Guía de Inicio a la Protección de Datos de Tdh.

2017.

Terre des hommes
Helping children worldwide.

Producido por
cartong

Parte I : Introducción a la protección de los datos en el campo.

1. Reseña.

Los equipos de Terre des hommes (Tdh) usan datos para muchos propósitos: identificar necesidades y tendencias, desarrollar estrategias, planificar un uso eficiente y estratégico de los recursos y entender si nuestros programas han ayudado a empoderar y mejorar las vidas de algunas de las personas y comunidades más vulnerables en el mundo.

Para obtener estos valiosos conocimientos, el personal de Tdh recolecta, analiza, comparte y almacena datos todos los días. Pero los datos también pueden causar daño, por ejemplo, si se pierden o si caen en las manos equivocadas. El personal de Tdh, es decir, usted, tiene la responsabilidad de proteger los datos que nos han sido confiados. El Kit Básico de Protección de Datos de Terre des Hommes le ayudará a recolectar y gestionar los datos de forma responsable.

01	02	03
La Parte I es una **introducción a la protección de los datos** y le ayuda a **identificar** y **entender sus riesgos**.	La Parte II está compuesta por t**utoriales prácticos** que demuestran paso a paso, cómo puede **proteger mejor los datos**.	La Parte III contiene un conjunto de plantillas de **Procedimientos Operativos Estándar (POE)** para ayudar a las oficinas en el campo a implementar cambios estructurales que mejoran la gestión de datos y la protección de los datos.

Este documento ha sido elaborado principalmente para el personal de campo de Tdh que está involucrado en la recolección o trabajo con datos que han sido obtenidos directamente de personas o comunidades a quienes apoyamos con nuestros programas. Esta guía no se centra en otras fuentes de datos, como registros de datos de llamadas u otros meta-datos, que pueden obtenerse a través de terceros.

Además, dado que esta guía ha sido elaborada para personal que trabaja en más de 30 países, no puede ser un documento de referencia legal, ya que más de 100 países tienen sus propias leyes y reglamentos de protección de datos. Sin embargo, siguiendo las buenas prácticas y consejos descritos en este paquete de herramientas, usted estará en el camino correcto para cumplir con sus obligaciones legales de protección de datos y para prevenir el daño de aquellos a los que intentamos servir.

En paralelo a este kit básico para el campo, la sede de Tdh en Suiza está trabajando en un documento de política separado para toda la organización para asegurarse de que Tdh cumpla con la Regulación General de Protección de los Datos de l a UE, que entrará en vigor en mayo de 2018 .

Figura 1 Adaptada de "El Manual de los Datos Responsables".

2. Por qué es importante la protección de los datos.

Todo lo que está escrito en papel o guardado en un archivo digital son datos. Por ejemplo: las notas escritas a mano de una entrevista con una chica no acompañada, un foto digital de un chico no acompañado en su cámara, o un mapa impreso que muestre a las comunidades donde Tdh está planeando construir letrinas.

Necesitamos y dependemos de los datos, pero la pérdida, corrupción, uso ilegitimo, distribución no autorizada e incluso la recolección de datos misma pueden ser perjudiciales para los beneficiarios, la organización o el personal.

Tres ejemplos:

Perjudicial para los beneficiarios: Una chica de 14 años ha sido violada mientras huía de un área en conflicto. Ella quedó embarazada y dio a luz al bebé. La chica y su familia recibieron asistencia de Tdh. Como parte de una misión de monitoreo y evaluación en el área de programa, un miembro del personal de Tdh visita a la chica y le hace múltiples preguntas sobre qué le pasó y cuándo. La chica revive la experiencia y vuelve a ser traumatizada.

Perjudicial para el personal: Alguien que no conoce a Tdh observa que su cámara digital está llena de fotos de niños. Esta persona ha oído el rumor de que hay niños que han sido adoptados por extranjeros y rápidamente organiza a un grupo de personas que lo amenazan y lo expulsan de la aldea.

Perjudicial para la organización: Mientras se encuentra en el campo, pierde un mapa que muestra la ubicación de las aldeas donde Tdh planea construir letrinas. Usted no conoce la zona y tiene que volver a la oficina para imprimir el mapa de nuevo. Pierde todo un día de trabajo y pierde una reunión con un anciano de la aldea programada para ese día. Esto disminuye la confianza que el anciano del pueblo tiene en Tdh.

Aunque muchos de estos riesgos han estado presentes en el ámbito humanitario durante muchos años, la protección de datos se ha vuelto más importante recientemente. Esto se debe en parte a obligaciones legales: más de la mitad de todos los países del mundo tienen leyes de protección de datos. Y más importante aún, la protección de datos se ha convertido en un problema porque ha aumentado la probabilidad de que se haga un uso indebido de los datos.

Las organizaciones de la sociedad civil que trabajan con los tibetanos, por ejemplo, informan que sufren ataques frecuentes a sus sistemas de TI1. Además, la Oficina de las Naciones Unidas de Coordinación de Asuntos Humanitarios (OCAH) informó de que a los refugiados sirios que viven en el Líbano les preocupaba que se estuvieran compartiendo sus datos de registro biométrico con el gobierno sirio2. Por último, pero no menos importante, todos los días se pierden datos a través de virus informáticos o por descuido.

La mejor manera de reducir el riesgo de que los datos causen daño es no recolectarlos en primer lugar. Por lo tanto, para proteger a las personas de verse perjudicadas, el personal de Tdh solo debe recopilar los datos necesarios, para los cuales tienen un uso concreto y específico. Además, tener procedimientos sólidos de protección de los datos puede ayudar a reducir aún más la probabilidad de incidentes como los descritos anteriormente y puede mitigar el impacto, en caso de que ocurra un incidente.

3. Funciones y responsabilidades dentro de la delegación.

Todos son responsables de ayudar a proteger los datos que se le han confiado a Tdh, bpero las responsabilidades concretas dependen de la función de cada miembro del equipo. A continuación se presenta un esquema de cuáles pueden ser estas responsabilidades en una delegación, sin embargo, esto variará dependiendo de la estructura y los recursos en cada país.

Dirección.

Representante de la oficina de país:

√ es responsable del proceso general, asegurándose de que se analicen los riesgos y se tomen medidas de mitigación dentro de su área de operaciones. Se asegura de que todos los equipos reciban la información adecuada y conozcan las herramientas, los Procedimientos Operativos Estándar, etc.

√ negocia acuerdos de no divulgación con los aliados cuando es necesario.

√ es responsable de designar a un punto focal encargado de las cuestiones de protección de datos. Dependiendo de la estructura de la delegación, podría ser:

- el oficial/gerente de gestión de la información (IM).
- el oficial/gerente de monitoreo y evaluación (M&E).
- el coordinador de programa.
- el gerente de TI.
- el representante adjunto.

Personal del programa.

Coordinador de programa:

√ inicia, coordina y supervisa el análisis de riesgos de protección de los datos con el apoyo del personal de TI / calidad y rendición de cuentas (Q&A) (coordinador de IM, M&E, coordinador de Q&A) y el personal de proyecto.

√ se asegura de que los socios estén al tanto de los requerimientos de protección de datos de Tdh.

Directores / oficiales de proyectos:

√ se asegura de que su proyecto sea analizado respecto a los riesgos de protección de los datos y que se estén definiendo e implementando medidas de mitigación.

√ informa de cualquier pregunta o preocupación al personal relevante; solicita asistencia del personal de apoyo o de los coordinadores de programa.

√ monitorea si los socios cumplen con los requerimientos de protección de los datos de Tdh.

Departamentos / personal de apoyo.

Personal de calidad y rendición de cuenta:

- √ contribuye al análisis de riesgos de protección de los datos al ofrecer soporte técnico y metodológico a los equipos de programa.
- √ se asegura de que cualquier plan de monitoreo incluya un análisis del sistema de gestión de la información, que a su vez incluya una reflexión sobre la protección de los datos.
- √ proporciona apoyo ético, metodológico (M & E) y técnico (IM) y asegura que la protección de datos se incluya dentro del marco de los planes de M&E.
- √ garantiza que la protección de datos y el principio de no causar daño se integren en cualquier proceso de monitoreo y evaluación que implique la recolección, el procesamiento, el uso y el intercambio de datos.

Persona del TI:

- √ apoya a los equipos de programa cuando lo solicitan e informa de cualquier pregunta / inconsistencia.
- √ alerta a los equipos de programa si se detecta algún riesgo y sugiere soluciones.

Personal de RR.HH.:

- √ se asegura de que la protección de los datos se incluya en el paquete de inducción para el personal nuevo.

Ejemplos.

A continuación se presenta una combinación de ejemplos relacionados con cuestiones de protección de datos en el terreno, y se incluyen sugerencias sobre cómo podrían haberse evitado estas situaciones. Algunos de estos ejemplos han ocurrido realmente, otros podrían ocurrir plausiblemente.

El rol que usted puede desempeñar para asegurar que los datos se protejan adecuadamente depende de su función en Tdh.

[1] *See: "Communities @ Risk - Targeted Digital Threats Against Civil Society"; Accessed: 13 October 2017*
[2] *UNOCHA, "Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies", p. 9; Accessed: 13 October 2017*

1.

Qué sucedió?

Una computadora que contiene los archivos de 143 niños y sus familias se malogra.

No hay copia de respaldo.

¿Cuál es el daño?

Se tiene que recrear los datos. El personal de Tdh se pasa semanas recreando los archivos.

Mientras tanto, las actividades del programa están detenidas porque ya no está claro qué se debe hacer, dónde y para quién.

Los beneficiarios están contrariados por las preguntas, así como por los retrasos y empiezan a dudar si pueden confiar en Tdh.

Un donante está disgustado porque su dinero no se está gastando tan rápido como se acordó.

Al final, el personal de Tdh solo pudo encontrar a 135 de los niños; la información de los ocho restantes sigue perdida.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

- √ **Punto focal de protección de los datos:** asegurarse de que se tenga y siga un plan de respaldo.
- √ **Director de programa/TI:** realizar copias de respaldo semanales, incrementales en un disco duro externo cifrado que se guarda en la caja fuerte de la oficina. Asegurarse de que exista un procedimiento de gestión de contraseñas adecuado para los archivos cifrados, de manera que no se pueda perder ni adivinar la contraseña. Enviar copias del disco duro a la oficina del país una vez al mes.

2.

Qué sucedió?

Una organización aliada comparte por correo electrónico con un grupo numeroso de personas los nombres y la ubicación de 50 niños y niñas que corren el riesgo de ser víctimas de trata.

Uno de los destinatarios comparte la información con un grupo criminal.

¿Cuál es el daño?

El grupo criminal se pone en contacto con muchos de los niños, cinco de los cuales desaparecen.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

- √ **Representante de país / punto focal de protección de datos / director de programa:** Exigir a las organizaciones aliadas que sigan prácticas responsables para compartir datos, como limitar el número de destinatarios de datos sensibles. Discute opciones para anonimizar los datos cuando sea posible.

3.

Qué sucedió?

Un coordinador de programa comparte con sus contrapartes de otras organizaciones un informe sobre soldados que abusan de niñas en una aldea.

El informe contiene un enlace a una carpeta de Dropbox con información personal sensible a la que ahora puede acceder cualquier persona que tenga el enlace.

¿Cuál es el daño?

El informe se comparte con más personas y finalmente llega a un miembro de alto rango del ejército.

Los soldados regresan a la aldea e intimidan a las niñas que han denunciado el abuso.

Los aldeanos ya no quieren hablar ni confían en Tdh.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

√ **Punto focal de protección de datos / coordinador del programa:** Definir POE claros que regulan quién puede tener acceso a qué tipo de información y cómo puede ser compartida.

√ **Coordinador de programa / director del programa / Calidad y Rendición de cuentas:** Restringir quién tiene acceso a los datos personales y para qué fines. Si utiliza una unidad compartida como Google Drive, dar acceso solo a usuarios con nombre.

4.

Qué sucedió?

La hoja de asistencia impresa y firmada de un curso de sensibilización sobre el VIH/SIDA se deja accidentalmente en el hotel donde se llevó a cabo el curso.

Un empleado de un hotel comparte la lista con un miembro del ministerio de salud del gobierno.

¿Cuál es el daño?

Todos los participantes masculinos en el entrenamiento están siendo detenidos bajo la sospecha de homosexualidad, que es ilegal en este país.

Los detenidos tienen que someterse a exámenes anales en el hospital.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

√ **Director de programa / Calidad y rendición de cuentas:** Evaluar si es necesaria una hoja de asistencia para este evento.

5.

Qué sucedió?

Las copias impresas de todos los archivos de gestión de casos se guardan en un gabinete con llave. Sin embargo, el personal local exporta información de la base de datos a sus memorias USB y computadoras portátiles personales cuando va al campo.

Un día un empleado renuncia. Los datos siguen en su computadora.

¿Cuál es el daño?

Dado que el personal estaba trabajando en una operación transfronteriza, los datos, que incluían direcciones y nacionalidades, podrían haberse utilizado para identificar a las familias de refugiados y ejercer presión sobre ellas.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

√ **Sede:** Proporcionar presupuesto para asegurar que el personal local relevante tenga computadoras personales.

√ **Coordinador del programa / representante del país / Calidad y rendición de cuentas:** Definir quién tiene acceso a la base de datos y para qué fines. Definir una política sobre el uso de dispositivos electrónicos personales para el trabajo y compartirla con todo el personal.

√ **Oficina de campo:** Preguntar explícitamente a los empleados durante las entrevistas de salida sobre cualquier dato de Tdh que tengan en su poder.

6.

Qué sucedió?

Un miembro del personal recibe un correo electrónico con un archivo adjunto. El archivo adjunto contiene el virus WannaCry que bloquea y cifra el disco duro.

Un mensaje aparece en la pantalla, diciendo que el usuario tiene siete días para pagar varios cientos de dólares para liberar los datos, de lo contrario los datos serán eliminados.

¿Cuál es el daño?

Tdh no le paga a los delincuentes y se pierden todos los datos en la computadora.

¿Qué se podría haber hecho diferente y quién lo habría hecho?

√ **IT:** Asegurarse de que la protección antivirus esté actualizada en todas las computadoras.

√ **Director de programa / TI:** realizar copias de respaldo incrementales semanales en un disco duro externo cifrado que se guarda en la caja fuerte de la oficina. Asegurarse de que exista un procedimiento de gestión de contraseñas adecuado para los archivos cifrados, de modo que no se pierda ni se adivine la contraseña Enviar copias del disco duro a la oficina de país una vez al mes.

4. Términos y conceptos claves.

Tdh se compromete a utilizar los datos de forma responsable para defender los derechos de las personas, grupos y organizaciones con los que trabajamos. Este paquete de herramientas le proporciona muchas herramientas prácticas para ayudarle a cumplir con este compromiso en su trabajo diario. Estos son algunos de los términos y conceptos clave que debe conocer:

Uso responsable de los datos es :
"el deber de garantizar el derecho de las personas a dar su consentimiento, a la privacidad, la seguridad y la propiedad en torno a los procesos de recolección, análisis, almacenamiento, presentación y reutilización de datos, respetando los valores de transparencia y apertura".[3]

Esto significa que las buenas políticas y prácticas de gestión de datos no solo buscan evitar daños, sino que también tratan de empoderar a las personas que están en el centro de los datos mediante el establecimiento de circuitos de retroalimentación.

Riesgos son la intersección del daño y la amenaza y describen la probabilidad y el impacto de que ocurra un evento perjudicial.

Amenazas son cualquier cosa que pueda causar daño, sea intencionalmente o no.

Obtención del consentimiento informado de niños– una tarea difícil.
Obtener el consentimiento informado de los niños puede ser difícil y depende en parte de la edad y madurez del niño. No hay una solución fácil para todos los países, demografías y edades. Sin embargo, el personal de Tdh tiene la obligación de tratar de obtener el consentimiento informado de los niños si sus datos están siendo recopilados. Además, el consentimiento informado de los tutores legales es obligatorio. La siguiente es una lista de sugerencias para ayudar a los niños a entender lo que están consintiendo.

- Preséntese como una persona y no con su estatus.
- Explique la finalidad de la recolección de datos.
- Informe a los niños sobre la importancia de los datos.
- Informe a los niños y niñas sobre cómo participarán, cuánto tiempo les tomará y cómo se garantizará la confidencialidad.
- Informe a los niños sobre el tipo de información que se recolectaría, cómo se recolectará y cómo se usará.
- Asegúrese de que los niños realmente entiendan lo que usted les ha dicho pidiéndoles que repitan lo que usted les ha dicho.
- Dé tiempo a los niños para hacer preguntas o plantear inquietudes.
- Escuche a los niños.
- Asegúrese de que los niños sepan que pueden dejar de participar en cualquier momento.
- Asegúrese de que los niños entiendan que usted no está haciendo promesas de mejorar sus condiciones de vida.
- No haga otras promesas que no pueda cumplir.
- Cuando los niños han hecho dibujos o materiales escritos, se les debe decir cómo se pueden usar y preguntarles después si desean que se les identifique como artista/autor.

En situaciones en las que el personal se encuentra con menores no acompañados que no cuentan con un adulto legalmente responsable que vele por sus intereses, se debe prestar especial atención a si acercarse a un menor redunda en el interés superior de cada uno de ellos.

Adaptado de: "Handbook for action-oriented research on the worst forms of child labour including trafficking in children", p. 115 ff, Regional Working Group on Child Labour in Asia (RWG-CL), Diciembre 2002.

[3] *Responsible Data Forum, working definition, September 2014; https://responsibledata.io/about/ Consultado: 28 agosto 2017.*

[4] *"The Signal Code: A Human Rights Approach to Information During Crisis" by Signal Program on Human Security and Technology at the Harvard Humanitarian Initiative; Consultado: 28 agosto 2017.*

Protección de los datos son todos los procesos, prácticas y sistemas que se utilizan para salvaguardar la información para evitar que se pierda, se corrompa o que partes no autorizadas accedan a ella.

Daño significa cualquier daño, lesión o impacto negativo, sea tangible o intangible o económico, a una persona u organización que puede fluir del procesamiento de los datos personales. Se extiende a cualquier negación de los derechos y libertades fundamentales.

Consentimiento informado debe ser dado explícitamente para recolectar datos y debe ser específico para los fines para los que se utilizan los datos. El consentimiento para los niños debe ser dado por el padre o tutor legal del niño.

En los casos en que se prevén usos secundarios de los datos, es necesario explicarlos a la persona que proporciona la información. También es aconsejable verificar cuál es la edad nacional de adultez, ya que en algunos contextos se considera que los individuos son adultos a la edad de 15 o 16 años.

El derecho a la agencia y rectificación de datos
Describe el derecho de todos a tener control sobre la recolección, uso y divulgación de su información. Esto incluye el derecho de una persona a obtener acceso a su propia información y corregir la información que sea inexacta[4].

Una recolección y procesamiento de datos **legal, justa y específica** significa que:

a) las personas no deben estar expuestas a violaciones de derechos, daños o trato indecoroso o discriminatorio como consecuencia de la recolección y procesamiento de datos personales. Esto incluye el deber de obtener el consentimiento informado de las personas a las que está recolectando datos. También significa que la negativa a proporcionar datos no debe dar lugar a consecuencias negativas para la persona.

b) solo se deben recolectar los datos necesarios para un propósito determinado y suprimirla si ya no es necesaria para tal fin[5].

Datos personales
es cualquier información relacionada con una persona que pueda ayudar a identificarlo(a) ya sea directamente (p. ej., primer nombre y apellido o número de registro único) o indirectamente combinando diferentes fuentes de datos.

[5] *Adaptado from Conducting Mobile Surveys Responsibly: A Field Book for WFP Staff, May 2017" and "How to Do A Privacy Impact Assessment", Privacy Commissioner of New Zealand; Consultado: 28 agosto 2017.*

Moldavie. © Tdh / François Struzik

Siège | Hauptsitz | Sede | Headquarters
Avenue de Montchoisi 15, CH-1006 Lausanne
T +41 58 611 06 66, F +41 58 611 06 77
E-Mail: info@tdh.ch, CCP / PCK: 10-11504-8

Copyrights ©
La mayoría de íconos OCHA
Ilustración de CartONG

Producido por