Cómo Operar como un Centro de Trabajo Remoto Durante una Crisis de Salud Pública

En una crisis de salud pública como la actual pandemia de COVID-19, en la cual los/las funcionarios/as de salud pública recomiendan el "aislamiento social" para disminuir la propagación de la infección, las tecnologías que permiten el acceso remoto a los archivos, la mensajería instantánea y las videollamadas pueden utilizarse para mantener el funcionamiento del programa y permitir que el personal y los voluntarios trabajen de forma remota. Muchas de estas herramientas pueden ser beneficiosas para la intercesoría móvil en cualquier momento.

A la hora de considerar nuevas tecnologías, los/las sobrevivientes deben estar en el centro de nuestra toma de decisiones. Esto es válido en tiempos corrientes y debe aplicarse incluso ante una crisis de salud pública.

Si bien la Red de Seguridad Tecnológica recomienda un enfoque reflexivo y planificado para el uso de la tecnología, el carácter de urgencia de la actual crisis de salud pública puede dar lugar a que muchos programas consideren el uso de la tecnología en el corto plazo. **Aconsejamos a los programas que implementan estas tecnologías durante la actual pandemia de COVID-19, hacerlo temporalmente** y a reconsiderar su decisión cuando la pandemia haya terminado.

1. Analice qué servicios pueden prestarse de forma remota a través de *web chat* o videollamadas. Lea más sobre el Uso de Tecnología para Comunicarse los Sobrevivientes Durante una Crisis de Salud Pública y acceda a nuestro Conjunto de Herramientas de Servicios Digitales.

2. Use herramientas que le permita al personal y a los/las intercesores/as trabajar desde el hogar. Esto incluye herramientas que facilitan la comunicación entre el personal y los/las voluntarios/as (por ejemplo llamadas, mensajería instantánea, videos) y herramientas para compartir

información mientras que mantienen la confidencialidad (por ejemplo, el intercambio seguro de archivos).

A continuación se detalla una lista de herramientas que los programas podrían contemplar para comunicarse con los/las sobrevivientes de forma remota que creemos que cumplen con los estándares de mejores prácticas actuales. Dos factores clave que se deben tener en cuenta al seleccionar una herramienta son: 1) las opciones de cifrado cuando la propia empresa de tecnología no puede ver el contenido de los archivos porque no cuentan con la clave de cifrado y solo usted la tiene, y 2) las opciones de acceso del usuario que le permiten controlar el acceso al contenido por usuario. **Si bien no respaldamos estas herramientas**, son apropiadas para proteger la privacidad de la manera en la que están configuradas actualmente.

- ResourceConnect: mensajería instantánea para el personal y los/las voluntarios/as
- Gruveo: videollamadas
- Cyph: videollamadas, mensajería y grupos
- Tresorit, SpiderOak's CrossClave, Mega, Sync, y pCloud: intercambio de archivos

Compartimos esta lista en un intento de reducir los riesgos de privacidad que provienen de adoptar herramientas de forma precipitada, sin dedicarles el tiempo necesario para evaluarlas detenidamente.

Además de estas herramientas más modernas, analice de qué manera puede aumentar la seguridad y la privacidad cuando emplea tecnología más antigua, como el correo electrónico o el teléfono:

- Prácticas recomendadas al utilizar el correo electrónico
- Prácticas recomendadas para utilizar teléfonos móviles

Recomendamos ofrecer cuentas y dispositivos propios del programa. Esto

permite un mejor control del personal entre turnos y puede aumentar las medidas de seguridad y privacidad. Lea más acerca de las mejores prácticas para la intercesoría móvil.

La seguridad y privacidad del sobreviviente son importantes. Cuando los/las intercesores/as usan dispositivos móviles para hablar sobre los/las sobrevivientes o para comunicarse con ellos, los hilos, las conversaciones y otros expedientes relacionados probablemente incluyan información personal identificable. Tenga en cuenta las directrices sobre cómo y cuándo ocurrirán estas comunicaciones.

El uso de la tecnología para trabajar de forma remota permite colaborar con la salud y el bienestar del/de la intercesor/a. Una crisis como la del COVID-19 no debería contrarrestar nuestro compromiso por defender el bienestar. Los/las intercesores/as no deben correr el riesgo de contraer la infección en el desempeño de su trabajo. Los/las intercesores/as deben tener días libres de servicio para obtener el descanso y la alimentación adecuados, dos puntos clave determinados por los/las funcionarios/as de la salud pública para mantener un sistema inmunológico fuerte.

Entendemos que, en cualquier crisis de salud pública, el acceso a los servicios puede ser aun más difícil para los/las sobrevivientes que buscan recursos y apoyo. Adaptar las operaciones para satisfacer las necesidades de los/las sobrevivientes y los/las intercesores/as y comprender los riesgos que conlleva el uso de la tecnología ayuda a garantizar que los/las sobrevivientes y los/las intercesores/as cuenten con la información que necesitan para obtener ayuda y llevar a cabo su trabajo de la mejor forma posible.

TechSoup cuenta con una gran cantidad de recursos en materia de tecnología para organizaciones sin fines de lucro, que incluyen descuentos en hardware y licencias de software, capacitación tecnológica para el personal e información. Estos son algunas publicaciones de blog sobre el trabajo a distancia (en Inglés):

- Recursos no lucrativos para el trabajo a distancia durante el brote de

COVID-19

- Consejos prácticos para el trabajo a distancia dentro de su organización sin fines de lucro
- Comprender las Herramientas de Videoconferencia Disponibles para su Organización sin Fines de Lucro

Tenga en cuenta que estas sugerencias están dirigidas, de forma general, a organizaciones sin fines de lucro. **Muchas de las herramientas tecnológicas sugeridas pueden ser adecuadas para las operaciones diarias, pero tal vez no sean apropiadas para comunicarse con los/las sobrevivientes o para compartir información personal identificable.**

Si su agencia tiene preguntas o necesita asesoramiento adicional respecto de la implementación de los servicios digitales. Póngase en contacto con el Equipo de la Red de Seguridad escribiendo a safetynet@nnedv.org. También puede comunicarse con el equipo de Capacitación de Asistencia Técnica de Coaliciones para realizar otras consultas sobre el virus COVID-19.

 Este producto fue financiado por el acuerdo de cooperación n.° 2019-V3-GX-K017, otorgado por la Oficina para Víctimas de Delito, Oficina de Programas de Justicia, Departamento de Justicia de los Estados Unidos. Las opiniones, hallazgos, conclusiones o recomendaciones aquí expresados pertenecen a los/las contribuyentes y no necesariamente reflejan la postura oficial ni las políticas del Departamento de Justicia de los Estados Unidos.

Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.