Hesham Othman Hassan y Nami Ghadri, Sociedad de la Media Luna Roja de Qatar

7 - 18 Monólogos de datos

Un " Monólogo de datos " es un resumen de una "enseñanza sobre un proyecto de datos" o de un "fracaso en materia datos". Las personas presentan el caso, los problemas, las medidas de mitigación y los resultados.

RESPONSABILIDAD EN MATERIA DE DATOS ES:

"Responsabilidad en materia de datos en la acción humanitaria es la gestión segura, ética y eficaz de los datos personales y no personales para la respuesta operativa".

Protección de datos:

Protección de datos se refiere a un conjunto de principios y prácticas establecidos para garantizar que todos los datos personales recolectados y utilizados por, o en nombre de, la Federación sean precisos y pertinentes, y que los datos personales no se utilicen indebidamente, se pierdan, se corrompan o se compartan y accedan indebidamente.. (Política de la FICR sobre Protección de Datos Personales)

La protección de los datos personales de las personas es parte integrante de la protección de su vida, integridad y dignidad. Por ello, la Protección de Datos Personales reviste una importancia fundamental para las Organizaciones Humanitarias.. (Bruselas Privacy Hub/ICRC Handbook on Data Protection, CICR, 2017)

Objetivos de la Sesión

La siguiente es una sesión de 1 hora a 1,5 horas para ayudarle a usted y a su equipo a hablar sobre el Uso Responsable de Datos y las Directrices de Protección de Datos. Objetivos de esta sesión:

- Crear defensores y expertos que apoyen el uso responsable de los datos en la respuesta humanitaria.
- Desarrollar un lenguaje común en torno al uso responsable de los datos.
- Fomentar la protección de datos y la alfabetización responsable en materia de datos para la CRMLR.
- Introducir políticas de protección de datos, obtener aportaciones para las necesidades de formación.
- Introducir el Manual sobre Protección de Datos en la Acción Humanitaria Internacional (2ª edición, CICR/Brussels Privacy Hub Publication)

- **Personas:** 12 a 24 personas
- **Tiempo:** 90 Minutos
- **Dificultad:** Fácil
- **Materiales Virtual:** plataforma de reunión virtual, documento/ espacio de escritura compartido
- **Materiales Presencial:** Rotafolios/pizarras, notas adhesivas, rotuladores
- **Preparación:** Pida a 3 ó 4 personas que le ayuden a guiar la sesión. Explíqueles los objetivos, metodología y resultados de la reunión. Asígneles diferentes áreas del espacio.

  - Disponer las sillas o mesas en círculo o en pequeños grupos/Utilizar salas para sesiones virtuales
  - Colocar carteles de bienvenida en la puerta/ Disponer de un espacio de documentación compartido
  - Cada grupo necesitará:
  - Facilitador asignado
  - Tomador(es) de notas designado(s).
  - Ejemplos de casos en formato impreso y digital

- Dé la bienvenida a todos a medida que se incorporen. Pida a los participantes que guarden sus portátiles y teléfonos. Comience y finalice puntualmente.

Compartir de manera saludable

- Sería aconsejable fomentar un espacio de confianza utilizando las "reglas de Chatham House" – centrarse en el tema y las lecciones más que en las personas/organización/división.
  - "una norma o principio según el cual la información divulgada durante una reunión puede ser comunicada por los presentes, pero la fuente de dicha información no puede ser identificada explícita o implícitamente"

Facilite a los participantes el siguiente resumen: El objetivo de la sesión es compartir y actualizar a los participantes sobre la creciente atención que se presta a las prácticas responsables en materia de datos, incluido el Manual del CICR sobre Protección de Datos en la Acción Humanitaria, la Política de Protección de Datos de la FICR, la IATI y otros temas relacionados.

Antecedentes de la sesión: El tratamiento más fácil y más rápido de cantidades cada vez mayores de datos personales ha suscitado preocupaciones éticas sobre el equilibrio entre la transparencia y el acceso abierto a la información y las cuestiones de confidencialidad y la posible intrusión en la esfera privada de las personas. Desde el punto de vista organizacional, esto exige prestar atención a las prácticas responsables en materia de datos, la planificación de la protección de datos y la alfabetización general en materia de datos, transparencia y confidencialidad. Así, organizaciones como la FICR, el CICR, CRS y Oxfam han publicado o están trabajando en políticas de datos. En esta sesión se compartirán lecciones y consideraciones clave sobre este tema.

¿Qué es un Monólogo de datos?

- Un " Monólogo de datos " es un resumen de una "enseñanza sobre un proyecto de datos" o de un "fracaso en materia datos". Las personas presentan el caso, los problemas, las medidas de mitigación y los resultados.
- El grupo compartirá algunas historias de proyectos basados en datos, seleccionará el mejor ejemplo de una cuestión compleja y, a continuación, preparará un "pitch" para ilustrar algunas cuestiones/observaciones fundamentales.
- Los "Monólogos de datos" pueden incluir nombres de personas u organizaciones eliminados. Se aplicarán las normas de Chatham House (es decir, pediremos a los participantes que no compartan la información hasta que se les conceda permiso). Los participantes describirán el problema, los riesgos, las medidas paliativas adoptadas, los resultados y lo que podría mejorarse.

Parte 1: Monólogos de datos: Debate en pequeños grupos (20 minutos)

- Dividirse en grupos de 4 o 5 personas
- Compartir historias de datos durante 20 minutos
- Cada persona comparte un ejemplo de problemas/situaciones con los que se ha encontrado.
- Intente utilizar ejemplos personales o de su organización, en lugar de ejemplos de terceros.

Parte 2: Monólogos de datos (40 minutos)

- Elija uno de los ejemplos para compartirlo en sesión plenaria, incluyendo lo sucedido, los resultados y las medidas adoptadas para mitigarlo.
- El facilitador del grupo documenta las preguntas/conceptos básicos en rotafolios.
- Regresar a la sesión plenaria

- El "pitch" del monólogo de datos debe ser como una charla "Pecha Kucha" o "ignite": resumen, lecciones y próximos pasos. El monólogo no debe durar más de cinco minutos. Habrá entre 4 y 5 presentaciones (pitches).

Parte 3: Añadir Protección de Datos y Uso Responsable de Datos (15 minutos)

- Durante los debates, los participantes inevitablemente abordarán cuestiones como el consentimiento, la filtración de datos, el intercambio de datos, el almacenamiento de datos, la protección de datos, etc.
- Prepare diapositivas para ilustrar estos términos clave.
- Proporcionar recursos para profundizar en la aplicación de la protección y el uso responsable de los datos en la labor humanitaria.

Parte 4 Concluir (10 minutos)

- Finalice con una rápida ronda pidiendo a los participantes que compartan un único "aha" o aprendizaje de los monólogos antes de terminar.

Después de la sesión:

- Recopile las preguntas clave de los grupos.
- El ejemplo "Monólogos de datos" sólo debe volver a utilizarse si está permitido.
- Envíe notas de agradecimiento a los ayudantes y participantes.

Recursos

Heather Leson and PMER Network, IFRC Data Protection Policy, IASC Operational Guidance on Data Responsibility