Protección a los implementadores y mejora de resultados

Orientación y herramientas para fortalecerla seguridad en los programas para poblaciones clave que apoya el Fondo Mundial

Reconocimientos

El desarrollo de este paquete estuvo a cargo de CSIH-WCA y FHI360. Se basa en las herramientas de seguridad y las orientaciones elaboradas por FHI 360 y sus colaboradores en el marco de los proyectos LINKAGES y EpiC[1,2] (financiados por USAID y PEPFAR) y las adapta para que respondan específicamente a las necesidades y realidades de los programas que reciben el apoyo del Fondo Mundial en África Occidental y Central. La adaptación se llevó a cabo en 2022 con las aportaciones de los principales programas y organizaciones de poblaciones clave de la región de África Occidental y Central. El departamento de Comunidad, Derechos y Género del Fondo Mundial de Lucha contra el Sida, la Tuberculosis y la Malaria prestó apoyo para esta adaptación. Agradecemos y reconocemos las contribuciones de las siguientes organizaciones al proceso:

Burkina Faso
AIDSETI
AVP
AWEYA
SPCNLS

Camerún
Affirmative Action
CHP
Empower-Cameroun
ESPOIR+
Ndop
Reach Out

Senegal
AJDPASTEEF
ANCS
APCSID
ENDA Santé
ONG AWA
ONG 3D
RENAPOC
RNP+

Sierra Leone
Dignity
IHPAU
RODA
SLYDCL
SWAASL
Women in crisis

[1] https://www.fhi360.org/resource/aman-mena-toolkit
[2] https://www.fhi360.org/resource/implementer-and-data-security

Tabla de contenidos

1. *Orientación sobre la herramienta*

1.1 Antecedentes

Los riesgos y barreras en materia de derechos humanos a los que se enfrentan las poblaciones clave son algo bien conocido, y su abordaje supone un componente esencial de los programas integrales para las poblaciones clave de VIH. Otro desafío que se asocia con esto, si bien menos comprendido, es la seguridad de quienes participan en la implementación de los programas para las poblaciones clave de VIH y en la prestación de servicios a estos grupos. Las organizaciones de implementación –a menudo dirigidas por miembros de poblaciones clave– con frecuencia reciben amenazas y ataques violentos que se relacionan directamente con su trabajo. Esta inseguridad tiene un alto costo en la salud física y mental de quienes trabajan en los programas. Asimismo, reduce la eficacia de estos programas ya que cuando se enfrentan a detenciones de personal, daños a la reputación de la organización, limitación de movilidad y robo de datos, entre otras cuestiones, además de desviar la atención de la programación, limitan el alcance de los programas y provocan que los beneficiarios decidan evitar estos servicios.

El seguimiento y la evaluación sistemáticos de los riesgos, así como la puesta en marcha de recursos y medidas para reducirlos y responder a los incidentes, forman una parte esencial de todos los programas para poblaciones clave de VIH, y son indispensables para lograr y mantener los resultados. También forman parte del compromiso de cuidado hacia las organizaciones de primera línea, los trabajadores y los voluntarios, y son fundamentales para que los programas dirigidos por la comunidad sean una opción segura y sostenible.

El Fondo Mundial está colaborando con FHI 360 y con el Instituto de la Civil Society Institute for Health in West and Central Africa (CSIH-WCA, por sus siglas en inglés), para adaptar las herramientas que los programas pueden utilizar para anticiparse a los riesgos de seguridad, planificar con anticipación la reducción de estos y responder a los incidentes y amenazas. Este documento presenta las herramientas que están disponibles para los implementadores de los programas del Fondo Mundial, mismas que pueden utilizarse para incorporar sistemáticamente medidas de seguridad en los programas existentes, y para servir de base para asignar recursos a la seguridad dentro de los procesos de reprogramación o de diálogo de los países.

1.2 Ejemplos de desafíos de seguridad para los programas

Las organizaciones de las poblaciones clave que participaron en el desarrollo de estas herramientas han descrito una amplia y variada gama de amenazas o incidentes de seguridad mediante los cuales los perpetradores amenazan o atacan *intencionalmente* al programa debido a su asociación con el VIH y las poblaciones clave. Algunos ejemplos de las amenazas e incidentes a los que se enfrentan frecuentemente las organizaciones y programas de poblaciones clave incluyen:

- Campañas mediáticas contra una OSC —en las que se acusa a los dirigentes y al personal de la OSC de promover la homosexualidad y la prostitución— que provocaron daños en la salud mental y el ostracismo social de los trabajadores de la OSC. La organización se vio obligada a cerrar durante varias semanas hasta que se calmó la ira popular, lo que limitó el acceso a los servicios en materia de VIH.
- Un individuo que se hizo pasar por beneficiario entró en una OSC que daba servicio a miembros de la PC y filmó la distribución de condones. El individuo difundió el vídeo en internet y alegó que la OSC realizaba actividades ilegales e inmorales. Los vecinos enfurecidos atacaron la OSC, por lo que tuvieron que interrumpir sus actividades durante un tiempo.
- Un promotor de actividades de alcance fue arrestado por varios días por llevar condones. Una vez puesto en libertad, sufrió el rechazo de sus familiares y se quedón sin hogar. Esto afectó tanto a la capacidad de trabajo del individuo como a la moral del resto del personal de alcance.
- Los beneficiarios se enfadaron y abusaron verbalmente de los trabajadores de la OSC porque no pudieron satisfacer sus necesidades integrales, como por ejemplo brindar apoyo nutricional. Los trabajadores de la OSC experimentaron angustia mental y temieron por su seguridad física. En algunos casos, los trabajadores dejaron la organización debido al estrés.
- Han detenido a promotores de actividades de alcance debido a falsas acusaciones de solicitar sexo cuando distribuían condones, lo cual limita su capacidad de provisión efectiva de productos.
- Una multitud de estudiantes universitarios extremistas estuvo a punto de volcar una unidad de pruebas móviles como protesta contra mensajes que considerban inmorales (por ejemplo, la importancia del uso de preservativos). Esto limitó los futuros esfuerzos de alcance en el distrito.
- Después de que una OSC buscara disminuir el estigma contra miembros de la PC por medio de mensajes públicos, su sitio web fue víctima de hackeo y de campañas de troleo en línea en su contra. Fue necesario desviar dinero de otros programas u obtenerlo mediante la recaudación de fondos para aumentar la ciberseguridad.
- En los centros de acogida se reportaron abusos verbales, robos y, en ocasiones, agresiones físicas contra el personal de implementación del programa, incluído el equipo médico. Esto provocó estrés, pérdidas económicas y rotación de personal.
- La familia de un beneficiario se enteró que su hijo estaba recibiendo servicios de una OSC que buscaba disminuir el riesgo de infecciones de VIH entre los miembros de las PC. La familia acusó a la OSC de traficar con el beneficiario e intentó presentar cargos penales. La reputación de la OSC se vio afectada y hubo que dedicar tiempo del personal para responder ante la falsa acusación.

1.3 Recomendaciones clave para la seguridad del programa

Las siguientes recomendaciones se han desarrollado por consenso durante el trabajo en torno a la seguridad de los programas con poblaciones clave a nivel mundial. Resultan pertinentes no sólo para los programas de primera línea, sino también para los Receptores Principales, los Sub-Receptores y el Fondo Mundial. Se comparten aquí para contribuir a la reflexión general en materia de seguridad.

1. Busque que los principios y enfoques del programa de VIH sean la base de los esfuerzos de seguridad. Esto incluye "Nada de nosotros sin nosotros" y "Lo primero es no hacer daño".
2. .Convierta a la seguridad en una prioridad y asígnale recursos de manera explícita.
3. Cree un entorno de trabajo seguro que proteja y promueva la salud mental como parte de su responsabilidad como organización.
4. Planifique con antelación y asegúrese de que todos conocen el plan (conservando cierta flexibilidad).
5. Discuta abiertamente el nivel de riesgo que resulta aceptable a nivel organizacional e individual.
6. Opere con un conocimiento tanto de los riesgos reales como de sus causas subyacentes (incluyendo los marcos legales).
7. Reconozca las distintas vulnerabilidades y capacidades de cada trabajador dentro de la planificación sobre seguridad.
8. Conozca a todos los actores clave, no sólo a los aliados obvios.
9. Identifique las amenazas (físicas, digitales, psicológicas) y las estrategias de seguridad de forma holística.
10. Conéctese con otros programas, trabaje en coalición y aprendan unos de los otros.

1.4 Descripción general de las herramientas

¿Qué se entiende por seguridad de los programas?

La seguridad de los programas consiste en reducir y responder a la violencia intencionada y a las amenazas contra los programas y cualquier persona que participe en ellos. En el caso de los programas para las poblaciones clave de VIH, esto se refiere normalmente a que los programas sufren amenazas o ataques precisamente por su trabajo con poblaciones clave en materia de VIH. Aunque existe una diversidad de causas y perpetradores, dichas amenazas y ataques suelen tener su origen en la estigmatización y la falta de aceptación de las poblaciones clave.

¿Para qué sirven estas herramientas?

Estas herramientas han sido diseñadas para ayudar a las organizaciones involucradas en los programas para las poblaciones clave de VIH a:

- identificar de forma sistemática sus capacidades, fortalezas y debilidades en materia de seguridad;
- identificar los riesgos prioritarios que hay que abordar y hacer un seguimiento de las amenazas hacia sus organizaciones y trabajadores;
- elaborar planes que les permitirán reducir estos riesgos y amenazas o, en todo caso, su vulnerabilidad a ellos;
- y garantizar una respuesta efectiva cuando ocurra un incidente.

Muchas de las estrategias para mejorar la seguridad de los programas requieren un cambio en la forma de trabajar de la organización o la adopción de medidas para reducir riesgos. En algunos casos también puede ser necesario incluir nuevas actividades en el programa –por ejemplo, una mayor incidencia con las autoridades y las agencias de seguridad locales–, comprar equipos o contratar servicios y expertos que ayuden a reforzar la seguridad. Estos costos son eligiles para recibir financiamiento del Fondo Mundial, por lo que es importante asegurarse de que se incluyan en las solicitudes de financiamiento al Fondo Mundial, así como en las sub-subvenciones o subcontratos con las organizaciones de implementación de primera línea. Los resultados derivados del uso de estas herramientas pueden servir para fundamentar la planificación y elaboración de los presupuestos de las subvenciones del Fondo Mundial.

¿Quién debe utilizar las herramientas?

Los problemas de seguridad a los que se enfrentan los programas para las poblaciones clave de VIH son muy particulares para cada organización y lugar donde se llevan a cabo los programas. Las acciones necesarias para reducir los problemas de seguridad también son específicas de cada organización y lugar. A pesar de que distintos programas para poblaciones clave se enfrenten a amenazas e incidentes similares, es importante que cada uno identifique las soluciones que funcionen mejor para ellos.

Por esta razón, estas herramientas han sido diseñadas principalmente para el uso de organizaciones de primera línea que trabajan en la provisión de programas, por ejemplo, en el apoyo a tratamientos contra el VIH, la educación entre pares o el trabajo de derechos humanos para poblaciones clave.

En los programas que apoya el Fondo Mundial, las organizaciones de primera línea con frecuencia no reciben fondos directamente del Fondo Mundial, sino de los Receptores Principales (RP) o de los Sub-Receptores (SR). Los RP y los SR desempeñan un papel en el apoyo y el fortalecimiento de las capacidades de las organizaciones de primera línea, especialmente cuando se trata de organizaciones dirigidas por la comunidad. Por lo tanto, los RP y los SR también pueden utilizar estas herramientas de seguridad de los programas para facilitar las planificaciones de seguridad con las organizaciones de primera línea a las que apoyan. Asimismo, ya que muchos RP y SR también están expuestos a riesgos de seguridad, pueden utilizar estas herramientas para cerciorarse de que trabajan con la máxima seguridad posible.

1.5 Resumen de las herramientas de planificación y procesos de planificación de seguridad

Las organizaciones que participan en los programas para las poblaciones clave de VIH encontrarán que cada una de las herramientas de este paquete resulta útil por mérito propio. Incluso es posible que la utilización de apenas una de estas herramientas contribuya a mejorar la manera en que el programa piensa y actúa con respecto a sus cuestiones de seguridad.

Al mismo tiempo, las herramientas también pueden considerarse como los distintos pasos de un proceso de planificación que conducirá a una incorporación efectiva de los temas de seguridad en las solicitudes y subvenciones de financiamiento del Fondo Mundial. Este proceso y sus herramientas correspondientes pueden verse resumidos en el siguiente diagrama.

1. Registro de incidentes de seguridad: garantiza que los programas tengan un registro concreto de los incidentes y daños que les afectan
2. Listado de control de las estrategias de seguridad: mejora la comprensión de las fortalezas y debilidades actuales del programa
3. Evaluación de las amenazas, riesgos y vulnerabilidad: permite comprender en detalle la procedencia de los riesgos y la forma de reducirlos
4. Plan de seguridad: identifica las acciones para reforzar la seguridad de las diferentes actividades del programa
5. Consejos prácticos para incluir la seguridad de los programas en las subvenciones del Fondo Mundial: incorpora los temas de seguridad al proceso de solicitud del Fondo Mundial

1.6 Recursos útiles

https://www.fhi360.org/resource/aman-mena-toolkit

https://www.fhi360.org/resource/implementer-and-data-security

https://www.fhi360.org/resource/when-situations-go-bad-worse-guidance-international-and-regional-actors-responding-acute

https://www.fhi360.org/sites/default/files/media/documents/resource-secure-mobile-devices-apps.pdf

https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-safety-security-toolkit.pdf

2. *Las herramientas*

2.1 Registro de incidentes de seguridad

Descripción

Esta herramienta proporciona una plantilla para registrar sistemáticamente los incidentes de seguridad, incluidas las amenazas, a los que se enfrentan la organización o los individuos que trabajan en el programa. Los usuarios pueden describir el incidente, cuándo se produjo, por qué y quién lo perpetró, junto con una serie de otros detalles. Puede registrar patrones en términos de tipos de incidentes o perpetradores, o incluso los momentos (del año, de la semana o del día) en que ocurren los incidentes con más frecuencia. Esto es útil porque permite a la organización comprender a lo largo del tiempo qué tipos de incidentes se producen, y cómo prevenirlos y responder a ellos de la mejor manera. El registro también puede utilizarse para compartir información con otras organizaciones similares para alertarlas de posibles amenazas, y para compartir información con los financiadores con el fin de incentivarlos a cubrir los costos para mejorar la seguridad. Puede ayudar a identificar:

- Lugares o actividades de mayor riesgo
- Perpetradores habituales
- Si un determinado incidente o amenaza también representa una amenaza indirecta para otros
- Si la violencia se está intensificando
- Quién corre más riesgo

Cómo utilizarlo

El registro puede utilizarse de muchas maneras diferentes, y depende de cada organización identificar la que funcione mejor para ellos. La herramienta que se proporciona en este paquete está en forma de tabla en formato MS Word. Los usuarios pueden hacer una nueva copia del archivo (de forma electrónica o impresa) para cada incidente. Si se utilizan versiones electrónicas, los usuarios deben decidir si copian y pegan la tabla en el mismo documento o si guardan un nuevo archivo para cada incidente; lo más importante es mantener los registros de todos los incidentes en un solo lugar (por ejemplo, en una carpeta electrónica específica). Otra alternativa es transferir la herramienta a un formato de base de datos o Excel para ayudar a almacenar la información en un solo lugar. Si se utilizan copias impresas, también se debe guardar cada nuevo formulario en el mismo lugar. En ambos casos, la información debe guardarse de forma segura, por ejemplo, como un archivo protegido por contraseña o encriptado (para el formato electrónico) o en un gabinete cerrado con llave (para el formato impreso).

Los usuarios también deben decidir quién se encargará de llenar los registros y quién de analizarlos. La persona o personas que se hayan visto directamente afectadas por el incidente deben participar siempre en la elaboración del registro, aunque la organización puede decidir si la persona lo hace por sí misma o con el apoyo de alguien más. No se debe recoger información que identifique a la persona en los formularios sin el permiso

de quien comparte el incidente. Es útil tener un responsable en la organización que se encargue de almacenar y analizar la información. Una forma de utilizar la información es revisar todos los incidentes periódicamente (por ejemplo, durante las reuniones o retiros de equipo, o en las sesiones de planificación de actividades) e identificar los patrones y las medidas que deben tomarse para abordarlos.

Por último, como sucede con todas las herramientas, ésta puede adaptarse. Algunos usuarios pueden considerar que no todas las preguntas son pertinentes o que es necesario añadir preguntas adicionales. El principio fundamental debe ser recabar únicamente la información que pueda ser útil y evitar que el proceso sea demasiado pesado, especialmente para las personas que han sufrido recientemente una experiencia traumática.

Nota: Tenga en cuenta que este registro puede contener información confidencial y sensible. Considere la posibilidad de desarrollar un sistema de codificación para evitar la inclusión de información personal, en particular en los puntos "6. Blanco del ataque" y "7. Dónde ocurrió el incidente".

Registro de incidentes de seguridad

	Pregunta	Cómo contestar	Respuesta
1	Incidente #	Comience por el número 1 y continúe con los siguientes; la numeración permite relacionar los incidentes de seguridad entre sí (véase la pregunta #14)	
2	Fecha del incidente	Anótela como AÑO-MES-DÍA (por ejemplo, 2019-02-17 para el 17 de febrero de 2019) para organizar este registro de incidentes de seguridad por fecha	
3	Hora del incidente	Hora específica del día (si se conoce), o más general (mañana, mediodía, tarde, noche)	
4	Perpetrador	Si se conoce y resulta seguro indicarlo, o utilice un término más general como "agente de policía"	
5	Organización afectada	Nombre del socio implementador del programa	

		de VIH (es decir, el nombre de la organización de base comunitaria)	
6	Blanco del ataque	Persona o tipo de personal concretos, espacio físico (por ejemplo, socio implementador, nombre de un punto específico), sitio web, base de datos, etc. No indique aquí el nombre de las personas a menos que tenga su permiso.	
7	Dónde ocurrió el incidente	Dirección física, en línea, por teléfono, etc.	
8	Presunto motivo del agresor (si se conoce)	Por ejemplo: intimidación, suspender el programa, desviar la atención de otros problemas locales	
9	Descripción del incidente de seguridad	Por ejemplo: Los mensajes de Facebook en la página del proyecto decían "[adjunte el mensaje correspondiente aquí"]; o, arrestaron sin cargos a los educadores de pares mientras distribuían preservativos a un grupo de HSH durante un evento de pruebas móviles de VIH	
10	Consecuencias del incidente de seguridad en el programa	Por ejemplo: El socio implementador sólo llevará a cabo actividades de alcance en línea hasta que se considere seguro llevar a cabo actividades de alcance físico	
11	Descripción de las acciones que se tomaron para responder al incidente de seguridad	Por ejemplo: El AÑO-MES-DÍA, el socio implementador al que se dirigía la publicación en Facebook decidió que no era seguro llevar a cabo actividades de alcance durante un período de dos semanas y presentó una denuncia ante la policía.	

		Por favor, incluya las fechas de las acciones tomadas (y continúe actualizando esta fila a medida que se toman acciones).	
14	¿Con qué otros incidentes de seguridad se relaciona? (si es el caso)	Si este episodio se relaciona con otros incidentes de seguridad, indíquelo aquí con los números de los otros incidentes de seguridad.	
15	Resolución del incidente (si es el caso)	Por ejemplo: El AÑO-MES-DÍA, pusieron en libertad a los educadores de pares y se les brindó apoyo en materia de salud mental.	

Para obtener una versión descargable de esta herramienta, haga clic en los siguientes enlaces:

- Registro de incidentes de seguridad (Word)
- Registro de incidentes de seguridad (Excel)

2.2 Listado de control de las estrategias de seguridad

Descripción

Este listado de control busca ayudar a los responsables de la implementación a comprender mejor los aspectos en que su organización cuenta ya con medidas de seguridad sólidas y en cuáles hay oportunidades para reforzarlas aún más. Las organizaciones responden a una autoevaluación de lo que están haciendo actualmente en función de una serie de categorías. La herramienta proporciona posteriormente un gráfico que representa visualmente las fortalezas y debilidades de la organización.

Además de utilizar esta herramienta para identificar las necesidades de la propia organización, es posible utilizar los resultados para facilitar el desarrollo de habilidades entre pares con otras organizaciones similares.

Utilizar este listado de control periódicamente puede ayudar a las organizaciones a evaluar si están progresando en algún área o si están surgiendo nuevos retos que deben abordar.

Cómo utilizarlo

La herramienta está disponible en formato Excel e incluye instrucciones detalladas para su uso, incluyendo quién debe responder a cada componente de la evaluación. Aunque su uso está pensado para organizaciones individuales, también puede utilizarse en el contexto de una reunión o taller con múltiples organizaciones para facilitar el aprendizaje entre pares. Por ejemplo, los representantes de cada organización pueden realizar la autoevaluación de su propia organización y, a continuación, cada organización puede compartir sus resultados y aportar más información al resto de participantes sobre las áreas en las que consideren que son más fuertes.

Para obtener una versión descargable de esta herramienta, haga clic en el siguientes enlaces:

- Listado de control de las estrategias de seguridad (Excel)

2.3 Evaluación de las amenazas, riesgos y vulnerabilidad

Descripción

Es importante que cualquier organización que esté enfrentando incidentes de seguridad comprenda mejor la razón por la que estos se producen. El Registro de Incidentes de Seguridad es un buen punto de partida para hacerlo, ya que recoge información detallada sobre las amenazas o los incidentes a los que se han enfrentado la organización, sus trabajadores y voluntarios. Al examinar con más detenimiento el Registro de Incidentes, se puede identificar lo que hace que la organización o sus trabajadores sean vulnerables, y la gravedad de las amenazas y los riesgos en términos de probabilidad de que se materialicen, así como sus consecuencias. Esto, a su vez, ayuda a reflexionar sobre las medidas que hay que poner en marcha para prevenir y responder a los incidentes. Esta herramienta proporciona algunas preguntas que pueden utilizarse para evaluar las amenazas, los riesgos y la vulnerabilidad.

Cómo utilizarla

No hay un formato o enfoque predeterminado para utilizar esta herramienta. Las preguntas pueden servir a los directores o a los miembros de los equipos para analizar los incidentes ocurridos o también pueden formar parte de la planificación de los programas, a fin de garantizar que las consideraciones en materia de seguridad se contemplen dentro de los planes de actividades.

El enfoque sistemático de la **evaluación de amenazas** incluye la colaboración en grupo con otros trabajadores del programa para plantear las siguientes preguntas:

1. ¿Qué hechos rodean la amenaza? (¿Qué sabemos realmente, y no qué suponemos, acerca de esta amenaza?)
    - Este paso es útil porque nos recuerda que debemos apartarnos de los chismes o las conjeturas. A veces la percepción de los demás puede exagerar o subestimar una amenaza. Intente pensar sólo en los hechos.
2. ¿Hay una serie de amenazas que se han vuelto más sistemáticas o frecuentes con el tiempo? (¿La persona hace amenazas cada día o sólo acosa de forma oportunista? ¿Se están intensificando en términos de cercanía, como por ejemplo, buscando a las personas en su casa o en su lugar de trabajo?)
    - La seriedad aumenta si algo ocurre en múltiples ocasiones. Eso muestra que la persona o personas que hacen la amenaza se sienten comprometidas con ella. La escalada de la amenaza -por ejemplo, que alguien que gritaba cuando se realizaban actividades de alcance ahora también los haya encontrado en línea- es otra señal de que se trata de algo más serio.

3. ¿Quién es la persona que hace las amenazas? (¿Es alguien conocido? ¿Alguien que tiene la capacidad de influir sobre los demás? ¿Alguien que tiene información que podría perjudicarlo a usted o a sus colegas?)
    - Esta pregunta trata de entender cuánto poder tiene la persona que amenaza. Por ejemplo, un agente de policía que hace amenazas es probablemente más peligroso que un desconocido.
4. ¿Cuál es el objetivo de la amenaza? (¿Es para cambiar su comportamiento? ¿Es para asustarlo? ¿Es una herramienta política para captar votos?)
    - Pensar en este punto puede ayudarle a decidir si la persona podría estar dispuesta a ir más lejos. Por ejemplo, si esto es sólo para asustarlo, es posible que la persona nunca vaya a dañarlo físicamente, aunque lo diga. Saber esto también puede ayudarlo a decidir cómo actuar.
5. ¿Qué tan seria cree que es la amenaza? (Su opinión personal al respecto)
    - Aquí es donde permite que tu intuición y su comprensión del contexto más amplio lo ayuden a pensar en la seriedad de la amenaza. Puede realizar este análisis basándose en las amenazas o incidentes recogidos en el registro de seguridad de la organización.

En la práctica, la organización o el programa puede examinar cada amenaza o incidente recogido en el registro de seguridad (ver Herramienta 1) y elaborar una tabla que aborde cada una de las preguntas anteriores.

Pregunta	Respuesta
1. ¿Qué hechos rodean la amenaza?	
2. ¿Las amenazas son parte de una serie que se ha vuelto más sistemática o frecuente con el tiempo?	
3. ¿Quién es la persona o personas que hace las amenazas?	
4. ¿Cuál es el objetivo de la amenaza?	
5. ¿Qué tan seria cree que sea la amenaza?	

Las amenazas pueden analizarse con más detalle al examinar detenidamente a los perpetradores o agresores. Los perpetradores o agresores necesitan los siguientes elementos para llevar a cabo una amenaza o un acto de violencia:

A. **Acceso:** ya sea físico o virtual, a la posible víctima u organización. Esto podría suponer que saben dónde se encuentra el programa y que pueden entrar libremente; o que pueden identificar a los trabajadores en línea por medio de sus identidades electrónicas y utilizar esto para atacarlos o robar información.
B. **Recursos**: cualquier cosa que pueda utilizarse para llevar a cabo el ataque; por ejemplo, información sobre la ubicación o los puntos débiles de la víctima; disponer de un arma o de un medio de transporte o dinero que les permita llevar a cabo un ataque.
C. **Impunidad**: significa que no hay consecuencias al cometer un ataque: por ejemplo, no hay consecuencias legales o no hay oposición social a su realización.
D. **Motivo**: una razón para llevar a cabo un ataque o una amenaza. Puede estar relacionado con las actitudes o prejuicios que el agresor tenga hacia el programa o la población. En algunos casos, conviene limitar lo que los demás saben sobre el tipo de trabajo que se realiza. En otros casos, es posible desear que entiendan mejor lo que se hace porque eso beneficia a la sociedad en general. Y en otros casos, quizá cambiar la opinión de los demás no sea nuestro objetivo y sea preferible limitar los otros tres ámbitos.

Examinar estos cuatro factores también puede ayudar a identificar cómo reducir o mitigar cada uno de ellos. No hay respuestas "correctas", y a menudo limitar a los agresores también puede limitar a los beneficiarios del programa (por ejemplo, si se limita el acceso al no compartir en línea la dirección de la clínica, ni los agresores ni las personas que busquen hacerse la prueba del VIH la encontrarán fácilmente). Tomar estas decisiones implica hacer concesiones. También en este caso, puede utilizarse una tabla para realizar este análisis de manera sistemática.

	¿Con qué cuenta el agresor en la actualidad?	¿Cómo puede reducirlo el programa?	¿Qué concesiones tendrán que hacerse si se decide actuar de esta manera?
A. Acceso			
B. Recursos			
C. Impunidad			
D. Motivo			

2.4 Plan de seguridad

Descripción

Esta herramienta proporciona un marco básico que reúne la información de las otras herramientas (sobre capacidad, amenazas, riesgos, vulnerabilidades e incidentes) en un plan que probablemente sirva para evitar que se produzcan incidentes y que ayude al programa a responder eficazmente cuando se produzcan amenazas o incidentes.

Dentro de un programa para poblaciones clave existen diferentes riesgos o vulnerabilidades asociados a las distintas actividades; por ejemplo, las actividades de alcance en persona y en línea, así como los diferentes lugares, tienen distintos riesgos asociados. Si el programa incluye instalaciones como una clínica o un centro de acogida, estos también pueden tener vulnerabilidades específicas que deben abordarse mediante medidas de seguridad.

Muchas medidas de seguridad implican cambios sencillos en la forma de trabajar de una organización o un programa y no necesariamente conllevan costos. Sin embargo, el fortalecimiento de la seguridad también puede requerir nuevos equipos, asesoramiento o personal cuyos costos deben calcularse e incluirse como parte de los presupuestos de los programas.

Cómo utilizarlo

El enfoque de planificación recomendado en esta herramienta tiene como objetivo evaluar los riesgos y elaborar un plan para cada tipo de actividad que se realice dentro del programa. El resultado del ejercicio de la planificación de seguridad no es un único plan de seguridad para todo el programa u organización, sino un conjunto de planes de seguridad específicos, cada uno relacionado con cada actividad que el programa lleva a cabo o con el riesgo al que se enfrenta.

Dado que la planificación de seguridad debe ser una parte integral de la planificación de las actividades o del trabajo, y no un proceso separado, es recomendable utilizar esta herramienta de planificación de seguridad cada vez que se diseñen o revisen los planes de actividades. Los indicadores del registro de incidentes, el listado de control de las estrategias de seguridad y el análisis de amenazas deben utilizarse para fundamentar este proceso.

Al final del proceso, las personas que participan en la implementación de cada actividad deben haber participado en la identificación de los riesgos de seguridad y haber llegado a un acuerdo sobre las medidas de seguridad adecuadas. Dado que los riesgos de seguridad pueden cambiar con el tiempo, los planes de seguridad de cada actividad también deben actualizarse periódicamente, sobre todo cuando se sepa que ha cambiado la situación.

La planificación de seguridad conlleva la elaboración de un plan para reducir los riesgos de daños a implementadores en relación con una actividad determinada. Al mismo tiempo, esto también puede favorecer a los beneficiarios y a la comunidad en general. Por lo tanto, esta herramienta debe utilizarse para la planificación de seguridad de cada una de las actividades

de la organización o del programa y para cada uno de los asuntos de seguridad más importantes relacionados con esa actividad.

Es necesario que cada centro de acogida, así como cada sitio o actividad de alcance cuente con un plan por separado (con planes diferentes para las actividades de alcance en persona y en línea), etc.

Estos planes también deben revisarse con el paso del tiempo. Es recomendable hacerlo durante las reuniones rutinarias del equipo de programación o en las juntas de planificación para que se convierta en una parte fundamental de la planificación, en vez de ser una actividad separada.

Los planes de seguridad deben fundamentarse en la información y los análisis realizados con las herramientas 1, 2 y 3.

Los planes de seguridad pueden consistir en una simple tabla:

Plan de seguridad para :	**[Inserte aquí el nombre de la actividad]**		
Fecha de desarrollo/última revisión del plan de seguridad:	**[Inserte aquí la fecha]**		
Persona responsable:	[Esta es la persona dentro de la organización que estará encargada de garantizar la implementación de este plan]		
Riesgo a tratar:	[Describa el riesgo con el máximo detalle posible, incluyendo, por ejemplo, el lugar, la hora, la actividad, las personas, etc.]		
Amenazas	**Vulnerabilidades**	**Capacidad existente**	**Capacidad necesaria**
[Describa las amenazas que hacen que este riesgo sea más o menos probable.]	[Describa lo qué hace que el programa / el personal sean vulnerables a este riesgo.]	[Describa las medidas que se utilizan actualmente para reducir el riesgo.]	[Describa qué más se hará para reducir el riesgo, en términos de métodos de trabajo, equipos, procedimientos, etc.; describa también cómo se procederá al respecto. Piense en cómo reducir las vulnerabilidades e incrementar la capacidad del

			programa para responder en cada caso.]

A continuación se presenta un ejemplo de una tabla elaborada con respecto a los riesgos que se corren durante las actividades de alcance a las poblaciones clave en bares:

Plan de seguridad para :	*Actividades de alcance en bares por parte de trabajadoras sexuales educadoras de pares*
Fecha de desarrollo/última revisión del plan de seguridad:	*1/1/2020*
Persona responsable:	*A. Director*
Riesgo a tratar:	*Riesgo de que agredan físicamente a las trabajadoras durante las actividades de alcance en bares*

Amenazas	Vulnerabilidades	Capacidad existente	Capacidad necesaria
Los abusos verbales, incluidas amenazas de violencia física, se han dado desde el inicio del proyecto y han aumentado recientemente; los perpetradores suelen ser los propietarios de los bares, que no quieren que se realicen actividades de alcance en sus negocios.	*Las actividades de alcance las realizan trabajadoras sexuales que difícilmente denunciarán los abusos; el alcance se realiza con regularidad por la noche; los traslados se realizan a pie; los propietarios de los bares no quieren que el personal de alcance animaen a las trbajadores sexuales a utilizar preservativos porque creen que los clientes pagarán menos.*	*El personal de alcance de pares porta tarjetas de identificación que muestran su conexión con el Ministerio de Salud e incluyen un número telefónico para comunicarse con un oficial capacitado de la policía local; las promotoras trabajan en parejas; las promotoras tienen tiempo aire prepago en caso de emergencia; las promotoras reciben capacitación para describir su labor de manera no controversial; sus*	*Además de la capacidad existente, comenzar a sensibilizar a los propietarios de bares para que disminuyan sus comportamientos abusivos.* *Si los riesgos para las promotoras siguen siendo elevados, reubicar las actividades en otros sitios donde se reúnan las*

		ubicaciones quedan asentadas en un libro de registro; cuentan con refugios seguros en cada vecindario en el que trabajan ya que las trabajadoras sexuales las conocen y respetan.	*trabajadoras sexuales.*

Aunque cada actividad requiere de su propio plan de seguridad, es muy probable que los distintos planes incluyan medidas similares. Por lo tanto, los directores del programa deben revisar todos los planes e identificar si algunas medidas pueden adoptarse de forma conjunta, por ejemplo, en relación con la formación del personal o de los aliados, o con la compra de equipos que sirvan para hacer más seguras todas las actividades.

Considere también priorizar el desarrollo de planes de seguridad para las amenazas más importantes a las que se enfrenta su programa.

2.5 Consejos prácticos para incluir la seguridad de los programas en las subvenciones del Fondo Mundial

Descripción

Aunque las medidas de seguridad dependen mucho del contexto y no hay una fórmula única para todos los casos, la experiencia demuestra que es útil ofrecer algunas sugerencias sobre los tipos de acciones que pueden planificarse y cómo incluirlas en las subvenciones del Fondo Mundial, en particular si implican costos. Esta herramienta proporciona algunas ideas básicas y algunas pautas sobre cómo incluirlas en los planes de subvención.

Cómo utilizarlos

A diferencia de las demás herramientas, ésta no es un listado de control ni una actividad específica sino un conjunto de sugerencias que los usuarios pueden tener en cuenta. No se recomienda incluir todas las actividades de forma automática en el plan de un programa, sino que los implementadores deben considerar si alguna de estas actividades podría ayudarles a hacer que sus programas sean más seguros.

Medidas básicas de seguridad

Aunque cada organización y programa se enfrenta a retos de seguridad diferentes que pueden variar con el tiempo, la experiencia demuestra que hay algunas actividades y prácticas básicas que resultan relevantes para la mayoría de los programas. Examinar su listado de control relevancia en el programa puede ser una buena manera de reflexionar sobre cómo mejorar la seguridad.

1. Incorpore la seguridad del programa a la rutina del programa: revise todas las actividades que se han planificado para detectar posibles problemas de seguridad, poniendo en marcha las medidas de mitigación y respuesta que sean necesarias. Las ideas de mitigación o respuesta podrían incluir:
    - Proporcionar a todo el personal y a los voluntarios tarjetas de identificación con su nombre, organización, cargo y datos de contacto de su organización o supervisor.
    - Establecer un acuerdo con un abogado (por ejemplo, contratar un abogado por iguala) que pueda proporcionar apoyo cuando se produzcan incidentes.
    - Identificar en un mapa debidamente guardado (que no incluya información que pueda ser identificada por terceros) los lugares cubiertos por el programa, incluidos los que son más seguros/riesgosos, e información sobre cómo llegar a ellos. Anotar también para cada lugar la disponibilidad de aliados o colegas (por ejemplo, policía, personal de salud, líderes comunitarios) que puedan ayudar en caso de emergencia.

- Invertir en infraestructuras de seguridad como cerraduras y barrotes en las ventanas, en las oficinas y en los centros de acogida.
- Procurar que los equipos de alcance trabajen por lo menos en parejas. Disponer de procedimientos de registro de entrada y salida para los promotores de las actividades de alcance y los otros equipos de campo, así como proporcionar un traslado seguro de ida y vuelta a los sitios de alcance.
- Utilizar registros de visitantes para anotar quiénes entran y salen de las instalaciones o del centro de acogida.

2. Discuta los incidentes y las inquietudes en materia de seguridad durante las reuniones regulares del equipo (al menos una vez al mes) y anime a todos los miembros del personal y los voluntarios a compartir sus preocupaciones y temores respecto a la seguridad. Anote en un registro todos los incidentes y amenazas, así como las medidas adoptadas, y consulte las notas de forma periódica para identificar las tendencias y realizar cambios en los planes de actividad (por ejemplo, si identifica que algunos puntos conflictivos son cada vez más peligrosos, cambie los patrones de asignación de personal o aumente las medidas de seguridad para esos lugares).
3. Capacite a todos los trabajadores (incluyendo al personal y a los voluntarios) para que sepan cómo abordar los temas de seguridad durante la implementación del programa. Aquí deben incluirse la identificación y evaluación de las amenazas así como lo que se espera de cada trabajador en caso de que se produzca una amenaza (por ejemplo, ¿qué deben hacer para evitar daños? ¿A quién deben dirigirse para pedir ayuda si se producen daños? ¿Qué acciones (como la interrupción inmediata de las actividades de alcance) están en capacidad para llevar a cabo? ¿Qué medidas de protección existen si sufren lesiones en el trabajo o son víctimas de robos u otros delitos?) No es necesario proporcionar una capacitación especial en materia de seguridad, sino que esto puede lograrse con la integración de los temas de seguridad en todas las capacitaciones relacionadas con el programa (incluyendo las dirigidas a los pares y a los proveedores de atención médica).
4. Cuente con un plan de respuesta rápida para hacer frente a las crisis y emergencias. Éste debe incluir canales de comunicación claros, procesos de toma de decisiones claros y recursos financieros flexibles a los que se pueda acceder fácilmente.
5. Designe a una persona de enlace para los temas de seguridad en la organización: puede ser alguien que ya cuente con responsabilidades de gestión o coordinación. Su función será explicar y recordar a los compañeros las políticas y procedimientos. Es necesario capacitar y supervisar a esta persona.
6. Identifique a los aliados que pueden prestar apoyo en caso de incidentes y manténgalos informados sobre cualquier cambio respecto al estado de la seguridad (por medio de líneas de comunicación claras establecidas antes de que se produzcan los incidentes).
7. Desarrolle un árbol telefónico o grupo de comunicación de emergencia para todo el personal y los voluntarios, de modo que todos sepan con quién ponerse en contacto en una situación determinada y cómo compartir las actualizaciones urgentes si se produce una emergencia.

8. El personal y los voluntarios deben decidir cuidadosamente qué información hacer pública (por ejemplo, la ubicación de las instalaciones o su información personal en el caso de los educadores de pares en línea) sopesando los pros y los contras de esto.

Inclusión de temas de seguridad en las solicitudes de financiamiento del Fondo Mundial

Decidir cómo integrar las actividades de seguridad

No todas las actividades de seguridad requieren de financiamiento o de una partida presupuestaria específica. Por ejemplo, asegurarse de que los temas de seguridad se incluyan en el orden del día de todas las reuniones de equipo o de planificación no implica ningún costo, puesto que estas reuniones ya se llevan a cabo. Otras actividades, como la inclusión de procedimientos de seguridad en la capacitación de los equipos y la implementación de un registro de visitantes y de incidentes de seguridad, pueden requerir cierto incremento en los presupuestos existentes (por ejemplo, el costo que implica prolongar una capacitación por medio día más). En estos casos, debe buscarse garantizar que los presupuestos para las actividades existentes sean suficientes para cubrir cualquier proceso adicional relacionado con la seguridad.

En algunos casos, mejorar la seguridad requerirá inversiones específicas destinadas para actividades o equipos adicionales. Algunos ejemplos son asesoría y equipos para un mejor almacenamiento de la información digital, medidas de seguridad física (por ejemplo, cerraduras, alarmas, cámaras) o personal nuevo (guardias de seguridad). Los costos adicionales también pueden corresponder a reuniones adicionales con los actores clave para mejorar la seguridad. Otro ejemplo son los fondos de emergencia o de respuesta rápida, que pueden utilizarse para prestar apoyo al personal o a los voluntarios afectados por un incidente de seguridad.

Elegibilidad de costos relacionados con la seguridad

Todos los costos de seguridad son elegibles para recibir financiamiento en las subvenciones del Fondo Mundial, tal como se indica en los materiales de solicitud pertinentes (por ejemplo, las notas informativas, los informes técnicos y el Marco Modular)[3]. Como en todas las solicitudes de financiamiento del Fondo Mundial, es importante que estén bien justificadas y que dichas necesidades cuenten con evidencia suficiente. (El uso de la autoevaluación de las estrategias de seguridad, el registro de incidentes y las herramientas de planificación resultará muy útil para este punto.) El formulario de solicitud de financiamiento deberá utilizarse para explicar los problemas de seguridad a los que el proyecto se enfrenta en la actualidad, o a los que es probable que se enfrente en un futuro. Asimismo, en el rubro o la actividad solicitados en la partida presupuestaria se deberá señalar de qué manera estos servirán para resolver dichos problemas.

[3] https://www.theglobalfund.org/en/applying-for-funding/design-and-submit-funding-requests/applicant-guidance-materials/ [¿Existe versión en español?]

En qué parte del presupuesto del Fondo Mundial pueden incluirse los costos de seguridad

A la hora de incorporar los costos de seguridad en el presupuesto del Fondo Mundial, lo óptimo es integrarlos en el módulo del programa con el que están directamente relacionados, en lugar de considerar la seguridad como un programa o área de trabajo independiente. Por ejemplo, si están relacionados con la implementación del programa de HSH, deberán incluirse como intervenciones dentro del módulo de VIH/HSH. Si están relacionadas con la protección de las personas que participan en los programas de Derechos Humanos, deberán aparecer en el módulo de Derechos Humanos. Muchas de las organizaciones implementadoras trabajan con diferentes poblaciones clave y realizan actividades de derechos humanos de forma simultánea. En estos casos, en lugar de dividir los costos de las intervenciones de seguridad que corresponden a todas estas áreas del programa, resulta más lógico incluirlas en un solo lugar, por ejemplo, en el módulo de Fortalecimiento de los Sistemas Comunitarios - Desarrollo de la Capacidad Institucional.

Garantizar que los implementadores de primera línea reciban el financiamiento para los costos en materia de seguridad

Muchos programas para las poblaciones clave de VIH reciben financiamiento del Fondo Mundial para la lucha contral el sida, la tuberculosis y la malaria. La mayoría no recibe directamente este financiamiento, sino que llega a través de un Receptor Principal (RP) que tiene un acuerdo con el Fondo Mundial y, a veces, a través de Subreceptores (SR) que el RP ha contratado.

El Mecanismo de Coordinación de País (MCP) es el principal responsable de desarrollar las solicitudes de financiamiento en cada país, mientras que los RP desempeñan una función primordial en el desarrollo de los planes de trabajo y presupuestos detallados y en la implementación de las subvenciones. Es indispensable que el MCP y los encargados de la implementación comprendan los problemas de seguridad a los que se enfrentan los programas para poblaciones clave para que durante el desarrollo de las solicitudes de financiamiento y los presupuestos detallados puedan tomar en consideración posibles costos destinados a mejorar la seguridad de los programas. Una vez que estén incluidos, también es vital incorporar estas partidas en las sub-subvenciones o subcontratos de los RP y SR con los programas de poblaciones clave.

Es necesario que durante el desarrollo de la Solicitud de Financiamiento los MCP garanticen que exista una adecuada comprensión de las necesidades de los programas para las poblaciones clave de VIH. Es posible lograr esto si se aseguran de que los implementadores actuales utilicen las herramientas de este paquete para registrar incidentes, evaluar capacidades, identificar riesgos y elaborar planes de seguridad. Esta información debe fundamentar el diseño del programa y garantizar que el cálculo de costos de éste refleje todos los costos en materia de seguridad.