



Protocolo de Intercambio de Información del Clúster de Protección

1. Introducción

Este Protocolo de Intercambio de Información (PII) está diseñado para respaldar la gestión segura, ética y eficaz dentro del Clúster de Protección de Venezuela. Establece principios comunes, enfoques y responsabilidades para el intercambio de datos e información entre las diferentes funciones y actividades humanitarias. Proporciona un marco basado en una definición compartida de sensibilidad y condiciones para la divulgación.

Este documento ha sido diseñado para complementar las políticas y directrices existentes, sin que esto afecte ni sustituya en modo alguno las obligaciones contenidas en el ordenamiento jurídico nacional y reglamentos aplicables, los protocolos específicos de otros clústeres, ni las políticas de las organizaciones, incluido para la derivación de casos individuales.

El PII será revisado y actualizado anualmente, o a solicitud de los miembros del Clúster de Protección, a través de un proceso colaborativo supervisado por el Grupo Asesor Estratégico (GAE) del Clúster de Protección y sujeto a aprobación por parte los miembros regulares por mayoría simple.

2. Objetivo

Este documento establece directrices claras para el intercambio de información entre el equipo de Coordinación del Clúster de Protección y sus miembros, garantizando la confidencialidad, integridad y disponibilidad de la información. El Protocolo de Intercambio de Información (PII) abarca todas las actividades de gestión de datos e información en la respuesta humanitaria del Clúster de Protección de Venezuela, incluyendo tanto los datos brutos como los productos de información derivados.

3. Definiciones

Por “intercambio de información” se entiende la transferencia de datos o productos de información desarrollados a partir de ellos, ya sea a través de medios digitales (por ejemplo, correo electrónico, servicios de transferencia de archivos u otros) o medios físicos (por ejemplo, documentos impresos). La exposición de la información (por ejemplo, mostrar una pantalla con información, mostrar un informe) está incluida en esta definición y está sujeta a las mismas restricciones que la transferencia real de datos o información.

. A efectos de este PII, los datos y los productos de información (por ejemplo, infografías, gráficos y mapas, informes de situación, etcétera) desarrollados a partir de ellos se denominan “información”; ésta incluye lo siguiente:

- Datos sobre el contexto en el que se está produciendo una respuesta (por ejemplo, marcos jurídicos, condiciones políticas, sociales y económicas, infraestructura, entre otras) y la situación humanitaria de la que se centra (por ejemplo, incidentes de seguridad, riesgos de protección, impulsores y causas/factores subyacentes de la situación o crisis).
- Datos sobre las personas afectadas por la situación y sus necesidades, las amenazas y vulnerabilidades a las que se enfrentan, así como sus capacidades. En este sentido, se debe salvaguardar cualquier información personal que pueda identificar a la persona o personas afectadas con el evento que se comparte (ubicación, características personales/familiares, edad y por supuesto nombre y número de identificación).
- Datos sobre los actores de la respuesta humanitaria y sus actividades (por ejemplo, como se informa en 3W/4W/5W).



3.1 Tipos de Información

La información que se maneja desde el Clúster de Protección se divide en estas dos categorías:

- **Información Sensible:** Datos personales, informes de incidentes, evaluaciones de riesgos, productos del análisis de protección. Este tipo de información es de carácter confidencial.
- **Información Pública:** Informes generales, estadísticas agregadas, comunicados de prensa.

El Clúster de Protección será responsable de etiquetar la información compartida según estas categorías. Esto permitirá a los socios identificar claramente el tipo de información que reciben en todo momento.

3.2 Consideraciones

- **Documentos producto del Clúster de carácter restringido:** Documentos que incluyen análisis de protección, evaluación de riesgos e incluso información de contexto, contienen información sensible y confidencial con acceso restringido solo a miembros regulares.
- **Documentos de información clave:** Los informes detallados, que incluyen información de contexto como mapas de riesgo, evaluaciones de necesidades y análisis de protección, se compartirán exclusivamente con los miembros regulares. Como parte de este Protocolo, los miembros se comprometen a la información internamente y no redistribuirla sin autorización
- **Información para miembros Afiliados:** Se compartirá información general y pública relevante para sus actividades. No se brindará acceso a datos sensibles sin una verificación previa y aprobación del GAE.

4. Alcance

Este protocolo se aplica a todos los miembros regulares del Clúster de Protección, así como observadores y afiliados y a cualquier entidad colaboradora con la que se intercambie información desde el Clúster.

El PII cubre todos los datos operativos y la información generada y utilizada en la respuesta del Clúster de Protección, incluidos los productos de información

Este PII no se aplica a la gestión de datos "corporativos", como los datos relacionados con la gestión financiera interna, los suministros, los recursos humanos y el personal, y otras funciones administrativas de las organizaciones humanitarias. La gestión de dichos datos debe regirse por las políticas organizativas pertinentes. Este PII no sustituye ni modifica las políticas internas existentes relacionadas con las políticas organizativas obligatorias.

5. Principios

Este protocolo se basa en los siguientes principios de intercambio de información:

- **Confidencialidad:** Asegurar que la información sensible se maneje de manera segura y solo sea accesible para personas autorizadas. Para esto, se implementarán medidas de ciberseguridad adecuadas, como el uso de contraseñas, cifrado de datos y controles de acceso.
- **Integridad:** Garantizar que la información no sea alterada de manera no autorizada.
- **Disponibilidad:** Asegurar que la información esté disponible para los miembros autorizados cuando sea necesaria.

Además, haciendo referencia a los Términos de Referencia del Clúster, todo el trabajo hecho por el Clúster de Protección entendido como sus organizaciones socias se hace basado en los principios humanitarios, los principios de asociación y los principios de protección.



6. Procedimientos de Intercambio

- **Solicitudes de información:** Todas las solicitudes deben ser enviadas mediante correo electrónico al Clúster de Protección y deberán ser aprobadas por el GAE. Una vez aprobadas dichas solicitudes, la información será transmitida a los puntos focales registrados por cada organización para el clúster, y estos deberán salvaguardarla y solamente compartirla con otras personas de su organización en caso tener la autorización del GAE para ello.
- **Transmisión de información:** Se utilizarán canales seguros (correo electrónico cifrado, plataformas seguras de intercambio de archivos). Cuando se considere pertinente, algunas informaciones se transmitirán exclusivamente de forma oral durante espacios presenciales (como en reuniones mensuales o ad-hoc del clúster), para garantizar así el intercambio en un espacio seguro.
- **Almacenamiento de información:** La información debe ser almacenada en sistemas seguros con acceso restringido.
- **Accesibilidad:** El equipo del Clúster de Protección facilitará el acceso de los miembros a la información pertinente según su membresía considerando las barreras tecnológicas que puedan presentar.

7. Roles y Responsabilidades

- **Equipo de coordinación del Clúster:** Aprueba solicitudes de información junto al GAE, supervisa el cumplimiento del protocolo y se asegura que los diferentes roles estén alineados con los principios y objetivos de este protocolo para su efectiva implementación.
- **Miembros del Clúster:** Siguen las directrices del protocolo y reportan cualquier incidente de seguridad.
- **Equipo de reporte:** Consolida y presenta información relevante para el Clúster. Se asegura de que la información compartida sea precisa, oportuna y cumpla con los principios establecidos en este protocolo siguiendo las directrices de la coordinación.
- **Equipo de gestión de información:** Diseña, implementa y mantiene los sistemas seguros para la recopilación, almacenamiento y análisis de datos. Genera productos de información alineados con las directrices del protocolo.
- **Grupo Asesor Estratégico (GAE):** Proporciona dirección y orientación estratégica al Clúster de Protección. Contribuye con la revisión de documentos estratégicos y de políticas de protección clave.

8. Medidas de seguridad

- **Cifrado:** Se implementará el cifrado para la transmisión y almacenamiento de información sensible.
- **Acceso Restringido:** Implica limitar el acceso a la información compartida solo a individuos específicos. Esto se logra a través de la implementación de controles de acceso a nivel de gestión de documentación para minimizar el riesgo de que personas no autorizadas hagan uso inapropiado de esta información y afecten la integridad y confidencialidad de la misma.
- **Capacitación:** Proveer capacitación regular a los miembros sobre la importancia de la seguridad de la información y el uso de canales seguros para su divulgación.

9. Consideraciones de intercambio de información por tipo de membresía

9.1 Miembros Regulares

- **Acceso a Información:** Tienen acceso completo a todas las actas de reuniones del Clúster de Protección (CP) y otros productos del Clúster.
- **Intercambio de información:** Se espera que compartan información regularmente en los espacios del Clúster y reporten mensualmente a la 345W.



- **Confidencialidad y seguridad:** Deben adherirse estrictamente a las directrices del Protocolo de Intercambio de Información del Clúster de Protección, asegurando la confidencialidad y seguridad de la información sensible.
- **Tipos de información:** Los miembros regulares tienen acceso tanto a información pública y general como a información confidencial y sensible.

9.2 Observadores

- **Acceso a información:** Los miembros observadores pueden asistir a reuniones y eventos específicos del Clúster, así como podrán tener espacios de intercambio bilaterales previa solicitud y acceso a toda la información publicada en la página web. Asimismo, recibirán por correo electrónico los productos de información publicados.
- **Intercambio de Información:** Se les invita a participar en reuniones con socios, eventos específicos y encuentros bilaterales que promuevan el intercambio de información.
- **Confidencialidad y seguridad:** Deben adherirse estrictamente a las directrices del Protocolo de Intercambio de Información del Clúster de Protección, asegurando la confidencialidad y seguridad de la información sensible.
- **Tipos de información:** Pueden acceder a información pública y general, así como a información de interés que pueda ser sensible o confidencial.

9.3 Afiliados

- **Acceso a información:** Limitado. Pueden beneficiarse de la información compartida por el Clúster cuando se considere pertinente y seguro, y podrán solicitar espacios de intercambio bilateral.
- **Intercambio de información:** Se les invita a participar en reuniones o eventos ad-hoc del Clúster.
- **Confidencialidad y seguridad:** Deben adherirse estrictamente a las directrices del Protocolo de Intercambio de Información del Clúster de Protección.
- **Tipos de información:** Tienen acceso a información pública y general. En algunos casos, podrán acceder a información sensible luego de verificación previa por parte del GAE.

10. Mecanismos de intercambio de información

Para garantizar un intercambio de información eficiente y alineado con los principios de este protocolo, se adoptan los siguientes mecanismos:

- a. **Plataformas digitales:** Espacios virtuales y accesibles para todos los miembros, se gestionan a nivel central por el Clúster de Protección. Estos espacios son:
 - **Página web del Clúster de Protección:** Sitio web con información dedicada de los productos de información del Clúster con nivel de acceso público a documentos, factsheets, mapas, documentos de interés, entre otros. La información aquí presentada no compromete datos sensibles.
 - **Grupos de mensajería instantánea:** Canales privados para comunicaciones rápidas o urgentes, que serán utilizados solamente para informaciones logísticas y recordatorios de reuniones, pero nunca para compartir documentos o información sensible de contexto.
 - **Almacenamiento en la nube:** Carpetas o documentos compartidos para distribución o colaboración entre organizaciones.
- b. **Reuniones del Clúster:** Encuentros mensuales periódicos (presenciales, virtuales o híbridos) con los miembros del Clúster para discutir temas clave, coordinar acciones y tomar decisiones conjuntas.



- *Reuniones generales:* Se llevan a cabo mensualmente con las organizaciones miembros del Clúster de la que se hace una convocatoria de registro general que puede ser de formato presencial, híbrido o virtual. Para las reuniones de formato híbrido o virtual, la asistencia en línea es revisada y aprobada previamente por el equipo de coordinación antes de la emisión del enlace. En estas reuniones se comparte información de contexto, información de interés y acciones clave que pueden ser de carácter sensible o confidencial.
 - *Reuniones de grupo de trabajo:* Encuentros específicos entre las distintas temáticas de los grupos de trabajo. La información sobre los avances puede ser compartida durante las reuniones generales y, dependiendo del carácter de la información de los productos creados bajo estos grupos de trabajo, se publicarán en la página web del Clúster de Protección.
 - *Reuniones con Clústeres Subnacionales:* Reuniones de coordinación solo con puntos focales subnacionales. La información que se maneja en estos espacios es de carácter sensible y confidencial.
 - *Reuniones del GAE:* Reuniones periódicas o ad hoc solo con las organizaciones que han sido electas al GAE. La información que se maneja en estos espacios es de carácter sensible y confidencial
- c. Informes periódicos: Documentos elaborados de forma periódica para mantener informados a los miembros sobre avances de la respuesta, análisis de protección, riesgos de protección. Dependiendo de la información de estos documentos, serán compartidos de acuerdo al tipo de membresía.
- d. Redes de contacto: Son los canales de comunicación establecidos para facilitar el intercambio de información y comunicación entre el Clúster y los miembros. Algunos de estos canales son los siguientes:
- *Listas de correo electrónico:* Creadas para compartir información de forma eficiente y determinadas por tipo de membresía.
 - *Contactos personales:* Correo electrónico o números de teléfono para contacto directo.
 - *Eventos ad-hoc:* Espacios fomentados por el Clúster para conocer a otros miembros e intercambiar experiencias.
- e. Capacitaciones y asistencia técnica: Actividades formativas y de apoyo para fortalecer las capacidades de los miembros en áreas relevantes para el intercambio de información.
- *Talleres/webinars:* Sesiones prácticas sobre el uso de plataformas digitales, herramientas de recolección de información o análisis de datos.
 - *Asistencia Técnica (individual o grupal):* Espacios de apoyo técnico personalizado a miembros de forma individual o grupal para resolver dudas.

11. Cláusula de Responsabilidad.

Los socios serán responsables del manejo de la información suministrada por el Clúster de Protección, así como del cumplimiento de los principios expuestos en este protocolo, al que se adhieren. En caso de cualquier irregularidad presentada en la gestión de información sensible, esta será elevada al Grupo Asesor Estratégico, quien se encargará de evaluar y tomar las medidas pertinentes de acuerdo con el caso.

12. Revisión y Actualización

Este protocolo es un documento dinámico que será revisado y actualizado anualmente, o bien, cuando se considere necesario debido a cambios en las políticas o en el entorno de seguridad.

Fecha de lanzamiento: 01/04/2025



Fecha de revisión: 24/04/2025