



NNEDV

## Videovigilancia externa: Minimizar los daños

Si bien [la videovigilancia interior](#) no es una práctica adecuada para los programas comunitarios, la videovigilancia exterior de las instalaciones del refugio u otros tipos de servicios de apoyo puede tener beneficios limitados. La videovigilancia colocada adecuadamente puede mejorar la percepción de seguridad de las personas sobrevivientes y del personal, y podría disuadir a una persona agresora de acercarse a una instalación. Sin embargo, no se ha demostrado que la videovigilancia sea eficaz para reducir los delitos violentos y también puede conllevar importantes riesgos en contra de la privacidad y la confidencialidad.

Este recurso pretende ayudar a los programas a decidir si se debe utilizar la videovigilancia externa y cómo hacerlo de forma que se minimice el daño a las personas sobrevivientes en caso de utilizarla.

**ATENCIÓN:** El uso de videovigilancia en el interior de los refugios no es una práctica adecuada. Obtenga más información sobre [la videovigilancia interna](#).

### ¿Deberíamos utilizar la videovigilancia externa?

Tanto si su programa ya utiliza la videovigilancia externa como si no, esta primera decisión es importante. Si su programa está considerando la posibilidad de utilizar la videovigilancia externa, esta evaluación le ayudará a determinar si los beneficios superan los riesgos para las personas a las que atiende. Si ya utiliza la videovigilancia externa, utilice esta guía para reflexionar sobre las necesidades y el bienestar de las personas sobrevivientes a las que atiende.

Esta evaluación es una adaptación de la publicación de [Las seis preguntas de la ACLU, lo que debe preguntarse antes de aceptar una tecnología de vigilancia](#).

### 1. **¿Cuál es la eficacia de la tecnología?**

¿Cuáles son los objetivos del uso de la videovigilancia externa? ¿Ayudará la vigilancia a alcanzar esos objetivos? ¿Qué problemas espera que resuelva la vigilancia?

La mayoría de las investigaciones no muestran una conexión entre la videovigilancia y una disminución real de los delitos violentos. Aunque no es una herramienta eficaz para prevenir la delincuencia, la presencia de videovigilancia externa puede ayudar a algunas personas a sentirse más seguras. Las grabaciones de vídeo también podrían representar pruebas documentadas cuando se produce un incidente. Sin embargo, si las grabaciones de vídeo incluyen a personas sobrevivientes que no quieren ser identificadas, el uso de esas grabaciones puede infringir las obligaciones de confidencialidad, tanto de la organización como de los miembros individuales del personal.

### 2. **¿Cuáles son los efectos secundarios negativos?**

Aunque la vigilancia puede ayudar a algunas personas a sentirse más seguras, otras personas sobrevivientes o el personal pueden sentir que la vigilancia es una violación de la intimidad o una herramienta abusiva de control. La retraumatización puede ser una consecuencia real. La existencia de videovigilancia también puede dar lugar a solicitudes (o exigencias) por parte de las fuerzas del orden y otras personas para entregar las grabaciones; lo que genera problemas de privacidad y confidencialidad. Si no se instala y mantiene adecuadamente, la videovigilancia puede dar lugar a filtraciones de datos y también vulnerar la confidencialidad.

### 3. **¿Cuáles son los costos de esta tecnología?**

Para que los programas instalen la videovigilancia externa de forma eficaz y adecuada, el sistema debe funcionar de forma segura y ser objeto de un mantenimiento periódico. Debido a las estrictas obligaciones de confidencialidad de los programas, será importante seguir las mejores prácticas para garantizar que el programa mantenga el control de las grabaciones y conserve un contenido mínimo. Esto requiere contemplar los costos iniciales y continuos. Es probable que las opciones menos caras sean menos seguras. También habrá costos en términos de formación del personal e implementación. El obtener y hacer funcionar un sistema de videovigilancia llevará tiempo y necesitará fondos.

### 4. **¿Su comunidad lo desea?**

Como ya se ha mencionado, algunas personas se sienten más seguras bajo videovigilancia, mientras que otras no. Si las personas sobrevivientes no se sienten más seguras, y de hecho se sienten vulneradas o controladas, esto socava el propósito de su programa y puede disuadir a las personas sobrevivientes de buscar servicios.

Si la comunidad en general apoya o no la videovigilancia es también una cuestión importante. Diferentes programas ubicados en la misma ciudad pueden llegar a respuestas diferentes. Por ejemplo, un programa en una zona comercial puede sentirse más cómodo con la vigilancia, mientras que un programa en una zona residencial puede sentirse menos cómodo debido a los riesgos en contra de la privacidad o a experiencias de vigilancia o el exceso de esta.

Es posible que el personal ya tenga una idea de lo que piensan la mayoría de las personas sobrevivientes sobre la videovigilancia. ¿Las personas sobrevivientes que llegan preguntan si hay videovigilancia y se sienten aliviadas cuando se enteran de que sí hay? ¿O preguntan por qué hay videovigilancia y expresan preocupación o frustración por sentirse vigiladas?

### **La segunda decisión: ¿Qué productos cumplen nuestros objetivos y minimizan los daños?**

Si su programa ha pasado por la discusión anterior y ha determinado que la videovigilancia es útil y deseada por las personas sobrevivientes, esta segunda decisión puede ayudarle a elegir el mejor tipo de producto. Existe un amplio mercado de dispositivos y sistemas de videovigilancia y también una gran variedad de opciones para el consumidor. Algunos sistemas pueden proporcionar una transmisión en directo, mientras que otros sólo ofrecen la opción de ver las grabaciones guardadas. Algunos sistemas no realizan grabaciones, mientras que otros almacenan las grabaciones en línea, o en un dispositivo físico en su programa, o en ambos. Algunos dispositivos y sistemas son más seguros que otros. Muchos sistemas están diseñados teniendo en cuenta las necesidades de gestión de riesgos comerciales o personales, que son diferentes de las necesidades de un programa de refugio con estrictas obligaciones de confidencialidad.

Los programas deben limitar sus consideraciones a los sistemas de videovigilancia que:

- Están pensados para instalarse en el exterior de un edificio.
- Utilizan un cifrado o encriptado potente para la transferencia y el almacenamiento de datos, de modo que las grabaciones no puedan ser interceptadas (cifrado de datos almacenados y en tránsito).

- Están diseñados para que sólo su organización pueda acceder a las grabaciones almacenadas y no la empresa del sistema de vídeo. Esto puede denominarse cifrado sin conocimiento, de conocimiento cero o solamente por parte del cliente.

**ATENCIÓN:** El proyecto \*[Privacy Not Included](#) de la Fundación Mozilla puede ayudarle a evaluar algunos sistemas de vigilancia.

### **La tercera (y última) decisión: ¿Qué políticas minimizan los daños?**

Los programas deben contar con políticas claras que guíen la configuración y el uso de los sistemas de vigilancia. Estas prácticas ayudan a minimizar los daños de las personas sobrevivientes y al personal del programa cuando se utiliza la videovigilancia externa.

Los sistemas y políticas de videovigilancia externa deben:

- Utilizar la seguridad de datos más estricta en todo momento.
- Eliminar las grabaciones de forma frecuente, regular y continua. Se recomienda purgar las grabaciones cada 24 o 48 horas.
- Contar con un acceso estrictamente limitado al sistema, incluidas las grabaciones y las visualizaciones en directo.
- Recopilar y tener una retención mínima de grabaciones que incluyan a las personas sobrevivientes.

Los sistemas externos de videovigilancia **no deben**:

- ser accesibles para el personal en dispositivos personales, o a través de un sitio web al que puedan acceder fuera de las instalaciones.

Las políticas también deben incluir detalles sobre:

- Procedimientos para responder a demandas legales u otras solicitudes de grabaciones de vídeo.

- **ATENCIÓN:** Las obligaciones de confidencialidad prohíben a los programas compartir información identificatoria sobre las personas sobrevivientes, incluidas las grabaciones, con cualquier persona ajena al programa sin una orden judicial válida o un requisito de conformidad con la ley estatal.
- Procedimientos para responder a las solicitudes de las personas sobrevivientes de revisar o utilizar las grabaciones si sospechan o identifican el hecho de que una persona agresora se encontraba cerca de las instalaciones.

© 2023 National Network to End Domestic Violence, Safety Net Project. Financiado por US DOJ-OVW Subvención Número 15JOVW-21-GK-02255-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia (DOJ).

Actualizamos nuestros materiales con frecuencia. Visite [TechSafety.org](https://TechSafety.org) para consultar la última versión de este y otros materiales.