Uso de los datos sensibles

Orientación para el tratamiento de datos sensibles

Índice de contenidos

Uso de los datos sensibles 1

Orientación para el tratamiento de datos sensibles 1

Justificación 1

Ámbito de aplicación 1

¿Qué son los datos sensibles y por qué son diferentes de otros tipos de datos personales? 2

Definiciones de la terminología clave 2

Planeación 5

Planeación de la recolección de datos 7

Recolección de datos 8

Almacenamiento de datos 8

Análisis de datos 8

Presentación de datos al donante, al socio o a un tercero (si corresponde) 9

Preguntas frecuentes 9

Documentos relacionados: 11

Justificación

La mayoría de los programas y demás actividades de Mercy Corps recolectan algún tipo de información personal sobre las personas a las que servimos y con las que trabajamos, y muchos de ellos también recolectan información sobre personas que se clasificaría como sensible. La recolección de datos sensibles es esencial para que podamos llevar a cabo nuestro trabajo y servir a los participantes del programa y a las comunidades en las que trabajamos. Por lo tanto, al recolectar y utilizar datos sensibles, es de suma importancia que se tomen todas las medidas necesarias para garantizar la protección de dichos datos. La falta de protección de los datos sensibles puede provocar graves perjuicios a los Datos Persona de interés, entre ellos la discriminación y las amenazas a su seguridad.

Ámbito de aplicación

Estas directrices rigen para todo el tratamiento de datos sensibles de toda la agencia. Se aplica a los datos sensibles recolectados con fines programáticos y operativos y a cualquier otra situación en la que haya datos sensibles. Este documento detalla los pasos necesarios siempre que se procesen datos sensibles.

¿Qué son los datos sensibles y por qué son diferentes de otros tipos de datos personales?

Los datos sensibles suelen ser datos como el perfil cultural de una persona, su orientación sexual, datos médicos, biométricos y genéticos. Son datos que, si se divulgan, acceden o comparten indebidamente, podrían provocar:

- un perjuicio (como sanciones, discriminación y amenazas a la seguridad) para una persona, lo que incluye a la fuente de la información u otras personas o grupos identificables;
- un impacto negativo en la capacidad de una organización para llevar a cabo sus actividades o en la percepción pública de dicha organización.

Ejemplo 1:

Un programa trabaja en una comunidad y, durante el proyecto, varios participantes revelan que son seropositivos. Esta información se comparte accidentalmente con miembros de alto nivel de la comunidad, lo que puede suponer un daño significativo e incluso un peligro físico para los participantes en el programa.

Ejemplo 2:

Una oficina está planeando una celebración y está recolectando los requisitos dietéticos de los miembros del equipo. Varios miembros del equipo han indicado que requieren comidas Kósher o Halal. Se comparte con todo el equipo una hoja de cálculo en la que se identifican los miembros del equipo que tienen requisitos dietéticos específicos. Algunos miembros del equipo no compartieron su religión porque les preocupa la discriminación.

Los datos sensibles se deben tratar con mayor cuidado, ya que es más probable que su recolección y uso interfieran con los derechos o libertades fundamentales de una persona, o que causen un daño significativo, lo que incluye a la discriminación o el peligro físico, si se utilizan indebidamente.

El Reglamento General de Protección de Datos (RGPD) define una serie de tipos de datos que se clasifican como datos sensibles de categoría especial y detalla las condiciones específicas de tratamiento para estos tipos de datos. Sin embargo, es importante tener en cuenta que en algunos contextos, aún los datos que están por fuera del estándar de categoría especial pueden ser confidenciales debido a un contexto específico. A efectos de la presente nota orientativa, estos tipos de datos se denominarán datos contextualmente confidenciales.

Esta nota orientativa tiene la intención de cumplimentar la Política de Datos Responsables de Mercy Corps, como también la Política para la Gestión de programas (que también incorpora a la Política MEL de la agencia) y rige para la recolección datos sensibles en todos los contextos, lo que no se limita a los datos de la sede, los programáticos y los de MEL.

Definiciones de la terminología clave

- **Datos operativos de Mercy Corps**: cualquier unidad de información, compuesta por letras, números, símbolos, imágenes, grabaciones de vídeo y voz, coordenadas geoespaciales o identificadores de ubicación, cartografía o cualquier combinación de los mismos procesada por

Mercy Corps. Esto no se limita simplemente a los datos de los miembros del equipo de Mercy Corps, proveedores, donantes o socios. Los datos existen tanto en formato físico como digital.

- **Datos sensibles:** por lo general, esta información se utiliza como base para apuntar a un grupo o individuo en particular. Los ejemplos más comunes son: raza, religión, opinión política, orientación sexual, salud o información biométrica.

  A los efectos de esta nota, los datos sensibles incluirán los “datos sensibles de categoría especial”, tal como se indica en el RGPD, y los “datos contextualmente confidenciales”

- **Datos sensibles de categoría especial:** el GDPR establece los requisitos específicos que se deben cumplir para el tratamiento de todos los datos sensibles de categoría especial. El RGPD define los datos sensibles de categoría especial como:

  - datos personales que revelan el origen racial o étnico;
  - datos personales que revelen opiniones políticas;
  - datos personales que revelen creencias religiosas o filosóficas;
  - datos personales que revelen la pertenencia a un sindicato;
  - datos genéticos;
  - datos biométricos (cuando se usan para identificación);
  - datos relacionados con la salud;
  - datos relacionados con la vida sexual de la persona y
  - datos relacionados con la orientación sexual de la persona

- **Datos contextualmente confidenciales**: datos que no entran en las categorías de datos sensibles definidas por el RGPD, pero que, debido al contexto en el que se tratan, son confidenciales por su naturaleza y podrían causar un daño significativo Datos Persona de interés si se revelan.

- **Filtración de datos personales**: a una filtración de datos personales se la puede definir en términos generales como un incidente de seguridad que afectó la confidencialidad, integridad o disponibilidad de los datos personales. En resumen, habrá una filtración de datos personales siempre que se pierdan, destruyan, corrompan o divulguen datos personales; si alguien accede a los datos o los transmite sin la debida autorización; o si los datos dejan de estar disponibles, por ejemplo, cuando fueron cifrados por un ransomware,o secuestro de datos, o se perdieron o destruyeron accidentalmente.

- **Datos del programa**: cualquier unidad de información, compuesta por letras, números, símbolos, imágenes, grabaciones de vídeo y de voz, o cualquier combinación, relacionada con los participantes, la ejecución y los resultados del programa. Los datos existen tanto en formato físico como digital.

- La **Política de datos responsables** de **Mercy Corps** se utiliza para establecer principios para el uso transparente, seguro y responsable de los datos personales en la agencia e incorporar esos principios a nuestro trabajo diario.

- **Consentimiento informado**: proceso para obtener el permiso voluntario para recolectar datos de cualquier tipo, a partir de una clara apreciación y comprensión de los hechos, implicaciones y consecuencias de cualquier compromiso de los participantes. Este acuerdo se puede hacer mediante una declaración verbal o escrita o una clara acción afirmativa. El acuerdo se debe obtener en el momento de la recolección de los datos personales, o tan pronto como sea posible posteriormente.

- **Consentimiento explícito**: el consentimiento explícito requiere una declaración de consentimiento muy clara y específica. Debe quedar constancia del momento y manera en que se obtuvo y de lo que se dijo exactamente a los Datos Persona de interés cuando se lo obtuvo. El consentimiento explícito debe especificar la naturaleza de los datos de categoría especial y debe ser independiente de cualquier otro consentimiento solicitado.

- **Desidentificación**: todos los métodos o actividades de procesamiento de datos que funcionan para evitar que se revele la identidad de la persona de interés. Tipos: Anonimización (la eliminación de ciertas cantidades de datos personales, o la aplicación de un rango de valores a través de ciertos conjuntos de datos personales) y seudonimización (el tratamiento de datos personales de tal manera que los datos personales ya no se pueden atribuir a los Datos Persona de interés específicos o a un grupo de Datos Persona de interés sin el uso de información adicional, como identificaciones o etiquetas únicas).

- **Información de identificación personal (PII por sus siglas en inglés)**: información que está relacionada con una persona física identificada o identificable (“Datos Persona de interés”); una persona identificable es una persona que puede ser identificada, directa o indirectamente, especialmente mediante referencia a un número de identificación o a uno o más factores específicos de su identidad física, fisiológica, mental, económica, cultural o social. Esto tiene una estrecha relación con la **Información de identificación demográfica (DII)**, que se puede usar para identificar a una comunidad o a un grupo en particular, ya sea geográfico, étnico, religioso, económico o político.

- **Almacenamiento seguro**: solo los miembros necesarios del equipo de Mercy Corps pueden acceder a los datos; se deben tomar medidas para evitar el robo y el uso indebido de los datos. Almacenamiento seguro: solo los miembros necesarios del equipo de Mercy Corps pueden acceder a los datos; se deben tomar medidas para evitar el robo y el uso indebido de los datos. Un archivo está almacenado de forma segura cuando:
  - Vive en una plataforma que tiene o cumple con fuertes estándares de seguridad, protección de datos y privacidad
  - Solo se permite el acceso a las partes necesarias
  - El acceso se revisa regularmente y se ajusta según sea necesario

- Se establecen requisitos adicionales para los programas de Mercy Corps en la recientemente adoptada Política MEL, en particular el Estándar 9, que requiere que todos los programas

garanticen prácticas de manejo seguro, en línea con la Política de Datos Responsables y los requisitos de los donantes.

- **Miembros necesarios del equipo de Mercy Corps**: miembros del equipo que requieren acceso a la información identificada para cumplir con las tareas específicas de su trabajo, como atender las necesidades de los participantes del programa y completar los resultados del mismo

- Datos Persona de interés**:** cualquier individuo del que se recolectan datos directa, indirectamente o a través de un tercero, y que puede ser identificado, directa o indirectamente, en particular por referencia a los datos personales.

- **Protección de datos**: salvaguardar e impedir el acceso, el uso o la distribución no autorizados de la Información de identificación personal (PII), la Información de identificación demográfica (DII) y otros datos sensibles sobre un individuo o un grupo a lo largo del ciclo de datos de la gestión del programa o proyecto, o tras la finalización del programa o proyecto. La Política de Datos Responsables de Mercy Corps describe los requisitos de protección de datos, y la agencia también está sujeta a otros marcos legales o regulatorios como el del Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Para más definiciones relacionadas con los datos responsables, consulte el documento Definiciones de datos responsables.

Planeación

- Considere los tipos de datos que se recolectarán y documéntelo en la fase de planeación del proyecto, en la Evaluación de impacto en la privacidad (PIA).

- Cuando un plan incluya la recolección, documentación o el almacenamiento de cualquier tipo de datos sensibles, se deberá prestar especial atención a la manera y al motivo del uso de los datos. Considere si la recolección de estos datos es necesaria para obtener los resultados requeridos por el programa o proyecto o si podría bastar otro tipo de datos. Solo si es necesario, se debe recolectar los datos sensibles. Tenga en cuenta que la recolección de datos sensibles, si se hace bien, es un proceso costoso. Al eliminar la carga de la recolección de datos innecesarios, permite a los equipos ahorrar tiempo y recursos para otras tareas necesarias. Si identifica que la PII es necesaria, no aplique atajos. Si los recursos asignados para la recolección y gestión de datos sensibles no son suficientes para hacerlo bien, reconsidere la posibilidad de sopesar todos los riesgos a los que podría someter a las comunidades con las que trabaja.

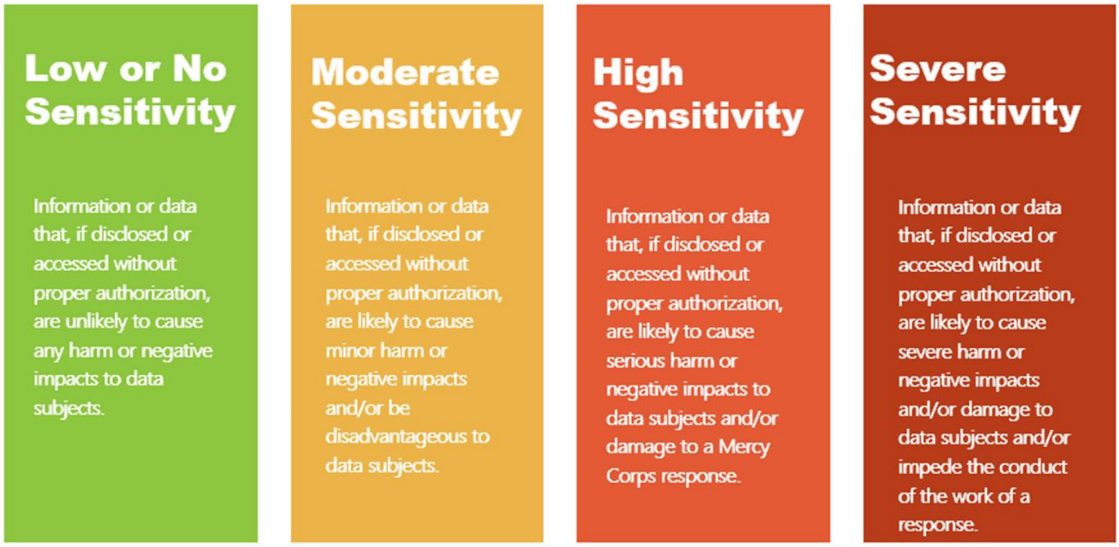
- Considere las tecnologías que se utilizarán para la recolección y el almacenamiento. Las tecnologías utilizadas deben incluir las salvaguardias adecuadas para la recolección de información confidencial.

- En general, cuanto más sensibles sean los datos, más salvaguardias habrá que tener. Los datos sensibles suelen ser de sensibilidad “alta” o “severa” (consulte la figura 1). Además, cuanto mayor sea la cantidad de conjuntos de datos recolectados, mayor será el riesgo y mayor la cantidad de salvaguardias a usar. Algunos ejemplos de salvaguardias son:

    - Cifrado
    - Seudonimización
    - Disociación
    - Almacenamiento de archivos de papel en armarios cerrados con acceso restringido
    - Almacenamiento de archivos en servidores de Mercy Corps con niveles de protección
    - Restringir el acceso a los dispositivos de Mercy Corps y solo a aquellos que deban tener acceso para realizar sus tareas
    - Garantizar que los dispositivos, como los equipos móviles estén bloqueados cuando no se utilicen
    - Para los datos espaciales, aleatorizar o agregar los puntos GPS

- Tenga en claro los fundamentos jurídicos para el tratamiento de datos sensibles que se utilizará y planee en consecuencia.
- Los requisitos de presentación de informes en los acuerdos de subsidio deben respetar los principios de “no hacer daño” (por ejemplo, no se espera que el programa recolecte información que pueda comprometer la seguridad de los participantes) y se describen claramente los compromisos y acuerdos para las plataformas de divulgación de datos, los procesos con los donantes, los socios y otras partes interesadas, incorporando los requisitos de desidentificación y anonimización.
- El protocolo de seguridad de los datos a nivel de programa forma parte del plan tecnológico de MEL (Estándar 6) y describe las consideraciones sobre los datos de los miembros del equipo, lo que incluye a los niveles de permiso y los protocolos para los miembros del equipo de MC y los que no lo son.
- Cuando se recolecten datos sensibles para los fines operativos de Mercy Corps, planee y esboce las consideraciones relativas a los datos, lo que incluye a los niveles de permiso y los protocolos.
- Debe pensar y poder justificar el tiempo que hay que conservar los datos (período de retención), lo que dependerá de las razones para recolectarlos, los requisitos legales, los requisitos de los donantes y las políticas de retención de registros del programa de MC.
- Disponga de un proceso para la destrucción de los datos cuando se cumplan los períodos de conservación.

Cuadro 1:



Planeación de la recolección de datos

- Se completa una Evaluación de impacto en la privacidad para identificar y manejar los riesgos de la privacidad relacionados con una nueva actividad, por ejemplo, nuevos programas, tecnología o políticas. Cuando se vayan a recolectar datos sensibles, los deberá revisar una persona competente. Esta sería el equipo de Protección de Datos y Privacidad, su DPO o según la Política MEL, (Estándar mínimo 9 – Privacidad y Seguridad de los Datos):
    - Responsable: Director de País, o Director de Programas y Gerente de Programa o Jefe de Parte
    - Responsable recomendado -Programa MEL/Líder de gestión del conocimiento

- Complete una Evaluación de información confidencial (SIA) que está relaciona con la PIA. Esto debe documentar todas las salvaguardias adicionales que se empleen para los datos sensibles.

- Si el consentimiento es el fundamento jurídico en el que se basa, el consentimiento informado requiere que se informe a los Datos Persona de interés de lo siguiente en un lenguaje sencillo:

    - Los datos que se recolectan y el motivo por el que son necesarios

    - Con quién se compartirán, lo que incluye a los socios y donantes externos

    - Si los datos se compartirán a nivel internacional

    - El tiempo que se conservarán los datos

- Debe quedar constancia de cuándo y cómo se ha recolectado el consentimiento y lo que se le dijo a los Datos Persona de interés. En la fase de planeación se debe incluir un modelo de lo que se dirá a los Datos Persona de interés para obtener el consentimiento.

Recolección de datos

- Existe un protocolo de recolección de datos para cada de sus instancias, lo que incluye:
    - Salvaguardias adicionales para los datos sensibles
    - Instrucciones documentadas para la recolección, limpieza, revisión y desidentificación de los datos, según proceda.
    - Instrucciones para posibles violaciones de la seguridad de los datos para todos los datos cuantitativos y cualitativos recolectados (por ejemplo, dispositivos perdidos o robados, inicios de sesión comprometidos, etc.)
    - Instrucciones para el uso y la protección de los formularios impresos durante la recolección
    - Controles puntuales y supervisión del nivel de cumplimiento de los protocolos de salvaguardia y protección por parte de la persona o personas encargadas de la recolección de datos
- Todo lo anterior debe estar vinculado a la SIA

Almacenamiento de datos

- Los archivos que contengan información confidencial deben estar restringidos a los miembros del equipo que necesiten acceder a esta información para completar los resultados necesarios, y la desidentificación sistemática de la información confidencial se lleva a cabo antes de vincularla a TolaData o de compartirla con terceros, según corresponda. El Estándar 8 de la política MEL proporciona orientación adicional sobre las mejores prácticas sobre el archivado y almacenamiento de datos
- Los datos se almacenan en un lugar que cumple con todas las políticas pertinentes de Mercy Corps (por ejemplo: Política de Datos Responsables, Uso Aceptable).
- No se deben conservar datos sensibles por más tiempo del necesario. Cuando se cumplan los periodos de conservación, los datos se deben destruir de forma segura o anonimizarse por completo.
- Se debe documentar y justificar los periodos de conservación.
- Recuerde: los datos también se pueden almacenar en sistemas móviles de recolección de datos. Todas las consideraciones sobre el almacenamiento de datos señaladas anteriormente también se aplican a los sistemas móviles de recolección de datos.

Análisis de datos

- Existe un protocolo para compartir datos con consultores, equipos de la sede central, socios y partes interesadas, que no se limita a los acuerdos para la divulgación de datos, aprobaciones por parte del MEL del país, funciones y responsabilidades, etc.
- Todos los consultores firman acuerdos de no divulgación (NDA) antes de acceder a cualquier conjunto de datos propiedad de Mercy Corps.

Presentación de datos al donante, al socio o a un tercero (si corresponde)

- Los datos sin procesar se desidentifican y se revisan para que cumplan con los principios de “no hacer daño” antes de su presentación.
- No se debe compartir datos sensibles con ningún tercero que no haya sido mencionado como parte del proceso de consentimiento informado.
- No se debe compartir datos sensibles con ningún tercero a menos que exista un acuerdo de divulgación de datos.
- Utilice únicamente sistemas organizativos autorizados, como Google Drive o Microsoft Sharepoint, para compartir documentos, y no plataformas de intercambio de terceros.

Preguntas frecuentes

Para garantizar el cumplimiento de los requisitos de diversidad, pedimos a los miembros del equipo que indiquen su condición étnica en los formularios de solicitud de empleo. ¿Debo hacer algo con esa información?

Sí, los datos sobre el origen racial o étnico se consideran datos personales confidenciales, por lo que deberá seguir las directrices sobre datos sensibles y usar salvaguardias adicionales para ~~a~~ esos datos.

¿Qué ocurre si yo o un miembro del equipo compartimos accidentalmente datos sensibles? ¿Qué medidas correctivas se pueden tomar?

Si se descubre que se compartieron datos personales de forma accidental, hay que dejar de hacerlo inmediatamente. Esto podría significar pedir al receptor accidental que borre cualquier copia de los datos, eliminar el acceso del receptor accidental a los datos, desconectar los datos o tomar otras medidas según sea necesario.

El intercambio accidental o involuntario de datos personales se considera una violación de datos y se debe notificar a **it-security@mercycorps.org** de inmediato de acuerdo con el Plan de Respuesta a Incidentes. Se debe proporcionar toda la información posible, lo antes posible, sobre la naturaleza de los datos compartidos.

¿Qué debo hacer cuando veo que un miembro del equipo comparte intencionalmente datos sensibles con alguien que no debería tener acceso a dichos datos?

Compartir datos sensibles de manera intencional con una persona no autorizada es extremadamente grave, ya que puede provocar graves daños Datos Persona de interés y a la agencia. Si sabe que un miembro del equipo comparte intencionalmente información confidencial de esta manera, debe informar inmediatamente al responsable del programa, al director regional o al director.

Compartir datos sensibles con quienes no deberían tener acceso es también una violación de datos, y debe notificarse de inmediato a **it-security@mercycorps.org** de acuerdo con el Plan de Respuesta a Incidentes. Se debe proporcionar toda la información posible sobre la naturaleza de los datos compartidos, tan pronto como sea posible.

¿Cómo decide el programa quién debe o no debe tener acceso a los datos sensibles?

Solo se debe dar acceso a los datos sensibles a las personas que lo necesiten para desempeñar su función. Los datos sensibles se deben enmascarar siempre antes de que sean compartidos, si es posible. Algunos ejemplos comunes de enmascaramiento son la anonimización o la seudonimización.

¿Qué son los datos disociados?

Los datos disociados son datos que se han separado de forma completa e irreversible de los Datos Persona de interés, de modo que ya no es posible volver a asociar los datos con los Datos Persona de interés. Los datos disociados son un tipo de anonimización de datos.

¿Debo activar alertas en el conjunto de datos electrónicos si una persona no autorizada accede a ellos?

Si es posible activar alertas por acceso no autorizado, deberían estar siempre activadas, pero no todas las plataformas electrónicas tienen esta capacidad. Compruebe la configuración del sistema de su plataforma y, si es posible, active las alertas.

¿Deben los miembros del equipo utilizar dispositivos personales para recolectar o almacenar información confidencial? En caso afirmativo, ¿qué protecciones se deben proporcionar?

Los dispositivos personales no se deben utilizar para recolectar o almacenar información personal, lo que incluye a la información de los participantes, *a menos que se haya instalado un software de gestión de dispositivos adecuado* y que el uso de dispositivos personales quede registrado en la PIA del proyecto. Nunca se deben utilizar dispositivos personales para recolectar datos de los participantes sin la autorización expresa del director del programa. No se debe utilizar dispositivos personales para recolectar o almacenar información confidencial.

¿Puede mi donante auditar mi manejo de los datos sensibles?

Sí, muchos donantes exigen auditorías internas y también realizan auditorías externas de la calidad de los datos y de las evaluaciones de la calidad de los datos. Uno de los aspectos de estas evaluaciones es valorar el sistema MEL en cuanto a choques, invasiones y seguridad, especialmente si el programa recolecta información confidencial.

¿Puedo vincular las listas de participantes a TolaData como prueba?

Las listas de participantes (por ejemplo: listas de asistencia a capacitaciones, etc.) se pueden vincular como pruebas, ya que dichas pruebas se deben alojar y almacenar fuera de TolaData, por lo que solo determinadas personas tendrán acceso a esas pruebas, en función de los permisos de ese lugar de almacenamiento externo. Se debe considerar si algún tipo de evidencia vinculada a TolaData requiere la inclusión de Información Personal. Es muy poco probable que la inclusión de información confidencial sea necesaria.

¿Cómo puedo saber si los proveedores o plataformas de tecnología de recolección o almacenamiento de datos cumplen con los requisitos de datos sensibles?

Las plataformas de recolección y almacenamiento de datos existentes en MEL Tech Suite ya cumplen con los requisitos de datos sensibles, siempre que estén configuradas adecuadamente para utilizar las salvaguardias y los protocolos indicados en este documento. Si se va a utilizar una plataforma ajena a MEL Tech Suite, se deberá realizar una Evaluación de impacto en la Privacidad (PIA) para determinar si se puede considerar que cumple los requisitos sobre datos sensibles. En cuanto a la evaluación de un proveedor de tecnología, y su disposición a cumplir con la Política de Datos Responsables y los requisitos de datos sensibles, una PIA es de nuevo la mejor herramienta para determinar si se considerarán que sus prácticas son compatibles.

¿Cómo puedo saber si los datos son personales o confidenciales?

Si está procesando datos que están en alguna de las categorías especiales de datos sensibles señaladas por el GDPR (consulte **Datos sensibles de categoría especial** más arriba), siempre serán datos sensibles. Si hay una razón específica de contexto por la que los datos entrarían en la categoría de “Confidencialidad severa” (consulte la Figura 1 anterior), esto también se debería clasificar como datos sensibles.

Documentos relacionados:

Consentimiento

Herramienta MEL: Plantilla de Consentimiento informado (para los participantes de la entrevista)

Orientación de Consentimiento informado para compartir los datos de CARM

Orientación para MERL remota por COVID-19

Cifrado

Uso de Ona.io en Mercy Corps: Cifrado de formularios y datos sensibles

Biometría

Biometría en Mercy Corps: Cartilla interna

Guías generales

- Herramientas para la responsabilidad de los datos: una guía para dinero y cupones para practicantes - https://www.calpnetwork.org/wp-content/uploads/2021/03/Data-Responsibility-Toolkit_A-guide-for-Cash-and-Voucher-Practitioners.pdf
- Kit de inicio para datos ELAN para el personal humanitario de campo: https://www.calpnetwork.org/wp-content/uploads/2020/06/DataStarterKitforFieldStaffELAN.pdf
- Manual del ICRC sobre la protección de datos en acciones humanitarias: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.

Desidentificación de la información

Guía del USDA para la revisión de la información de identificación personal (PII) en las evaluaciones de proyectos

Poverty Action Lab 'De-identification for data publication' (Desidentificación para la publicación de datos)

Generación de códigos únicos para los participantes del programa u otros Datos Persona de interés

Borrador de orientación de T4D

Evaluaciones

Evaluación de impacto en la privacidad (PIA): plantilla

Evaluación de impacto en la privacidad (PIA): orientación

Evaluación de información confidencial(SIA)