Humanitarian OpenStreetMap Team

1100 13th Street NW, Suite 800
Washington, DC 20005 USA
info@hotosm.org
www.hotosm.org

Política: Protección

Tipo de política:	☒ Original ☐Addendum
Propietario:	Director de Datos
Unidad responsable	Datos
Fecha de entrada en vigor:	1 de noviembre de 2022
Aprobado por:	SMT
Última actualización:	1 de octubre de 2023

Se aplica a:

☐ Solo Global ☐ Todas las oficinas excepto Global

☒ Todas las oficinas ☐Otros, especifique:

Versión	1.2
Última revisión por:	Paul Uithol, Jessie Pechmann
Próxima fecha de revisión:	Junio de 2024

Historial de versiones:

Proyecto final	3 de junio de 2022	Proyecto final propuesto para su aprobación por el SMT
1.0	1 de noviembre de 2022	Primera versión aprobada
1.1	1 de junio de 2023	Abordar los comentarios de la revisión externa
1.2	1 de octubre de 2023	Claridad del proceso de revisión y aprobación.

Contenido:

1. Objetivo

Los datos espaciales y las actividades cartográficas pueden crear riesgos o causar daños a personas y comunidades. HOT, como organismo que realiza y apoya actividades cartográficas y crea datos espaciales abiertos y de libre acceso con pocas restricciones de uso, es responsable de comprender, evaluar, mitigar y proteger contra los riesgos y daños derivados de las actividades que emprendemos o apoyamos.

Esta política establece las formas en que las partes interesadas en las actividades de recopilación de datos, almacenamiento de datos y uso de datos pueden abordar estas responsabilidades, y representa el compromiso de HOT con las prácticas responsables y éticas para proteger a las personas de cualquier daño. Las partes interesadas incluyen al personal de HOT, contratistas y voluntarios, también pueden incluir comunidades (OSM) que participan en actividades de recopilación de datos financiadas por HOT u otros donantes.

El enfoque de HOT respecto a los datos éticos se basa en los Principios de Datos de **"Datos abiertos y accesibles"**, **"Datos útiles y utilizables"**, **"Datos inclusivos y representativos"** y **"Datos éticos y protección"**. En concreto, El enfoque de HOT respecto a los datos éticos se basa en los Principios de Datos[1] de "**Datos abiertos y accesibles**", "**Datos útiles y utilizables**", "Datos **inclusivos y representativos**" y "**Datos éticos y protección**". En concreto, "Datos **éticos y protección**" significa que HOT aspira a la colaboración más significativa en la gestión y planificación de datos con las personas y comunidades con las que trabajamos, y a mantener políticas y orientaciones para minimizar el riesgo de daños, incluidas las evaluaciones de impacto y el consentimiento informado para cualquier recopilación o uso de datos. Esto incluye los cuatro principios siguientes: significa que HOT aspira a la colaboración más significativa en la gestión y planificación de datos con las personas y comunidades con las que trabajamos, y a mantener políticas y orientaciones para minimizar el riesgo de daños, incluidas las evaluaciones de impacto y el consentimiento informado para cualquier recopilación o uso de datos. Esto incluye los cuatro principios siguientes:

1. Aplicar un proceso viable de **compromiso y consentimiento informado** en todas nuestras actividades, incluidas la teledetección y la digitalización (teniendo en cuenta un panorama tecnológico cada vez más sofisticado).

[1] Del latín *Primum non nocere*, un principio de la labor humanitaria y de desarrollo tomado del ámbito sanitario que, según el artículo del enlace anterior, "se invoca cuando se debate el uso de una intervención que conlleva un riesgo evidente de daño pero una posibilidad menos cierta de beneficio".

A veces, esta máxima se amplía a "No hacer *más* daño", reconociendo que el trabajo humanitario se realiza más o menos por definición en contextos en los que el daño ya es frecuente, y el imperativo es minimizar el riesgo de que nuestras intervenciones causen más daño, en equilibrio con sus beneficios.

2. Garantizar el **respeto** de las creencias, culturas, estilos de vida y **elecciones de las comunidades en la toma de decisiones en torno a la recopilación y el intercambio de datos**, y en nuestro uso de la información recopilada. Involucrar a los socios en el uso ético de la información.
3. Llevar a cabo **evaluaciones del riesgo y del impacto de los datos** para evaluar y minimizar el riesgo de daños para todos los proyectos junto con las comunidades pertinentes. En situaciones en las que el conflicto sea un factor, siga la "Política de cartografía de zonas de conflicto".
4. Garantizar que **todo el personal de HOT cumple con la aplicación de los principios de protección de datos**.

Véase Política: Actividades HOT y cartografía en zonas (disponible en inglés) de conflicto para más información sobre cartografía en zonas de conflicto.

2. Aplicación y puesta en práctica

La Herramienta de Ética y Protección de Datos es el principal vehículo para la aplicación de esta política. Todos los proyectos de cartografía sobre el terreno, las activaciones y los proyectos de cartografía a distancia en zonas de conflicto/alto riesgo apoyados por HOT o que utilicen la infraestructura de HOT deben completar esta herramienta antes de comenzar las actividades (los proyectos de cartografía a distancia en zonas pacíficas y estables no necesitan completar esta herramienta).

Tenga en cuenta que este documento no pretende crear obstáculos al trabajo normal ni añadir burocracia. Para la mayoría de los proyectos HOT (en contextos pacíficos, que no traten datos sensibles), se espera que el ejercicio dure menos de 1 hora.

Todos los altos directivos y directores de HOT deben estar familiarizados con este documento y ser conscientes de las circunstancias en las que las actividades, los proyectos y los datos deben evaluarse para detectar posibles daños. También deben conocerlo los gestores de proyectos que trabajen en contextos de riesgo, como zonas de conflicto.

Este documento, así como las orientaciones y herramientas que lo sustentan, deben ser accesibles y estar a disposición de cualquier persona de la organización preocupada por el riesgo de protección. Además, en cualquier caso en el que sea probable que surja un riesgo de protección (como la cartografía en zonas de conflicto), **el director o directores responsables de los proyectos** (normalmente los directores de los centros de operaciones, pero en los casos de proyectos gestionados por miembros del equipo global, **el gestor senior o el director** en la línea

jerárquica de gestión) **son responsables de garantizar que esta política se consulte, se siga, se firme y se guarde junto con otra documentación del proyecto.**

3. Definición y alcance

La palabra "protección" se utiliza aquí de forma similar a su uso habitual en el ámbito humanitario, que engloba dos definiciones básicas:

1. Proteger la vida, los medios de subsistencia, la seguridad, la salud y la dignidad de las personas afectadas, y
2. Garantizar que nuestras propias acciones no provoquen o perpetúen la discriminación, el abuso, el abandono o la violencia.

En contextos humanitarios o de conflicto, se aplican ambas definiciones. Sin embargo, en contextos de desarrollo pacíficos y estables (en contraposición a los contextos humanitarios o de conflicto), se hace hincapié en la definición 2, que puede resumirse en el mandato común de "***no hacer daño***".[2] "

Alcance:

- Riesgo de daño a *las personas y comunidades que están siendo cartografiadas, o sobre las que se están recopilando datos* (a diferencia del personal y los cartógrafos) durante las actividades de recopilación de datos y cartografía, o resultante del uso y análisis de estos datos. Esto abarca:
    - Actividades propias de HOT,
    - proyectos apoyados directamente por HOT (financiación, material o apoyo en especie) o utilizando la infraestructura de HOT (Tasking Manager o similar),
    - cualquier dato disponible a través de plataformas de datos abiertos como OpenStreetMap,
    - cualquier dato que HOT posea o gestione (datos abiertos o no) y que, según una evaluación debidamente diligente, cree riesgos y/o daños para las personas o las comunidades,
    - y, por último, los datos propiedad de terceros y gestionados por ellos que se derivan directamente de actividades apoyadas por HOT.

[2] El Gestor de Tareas de HOT está licenciado bajo una licencia BSD de 2 Cláusulas, una licencia liberal (sin copyleft) que permite cualquier uso del código siempre que el aviso de copyright, las condiciones, el descargo de responsabilidad y el código fuente estén disponibles con cualquier distribución.

Fuera del alcance:

- Seguridad y protección operativas. Este documento se centra en el impacto y el riesgo potenciales sobre las comunidades cartografiadas como resultado de la creación de datos espaciales abiertos, no en la seguridad de los cartógrafos. La seguridad y la protección son importantes y se solapan en cierta medida con la protección, pero en última instancia constituyen una preocupación independiente. Esto se trata en la Política HOT: Seguridad (disponible en inglés).
- controlados por HOT. Mientras que la protección implica la responsabilidad de considerar cuidadosamente qué datos deben recopilarse y almacenarse, la prescripción de cómo asegurar adecuadamente cualquier dato sensible resultante (a veces denominada protección de datos[3]) se tratará en la política de seguridad de la información.
- Uso por parte de terceros de Software Libre y de Código Abierto (FOSS) creado o apoyado por HOT que está fuera del control y la infraestructura de HOT. Las licencias de estos softwares[4] son claras: cualquiera es libre de utilizar el software, y HOT no es responsable de su conducta.
- Uso por terceros de datos abiertos aportados o respaldados por HOT. El uso de los datos de OpenStreetMap se rige por la Licencia de base de datos abierta, que permite cualquier uso siempre que los datos se atribuyan, compartan y mantengan abiertos. HOT (o cualquier otro creador de tales Datos Abiertos) no es responsable de la conducta de los usuarios.

Nótese que ninguno de ellos se exime de responsabilidad por la *creación de datos abiertos* que puedan causar daños. En cierto sentido, una vez liberados al mundo, los datos abiertos no pueden retirarse. Por tanto, su creación y publicación conllevan responsabilidades.

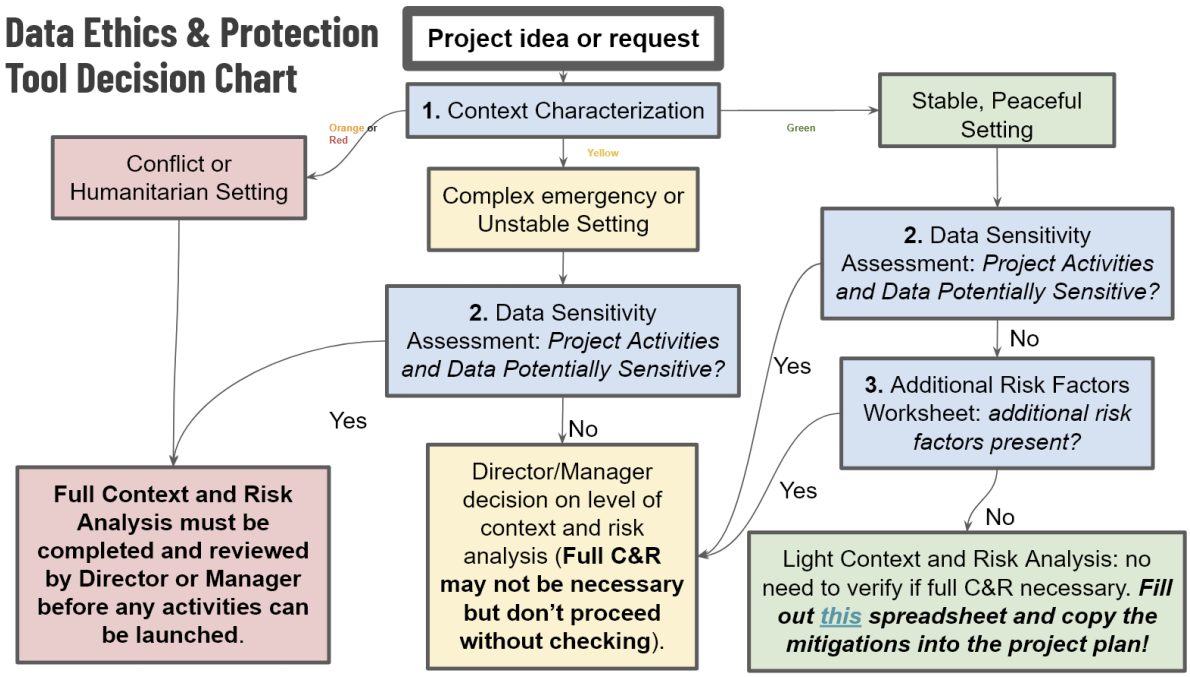
[3] https://www.hotosm.org/updates/data-principles/

[4] Aunque se trata de una definición estrecha e incompleta, una definición más completa de la protección de datos es la de privacidad de la información, que aborda cuestiones como qué datos tener o crear, y no sólo cómo protegerlos técnicamente.

4. Pasos necesarios antes de iniciar proyectos de cartografía abierta

- **Todos los proyectos de Cartografía Abierta apoyados por HOT** con un componente de campo requieren una evaluación del Riesgo de Protección.
- **Todas las "Activaciones"** requieren una Evaluación de Riesgos de Protección como parte del dimensionamiento.
- **Algunos proyectos de cartografía a distancia basados en el Gestor de Tareas** (principalmente aquellos en zonas identificadas de alto riesgo y/o alta sensibilidad) requieren una Evaluación del Riesgo de Protección.

En muchos casos, la Evaluación del Riesgo para la Protección puede ser un proceso muy ligero; esta política no pretende impedir o incomodar la "normalidad" de la Cartografía Abierta. Más bien, puede fomentar un diálogo constructivo sobre el uso potencial de los datos y sus implicaciones con las comunidades afectadas. La **Herramienta de Ética y Protección de Datos** contiene un diagrama de flujo que muestra el árbol de decisiones desde una idea o solicitud de proyecto hasta el nivel de supervisión necesario para la Evaluación del Riesgo para la Protección:



Hay tres categorías de proyectos, que corresponden a las casillas inferiores del organigrama. En todos los casos debe cumplimentarse la **Herramienta de Ética y Protección de Datos**. La diferencia entre los niveles de riesgo Verde, Amarillo y Rojo es el nivel de supervisión requerido:

- **Verde**: Contexto ligero y análisis de riesgo requerido. Esto significa que el proyecto se encuentra en (a) un entorno estable y tranquilo, (b) no implica datos sensibles y (c) no presenta factores de riesgo adicionales. El propietario del proyecto (que puede ser un becario comunitario o un mentor) realiza un sencillo ejercicio de hoja de cálculo. Se espera que dure una hora.
- **Amarillo**: Medio o incierto. Decisión del director o gerente sobre el nivel de evaluación necesario.
- **Rojo**: Equivalente a zona de conflicto y/o recopilación de datos altamente sensibles; requiere automáticamente la supervisión a nivel de Director (o a nivel de Gestor Senior si se delega) del proceso de Evaluación de Riesgos antes de comenzar las actividades.

Para los proyectos en las categorías **Amarilla** o **Roja**, el proceso completo debe ser completado y aprobado por el Director que supervisa directamente. Antes de comenzar con la Evaluación de Riesgos propiamente dicha, añada los datos relevantes del proyecto para la evaluación y las revisiones en la pestaña denominada "**0. Propuesta y Alcance**". Cada Evaluación de Riesgos consta de 5 pasos, que se explican con más detalle en la herramienta:

1. **Categorización del contexto:** identifica el tipo de contexto. Esto da lugar a una etiqueta de contexto roja, naranja, amarilla o verde.
2. **Evaluación de la sensibilidad de los datos**: no todos los datos tienen el mismo potencial de daño, y éste difiere en función de los factores contextuales. Identifique cualquier dato potencialmente sensible *dentro del contexto identificado.*
3. **Factores de riesgo adicionales**: un lugar determinado puede ser generalmente pacífico y estable, pero puede requerir algo más que una evaluación ligera del riesgo de protección si se dan factores contextuales específicos, como brotes de enfermedades o elecciones.
4. **Evaluación de riesgos de protección**: identificar riesgos específicos evaluando la vulnerabilidad, la probabilidad y el impacto. Crear medidas paliativas y modificaciones del proyecto basadas en los riesgos identificados.
5. **Lista de control y aprobaciones**: revise la Herramienta de Ética y Protección de Datos cumplimentada. Considere si el nivel de riesgo es aceptable o si se requieren modificaciones y mitigaciones adicionales. *Si el riesgo residual se considera inaceptable, la consecuencia última puede ser que el proyecto no siga adelante en la forma propuesta.* Existen dos niveles de aprobación:
    a. **Revisión**: dependiendo de la confianza en la evaluación del personal que la complete, pida a una o dos personas de los puntos focales de protección o a alguien familiarizado con el contexto que revisen la evaluación completa y

aporten comentarios y sugerencias. Si la evaluación es satisfactoria, los revisores deberán firmarla.

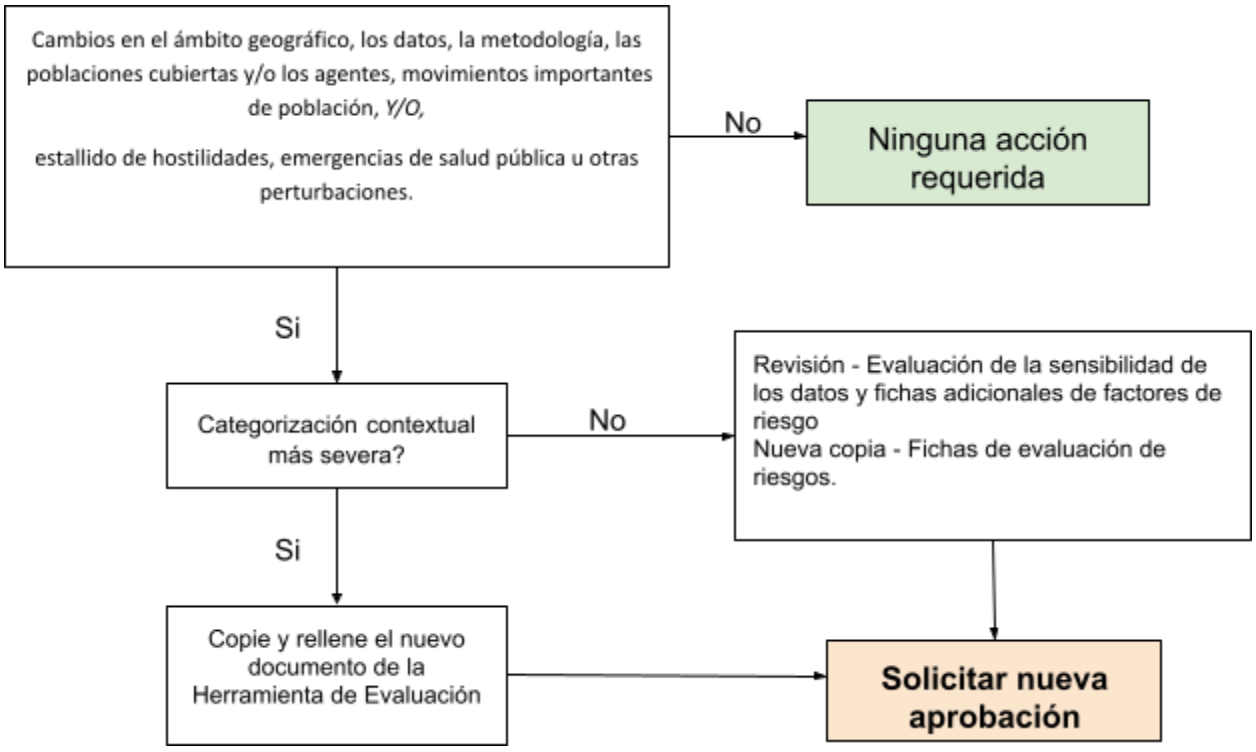
b. **Aprobación**: en principio, la aprobación final debe ser proporcionada por el Director que supervisa directamente al miembro del personal que está completando la evaluación del Riesgo de Protección, que debe ser un miembro del equipo que va a implementar y ejecutar las actividades propuestas. La aprobación de la evaluación debe situarse en la misma jerarquía que la implementación y ejecución del proyecto para garantizar que sea posible una supervisión significativa de las medidas de mitigación propuestas, y requerir una reevaluación cuando sea necesario. En circunstancias excepcionales, y en estrecha coordinación, esta autoridad puede delegarse en otro Director o miembro del Equipo de Alta Dirección. Para la aprobación final, por favor:
    i. Revisar la evaluación de riesgos para detectar posibles lagunas.
    ii. Revisar las medidas paliativas para garantizar la claridad de su aplicación en función de su viabilidad, capacidad, apropiación clara y eficacia.
    iii. Garantizar la comprensión de todos los riesgos y mitigaciones para orientar el trabajo futuro y responder a posibles preguntas en torno al proyecto.

La hoja de cálculo "Herramienta de ética y protección de datos" cumplimentada debe guardarse junto con la documentación pertinente del proyecto en la carpeta del proyecto.

5. Revisiones y versiones

Con el tiempo, los cambios en el alcance del proyecto, el área de operaciones, las peticiones de los socios o las circunstancias locales pueden hacer que una evaluación de Ética y Protección de Datos quede obsoleta y sea necesario revisarla. Una evaluación debe revisarse en las siguientes circunstancias:

- Si se producen cambios significativos en el alcance del proyecto, como el área de operaciones cubierta en la recogida de datos y la cartografía, los tipos de datos recogidos o la metodología.
- Solicitudes adicionales de los socios para la elaboración de mapas que amplíen los actores cubiertos, las poblaciones afectadas o los datos que se solicitan.
- Movimientos de población a una escala lo suficientemente grande como para afectar a la dinámica y los riesgos de la comunidad.
- Estallido de hostilidades, emergencias de salud pública u otras perturbaciones importantes.



Si se produce alguno de estos casos, vuelva a evaluar el primer paso: "**1. Categorización del contexto**". Si no se produce ninguna de estas situaciones, se recomienda reevaluar periódicamente la categorización del contexto, al menos semestralmente. Basándose en la reevaluación, haga lo siguiente:

1. **Si el resultado del árbol de decisión de categorización del contexto no ha cambiado** (sigue siendo rojo/amarillo/verde), **o ha disminuido** en gravedad, la evaluación actual puede modificarse del siguiente modo:
    a. Revise las pestañas "2. Evaluación de la sensibilidad de los datos" y "3. Factores de riesgo adicionales", y actualícelas si es necesario.
    b. Para preservar los riesgos y mitigaciones anteriores, cambie el nombre de la versión actual de "4. Evaluación de riesgos de protección" a la fecha de su aprobación original - por ejemplo, "4. Evaluación de riesgos de protección_11 de marzo de 2023"
    c. Cree una nueva copia de la pestaña "4. Evaluación de riesgos de protección" en la herramienta actual y modifíquela con la fecha de la nueva evaluación, por ejemplo, "4. Evaluación de riesgos de protección_20 de junio de 2023_última". Complete la nueva evaluación de riesgos.
    d. **Solicite una nueva aprobación de la evaluación** y anótelo explícitamente con un nuevo conjunto de firmas en la pestaña "Lista de control y aprobaciones".
2. **Si el** resultado del árbol de decisión **de Categorización del Contexto ha aumentado en gravedad** - ha pasado de verde a amarillo, o de amarillo a rojo - se creará una nueva evaluación completa.
    a. Poner fecha al documento antiguo: por ejemplo, "Data Ethics and Protection Tool_Somalia drought response_11-03-2023".
    b. Cree una nueva copia de la **Herramienta de Ética y Protección de Datos** y repita el proceso tal y como se indica en el apartado 4. Pasos necesarios antes de iniciar proyectos de cartografía abierta. Poner fecha y versión al nuevo documento - por ejemplo, "Data Ethics and Protection Tool_Somalia drought response_20-06-2023_latest".
    c. Solicitar la revisión y aprobación de la evaluación actualizada.

6. Funciones y responsabilidades

Rol	**Tareas**	**Responsabilidades**
Gestores de proyecto	Cumplimentar la Herramienta de Ética y Protección de Datos bajo la supervisión del Responsable Principal o el Director, y en colaboración con el equipo del proyecto, consultando a las comunidades (potencialmente) afectadas siempre que sea posible.	● Completar la herramienta y la evaluación de riesgos ● Identificación de riesgos ● Búsqueda y consulta adecuadas de información ● Ofrecer una representación honesta, justa y precisa ● Solicitar la revisión y aprobación oportunas
Supervisor directo de gestores de proyecto (a menudo jefes de equipo)	Garantizar que la Herramienta de Ética y Protección de Datos se cumplimenta adecuadamente y que los posibles riesgos se señalan, mitigan e incorporan a la implementación y ejecución del proyecto.	● Supervisar la planificación y ejecución de los proyectos
Revisores	Revisar las evaluaciones completadas basándose en la experiencia y la familiaridad con el proceso de evaluación de riesgos, los factores contextuales y/o las situaciones de conflicto. Se seleccionará y comunicará periódicamente un grupo de revisiones.	● Revisión de las evaluaciones completadas
Miembros del equipo directivo (SMT)	Supervisar, apoyar y, en última instancia, rendir cuentas de la aplicación y ejecución responsables de los proyectos.	● Firma y aprobación de las evaluaciones completadas y revisadas ● Supervisión de la aplicación y ejecución

Junta (Board)	Esta política está bajo la supervisión del Comité de "Gestión de Riesgos" del Consejo.	• Garantizar la integración de los riesgos prevalentes en el registro de riesgos

7. Aplicación de la política

En toda la organización:

- ~~Las evaluaciones de los riesgos de protección se incorporan al mecanismo de dimensionamiento de una activación~~
- Las evaluaciones de los riesgos de protección se incorporan a las listas de control de inicio de los proyectos de cartografía (listas maestras con el equipo de AMPS y cualquier procedimiento y lista de control específicos del Hub).
- ~~Taller específico SMT~~
- ~~Oportunidades de formación y talleres para todo el personal~~

Exteriores:

- ~~Publicado en forma de colaboración abierta curada (GitHub)~~
- ~~Revisión y comentarios de expertos del sector~~
- ~~Talleres externos e incorporación a los recursos del sector~~
- Lanzamiento público
-

Por proyecto (véase Pasos necesarios antes de iniciar proyectos de cartografía abierta para saber cuáles):

- Copie la plantilla **Herramienta de ética y protección de datos**
- Ejecute los pasos asociados a la "Herramienta de Ética y Protección de Datos".
- Revíselo con el director correspondiente y decida si lo aprueba.
- Incorpore las medidas de mitigación identificadas en la herramienta de ética y protección de datos de la hoja de trabajo "4. Evaluación de riesgos de protección" a la planificación de actividades del proyecto como procedimientos operativos estándar.

Anexo 1: Recursos, formación y seguimiento

- Repositorio GitHub (público) con recursos: https://github.com/hotosm/data_protection_project/
- Herramienta de ética y protección de datos
- Presentación base: Marco de protección Presentación_base (disponible en inglés)
- Presentación adaptada para taller presencial: Presentación del marco de protección_en persona (disponible en inglés)

Material para talleres:

- Presentación base: Marco de protección Presentación_base (disponible en inglés)
- Presentación adaptada para el taller presencial: Marco de protección (disponible en inglés) Presentación_presencial
    - 🌕 Imprima las diapositivas del escenario (31-35) y las cuatro partes de la herramienta de ética y protección de datos PLEASE_COPY 27-04-2023_latest: Categorización del contexto, Evaluación de la sensibilidad de los datos, Factores de riesgo adicionales, Evaluación del riesgo de protección.

Materiales aún por crear:

- Grabación en vídeo del taller virtual

Eventos de capacitación:

Cuando?	**Donde/quién**	**Facilitadores**
14 jul 2022	Mentores de la subvención de cartografía abierta de la ESA	Shamillah Nassozi & Michael Otieno
22 ago 2022	Estado del mapa Florencia	Shamillah Nassozi & Jessie Pechmann
19 oct 2022	SMT	Ivan Gayton & Paul Uithol
25 oct 2022	GeONG	Paul Uithol & Shazmen Mandjee
11 de enero de 2023	Reunión de todo el personal - taller	Paul Uithol & Ivan Gayton
1 de octubre de 2023	Formación de todo el personal	Jessie Pechmann, Paul Uithol, Ivan Gayton and Protection Focal Points