Principios de la Gestión de la Información de Protección (PIM)[1]

Con base en la definición previamente acordada de Gestión de la Información de Protección (PIM), los participantes debatieron ampliamente para desarrollar más en detalle los siguientes principios guía que son considerados centrales para el trabajo y la aplicación de PIM, y que han surgido de anteriores foros y discusiones inter-agenciales[2]. Estos principios son subyacentes y caracterizan a todos los sistemas PIM, indistintamente de sus propósitos, métodos o productos[3].

● **Centralidad en las personas e inclusión**: las actividades PIM estarán guiadas por los intereses y el bienestar de la población, la cual debe participar y estar incluida en todas las fases o etapas importantes del Proceso PIM. Estas actividades deben tener un enfoque de edad, el género y diversidad.

● **No causar daño**: las actividades PIM deben incluir una evaluación de riesgos y tomar las medidas necesarias, si es necesario, para mitigar los riesgos identificados. La evaluación de riesgos debe analizar las consecuencias negativas que pudieran resultar de la recolección de datos y de las acciones subsecuentes o la prestación de servicios mientras la actividad PIM se esté llevando a cabo.

● **Propósito definido:** dada la naturaleza sensible y con frecuencia personal de la información de protección, PIM debe servir para definir las necesidades y propósitos de información específicos. El propósito tiene que estar claramente definido, ser comunicado y ser proporcional tanto al riesgo identificado como a los costos vis-à-vis de la respuesta esperada, y además debe estar orientado a las medidas de acción para obtener resultados de protección, incluyendo el intercambio y la coordinación de la protección de los datos y la información.

● **Consentimiento informado y confidencialidad:** la información personal se puede recolectar ÚNICAMENTE después de que se haya obtenido el consentimiento informado firmado por la persona en cuestión, y dicha persona debe estar consciente y al tanto del propósito de la recolección de datos. Además, la confidencialidad se debe explicar claramente ANTES de que se pueda recoger esa información.

● **Protección y seguridad de datos:** las actividades PIM deben estar alineadas con el derecho y los estándares internacionales de protección y seguridad de datos[4]. Las personas de interés tienen el derecho de que sus datos sean protegidos de acuerdo con los estándares internacionales de protección de datos.

● **Competencias y capacidades:** los actores que realizan actividades PIM son responsables de asegurar que dichas actividades sean realizadas por personal de protección y de gestión de información que hayan sido equipados con las competencias básicas PIM y hayan sido capacitados adecuadamente.

---

[1] Principios de Gestión de la Información de Protección, según lo desarrollado y acordado por las Partes Interesadas PIM en la Primera Reunión de Trabajo PIM, mayo del 2015. Traducción al español realizada en octubre de 2020.

[2] Desarrollados por los participantes en la Primera Reunión de Trabajo PIM realizada en Copenhague, 26 – 29 de mayo del 2015. Los principios PIM tienen en consideración los "Principios de Gestión e Intercambio de Información Humanitaria" avalados en el Simposio Global +5 en Ginebra, Suiza (2007) y los "Estándares Profesionales para Trabajos de Protección y Gestión de Protección de Datos Sensibles" de la Cruz Roja, Capítulo 6 (2013).

[3] Para saber cómo operacionalizar estos principios, consulte el sitio internet PIM en: pim.guide

[4] Incluyendo las "Directrices para la Regulación de Archivos de Datos Personales" de la Asamblea General de las Naciones Unidas de 1990.

● **Imparcialidad:** todos los pasos o etapas del ciclo PIM deben ejecutarse de una manera objetiva, imparcial y transparente, identificando y minimizando los sesgos.

● **Coordinación y colaboración:** todos los implicados en la implementación de las actividades PIM deben aceptar y adherirse a los principios presentados anteriormente y promover la más amplia colaboración y coordinación de gestión de datos e información, tanto a nivel interno, entre colaboradores humanitarios, como a nivel externo, con y entre otras partes interesadas. Las actividades PIM deben evitar la duplicación de otros esfuerzos PIM y en su lugar construir sobre los esfuerzos y mecanismos ya existentes.

Propósito Definido: dada la naturaleza altamente sensible y personal de la información de protección, PIM debe servir para definir las necesidades y propósitos de información específicos. El propósito debe ser proporcional tanto al riesgo identificado como a los costos vis-à-vis de la respuesta esperada, y además debe estar orientado a las medidas de acción para obtener resultados de protección.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir el propósito y las necesidades de información:**

● Defina los objetivos y actividades específicas de protección que se estarán alimentando del sistema de gestión de información. El propósito del Sistema o actividad de gestión de información tiene que estar dirigido a mejorar la seguridad y dignidad de las personas y poblaciones involucradas. Este sistema debe utilizarse para informar las actividades de protección. El propósito debe tener en consideración las necesidades de información de los individuos o de las comunidades afectadas para asegurar una rendición de cuentas efectiva ante ellas.

● Enfóquese en el propósito y la información que se necesita para cumplir dicho propósito más que en los datos mismos. Piense ampliamente en el propósito del sistema, de modo que la información crítica no se subestime o pase por alto. Cuando se define el propósito para el cual va a recolectar esa información, es importante también saber cuál es el objetivo o para qué va a usar usted esa información.

● Evalúe y especifique la audiencia que va a recibir los datos, la información y el análisis; quién utilizará esa información y cómo.

● Distinga entre lo que se considera esencial (la información que usted necesita tener y que estará en capacidad de utilizar y analizar) versus la información deseable (la información que sería interesante tener). Esta priorización también permite examinar la relevancia de las necesidades de información en contraposición al propósito y a la proporcionalidad, o balance, entre las inquietudes sobre los riesgos y beneficios esperados de esa actividad de recolección de información.

● A medida que el proyecto se vaya implementando y los datos se vayan recolectando, puede que surjan nuevas necesidades de información. El propósito tendría entonces que revisarse nuevamente en relación con esta nueva circunstancia. Si la tarea o necesidades de información cambian de modo significativo, es posible que deba definirse y aplicarse un nuevo propósito (y todos sus componentes asociados).

● En línea con los principios de protección de datos, la información no se puede utilizar para otros propósitos diferentes para los cuales fue recolectada originalmente y, en el caso de los datos personales, para el consentimiento que se otorgó. No se debe utilizar para otros propósitos sin el nuevo consentimiento adicional de uso y una evaluación posterior de los riesgos asociados con ese nuevo (s) propósito (s).

● Los actores de protección deben recopilar únicamente la información relacionada con abusos o violaciones cuando sea necesario para mejorar o permitir una respuesta de protección. Cuando se definen las necesidades de información, se debe asegurar que existe la capacidad de respuesta a las necesidades identificadas, o existen los procedimientos para derivar a las personas de modo apropiado.

● Defina las necesidades de metadatos.

● Reúna un grupo o equipo multifuncional de especialistas de gestión de la información y de otros sectores, cuando defina las necesidades de información.

● Siempre se hace la recolección de datos únicamente cuando estos son necesarios, y se tiene la intención de usar toda la información que se recolecte.

❖ **Revisión de datos e información:**

● Una segunda tarea es la revisión y las consultas con los socios relevantes que puedan ayudar a determinar si existen necesidades de información, si se puede acceder a ella y cómo. La información que necesitamos para cumplir con el propósito puede estar disponible, o se puede poner a disposición en un futuro cercano. Una revisión y consulta secundarias con los socios relevantes puede ayudar a establecer si esa información ya existe, si se puede acceder a ella y cómo.

● Haga uso de lo que ya había sido previamente recolectado para evitar la duplicación de esfuerzos, así como cargas innecesarias en cuanto a los riesgos para los sujetos que proveen sus datos.

DECIDA Y DISEÑE

❖ **Compartir información:**

● Una vez que el propósito está definido, compártalo con los interesados clave que contribuyan a asegurar que el propósito de recolección de información está bien entendido y acordado.

● El propósito del ejercicio debe dirigir o guiar las decisiones sobre si los datos se van a entregar o difundir a otros y cómo, con quién y a qué nivel de agregación. Determine la necesidad de una red o protocolo para compartir esa información, qué tipo de información se puede compartir y a qué nivel, y con qué personas, conforme al propósito acordado en el sistema de gestión de dicha información.

● Así se piense compartir o no la información, comunique el propósito del sistema de gestión de información a todos los socios y a otras organizaciones presentes. Esto crea la oportunidad de colaboración para lograr propósitos complementarios, evitar situaciones donde se busquen propósitos parecidos en esfuerzos paralelos, y ayuda a determinar si compartir ese tipo de información sería deseable.

● Todo sistema de recolección de datos debe tener el propósito de compartirlos hasta cierto nivel o análisis.

❖ **Diseño con la población afectada:**

● Las percepciones y el conocimiento de las poblaciones afectadas ayudan a identificar y entender mejor las necesidades, amenazas, vulnerabilidades y prioridades de los individuos, comunidades y grupos específicos dentro de esas comunidades, obstáculos potenciales, riesgos y beneficios asociados con el propósito y actividades PIM propuestas, sensibilidades culturales y sociales alrededor del uso de ciertas metodologías de recolección de datos o las herramientas, contexto y consideraciones de seguridad, etc.

● Haga una revisión detallada del propósito ya definido con las personas involucradas para asegurar que el propósito esté bien entendido como acordado. Consulte con la población afectada para asegurar que el propósito esté anclado en una realidad realmente fundamentada. Esto quiere decir que esté bien

entendido, que sea adecuado y ajustado a las circunstancias y que tenga alta probabilidad de cumplir con las necesidades para las que fue creado.

● Discuta las conclusiones de evaluación de riesgos con la población afectada para asegurar que esa evaluación refleje adecuadamente sus preocupaciones y experiencias.

● Comunique el propósito amplia, clara y regularmente. Ponga a disposición los mensajes en los idiomas locales, adaptados, personalizados al contexto operativo, y entregados por medio de métodos pertinentes a la protección y canales que sean accesibles y entendibles por varios grupos, como, por ejemplo, las personas iletradas o analfabetas, las personas con limitaciones para ver u oír, las personas de la tercera edad, los niños, los grupos marginalizados y otros grupos vulnerables. Tome en consideración las perspectivas internas y externas para verificar que el propósito definido las contiene a ambas: está matizado y reduce los sesgos potenciales.

❖ **Diseño del sistema de información:**

● Asegure que las modalidades de la actividad PIM y sus sistemas de información asociados estén guiados explícita y deliberadamente por medio del propósito específico del ejercicio. Es decir, explique los detalles sobre quién o quiénes pueden ser la población de interés de esa recolección de datos, cómo y cuándo se recogería esa información y los retos o problemas que se podrían esperar para cumplir con el propósito expuesto.

● Comunique claramente la información sobre el propósito de la actividad PIM a los colegas internos y los socios que estarán involucrados en dicho proceso.

● Asegúrese de que existe un entendimiento compartido interno que ayudará a prevenir el uso del tiempo en potenciales discusiones sobre la población meta de la recolección de datos, las metodologías y herramientas que se van a usar, y las redes o protocolos para compartir información que están implementados.

● Trabaje con evaluación de riesgos para asegurar que se respeta el principio de acción sin daño.

IMPLEMENTE

❖ **Realizar la recolección de datos**:

● Antes de la recolección de datos es importante que los recolectores de datos y el personal de terreno tengan una comprensión clara del propósito específico de la actividad PIM. Con la claridad del propósito se pueden evitar situaciones en las cuales se omita información considerada valiosa porque no se vio qué tan importante es, o se exponga a las personas a daños colaterales mediante la recolección de información sensible que al fin y al cabo no se va a utilizar posteriormente. La claridad de propósito permite a los recolectores de datos definir el umbral entre lo que es relevante y lo que es interesante, esto es, entre lo que sí se necesita para el propósito expuesto y lo que no. Esto también le da un significado específico a la recolección de datos cualitativos, donde las preguntas y herramientas con frecuencia están estructuradas menos estrictamente y existe mucha más responsabilidad para quien recoge los datos en términos de guiar la discusión.

● Los recolectores de datos deben comenzar su participación con la población meta mediante la comunicación clara de la información sobre el propósito de la actividad PIM. Esto es importante por varias razones:

o Para construir confianza y promover la cooperación de las personas a quienes se les van a pedir los datos; particularmente mediante la desmitificación de rumores y malentendidos. Por ejemplo, los informantes clave y las comunidades locales podrían no desear compartir información por el temor de que dicha información se vaya a compartir con las autoridades y, en consecuencia, pueda ser utilizada en su contra. En otros casos, puede que la gente sí quiera compartir la información porque asume que resultará en la entrega de asistencia humanitaria, lo cual puede traducirse en un estado de hostilidad y de falta de disposición para cooperar cuando no reciben esta asistencia. Explicar claramente el propósito de la recolección de información desde el principio puede aumentar las probabilidades de que la población de interés comparta la información, disminuyendo sus miedos y manejando sus expectativas.

o Crear una base sobre la cual la población de interés pueda entregar o retener su consentimiento informado.

❖ **Procesamiento y análisis:**

● El alcance, las herramientas y el nivel de análisis de datos deben estar guiados por el propósito específico de la actividad PIM. Por ejemplo, si el propósito es identificar los riesgos de protección para las personas desplazadas internas para informar respuestas efectivas (monitoreo de protección), el análisis descriptivo debe realizarse para resumir y comparar los datos y así dar respuesta a lo básico: "quién, qué, cuándo, dónde." Si el propósito fuera explicar por qué ciertos grupos parecen ser víctimas de ciertos tipos específicos de ataque, el análisis explicativo es más pertinente.

● Los principios de protección también deben guiar el proceso de análisis de datos, particularmente cuando involucre datos personales. Estos datos NO se deben procesar de un modo incompatible, irrelevante o excesivo con el propósito para el cual fueron inicialmente recolectados.

❖**Difundir y compartir:**

● Examine las necesidades que se desarrollan para ciertos grupos o niveles de información de protección, que puedan llegar a ser necesarios para tomar decisiones para la población afectada y cuál es la temporalidad para esa información.

● Asegure que los datos y la información se compartan a tiempo y de manera apropiada, accesible y predecible; basado en la definición del propósito, el análisis de las partes interesadas, y el acuerdo (al que se debe haber llegado con antelación) con dichas partes interesadas.

● Asegure que los riesgos hayan sido evaluados (otra vez) con una mirada de 360 grados para determinar si el contexto o el ambiente ha cambiado a tal punto que el intercambio o entrega de esa información podría llegar a hacer daño en lugar de cumplir su función.

● A menos que se haya obtenido el consentimiento específico, los datos personales no se deben publicar o transferir para propósitos diferentes a los establecidos cuando se recogieron esos datos, y para los cuales se dio ese consentimiento.

❖ **Almacenar y conservar:**

● El almacenamiento y conservación de datos están guiados por los principios de conservación de datos, de acuerdo con lo cual:

- o El periodo durante el cual se mantienen o conservan los datos personales no debe exceder el tiempo en el que se alcanzaría el logro del propósito específico.
- o Los datos personales se deben actualizar cuando sea necesario para asegurar que cumplen con el propósito para el cual son procesados.

EVALÚE

● Monitoree y revise el propósito: a medida que el proyecto se implemente y se recolecten los datos, puede que surjan nuevas necesidades de información. Si la tarea o las necesidades de información cambian significativamente, se debe definir y aplicar un nuevo propósito PIM (y todos sus componentes asociados).

Consentimiento informado: la información personal se puede recolectar únicamente después que se haya otorgado un consentimiento informado por parte de la persona en cuestión, quien debe estar al tanto del propósito para el cual se le piden esos datos. Además, la confidencialidad debe quedar claramente explicada a la persona antes de que la información se pueda recolectar.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir las necesidades de información:**

● Defina los propósitos y usos específicos para los cuales se necesitan datos personales o sensibles.

● Todos los datos personales, dependiendo del contexto, se pueden considerar como sensibles y como tal se debe asegurar que siempre sean tratados de modo confidencial.

● Identifique la información que requerirá el consentimiento informado o donde la confidencialidad pueda ser un asunto delicado.

● Verifique que cualquier información sensible y personal sea esencial para el análisis, de otro modo no recolecte esos datos o hágalo de modo anónimo.

● Los datos que puedan ser relacionados o identificables con una persona o personas en particular son ejemplos de información que requieren consentimiento informado.

❖ **Revisión de datos e información:**

● No pida información personal identificable de otras fuentes a menos que fuera necesario.

● Asegure que la confidencialidad y las prácticas de consentimiento informado se respetan en cualquier revisión secundaria de datos.

● Obtenga suficientes detalles sobre el consentimiento informado que provenga de una fuente de datos secundaria, incluyendo los propósitos para los cuales fueron recolectados esos datos y para los cuales se dio el consentimiento informado, para asegurar que el consentimiento informado original incluya el nuevo uso que se les pretende dar.

● Identifique las limitaciones que se puedan presentar con el consentimiento informado que se obtuvo anteriormente frente al propósito definido.

● Realice una revisión secundaria de datos sobre datos anonimizados a menos que estén planeadas intervenciones en casos individuales.

● De acuerdo con los principios de protección, a menos que se haya obtenido el consentimiento específico, los datos personales NO se deben publicar o transferir para propósitos diferentes a los cuales se autorizó la recolección original de datos, y para los cuales se otorgó el consentimiento. Esto aplica para una revisión secundaria de datos también. Incluya referencias al consentimiento informado.

DECIDA Y DISEÑE

❖ **Compartir información:**

● Discuta con los socios implicados en el intercambio de información cuál es el propósito que ellos tienen para esos datos y asegúrese de que sus propósitos estén suficientemente bien reflejados en el propósito general cuando se obtenga el consentimiento, o cuando se haya obtenido.

● Discuta con los socios implicados en el intercambio de información cómo minimizar la recolección e intercambio de datos personales para reducir los riesgos de incumplimiento en confidencialidad.

● Discuta y acuerde con los socios implicados en el intercambio de información sobre cómo se gestionarían esos incumplimientos de confidencialidad, como por ejemplo cuando los datos se comparten sin el consentimiento adecuado.

● Acuerde los procedimientos y respuestas a seguir cuando el consentimiento para compartir datos o información no esté otorgado o se rechace (por ejemplo, cuando un miembro de un hogar no esté de acuerdo en compartir su información o la de sus familiares).

● Los protocolos de intercambio de datos deben especificar la naturaleza y sensibilidad de los datos confidenciales.

● Los protocolos de intercambio de datos deben tener propósito(s) coherentes con aquellos especificados cuando se obtenga el consentimiento informado.

❖ **Diseño con la población afectada:**

● Explique la confidencialidad y el consentimiento informado en un lenguaje adaptado a la población general y con ejemplos relevantes al contexto.

● Trabaje con la comunidad para facilitar y desarrollar mensajes clave que sean claros sobre el consentimiento informado y la confidencialidad en relación con el propósito de la actividad de recolección de información.

● Discuta las implicaciones que surgen si las personas deciden no participar en la recolección de datos, o no están de acuerdo con compartir datos o con el propósito específico previsto dentro del consentimiento.

● Explique los acuerdos de intercambio de datos planeados (con quién, para qué), por ejemplo, las derivaciones a servicios especializados.

● Trabaje con la comunidad para comprender cómo la elección de un encuestador puede influenciar el consentimiento informado.

❖ **Diseño del sistema de información:**

● Diseñe la recolección de datos, el análisis y el almacenamiento de modo tal que se asegure que el consentimiento informado se almacene en relación con el propósito o propósitos específicos.

● Asegure que los datos personales y la información sensible se puedan almacenar de modo confidencial.

● Asegure que hay suficiente tiempo dentro del proceso de recolección de datos para obtener el consentimiento informado correspondiente.

● Si se recogen datos personales o sensibles, asegúrese de que los datos confidenciales sean recolectados garantizando que la población de interés esté en un espacio seguro y de un modo que garantice la confidencialidad.

● Haga pruebas a las declaraciones o frases utilizadas en los formatos de consentimiento informado con las personas de interés antes de recoger los datos.

● Diseñe las herramientas de recolección de datos para registrar si el consentimiento ya se obtuvo o no, y para qué propósito(s).

● Brinde la información pertinente sobre los planes de almacenamiento y retención de datos en el propósito y las declaraciones de consentimiento.

● Dependiendo de los datos que se recolecten y de su propósito, determine si el consentimiento se debe entregar por escrito o basta solamente con el consentimiento verbal. El consentimiento escrito, aunque es siempre preferible, muchas veces podría ser inapropiado si no se va a recoger información personal identificable (por ejemplo, no pida nombres en los formatos de consentimiento escrito si esos nombres no van a funcionar como parte de los datos a ser recolectados).

● Incluya los pasos a seguir para la obtención del consentimiento informado mediante procedimientos operativos estándar para la recolección de datos.

● Establezca un mecanismo que permita que la población de interés verifique, modifique o retire su consentimiento si así lo desean durante y después de la entrega de los datos, con lo cual también deberá alertar a los socios a los que haya transferido los datos cuando algún consentimiento o los datos hayan sido modificados por el sujeto proveedor de estos.

IMPLEMENTE

❖ **Realizar la recolección de datos:**

● Lea las frases que componen el consentimiento informado a los respondientes al comienzo de la entrevista.

● Uno de los padres o tutor legal debe proveer el consentimiento antes de la participación de cualquier menor de edad.

● Cuando se entreviste a una persona, brinde a los respondientes la información sobre:

- o Propósito de la entrevista / evaluación.
- o Duración esperada de la entrevista y sus procedimientos.
- o Datos o información que se van a recolectar, incluyendo por ejemplo fotos, videos y audios, si fuere el caso.
- o Cómo se pretende utilizar los datos.
- o Cómo se van a almacenar los datos y por cuánto tiempo.

- Afirme que la participación es voluntaria.
- Riesgos conocidos para el entrevistado (¿es posible hacerlo o es un riesgo?)
- Beneficios potenciales para el respondiente.
- Derecho del respondiente para poner quejas en caso necesario y ante quién lo puede hacer.
- El respondiente podrá rehusarse a contestar cualquiera o todas las preguntas y podrá terminar su participación en cualquier momento si así lo desea.
- Derecho a la confidencialidad.

❖ **Procesamiento y análisis:**

● A menos que sea necesario para el propósito específico, los datos personales se deben anonimizar antes de almacenamiento y análisis.

● En caso de que se requieran datos personales para un propósito específico (por ejemplo, dirigir asistencia o ayuda a una persona en particular), el procesamiento no se debe hacer sin la previa descripción explícita de su propósito y únicamente se hará para ese propósito descrito, y después del consentimiento informado proporcionado por el individuo en cuestión.

● Retire cualquier dato o información para los que no se obtuvo consentimiento a partir del análisis y de los procedimientos para compartir datos.

❖**Difundir y compartir:**

● En general, el intercambio y la difusión de datos o información debería hacerse en un formato anexo o con base en datos anonimizados o no identificables.

● Comparta únicamente la información que sea identificable para los propósitos descritos en el consentimiento informado y cuando el consentimiento haya sido obtenido.

● Asegure que los procedimientos para compartir datos respeten la confidencialidad de los datos y la información.

● Cuando se difundan o compartan datos, comparta la información sobre el consentimiento obtenido y para qué propósito.

❖ **Almacenar y conservar:**

● Solo almacene información identificable cuando sea absolutamente necesario y cuando el consentimiento informado haya sido obtenido para este propósito.

● Almacene la información únicamente por el tiempo que sea necesario para cumplir el propósito establecido.

● Se deben establecer políticas y procedimientos de liberación o eliminación de datos con un enfoque particular en los datos personales y altamente sensibles.

● Se deben tener acuerdos de almacenamiento y rechazo de datos para propósitos particulares, de modo tal que el consentimiento informado siempre se pueda respetar durante todo el tiempo o periodo en el cual se tengan los datos bajo custodia.

● Disponga o elimine los datos según se haya establecido en el consentimiento informado.

No causar daño: las actividades PIM deben incluir evaluación de riesgos y toma de medidas, si se consideran necesarias, para mitigar esos riesgos identificados. La evaluación de riesgos debe enfocarse en las consecuencias negativas que puedan resultar de la recolección de datos y las acciones subsecuentes o la entrega de servicios durante el período en que se lleve a cabo la actividad PIM.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir el propósito y la necesidad de información:**

● Las necesidades de información deben ser pertinentes con el propósito y proporcionales a los riesgos del ejercicio. Los actores de protección solamente deben recolectar información sobre abusos y violaciones cuando sea necesario para el diseño o implementación de actividades de protección.

● Defina los datos sensibles dentro del contexto operativo específico. Este es el conjunto de información o datos que se pueden utilizar de forma inadecuada, ya sea voluntaria o involuntariamente, y causar daños en el bienestar físico, legal, material o psico-social y los intereses de la persona de interés. Revise periódicamente esta definición.

● Cuando se determina la naturaleza, el alcance y el nivel de detalle de las necesidades de información, deben evaluarse los riesgos potenciales para todas las partes involucradas o afectadas por tal ejercicio. Reflexione sobre quién será la población meta para la recolección de datos, y a qué nivel de precisión, profundidad, confiabilidad y exactitud se debe recolectar los datos para lograr el propósito.

● Haga un balance sobre la necesidad de recolectar información para lograr una acción positiva y el riesgo potencial de causar daño tanto a las personas que entregan y a las que recolectan esos datos. Piense cuidadosamente en el equilibrio aceptable entre los riesgos esperados y los beneficios de este tipo de ejercicios, y sus vulnerabilidades, o la afectación que se busca evitar o remediar.

● Cuando se evalúen riesgos, tenga presente que los datos recolectados para un propósito específico, podrían utilizarse en el futuro para otro propósito, y los datos que podrían estimarse inocuos en este momento, podrían convertirse en sensibles con el paso del tiempo, dependiendo de cómo se utilicen o cómo evoluciona el contexto de seguridad y político. No recolecte datos a menos este seguro que serán utilizados; al hacerlo así, se reduce significativamente el riesgo de causar daño.

● Los datos sobre violencia sexual solamente se deben recolectar cuando haya servicios disponibles; si los servicios no se encuentran disponibles, la información sobre violencia de género o sexual solamente se puede recolectar una vez se hayan identificado modalidades específicas dentro de un contexto seguro, incluyendo indicadores indirectos e información clave, para el propósito de establecer los servicios adecuados, brindar información a los actores o participantes que estén planeando facilitar los servicios adecuados o informar sobre los esfuerzos de incidencia.

● Realice un análisis de posibles acciones con daño para identificar riesgos, oportunidades, asuntos legales y éticos relacionados con los datos a recolectar, procesar, analizar y diseminar. El propósito definido debe evaluarse frente al riesgo potencial: riesgo en la recolección, no recolectar, riesgo al compartir o difundir esos datos, no compartir, riesgo para las personas, riesgo para los colegas, respuesta humanitaria. Esto debe ser una visión de 360° sobre el riesgo. – personas de interés, riesgos para el personal y colegas.

Explore las necesidades de revisar los asuntos éticos y legales a través de un asesor externo o independiente o a través del uso de paneles internos o alianzas.

● Defina, discuta y evalúe el riesgo del uso de datos e información a nivel comunitario.

❖ **Revisión de datos e información:**

● Haga una revisión de datos secundarios (SDR) para identificar riesgos asociados con ciertos tipos de categorías de datos o métodos de recolección.

● Consulte con socios y otras organizaciones presentes sobre sus actividades y lecciones aprendidas y para identificar oportunidades de colaboración y compartir datos. Esto permitiría evitar la duplicación de esfuerzos de recolección de datos, así como cargas innecesarias y riesgos para la población de interés.

● La revisión de datos secundarios y las consultas determinarán si las informaciones que se necesitan están disponibles, si son creíbles y confiables, y si se podría acceder a ellas. Siempre recolecte nicamente los datos que se necesitan y use todo lo que ya se encuentra disponible.

DECIDA Y DISEÑE

❖ **Compartir información:**

● La información que se comparte correctamente promueve los propósitos de protección ya que disemina información sobre las necesidades y posibles amenazas sin exponer a la población de interés a preguntas repetitivas o a una atención que no es bienvenida. No obstante, a las personas se les puede ayudar, así como también causarles daño cuando se comparten los datos.

● La decisión de compartir información se debe basar siempre en un análisis serio de riesgos y beneficios, consideraciones éticas y legales, tener en cuenta la sensibilidad de las variables específicas de los datos, la privacidad y seguridad de los individuos, y su consentimiento informado (en el caso de los datos personales). Dado que se evalúan los riesgos y beneficios de compartir los datos, los criterios deben ser el mejoramiento del entorno de protección de los individuos y de las comunidades evaluadas.

● Dentro del marco del consentimiento informado, es responsabilidad ética, de los titulares o custodios de los datos y la información, compartir la información de modo seguro y útil con los interesados que estén en posición o tengan la responsabilidad de responder a los asuntos que surjan de tales datos o manejo de esa información.

● Los datos que permitan identificar personas no se deben recolectar o compartir a menos que sean absolutamente esenciales para el bienestar y la protección de la persona en cuestión, y considerando lo ético y lo legal, sobre el alcance del consentimiento informado previamente obtenido, y si es proporcional al propósito específico para el cual esos datos fueron recolectados.

● Identifique formas de compartir los datos con seguridad dentro de un contexto particular para minimizar el impacto negativo sobre el individuo o su comunidad.

● Considere la estructura legal local sobre cualquier obligación de compartir información y datos bajo leyes nacionales dentro de un proceso de evaluación de riesgos, ya que precisamente la estructura legal local podría generar riesgos potenciales para los sujetos propietarios de los datos.

● Las decisiones de compartir o retener datos que puedan identificar individualmente a menores se deben tomar con base en la determinación del interés superior del (la) menor.

● Asegure que los datos son analizables y transferibles de una manera conveniente a través de la elaboración de metadatos adecuados.

● Los protocolos y acuerdos de intercambio datos deben utilizarse para formalizar las transferencias de datos y para asegurar que las consideraciones de protección se evalúan sistemáticamente. Además de las salvaguardas de protección de datos e información y los procedimientos en caso de brechas de seguridad de datos, los protocolos deben describir las modalidades procedimentales y técnicas mediante las cuales la información se va a compartir; el nivel de agregación (tipológica, demográfica, lugar, y tiempo); los metadatos específicos, y la naturaleza de la confidencialidad y la responsabilidad legal.

● También se pueden crear redes más amplias o más informales para compartir datos. Se debe realizar una evaluación para identificar los riesgos y beneficios que implica involucrar a diferentes partes interesadas en la red. Por ejemplo, las autoridades locales a veces pueden ayudar a solucionar asuntos de protección, pero también podrían tomar retaliaciones o castigar a individuos o comunidades por haber compartido ciertas informaciones. Para mitigar tales riesgos, las diferentes partes interesadas en la red podrían tener acceso a diferentes niveles y tipos de información. Un memorando de entendimiento (MOU, por sus siglas en inglés) debería también guiar los roles, funciones y responsabilidades para todos aquellos involucrados, así como las salvaguardas para preservar la privacidad, confidencialidad y seguridad de la información personal de acuerdo con los estándares de protección y recolección de datos.

● En la mayoría de los casos, los datos que pueden identificar a las personas se deben retirar, ya que con frecuencia se pierde el control de cómo esa información va a ser utilizada y con quién podría ser compartida. Cuando los datos son confidenciales o sensibles, se pueden analizar y compartir den forma de tendencias (SIN información personal), en lugar de los datos específicos, utilizando métodos como por ejemplo la codificación de datos, la pseudonimización y anonimización.

❖ **Diseño con la población afectada:**

● Las poblaciones afectadas y otras personas que estarán involucradas o afectadas por el trabajo PIM, pueden ser incluidos en el diseño del trabajo. Pueden ayudar a quienes realizan las estrategias a identificar y comprender mejor los riesgos de protección, vulnerabilidades, amenazas y estrategias de cubrimiento y alcance, así como las medidas de mitigación factibles y adecuadas.

●Las poblaciones afectadas pueden ayudar en el mapeo de partes o personas interesadas para identificar quiénes serían los afectados, bien sea directa o indirectamente, por medio del ejercicio PIM, y cuáles serían las afectaciones que podrían ocurrir a corto, mediano y largo plazo. También pueden ayudar a analizar ciertos escenarios y predicciones con base en su comprensión del contexto local.

❖ **Diseño del sistema de información:**

● Revise las necesidades de información o evite recolectar ciertos tipos de datos si el riesgo de causar una acción con daño es demasiado alto o desproporcionado comparado con los beneficios esperados, si las medidas de mitigación no se pueden implementar o si no existe suficiente información para determinar de manera informada el nivel de riesgo.

● Asegúrese de que los metadatos están suficientemente desarrollados para reflejar la información necesaria y evitar el daño, incluyendo el reporte sobre riesgos asociados con el uso y la recolección de datos.

● Defina los mecanismos de rendición de cuentas de todas las partes involucradas en los procedimientos operativos estándar.

● Defina un mecanismo claro de depuración de datos en todo análisis o conjunto de datos antes de compartirlos e integrarlos en las directrices escritas relacionadas con el sistema PIM que se esté implementando.

● Disponga medidas para reducir los riesgos identificados y potenciales (información anonimizada, codificación de organizaciones y nombres de personas o empleados, no registrar información sensible si no es necesario). Cuando los beneficios esperados impliquen riesgos, o las medidas de mitigación no sean posibles, no recolecte ningún tipo de información; identifique los elementos y grupos de datos potencialmente sensibles, y evalúe los riesgos asociados al almacenamiento de dichos datos. Si hay riesgos en la recopilación de los datos, considere fuentes y métodos alternativos, posibles sesgos, el impacto de la frecuencia de recolección, lugares y / o métodos de recolección alternativos, y las posibilidades de hacer imputación de datos mediante aproximaciones o extrapolaciones. En general, NO recolecte datos que sean especialmente sensibles.

● Incluya salvaguardas para preservar la privacidad, la confidencialidad y seguridad de la información personal de acuerdo con los estándares de protección y recolección de datos que deben quedar establecidos como parte de esta discusión antes de la recolección de los datos.

● Disponga salvaguardas para reducir la posibilidad de fraude o robo de identidad.

● Escoja un ambiente de entrevista que permita la confidencialidad (por ejemplo, no entreviste públicamente a una sobreviviente de violencia sexual basada en género (VSBG) siendo consiente del estigma social que puede estar relacionado con ese tipo de casos.

● Tenga en cuenta consideraciones de control de multitudes para el diseño de su sistema de recolección de datos o información y cómo reaccionar en caso de amenazas de seguridad o físicas.

● Recolecte únicamente los datos e información que se requieran para la programación y respuesta de protección, como los datos e información que no se encuentren disponibles a través de revisiones secundarias de datos, que no estén siendo recolectados por otros socios y que son cruciales para una respuesta informada de protección. Los actores de protección deben recolectar la información sobre abusos y violaciones únicamente cuando sea necesario para el diseño o implementación de actividades de protección. No recolecte datos a menos que esté segura(o) de que los va a utilizar.

● Evaluación de riesgos y beneficios previa a la implementación. Las metodologías de recolección potenciales se deben evaluar según su impacto esperado en cada categoría de personas involucradas en el ejercicio: el entrevistador o recolector de datos, las fuentes potenciales de información, incluyendo a sus familias, y otras personas que puedan cooperar (por ejemplo, conductores, intérpretes de idioma, personal de ONG locales, etc.).

● Ciertos elementos de datos podrían poner en riesgo tanto a la persona entrevistada o al grupo al que se le esté tomando la información como al entrevistador. Identifique métodos alternativos o indicadores

correlacionados si ciertos elementos de datos son demasiado sensibles, o identifique posibles medidas de mitigación. Las medidas para reducir amenazas y vulnerabilidades deben incluirse en todas las directrices o instrucciones. Los sesgos que pudieran afectar la recolección de información también deben identificarse y mitigarse.

● Los roles, funciones y responsabilidades de todos los actores involucrados en la recolección de datos se deben identificar claramente, así como los protocolos para la transferencia segura de datos desde el punto de recolección hasta su punto de almacenamiento y uso (ver principio de "Protección y seguridad de datos").

IMPLEMENTE

❖ **Realizar la recolección de datos:**

● Evalúe e informe a todo el personal involucrado si el proceso de recolección de datos y el contenido de los mismos podría poner en riesgo y causar algún tipo de daño a las personas involucradas o afectadas por el ejercicio. Continúe evaluando y monitoreando a los riesgos durante la recolección de los datos.

● No fuerce a los individuos / comunidades a contestar preguntas con las que no se sientan cómodos. Con base en el contexto específico, ponga atención a la presencia de otras personas que estén observando la actividad de recolección sin participar.

● Ponga atención a cualquier signo de miedo en los individuos / comunidades durante la recolección.

● Informe a las personas que pueden rehusarse a participar en la recolección de datos y no tienen que proveer ninguna información que no deseen. Las personas pueden dejar de dar información en cualquier momento.

● Cuando se recolectan datos personales, permita que las personas verifiquen que la información registrada es correcta y permítales hacer correcciones o eliminación de datos.

● Las medidas de prevención y mitigación son especialmente importantes durante esta fase, ya que con frecuencia involucrarán contacto directo entre el recolector y la persona que provee los datos. Estas medidas pueden incluir el uso de fuentes alternativas de datos, variables e indicadores de datos, y métodos alternativos de recolección, frecuencias de recolección, grupos objetivo y lugares.

● El proceso de recolección debe estar guiado por estándares éticos y un código de conducta que ha sido firmado y entendido por los encuestadores. Los códigos de conducta personal son esenciales para asegurar que ninguna acción o inacción individual pueda causar daño, bien sea intencional o no intencional, o genere riesgos adicionales para las comunidades afectadas y terceros involucrados en el ejercicio. También son cruciales en la definición clara de los perímetros de práctica aceptable, comportamientos y conducta personal, y enfatizan el deber de respetar los derechos de las personas proveedoras de la información. Entre otros, tienen el derecho de rehusarse a compartir información, a que se acceda a su información, y a reportar cualquier mal uso o abuso. Cuando se recolectan datos, los encuestadores deben informar a las personas sobre los propósitos específicos para los cuales se van a recoger y procesar esos datos, cómo se van a usar sus datos, si sus datos se van a compartir con otras organizaciones, y otras situaciones básicas sobre el ejercicio. Los respondientes tienen el derecho a no compartir información y nunca deben ser coaccionados.

● El proceso de recolección de datos debe estar monitoreado cuidadosamente para asegurar que tanto el código de conducta como los procedimientos operativos sean respetados. El monitoreo también permite adoptar medidas reparadoras si el ejercicio está originando riesgos de protección o de seguridad. En este sentido, la capacitación a los entrevistadores debe incluir guías escritas y ejemplos prácticos de cómo promover la participación de los respondientes y reaccionar a amenazas de protección. Por ejemplo, se deben recolectar datos en lugares seguros y silenciosos, teniendo en cuenta la privacidad, confidencialidad y seguridad, así como la sensibilidad de la información que se está recibiendo. También se debe poner atención a señales de los respondientes mostrando tener miedo o que están incómodos, o que otros individuos están presentes y están observando la recolección de los datos. Por ejemplo, las mujeres que reportan violencia sexual no deben ser entrevistadas en sitios públicos, donde probablemente no pueden compartir sus historias y podrían ser atacadas o estigmatizadas si su historia la escuchan otras personas. El personal nacional podría ser particularmente vulnerable, dado que ellos pueden ser vistos como facilitadores de la recolección de información sensible para actores internacionales quienes podrían o no ser de confianza para la comunidad, o ser chivos expiatorios cuando no se entregue asistencia después de la recolección de información.

❖ **Procesamiento y análisis:**

● Igual que con la recolección de datos, el proceso de análisis de datos puede poner a las personas involucradas en riesgo, dependiendo del tipo de análisis realizado, las herramientas utilizadas para el procesamiento de datos, las unidades de medida y el nivel de agregación.

● Considere si el análisis a realizar pudiera ser combinado con otros análisis pasados o actuales de forma tal que exponga las fuentes de información a daños y cómo podría suceder, o si el análisis de datos podría ser malinterpretado en detrimento de las personas de interés. El análisis siempre debe estar enlazado e informado por el propósito específico de la actividad PIM.

❖**Difundir y compartir:**

● Identifique y utilice mecanismos de gestión de información de base comunitaria y apóyelos para compartir retroalimentación o información importante de protección.

● Antes de compartir la información, esta podría tener que ser seleccionada o filtrada, y presentada de diferentes modos, a través de diferentes medios / canales, o en diferentes niveles de agregación. La necesidad de tales ajustes dependerá del receptor de la información y su audiencia(s), de porqué y cómo se usará esa información, y de la probabilidad de que sea compartida posteriormente con terceras partes.

● Se debe desarrollar una estrategia de diseminación en la fase de planeación, a través de un lente de protección. La estrategia debe comenzar con la premisa de que los datos, que permitan identificar a una persona en particular, deben compartirse con base en las necesidades y en las consideraciones de protección.

● El principio “no hacer daño” promueve una evaluación responsable de las diferentes herramientas y plataformas que se pueden utilizar para difundir la información, y a qué nivel de agregación. En muchos casos, especialmente cuando los datos son confidenciales y sensibles, la información se puede difundir a manera de tendencias para balancear los beneficios esperados de la recolección de datos con los riesgos potenciales.

❖ **Almacenar y conservar:**

● Para evitar afectaciones, los datos tienen que gestionarse, almacenarse, archivarse y depurarse o suspenderse de forma segura. Las personas involucradas o afectadas por el trabajo PIM podrían quedar expuestas a violencia física, discriminación, explotación o cualquier otra clase de afectaciones si los datos no se usan bien, se pierden, se los roban, se usan sin autorización, se modifican, se contaminan, se copian o se entregan a terceros. Tales consideraciones deben guiar el diseño de los sistemas de información que se utilizarán a lo largo del ciclo de vida del trabajo PIM, así como orientar las discusiones sobre la transferencia, la propiedad y las responsabilidades sobre esos datos.

● Asegúrese de tener planes de contingencia para destruir o transferir de manera segura los datos en casos de emergencia.

● Siempre de forma segura, los datos y la información deben transferirse desde el lugar donde fueron recolectados hacia los usuarios finales, así como gestionarse, archivarse y depurarse. Por ejemplo, enviar datos por medio de teléfonos móviles que luego se pueden borrar podría ser una opción más segura que viajar con cuestionarios impresos en papel, especialmente cuando se viaja a través de puntos de control militares, migratorios, cruces de fronteras o líneas de conflicto. La seguridad tanto del papel como de los registros electrónicos tiene que estar garantizada.

● Defina la propiedad del RESULTADO DE LOS DATOS ANALIZADOS recogidos y las personas que tendrían el derecho de acceso a esos archivos de datos y asegúrese de que la organización(es) que SON LOS CUSTODIOS de los datos han establecido soluciones técnicas para proteger el archivo (por ejemplo, con una clave de acceso).

● Se deben establecer salvaguardas para preservar la privacidad, confidencialidad y seguridad de la información personal de acuerdo con los estándares de protección y recolección de datos, como también con su almacenamiento y archivo. Si los datos se almacenan en línea, evalúe la seguridad del servidor que almacena esos datos y mitigue los riesgos al anonimizar la información personal.

● Los datos sensibles, incluyendo los datos personales en algunas circunstancias, deben borrarse cuando ya no se necesiten para el propósito identificado.

● Ver Principio de “Protección y Seguridad de Datos” para más detalles.

EVALÚE

● Realice una revisión sistemática para identificar subconjuntos de datos que no fueron usados para el análisis y para las acciones de respuesta, que pueden servir de insumo para futuros ejercicios de recolección de datos.

Protección y seguridad de datos: PIM debe respetar y cumplir los estándares internacionales de protección y seguridad de datos.[5]

EXPLORE EL PANORAMA DE LA INFORMACIÓN.

❖ **Defina las necesidades de información:**

● Identifique y comprenda las implicaciones de la protección de datos que traen consigo las necesidades de datos de sus operaciones y de sus socios. Familiarícese con los tipos de datos personales y sensibles dentro de su operación y documéntelos en un lenguaje sencillo y claro.

● Identifique las políticas y directrices de protección de datos sobre recolección, análisis y procesamiento de datos de su organización.

● Identifique el marco jurídico relevante que regula la recolección y protección de datos en la zona, incluyendo los derechos legales de los sujetos que proveen los datos.

● Identifique los datos e información que pudieran generar riesgos de protección en relación con el proyecto propuesto y defina las medidas de mitigación que se recomendarían para garantizar la protección y seguridad de los datos, incluyendo las violaciones de datos personales u otras fallas en las medidas de protección de los datos.

● Verifique que cualquier información sensible y / o personal propuesta para la recolección de datos tenga un propósito definido y que la utilidad de los datos supere los riesgos asociados con la adquisición de estos. Si los datos no son esenciales para la toma de decisiones o para las necesidades programáticas, no recolecte los datos.

● Documente los riesgos asociados con la recolección, análisis y procesamiento de datos e información. Si es apropiado, considere establecer un procedimiento para la autorización o uso de datos sensibles de protección para salvaguardar los procedimientos apropiados de intercambio y diseminación.

❖ **Revisión de datos e información:**

● Realice una revisión secundaria de datos (SDR, por sus siglas en inglés) para maximizar el uso de los datos ya existentes, evitar la duplicación y minimizar riesgos posibles tanto para la población de interés como para su información.

● Verifique si los datos existentes han sido recolectados y procesados de acuerdo con los principios de protección de datos. Evite utilizar datos que no hayan sido recolectados, procesados o utilizados de acuerdo con los procedimientos fundamentales de protección de datos.

[5] Incluyendo por ejemplo las Directrices de la Asamblea General de las Naciones Unidas de 1990 sobre la Regulación de los Archivos Computarizados de Datos Personales, "Estándares Profesionales para la Protección del Trabajo Realizado por Participantes Humanitarios y de Derechos Humanos en el Conflicto Armado y Otras Situaciones de Violencia" ICRC (2013), la Resolución de Madrid sobre los Estándares Internacionales para la Protección y Privacidad de los Datos Personales (2009), y la Política de Protección de Datos Personales de Personas de Interés para el Alto Comisionado de las Naciones Unidas para los Refugiados (UNHCR, 2015).

● Cualquier depósito de datos existentes, (materiales de revisión secundaria de datos, SDR) debe tener salvaguarda de los datos, información y fuentes dentro de la operación / zona de trabajo. Un depósito de SDR debe equilibrar el nivel de acceso y seguridad necesarios para garantizar un almacenamiento seguro y ético de todos los archivos recolectados de manera continua.

● Clarifique los inquietudes presentes y futuros sobre la propiedad de los datos, así como los mecanismos de rendición de cuentas en caso de brechas de seguridad de datos o el mal uso de los mismos.

● Realice una evaluación de riesgos y un análisis de correlación (ver las instrucciones de la Evaluación de Impacto de Privacidad (PIA, por sus siglas en inglés) / las Evaluaciones de Impacto de Protección de Datos, (DPIA, por sus siglas en inglés) para mayores detalles).

DECIDA Y DISEÑE

❖ **Intercambio de Información:**

● Verifique que los datos e información existentes se encuentran disponibles regularmente, son creíbles y confiables mediante la consulta con las fuentes de los datos. Si es así, trabaje con sus socios para implementar medidas predecibles para acceder, transferir y almacenar los datos de manera segura. Establezca protocolos para compartir los datos según sea necesario para fomentar el intercambio de datos de manera eficiente y ética a lo largo del tiempo.

● Establezca protocolos de intercambio de datos cuando sea necesario, y tome todas las medidas técnicas y organizacionales apropiadas para proteger los datos, en particular los datos sensibles de protección (incluyendo, pero no limitado a, los datos personales), del riesgo de destrucción accidental o ilegal / ilegítima, la pérdida, alteración y publicación no autorizada.

● Los protocolos para el intercambio de los datos deben estar diseñados bajo el principio de “No hacer daño”.

● Los protocolos para intercambiar los datos deben reflejar los riesgos evaluados para los recolectores de datos, y cómo estos riesgos serán mitigados cuando los datos se compartan y analicen. Los riesgos potenciales deben estar detallados en el protocolo.

● Los protocolos para intercambiar los datos deben definir los usos de datos anonimizados, así como los criterios para establecer cuáles datos se van a compartir y cuándo con las comunidades.

● Identifique las políticas, directrices y / o protocolos de protección de datos de la organización y sobre el intercambio, procesamiento y soluciones de almacenamiento de la información. Revise si la organización tiene un código de conducta (o una política semejante) que comprometa al personal para asegurar la confidencialidad de los datos, incluyendo cualquier medida obligatoria o rutinaria de confidencialidad.

● Verifique que cualquiera y todos los mecanismos de intercambio de información tengan procedimientos implementados para reportar y responder a posibles violaciones de datos (por ejemplo, los mecanismos de disputa jurídica).

❖ **Diseño con la población afectada:**

● Participe con las poblaciones afectadas para identificar qué tipos de datos e informaciones podrían ser vistos como sensibles, privados o confidenciales dentro de un contexto específico cultural, político y de seguridad.

● La protección de las personas es más importante que la participación de las comunidades.

● Respete los derechos de los sujetos que proveen los datos: el derecho a acceder a su propia información, el derecho a corregir y a borrar sus datos, y la posibilidad de quejarse si los datos se llegaren a utilizar de forma incorrecta.

● Trabaje con la comunidad para facilitar y desarrollar mensajes clave que sean claros sobre la protección y confidencialidad de los datos, específicamente relacionados con el propósito de la actividad.

● Explique a las personas de interés el principio de confidencialidad, la intención de uso de la información y cómo se protegerá la información, incluyendo los acuerdos de intercambio.

● Informe a las comunidades sobre los propósitos específicos para los cuales los datos se recolectan o procesan, y si los datos serán transferidos o compartidos con otras organizaciones.

❖ **Diseño del sistema de información:**

● Determine las medidas técnicas y organizacionales más adecuadas para garantizar la seguridad tanto de los archivos físicos como de los electrónicos de (pero no limitado a) los riesgos de destrucción accidental o ilegal / ilegítima, la pérdida, alteración, copiado, mal uso, contaminación y publicación o acceso no autorizados.

● Asegure que las medidas técnicas y organizacionales adecuadas estén implementadas para garantizar la seguridad tanto de los archivos físicos como de los electrónicos que se comparten, (incluyendo, pero no limitado a, un lugar seguro dentro de la oficina donde el acceso sea restringido a personal autorizado únicamente, barreras físicas, gabinetes metálicos con llave, etc.).

● Si cualquier parte de los procesos se van a subcontratar (recolección, análisis, almacenamiento de datos) con entidades privadas, verifique que existe un lugar definido para el almacenamiento, y que se conocen las leyes aplicables relacionadas con gestión y publicación de datos, que deben estar reflejadas en los acuerdos y contratos.

● Evalúe la metodología correcta a ser utilizada, incluyendo los mejores métodos de recolección de datos, y quién sería la persona indicada para recopilar los datos.

● Evalúe los riesgos con frecuencia y diseñe / adapte sistemas para garantizar un monitoreo y evaluación sistemáticos y consistentes sobre las amenazas y riesgos de protección de datos que vayan surgiendo. El monitoreo activo, así como la retroalimentación de las comunidades afectadas y de la población de interés, contribuirán a estas medidas.

● Verifique que los datos estén almacenados en un lugar seguro, donde el acceso esté limitado únicamente a personal autorizado (a través de tarjetas de acceso, barreras físicas, cerraduras, etc.).

● Determine los derechos apropiados de acceso a los datos dependiendo de las responsabilidades, necesidades y sensibilidad de los datos.

● Asegure que los parámetros del sistema estén en línea con los principios, y no solo desde un punto de vista técnico.

● Establezca medidas apropiadas de seguridad para archivos electrónicos y / o físicos, incluyendo, pero no limitado a:

- o Acceso regulado solamente por el personal autorizado, encriptado de archivos, y/o protección con contraseña;
- o Reducir al mínimo las contraseñas sistemáticas usadas para toda clase de equipo de tecnología, incluyendo dispositivos portátiles, como computadoras portátiles y teléfonos móviles;
- o Asegurar que se realicen copias de seguridad regularmente para prevenir la pérdida o daño accidental de los datos;
- o Proteja los medios para transferir datos a otras agencias/organizaciones (encriptado, archivos xml, etc.) durante todo el ciclo de gestión de información;
- o Establecer un procedimiento para reubicar (y, como último recurso, destruir) los archivos físicos y electrónicos en caso de una evacuación de emergencia;
- o Garantizar procedimientos para transportar los datos e información de manera segura a través de puntos de control y líneas de conflicto;
- o Definir las medidas adecuadas para proteger las entrevistas, por ejemplo, los datos de identificación personal (PID, por sus siglas en inglés) de los entrevistados y para que la información que brindan se mantenga separada de los reportes mediante un sistema de codificación estandarizado u otra medida similar.

● Desarrolle mecanismos de quejas y comentarios para que las poblaciones afectadas puedan reportar sus inquietudes sobre la seguridad de los datos y violaciones de la recopilación, el intercambio u otras inquietudes relacionadas con la protección de datos.

IMPLEMENTE

❖ **Realizar la recolección de datos**: la recopilación sistemática de datos según un propósito definido (paso 5)

● Asegure que existan medidas técnicas y organizacionales para garantizar la seguridad de los encuestadores, los entrevistados y de los archivos de datos físicos y electrónicos que se recopilan.

● Evalúe los riesgos con regularidad y diseñar/adaptar los enfoques de recopilación de datos para garantizar la seguridad de la recopilación de datos durante todo el ciclo de la iniciativa de recolección. El monitoreo activo, así como la retroalimentación de las comunidades afectadas y de los sujetos que proveen los datos, ayudarán con estas medidas.

● Verifique que existan medidas adecuadas para proteger los datos, en particular los datos sensibles de protección (incluidos, entre otros, los datos personales) ante el riesgo de destrucción accidental o ilegal/ilegítima, la pérdida, alteración y divulgación o acceso no autorizados (incluido el transporte y/o transferencias de los datos).

● En todo momento, esté atento a las señales de que la actividad de recopilación de datos pueda crear riesgos, o que las medidas de mitigación puedan estar fallando. Así, asegúrese de incluir "líneas rojas" o umbrales para cualquier momento o situación que pueda requerir el cese inmediato del proyecto y el despliegue de medidas correctivas o de mitigación.

❖ **Procesamiento y análisis:**

● Identifique y garantice el cumplimiento de las políticas y directrices de protección de datos de la organización sobre el procesamiento de cotejo, compilación y análisis de datos.

IDENTIFIQUE LOS DATOS QUE SE HAN RECOGIDO EN LA "ZONA GRIS"

● Identifique a un miembro del personal que sea responsable de la implementación y el cumplimiento de la política cuando corresponda.

● Capacite a todo el personal involucrado en el manejo de información sensible sobre protección de datos y estándares, habilidades, políticas y principios de seguridad. Esto incluye los tipos de datos personales y sensibles identificados dentro de la operación, (cerciórese de que éstos estén documentados y que sean conocidos por todos).

● Defina medidas apropiadas para proteger al usuario de problemas de privacidad, como la vigilancia, agregación inapropiada, exclusión, violación de la confidencialidad, al igual que la mayor accesibilidad, identificación de individuos o grupos y uso de datos secundarios.

❖**Difundir y compartir:**

● Asegúrese de que la decisión de difundir información públicamente se base en un análisis cuidadoso de los riesgos y beneficios, teniendo en cuenta los riesgos de protección de datos inherentes a cada herramienta y plataforma de difusión.

● No comparta datos si el riesgo de hacer daño es alto. Los datos se deben compartir solamente si el riesgo es bajo, si existen medidas para implementar la mitigación de este daño y si tiene suficiente información para tomar una determinación informada sobre el nivel de riesgo.

❖ **Almacenar y conservar:**

● En el contexto de los datos personales, los beneficiarios deben tener el derecho a acceder a su propia información sin demoras ni gastos indebidos, y en un formato que les resulte claro.

● Defina procedimientos claros para establecer la posesión/control/alojamiento/gestión de los datos, y los derechos relevantes de corrección, eliminación, archivo y destrucción de todo el almacenamiento y mantenimiento.

● Defina un sistema de clasificación para adaptar protocolos basados en evaluaciones de sensibilidad (por ejemplo, clasificando el daño potencial como bajo, moderado o alto).

● Redacte una lista maestra de quién tiene acceso a qué información y las autorizaciones necesarias.

● Para archivos físicos, mantenga archivadores con llave, acceso limitado a estos archivos al personal autorizado y cumpla todas y cada una de las políticas de protección de datos u otras pautas sobre el procesamiento de datos.

● Establezca medidas apropiadas de seguridad para archivos electrónicos y/o físicos, incluyendo, pero no limitado a:

- ● Acceso regulado por personal autorizado únicamente, encriptado de archivos y/o protección con contraseña;
- ● Cambie de manera regular las contraseñas usadas sistemáticamente para toda clase de equipo de tecnología, (incluyendo dispositivos portátiles, tales como computadoras portátiles y teléfonos móviles).
- ● Asegúrese de realizar copias de seguridad regularmente para prevenir la pérdida o daño accidental de los datos;
- ● Establezca procedimientos para reubicar (y, como último recurso, destruir) archivos físicos y electrónicos en caso de una evacuación de emergencia;
- ● Definir las medidas adecuadas para proteger las entrevistas, por ejemplo, los datos de identificación personal de los entrevistados y para que la información que brindan se mantenga separada de los reportes mediante un sistema de codificación estandarizado u otra medida similar.
- ● Desarrollar mecanismos de quejas y comentarios para que las poblaciones afectadas puedan, entre otras cosas, reportar inquietudes sobre la seguridad de los datos y violaciones de la recopilación, el intercambio u otras inquietudes relacionadas con los códigos de conducta.
- ● Para archivos físicos, mantenga archivadores con llave, acceso limitado a estos archivos al personal autorizado y cumpla todas y cada una de las políticas de protección de datos u otras pautas sobre el procesamiento de datos.

Imparcialidad: todos los pasos del Ciclo PIM se deben llevar a cabo de una manera objetiva, imparcial, y transparente identificando y reduciendo al mínimo los sesgos.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ Definir la necesidad de información:

● Asegure que las necesidades de información y de los datos se basen siguiendo un propósito definido, la proporcionalidad y la necesidad de establecer los hechos necesarios para una respuesta de protección informada.

● Aplique un acercamiento holístico que incluya todos los segmentos relevantes de la población, las ubicaciones y los riesgos. Identifique sesgos potenciales de todos los segmentos relevantes que puedan estar presentes.

● Confíe en la información y los hechos basados en la evidencia y en los supuestos fundamentados para fundamentar la comprensión y las decisiones como herramienta principal para garantizar la imparcialidad.

● Garantice la transparencia y que se consulte a todas las partes interesadas relevantes (incluyendo reevaluar las necesidades de información según los hallazgos) desde la recopilación de datos hasta el análisis en todos los aspectos de PIM con procedimientos operativos estándar claramente definidos que describan el propósito definido (necesidades de datos e información), la metodología, los roles y las responsabilidades, desde el inicio de cualquier actividad PIM.

❖ Revisión de datos e información:

●Asegúrese de que los criterios para la revisión secundaria de datos estén claramente establecidos, actualizados, sin sesgos y que las fuentes de los datos y la información sean objetivas y estén documentadas.

● Los datos y la información deben evaluarse/triangularse según la confiabilidad de la fuente, cuando sea posible, así como la credibilidad, la contextualización de la información, la metodología utilizada para producir la información y los posibles sesgos inherentes observados en cualquier fuente determinada. Los datos deben aceptarse mediante un proceso de colaboración con socios y partes interesadas o deben excluirse de la revisión de la revisión secundaria de datos.

DECIDA Y DISEÑE

❖ Compartir información:

● Asegúrese de que los procedimientos para la recopilación y el intercambio de información dentro de la comunidad de partes interesadas sean coordinados, imparciales, transparentes, documentados y compartidos.

● Asegure la imparcialidad contactando a todas las partes interesadas relevantes, a través de protocolos establecidos y mutuamente acordados para la recopilación, el intercambio y la revisión de información.

● Póngase de acuerdo en los usos y parámetros de los datos y la información compartidos que se han recopilado conjuntamente, es decir, los datos y la información compartidos solo pueden usarse de manera

transparente, dentro de los parámetros acordados para una interpretación responsable y para propósitos específicos definidos que beneficiarán a la población de interés.

● Establezca un acuerdo sobre cómo la comunidad de las partes interesadas puede responder o mitigar el sesgo identificado, es decir, posiblemente compartiendo los datos o la información, o acordando compartir el sesgo identificado u otras limitaciones de manera transparente en la metodología, lo cual asegura también la consistencia en el uso de los datos y la posibilidad de replicar el proceso. Se puede acompañar, por ejemplo, con un análisis final o cualquier interpretación o uso de los datos.

❖Diseño con la población afectada:

● Identifique y mitigue situaciones que pueden llevar a la exclusión de las personas de interés en función del tiempo, la capacidad en el lenguaje, etc.

● Trabaje con la población de interés para identificar áreas de posibles sesgos que puedan afectar la forma en que se relacionan con los colegas dentro de la comunidad humanitaria, especialmente en el contexto de ejercicios de recopilación de datos compartidos.

● Pruebe los cuestionarios con miembros de la población de interés para verificar y asegurarse de que no haya preguntas inductivas, sesgos ocultos o problemas de mala interpretación en las preguntas o cuestionarios de recopilación de datos.

● Trabaje con las partes interesadas de la comunidad humanitaria para definir y difundir mensajes transparentes sobre el propósito, el alcance y el uso de cualquier ejercicio de recopilación de datos con suficiente tiempo antes de su inicio.

● Asegúrese de que el personal que trabaja con las personas de interés esté bien informado y entregue un mensaje consistente y uniforme sobre el alcance y los resultados previstos del ejercicio de recopilación de datos, gestionando las expectativas en torno a los resultados previstos. Pruebe los mensajes dentro de la comunidad para comprenderlos antes de comenzar.

● Informe el abuso de autoridad y situaciones en las que el personal pueda estar actuando de manera poco ética, imparcial o no objetiva; incluya en los mensajes para las personas de interés (y al personal) instrucciones claras sobre cómo la población de interés (o el personal) puede quejarse y ante quién, incluida la forma en que se tratarán las quejas (es decir, de manera confidencial). Según corresponda, proporcione retroalimentación y dialogue con las personas de interés sobre las quejas presentadas. Pruebe los mensajes dentro de la población de interés para su comprensión, antes de continuar.

❖ Diseño del sistema de información:

● Revise y establezca protocolos en conjunto con miembros de la comunidad humanitaria (incluidos los actores nacionales y otras partes interesadas, según corresponda) antes del inicio de un ejercicio de recopilación de datos. Esto también asegura la coherencia en la revisión y la posibilidad de replicar el proceso.

● Establezca salvaguardas describiendo todos los objetivos y resultados de un sistema dado con base en una evaluación objetiva del propósito definido.

● Reflexione y mitigue sesgos potenciales del evaluador en la recopilación de datos.

● Proporcione guías de interpretación adecuadas para la recopilación de datos, lo que puede minimizar el margen de interpretación errónea por parte de los evaluadores.

● Como comunidad de respuesta humanitaria, identifique y sea consciente de factores culturales, sociales, económicos, políticos o de otro tipo específicos que puedan generar sesgos, falta de transparencia o imparcialidad, coteje esto con su plan de recopilación de datos.

● Revise rigurosamente su plan de recopilación de datos para asegurarse de que esté orientado a resultados y de que la información del método que se recopile sea creíble.

● Capacite a los encuestadores para verificar y revisar si hay sesgos, siga los métodos prescritos. Asegúrese de que los encuestadores estén bien capacitados y cumplan con el código de conducta, mediante revisiones periódicas y comentarios de las personas de interés.

● Las herramientas deben estar alineadas con el propósito previsto, la herramienta se debe construir de una manera que minimice las respuestas sesgadas, por ejemplo: busque preguntas engañosas, preguntas inductivas o problemas con el cuestionario que podrían resultar en sesgos.

IMPLEMENTE

❖ **Realizar la recolección de datos:**

● Las observaciones deberán incluirse en el análisis final y, según el alcance y el tipo de situación, es posible que deban tenerse en cuenta en la recopilación que se esté haciendo.

● A lo largo de la recopilación de datos, los recopiladores de datos deben asegurarse de que la respuesta de los encuestados sea capturada correctamente y permita al encuestado "no dar una respuesta a una pregunta".

● Revise constantemente el proceso ético o responsable o las implicaciones de los datos que está recopilando (a lo largo del ciclo de recopilación de datos; por ejemplo, suspenda la recopilación de datos si las preocupaciones se vuelven evidentes).

❖ **Procesamiento y análisis:**

● Evite que la comprensión parcial del contexto influya en la validación de los resultados del análisis. Reflexione sobre usar el conocimiento o juicio de expertos.

● Desarrolle un plan para un análisis de datos oportuno y preciso y para evitar malinterpretar los resultados.

  ● Examine los aspectos del análisis y las suposiciones realizadas con conocimiento de los expertos con segmentos clave de la población de interés.

  ● Garantice un proceso imparcial y sin sesgos al establecer protocolos y un proceso de análisis replicable.

  ● Establezca protocolos de análisis basados en un plan de análisis de datos transparente e imparcial, que también hará que los resultados sean replicables.

- Asegure que la documentación de análisis, decisiones, suposiciones y limitaciones sea transparente.

- Trabaje con la comunidad de partes interesadas para reconocer las limitaciones analíticas y examinar o triangular los hallazgos de manera imparcial y transparente.

❖**Difundir y compartir:**

- Trabaje con la comunidad humanitaria para examinar las solicitudes entrantes de datos e información, asegurando que estas solicitudes sean de naturaleza imparcial y sin sesgos, y se centren en un propósito definido comúnmente acordado, que sea proporcional y que pueda brindar resultados de protección en nombre de las personas de interés, reflejando al mismo tiempo los otros Principios PIM.

❖ **Almacenar y conservar:**

(N/A)

Centrado en las personas e inclusivo: las actividades PIM se guiarán por los intereses y el bienestar de la población, que debe participar e incluirse en todas las fases relevantes de PIM. Las actividades PIM deben ser sensibles al contexto sociodemográfico y cultural.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir el propósito y las necesidades de información:**

● Comuníquese con las personas afectadas para comprender su situación, vulnerabilidades, amenazas y capacidades, y la necesidad resultante de datos e información, el tiempo, el alcance y el formato de los datos o la información necesaria.

● Identifique la necesidad de desagregar datos por edad, género, diversidad y grupos específicos dentro del contexto sociocultural.

● Identifique las necesidades de información y datos preliminares para la estrategia y respuesta de protección, en función de las preocupaciones planteadas por la población afectada.

❖ **Revisión de datos e información:**

● Analice y triangule conjuntos de datos existentes para identificar las consistencias e inconsistencias; la relevancia y confiabilidad; las duplicaciones y vacíos; los datos de línea base y los secundarios. Identifique conjuntos de datos confiables y asegúrese de que las herramientas de recopilación de datos primarios no recopilen esta información nuevamente a menos que sea necesario.

● Identifique las buenas y malas prácticas relacionadas con la sensibilidad social y cultural en la selección de los datos secundarios que se revisarán.

● Incluya datos e información de los sistemas, organizaciones locales y redes de protección de la población afectada.

● Comprenda (o note las limitaciones en los datos o el conocimiento; identifique la razón de la brecha) las amenazas, vulnerabilidades y capacidades que rodean los riesgos de protección dentro de un determinado grupo, al contrastar con la comunidad afectada en general; incluso para las personas de diferentes edades, género y contexto.

● Mantenga una evaluación de riesgos que incluya los internos, externos y las personas de interés. Actualice y refleje los cambios en la situación y refleje el desglose de datos como corresponde.

DECIDA Y DISEÑE

❖ **Compartir información:**

● Busque un acuerdo sobre las prácticas y los procesos de intercambio de información preferidos por la población afectada, incluidos los datos identificables y anonimizados (como el intercambio con la comunidad/líderes comunitarios, etc.)

● Consulte e identifique si y cómo la población afectada preferiría recibir comentarios sobre los resultados y hallazgos de las actividades PIM.

● Identifique el tiempo, el alcance, el formato y las responsabilidades/roles organizacionales en términos de datos e información que se compartirán con la comunidad (según los resultados de los anteriores y las mejores prácticas de protección).

❖ **Diseño con la población afectada:**

● Trabaje con la comunidad para asegurar la participación de las personas en riesgo en todas las etapas de la planificación y programación. Busque dialogar con diferentes grupos de personas según la edad, género, diversidad, ubicaciones geográficas y las diferentes condiciones y necesidades.

● Asegure que se establezca un mecanismo de rendición de cuentas y que se comunique claramente a la población afectada, incluidos el tiempo, el alcance y la responsabilidad organizacional para comunicar/retroalimentar las necesidades de los datos e información (de protección) identificados por la comunidad.

● Identifique y utilice los mecanismos existentes de intercambio de información basados en la comunidad y apóyelos (especialmente aquellos que facilitan el intercambio de información entre las personas para su propia protección) y desarrolle estas capacidades dentro de la comunidad.

● Garantice que las consideraciones de las dinámicas contextuales, sociales y culturales se identifiquen a través de vínculos con la comunidad de interés, y se apliquen a las necesidades de datos identificada, haciendo los ajustes de manera apropiada.

❖ **Diseño del sistema de información:**

● Al diseñar herramientas de recopilación de datos, asegúrese de integrar la información sobre iniciativas, mecanismos y capacidades de protección liderados por la comunidad (no solo riesgos/amenazas de protección).

● Los especialistas en diseño de encuestas y los traductores deben trabajar con los miembros de la comunidad local y probar cuidadosamente las herramientas de recopilación de datos en el terreno para garantizar que las preguntas, la redacción y el orden de las preguntas respeten la cultura local y sean entendidas por la comunidad.

● Asegúrese de que los encuestadores estén capacitados y sean apropiados para el contexto y la población de los que recopilarán datos.

● Tenga en cuenta los aspectos culturales y sociales en cuanto a la hora y el lugar de las entrevistas (es decir, el horario de trabajo diario y los días feriados; lugares inaccesibles para determinadas categorías que limitan el acceso físico y/o social, etc.).

● Defina las herramientas y la metodología para reducir los sesgos al obtener información sobre y de diferentes grupos de personas en la comunidad (por ejemplo, edad; género; diversidad; vulnerabilidades; contexto social, político, religioso, económico).

● Cuando sea posible, incluya en los procedimientos operativos estándar detalles sobre el registro y la respuesta adecuados a las solicitudes de las personas de interés para acceder a la información, la corrección o eliminación de sus propios datos. Asegúrese de que la comunidad comprenda cuándo no será posible modificar esto (es decir, cuando los datos se recopilen de forma anónima).

● Diseñe un sistema de información para reducir la probabilidad de una relación de poder desigual (explícita o implícita en la forma en que se presenta el ejercicio o la organización que lo realiza) entre el recolector de datos y el encuestado.

● Capacite a los encuestadores, por ejemplo: métodos de recopilación de datos culturales sensibles, comunicación sobre el propósito y formas de gestionar las expectativas.

IMPLEMENTE

❖ **Realizar la recolección de datos.**

● Comunique claramente el propósito del ejercicio a la persona que proporciona sus datos (incluida la relación de las respuestas con la entrega de ayuda y asistencia para evitar generar expectativas, o para gestionarlas). Permítale participar activamente y haga preguntas de una manera que respete su contexto cultural y que le brinde a la persona la libertad de responder según desee, pero también para apoyar iniciativas de comunicación complementarias lideradas/impulsadas por las propias comunidades.

● Informe a la población afectada con quién se compartirá y difundirá la información.

❖ **Procesamiento y análisis:**

● Trabaje con la población afectada para evaluar y analizar las implicaciones de protección relacionadas con este paso del proceso.

● Revise y actualice periódicamente la evaluación de riesgos, ponga en práctica los principios de no causar daño (como se describe en este documento) y actualice el análisis de las partes interesadas.

● El análisis de los datos desagregados debe realizarse por edad, género y diversidad.

● Presente y discuta los resultados preliminares con los miembros de la comunidad e integre sus interpretaciones y comentarios en el análisis final.

❖**Difundir y compartir:**

● Trabaje con la comunidad para actualizar la evaluación de riesgos: vuelva a examinar los cambios en el contexto, en función de los niveles o tipos de datos que se van a compartir (según lo acordado en el paso "Intercambio de información").

● Asegúrese de que los datos difundidos se anonimicen y se agreguen de manera adecuada (eliminando las características que identifiquen a las personas).

● Garantice que los datos e información se compartan de manera oportuna, apropiada, accesible y predecible, y mantenga un diálogo con la comunidad.

● Utilice los mecanismos existentes de gestión de información basados en la comunidad y apóyelos para compartir comentarios o información relevante de protección.

● Reexamine las necesidades cambiantes que tienen las comunidades en ciertos conjuntos o niveles de protección (y otra) información, que pueden necesitar para tomar decisiones para ellos mismos y sus familias, y tenga en cuenta el tiempo para esta información.

❖ **Almacenar y conservar:**

● Siempre que sea posible, las personas afectadas han sido concientizadas de su derecho de acceder, y tienen acceso a los datos e información almacenados, que han proporcionado sobre sí mismos y son informados en los casos en que esto no sea posible.

● Asegúrese de que existan políticas y procedimientos de almacenamiento, retención y destrucción de datos que sean relevantes para el contexto/naturaleza de los datos/leyes locales/etc. y que se consulte e informe a la comunidad al respecto.

Coordinación y colaboración: todos los participantes que implementan las actividades PIM deben adherirse a los principios señalados anteriormente y promover la más amplia colaboración y coordinación tanto internamente, entre los actores humanitarios, como externamente, con y entre otras partes interesadas. En la medida de lo posible, las actividades PIM deben evitar la duplicación de otros esfuerzos PIM y, en cambio, aprovechar los esfuerzos y mecanismos existentes.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir el propósito y las necesidades de información:**

● Mapee los actores clave, sus prioridades iniciales, necesidades de información, capacidades de protección y de GI, e iniciativas existentes para identificar posibles repeticiones y oportunidades de colaboración, en consulta con los actores relevantes. Esto podría resultar en un análisis de las partes interesadas.

● Contacte y cree vínculos con las partes interesadas del sector para comprender qué datos e información de protección pueden ser necesarios para fines sectoriales.

● Tenga en cuenta un entorno más amplio de gestión de la información, identificando riesgos y oportunidades de colaboración.

● Evalúe varias partes interesadas e iniciativas para identificar los requisitos de información y detectar vínculos.

❖ **Revisión de datos e información:**

● Identifique y comuníquese con las partes interesadas clave, incluidas las que son esenciales para una respuesta de protección coordinada, para recopilar datos, información, reportes y otros recursos existentes que sean relevantes para la necesidad de información identificada, y para conocer los procesos de recopilación de datos actuales.

DECIDA Y DISEÑE

❖ **Compartir información:**

● Verifique la credibilidad y confiabilidad de los datos y la información existentes consultando las fuentes de datos. Si es creíble, trabaje con socios de datos para implementar medidas predecibles para acceder, transferir y almacenar datos de manera segura y continua. Establezca protocolos o acuerdos de intercambio de datos según sea necesario para ayudar a compartir de manera eficiente y ética a lo largo del tiempo.

● Si las estructuras de coordinación no existen, discuta la necesidad y la viabilidad de establecer una con la comunidad de las partes interesadas. Trabaje con ellas para realizar un análisis de las partes interesadas e identificar posibles participantes o recursos. Las partes involucradas variarán de un contexto a otro y pueden incluir actores humanitarios, autoridades nacionales, sociedad civil, actores de desarrollo y de preservación de la paz.

● Si se establece una red de intercambio de información, acuerde cuál es el propósito, la membresía, modalidades, estándares (por ejemplo, con respecto a la recopilación, análisis, uso, acceso y difusión de datos), roles y responsabilidades, y mecanismos de rendición de cuentas.

● Tenga listas de coordinación o de plataformas de comunicación para facilitar la creación de redes y la comunicación entre la comunidad de partes interesadas.

● Asegúrese de que los roles de los socios en el Proceso PIM estén determinados por su experticia técnica y su capacidad para gestionar la información de protección. Si un socio no está involucrado en la recopilación de datos no significa que no debería tener otro rol en el PIM y utilizar la información para dar asistencia.

● Garantice la transparencia entre los múltiples actores involucrados en la coordinación y adhiérase a los principios clave de PIM.

❖ **Diseño con la población afectada:**

● Contacte a la comunidad de interés (por ejemplo, estableciendo mecanismos de comunicación y coordinación transparentes e inclusivos regulares) para comprender su situación, contexto, necesidades y estructuras de comunicación interna.

● Transmita mensajes claros como comunidad humanitaria, sobre quién está haciendo qué, dónde, cómo y por qué.

● Garantice la retroalimentación coordinada a la comunidad de interés sobre los datos y la información que recopilan de ellos los actores humanitarios.

● Apoye y fortalezca los mecanismos de coordinación y comunicación impulsados por la comunidad, según lo solicite la comunidad.

❖ **Diseño del sistema de información:**

● Consulte las partes interesadas sobre posibles estándares comunes para la recopilación, transferencia/difusión, almacenamiento y protección de datos. Esto puede incluir acuerdos de intercambio de datos, procedimientos operativos estándar o términos de referencia para grupos de coordinación.

● Consulte las partes interesadas sobre posibles indicadores e indicadores correlacionados sobre los que podrían proporcionar datos, acordando las modalidades, el formato y el alcance de la información que se compartirá.

● Incluya un mecanismo de respuesta.

IMPLEMENTE

❖ **Realizar la recolección de datos.**

● Informe a los actores relevantes del propósito y los detalles logísticos de su actividad PIM, para evitar posibles conflictos o interrupciones logísticas.

● Comparta información sobre la situación observada y los cambios en el entorno de protección.

● Comparta su experiencia, su conocimiento del entorno de recopilación de datos y materiales para reducir los costos para las organizaciones individuales que implementan la recopilación de datos y para reducir riesgos.

❖ **Procesamiento y análisis:**

● Comuníquese con las partes relevantes para ayudar en la interpretación, validación y verificación del análisis de datos (hallazgos), según corresponda.

❖**Difundir y compartir:**

● Haga una evaluación de riesgos como comunidad y consulte a las personas de interés para comprender si ha habido cambios en la situación o el contexto que puedan afectar la conveniencia o viabilidad de compartir información o ciertos tipos o niveles de datos (en comparación con los planes previamente acordados).

● Considere métodos para rastrear si y cómo se utilizan los datos, la información o los informes, y por quién (tanto actores internos como externos).

❖ **Almacenar y conservar:**

● Implemente los sistemas de almacenamiento y mantenimiento de datos según los acuerdos existentes, incluso con respecto al acceso para los socios una vez que los datos se almacenan o archivan, y después de los procedimientos de liberación y eliminación.

Competencia y capacidad: los actores que participan en las actividades PIM son responsables de garantizar que las actividades PIM las lleve a cabo el personal de gestión de información y de protección que ha sido equipado con las competencias básicas PIM y ha recibido la formación adecuada.

EXPLORE EL PANORAMA DE LA INFORMACIÓN

❖ **Definir el propósito y las necesidades de información:**

● Reúna un equipo multifuncional de especialistas de gestión de la información, de protección y de sectoriales distintos a la gestión de información, cuando defina las necesidades de información.

● Garantice la claridad y la comprensión del sistema humanitario, incluidas las consideraciones específicas del sector, las fases de la respuesta humanitaria, los ciclos programáticos y la protección de datos cuando defina las necesidades de información.

● Analice el entorno de gestión de la información (amenazas, oportunidades, fortalezas, debilidades) para informar el diseño de la metodología y la planificación operativa adecuados y realizar un análisis de las partes interesadas.

● Incorpore el conocimiento local y el 'tejido social' a lo largo del proceso.

● Familiarícese con todas las comunidades de práctica (es decir, protección y gestión de la información), los principios, estándares y marcos que necesitan colaborar y complementarse sin distinción de su disciplina o experiencia específicas.

● Comunique claramente las necesidades de protección e información, y oriente la recopilación de datos y los esfuerzos de información en torno a un propósito definido, asegurando proporcionalmente que los datos, la información o el análisis se coordinarán y compartirán de la manera más amplia que sea apropiada.

● Asegúrese de que haya un acuerdo sobre la claridad en la orientación operativa dentro de la operación/región (en caso de que no haya un acuerdo a nivel global), con respecto a los principios, normas y estándares internacionales (es decir, los resultados de PIM).

● Analice y garantice que los vínculos entre la necesidad de información, el diseño de la recopilación de datos/información y el plan de monitoreo y evaluación estén bien considerados y con una base lógica. Asegure que haya una revisión periódica (incluido el aprendizaje y ajuste) de la estrategia PIM utilizando las técnicas de monitoreo y evaluación adecuadas.

❖ **Revisión de datos e información:**

● Lleve a cabo un taller inicial con todos los actores de protección para discutir la necesidad de información, los vacíos de información y cómo llenarlos (la Matriz PIM ayuda a guiar la discusión). Esto debe basarse en el diálogo inicial desde el primer paso. Identifique y garantice la inclusión de todas las partes interesadas relevantes en torno a los Principios PIM.

● Aplique un enfoque participativo, basado en los derechos y en la comunidad. Las áreas de protección y de gestión de la información deben tener la competencia y la capacidad para revisar conjuntamente las fuentes de información, evaluar su confiabilidad para asegurarse de que estén actualizadas, sean imparciales y que las fuentes y sus datos e información sean objetivos, (es decir, la explicación de los métodos utilizados para recopilar datos/información), y que los objetivos del ejercicio estén claramente especificados.

● Analice la validez de los métodos, la confiabilidad, la credibilidad y el sesgo que pueden llevar la iniciativa de análisis de datos a su punto más cercano de verdad. (También podría usarse en el paso de revisión de datos e información).

● Garantice que las capacidades técnicas estén disponibles (habilidades de gestión de datos, habilidades analíticas tanto cuantitativas como cualitativas, habilidades de diseño de sistemas, mapeo, etc.).

● Garantice y valide los hallazgos de todos y cada uno de los análisis con una entidad local que pueda proporcionar conocimiento local.

● Asegúrese de que los criterios de una revisión secundaria de datos estén claramente establecidos y de que se comuniquen los sesgos identificados (es decir, que se acepten mediante un proceso de colaboración o que el conjunto de datos/información se excluya de la revisión secundaria de datos). Después de la revisión secundaria de datos, tome una decisión informada liderada por la comunidad sobre qué sistemas son necesarios según un análisis exhaustivo de los requerimientos de información (y a lo largo del tiempo).

● Contextualice un análisis de vulnerabilidad (es decir, poder explicar las vulnerabilidades locales).

● Identifique fuentes de datos y socios disponibles, como actores nacionales, datos administrativos, datos judiciales, sector judicial, etc.

DECIDA Y DISEÑE

❖ **Compartir información:**

● Desarrolle el taller inicial de necesidades y planes de información, defina un mecanismo de intercambio de datos apropiado para asegurar medidas de colaboración adecuadas.

● Se debe empezar con el sector de protección para compartir de forma más predecible y transparente.

● Asegúrese de que cualquier protocolo de intercambio de datos respete los estándares y necesidades de protección y de gestión de la información (estos deben estar alineados).

● Difunda y promueva los productos PIM (habilidades de representación y comunicación) en todos los niveles de las partes interesadas.

● Asegúrese de que las decisiones y enfoques para difundir, compartir y establecer vínculos con los socios del sector sean consistentes con el propósito previsto. Verifique que las actividades y decisiones de PIM se revisen periódicamente a medida que evoluciona el contexto. Haga un acuerdo de intercambio de datos que se ajuste al contexto.

● Tenga en cuenta tanto los datos desagregados como los agregados. Comunique las sensibilidades en torno a la información confidencial y trabaje para establecer acuerdos con las partes interesadas en torno al intercambio de datos, información y análisis críticos de protección de una manera que sea adecuada en términos de protección. (Reformular)

● Asegure que el inicio de cualquier colaboración de PIM incluya sesiones informativas intersectoriales que destaquen lo que significa protección y gestión de la información dentro de cada sector. Es decir, qué significa protección en WASH, albergue, etc. Los actores de protección también deben estar preparados para explicar el marco de PIM que es aplicable al contexto dado (qué propósitos están impulsando el panorama del sistema). Comparta estos enfoques. Todos los actores de protección deben entender la protección a través de la lente de otros sectores.

● Asegure que la información y el análisis relacionados con PIM sean coherentes en las diferentes etapas del ciclo del programa, esto no debe ser una excepción. Defina las audiencias de los resultados del intercambio de datos e información.

● Explore y/o establezca alianzas con otros sectores y detecte vínculos para los sistemas PIM con otros procesos. Mantenga a las personas informadas y comuníquese de manera efectiva y predecible con las partes interesadas, incluida la configuración de protocolos de intercambio de información, y realice evaluaciones de impacto de privacidad o algo similar.

● Involucre a la comunidad de partes interesadas y difunda las lecciones aprendidas y las buenas prácticas con colegas a nivel local y mundial para apoyar la sostenibilidad y la gestión del conocimiento.

● Fomente de manera proactiva el compromiso y la contribución de los socios para apoyar las actividades de PIM y comuníquese de manera efectiva con una variedad de partes interesadas: los colegas internos y externos y entre técnicos y tomadores de decisiones. Traduzca las discusiones técnicas para una audiencia no técnica.

❖ **Diseño con la población afectada:**

● Involúcrese y comuníquese con las comunidades de una manera responsable y conozca los principios de rendición de cuentas a las poblaciones afectadas. Comprenda y aplique un enfoque de derechos, participativo y basado en la comunidad al diseñar un sistema de gestión de la información de protección..

● Defina esto en un procedimiento operativo estándar para involucrar y explicarle a la población en todos los aspectos de las iniciativas de recolección de datos y en los pasos dentro del proceso.

● Participe en un apoyo coordinado, significativo y sostenible, y colabore con los mecanismos de coordinación dirigidos por la comunidad, según corresponda.

● Participe y comuníquese con las comunidades de manera responsable y conozca los principios de rendición de cuentas a las poblaciones afectadas.

● Asegure que haya experticia diseñando e implementando eficazmente la recopilación de datos a través de entrevistas, incluso en entornos interculturales y entornos de seguridad complejos.

● Asegure que haya fuentes de conocimiento existentes y un plan de talento humano para involucrar el conocimiento local cuando sea apropiado.

❖ **Diseño del sistema de información:**

● Haga un balance entre las metas a las que se aspira y la viabilidad según las limitaciones del contexto operativo y las restricciones programáticas.

● Tome decisiones informadas sobre qué sistemas son necesarios basándose en un análisis integral de los requisitos de información (y a lo largo del tiempo).

● Confirme la capacidad para planificar y liderar o participar en la recopilación de datos: asegúrese de que la recopilación de datos se base en principios, es segura y tiene un propósito definido en todos los pasos.

● Adapte las técnicas de recopilación de datos a una amplia variedad de situaciones, incluidos los entornos con bajo acceso a tecnología.

● Diseñe y desarrolle técnicas de muestreo adecuadas, así como métodos de recopilación de datos cuantitativos y cualitativos, incluido el diseño de recopilación de datos.

● Diseñe métodos apropiados de mapeo de la comunidad/población objetivo.

● Acuerde un marco que identifique y contextualice las normas y estándares locales e internacionales relevantes sobre protección de datos, consultando los participantes locales (es decir, asegure la operacionalidad).

● Desarrolle, en consulta con los colegas pertinentes, las técnicas adecuadas de monitoreo y evaluación, incluidos los diferentes tipos de indicadores, y cómo aplicarlas a la gestión de información de protección. Según sea necesario, redacte documentos técnicos para articular y analizar claramente los sistemas y planes de gestión de la información.

● Priorice los múltiples plazos y tareas, que en ocasiones tienen la misma importancia, en torno a las actividades PIM. Se requiere tener la capacidad para solucionar problemas o pasar a los planes de contingencia según sea necesario.

● Habilidades en técnicas de entrevistas y diferentes procesos de recopilación de datos.

● Comprenda la ética de la investigación, el conocimiento cultural y el contexto operativo. Sea capaz de desarrollar una estrategia y un plan operativo de PIM basados en principios, e incorpore los riesgos contextuales, vulnerabilidades y mecanismos de afrontamiento dentro de los procesos de análisis de datos de protección.

● Capacidad para utilizar soluciones tecnológicas nuevas y existentes para la gestión de la información y poder evaluar su idoneidad para diferentes contextos, incluida la adaptación de los sistemas de gestión de la información en entornos con bajo acceso a tecnología.

● Capacidad para adaptar las técnicas de recopilación de datos a una amplia variedad de situaciones, incluidos los entornos con bajo acceso a tecnología.

● Conozca las normas y estándares clave de protección y tenga un enfoque holístico de protección, así como la capacidad de incorporarlos en soluciones operativas y técnicas. Esté familiarizado con las técnicas apropiadas de mapeo y muestreo, así como con los métodos de recopilación de datos cuantitativos y cualitativos, incluido el diseño de recopilación de datos.

● Familiarícese con el ciclo de gestión de proyectos y tenga habilidades sólidas de gestión de proyectos, incluida la creación de planes de trabajo, la elaboración de presupuestos y la delegación de responsabilidades. Sea capaz de establecer metas claras, organizar el trabajo en consecuencia y supervisar el progreso. Sea capaz de analizar y gestionar las expectativas de gestión de la información.

● Tanto los colegas de protección como de gestión de la información deben asumir la responsabilidad de los requisitos de datos e información y sistemas de gestión de la información, incluida la grabación de información en archivos físicos y el cumplimiento de los protocolos de protección de datos. Esto ya no es responsabilidad exclusiva de los colegas técnicos. Si existen limitaciones en la habilidad, es necesario identificarlas y capacitar a los colegas y responsabilizarlos.

● Asegúrese de que haya sistemas y capacidad de recursos humanos para almacenar y procesar datos/información.

● Evalúe varias partes interesadas e iniciativas para confirmar los requisitos de información frente al enfoque del sistema.

IMPLEMENTE

❖ **Realizar la recolección de datos.**

● Los elementos anteriores (en la definición) deben incluirse en el cómo a continuación.

● Participe y comuníquese con las comunidades de manera responsable y conozca los principios de la rendición de cuentas a las poblaciones afectadas.

● Diseñe e implemente la recopilación de datos mediante entrevistas, incluso en entornos multiculturales y entornos de seguridad complejos.

● Asegúrese de que se realicen copias de seguridad con regularidad para evitar pérdidas accidentales o daños en los datos. En el caso de transferencias de datos, asegúrese de que la organización tenga medios seguros para transferir datos a otras agencias/organizaciones (encriptado, archivos xml, etc.). Asegúrese de que exista un procedimiento para reubicar (y, como último recurso, destruir) los archivos físicos y electrónicos en caso de una evacuación de emergencia.

❖ **Procesamiento y análisis:**

● Participe y comuníquese con las comunidades de manera responsable y conozca los principios de la rendición de cuentas a las poblaciones afectadas.

● Mantenga a las personas informadas y comuníquese de manera eficaz con una variedad de partes interesadas.

● Asegúrese de que todo el personal involucrado en el manejo y análisis de información sensible esté adecuadamente capacitado en protección de datos y sobre estándares, habilidades, políticas y principios de seguridad.

● Sea consciente y capaz de garantizar que existen medidas apropiadas para proteger al usuario contra problemas de privacidad, como la vigilancia, la agregación inapropiada, la exclusión, la violación de la

confidencialidad, al igual que mayor accesibilidad, identificación de individuos o grupos y uso de datos secundarios.

● Sea capaz de trabajar en colaboración con los colegas de protección, gestión de la información y otros colegas sectoriales para procesar, analizar y llegar a resultados. Debe estar familiarizado con el contexto y tener experiencia trabajando con poblaciones desplazadas (incluidos los desplazados internos, refugiados, solicitantes de asilo y repatriados, así como con civiles en áreas de desplazamiento), así como con una variedad de contextos de protección, desde situaciones de emergencia hasta el retorno y la recuperación.

❖**Difundir y compartir:**

● Los resultados deben ser respaldados por la comunidad de las partes interesadas que contribuyen al ejercicio o sistemas PIM.

● Fomente el compromiso y la contribución de/hacia y entre socios para apoyar las actividades PIM.

● Mantenga a las personas informadas y comuníquese de manera efectiva con una variedad de partes interesadas: colegas internos y externos y entre especialistas técnicos y tomadores de decisiones, traduciendo las discusiones técnicas para una audiencia no técnica.

● Referencie y aplique los principios humanitarios y de protección.

● Utilice análisis cuantitativos y cualitativos, así como métodos de visualización, software y capacidad para producir y difundir productos de gestión de la información regulares adaptados a las audiencias adecuadas.

● Capacidad de redactar claramente diferentes tipos de documentos técnicos.

❖ **Almacenar y conservar:**

● Asegúrese de que existen los sistemas y que existen los recursos humanos necesarios y capacitados para almacenar y procesar datos/información.