GUÍA FÁCIL

PARA COMUNICARNOS EN ESPACIOS SEGUROS DURANTE COVID19 (Y CONSPIRAR)

ALTERNATIVAS PARA QUE TE COMUNIQUES DE MANERA SEGURA Y HABITES ESPACIOS EN DONDE LOS RIESGOS ESTÉN MINIMIZADOS

INICIATIVA MESOAMERICANA de mujeres defensoras DE DERECHOS HUMANOS

dominemos la tecnología

Encerradas (por ahora)
y comunicadas (de manera segura)

Desde que se impusieron las medidas de distanciamiento físico, quienes, básicamente, tenemos la oportunidad de quedarnos en casa y trabajar desde la computadora, vemos un aumento considerable en el uso de las videollamadas, usadas para trabajar, estudiar y mantener el contacto con las comunidades y personas queridas.

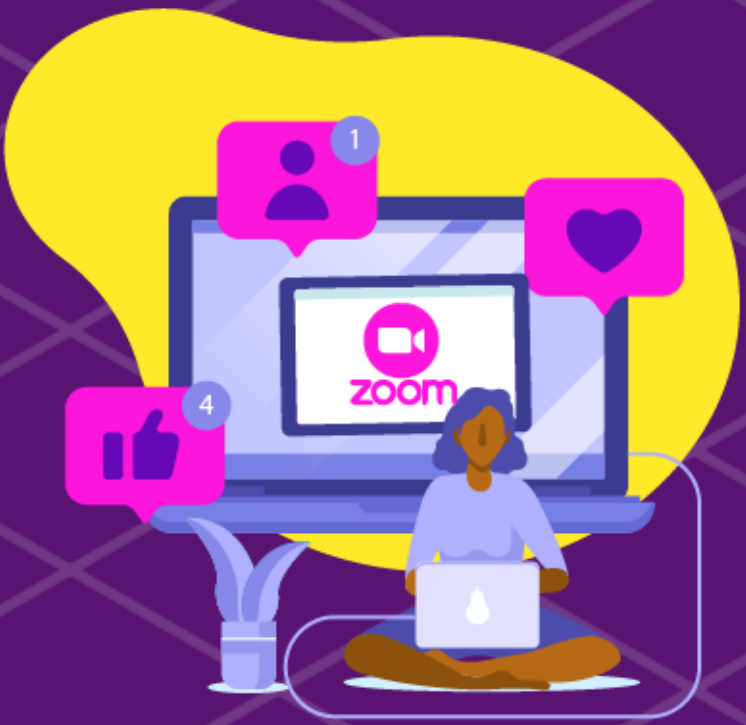
ZOOM, una plataforma para videollamadas experimentó un aumento notable desde el inicio de la emergencia sanitaria. Al mismo tiempo, hemos sido testigas de distintas agresiones en este espacio, interrupciones continuas, boicot a las participantes, ataques racistas y misóginos por parte de personas que se "auto-invitan" a nuestras conversas en dicha plataforma. Aún después de que Zoom implementara medidas de seguridad, las preocupaciones acerca de la venta de datos y de las vulnerabilidades de seguridad siguen en pie.

Por eso, te ofrecemos alternativas para que te comuniques de manera segura y habites espacios en donde los riesgos estén minimizados.

Para videollamadas, webinarios o conferencias

Si necesitas realizar una actividad pública y llegar a una audiencia amplia, ya que sabemos que muchos eventos públicos han tenido que ser cancelados, **pon atención.**
Si piensas en organizar un conversatorio, el lanzamiento de un informe o realizar un webinario, recomendamos evaluar si lo que necesitas realmente es una videollamada. Tal vez lo más adecuado es usar una plataforma de **streaming**.

El streaming te permite transmitir audio y video en tiempo real a través de internet. Algunas de las alternativas gratuitas más populares son Youtube Live (de Google), Facebook Live (de Facebook) y Periscope (de Twitter). Otra alternativa segura es usar **Meet.jit.si** solo para las expositoras y replicar la transmisión por Youtube o Facebook para canalizar los comentarios.



Recuerda que los comentarios estarán abiertos y que pueden ser un punto débil para ataques (los machitrolls pueden inundar tu transmisión con mensajes o videos machiracistas). **Organízate para moderarlos y expulsarles (caso sea necesario).**

Para conversaciones privadas y grupos grandes

Si lo que necesitas es tener una conversación privada con un grupo grande de personas. Recomendamos tomar unas medidas previas que te ayudarán a mantener ese espacio mas seguro y reducir los riesgos:

- Solicita un registro previo en el que las personas manden un correo y señalen a cuál colectiva pertenecen. Esto es más tardado pero te permitirá checar que esa persona y esa colectiva efectivamente existen y podrían ser parte de tu actividad.

- Difunde la actividad solo en grupos de confianza y solicita explícitamente el pedido de no circular la actividad por fuera de espacios de confianza. Piensa si en lugar de difundir en redes sociales puedes solo avisar por correo electrónico o sistemas de mensajería.


0 1 0
1
******

Plataformas a considerar:

- **Meet Jitsi** (gratuita, libre, permite grabar y compartir pantalla, número máximo personas 75). La función de cifrado de extremo a extremo se activa solo cuando 2 personas participan. Para paliar esta limitación hay que usar instancias de Meet Jitsi alojadas en servidores seguros y confiables, algunos recomendados son los mantenidos por Greenhost, Mayfirst, Framatalk y/ o Disroot.

- **Wahay.org** (gratuita, cifrada, libre y no requiere servidores). Wahay es un sistema para conferencias de audio que combina los proyectos Mumble y Tor. A diferencia de otros sistemas, Wahay no está intermediado por un servidor. Solamente las personas que participan en la reunión pueden saber que la misma existió. Para usarla hay que descargar un programa disponible para Linux, pero en el futuro estará para Windows y Mac.

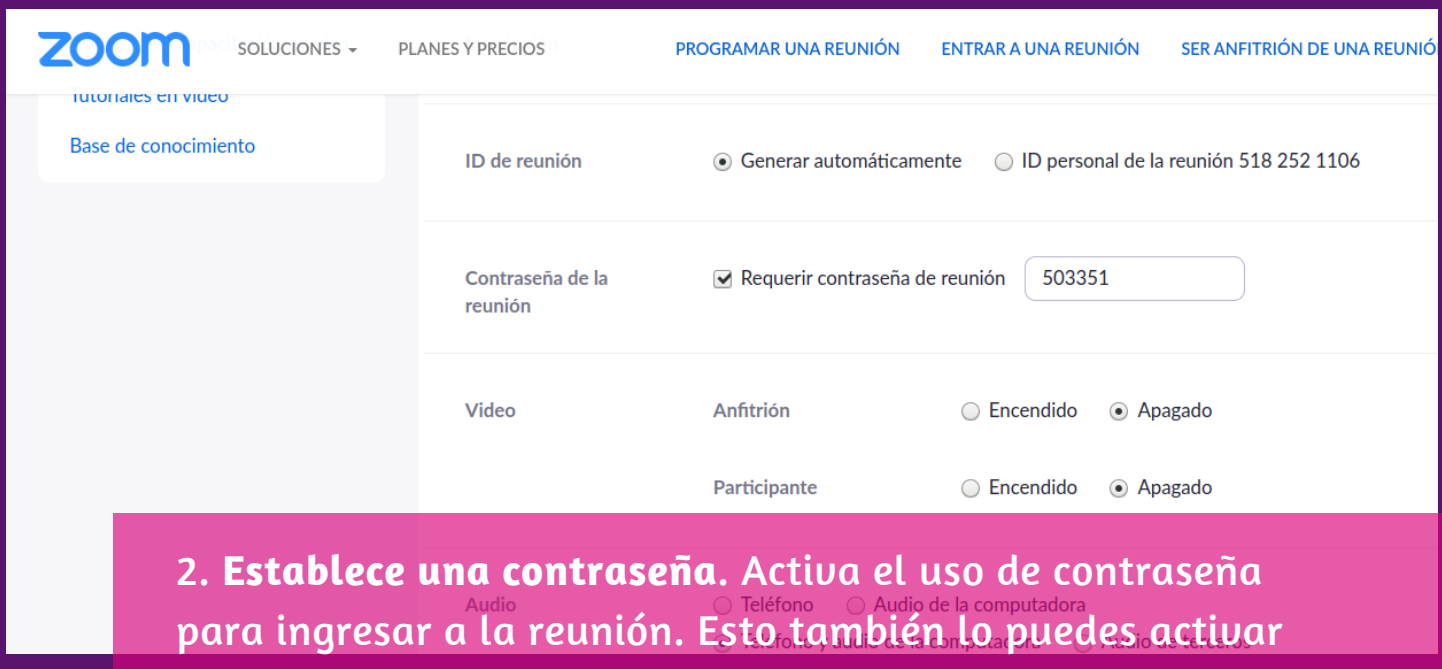
- **BigBlueButton** (gratuita, libre, código abierto, cifrada, se puede instalar en un servidor propio). Permite designar a una persona moderadora para que comparta pantalla, use un puntero, y designe a otras personas coordinadoras. Hay que hacer *registro* para crear una sala. Les participantes pueden entrar sin hacer *log in*. Permite crear grupos de trabajo y tiene un *pad* de notas propio.

Cada una de estas plataformas tiene sus especificidades. Recomendamos visitar sus sitios web oficiales para comprender en detalle sus características y políticas de privacidad de los datos.

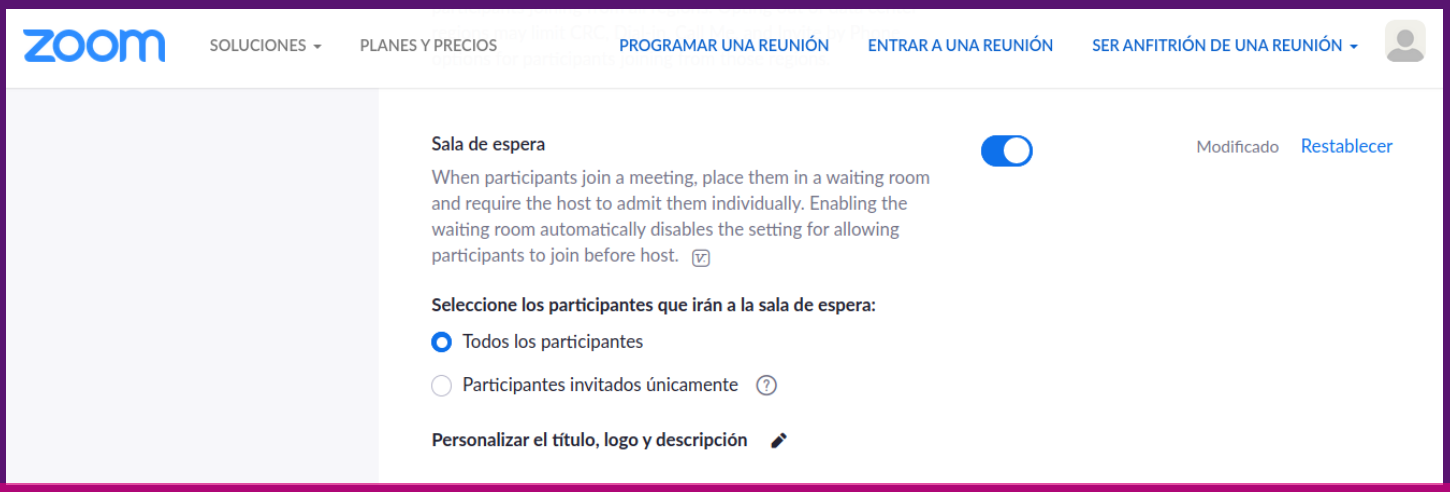
ALGUNAS RECOMENDACIONES EN CASO DE QUE AÚN TENGAS QUE USAR ZOOM...

Ingresa al sitio de Zoom y revisa en tu cuenta personal las siguientes configuraciones para reducir la posibilidad de ataques:

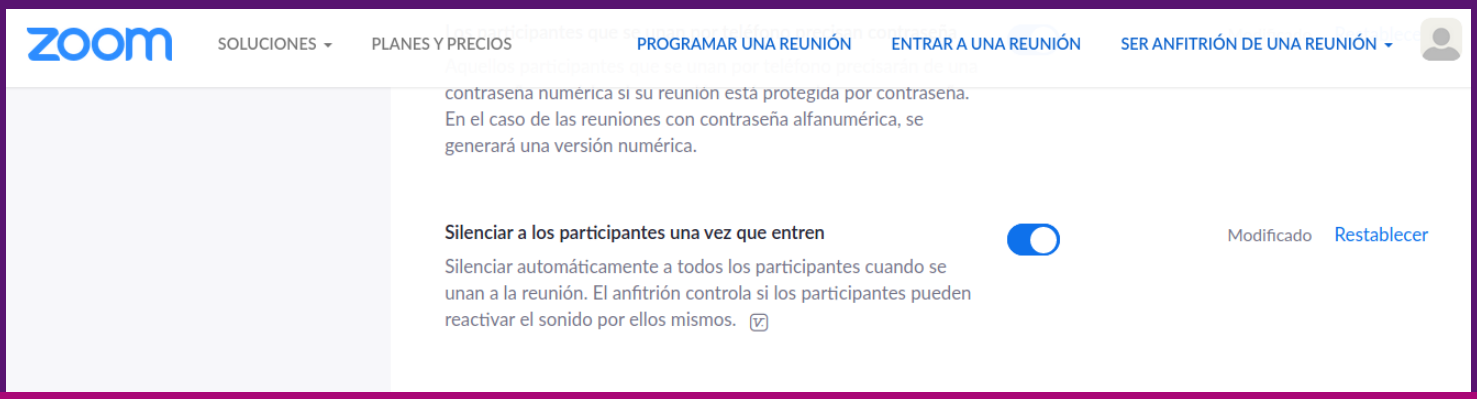
1. **Generar ID de sesión automática**. No circules tu ID personal como ID de reunión. Si tienes reuniones recurrentes, cambia sus ID frecuentemente.



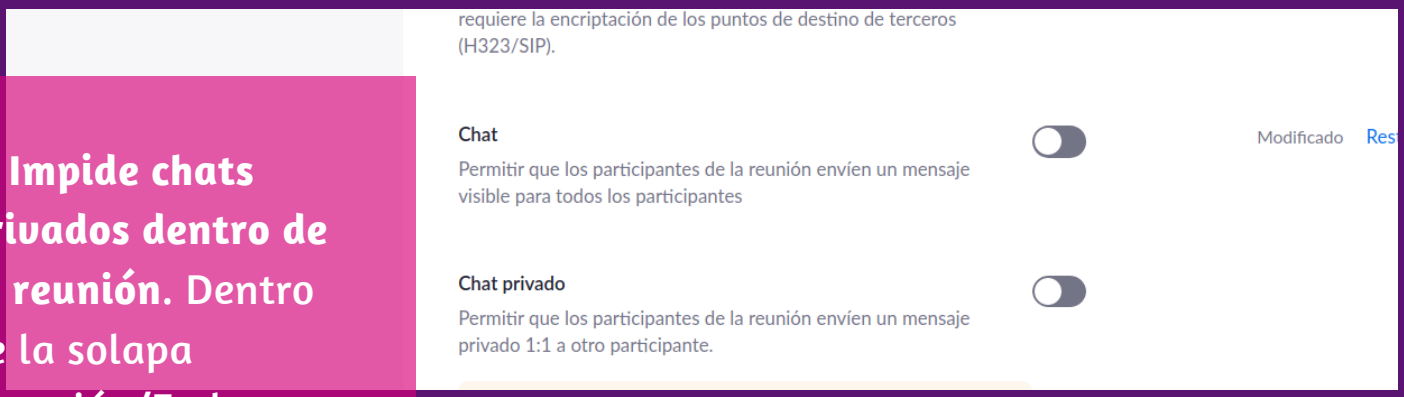
2. **Establece una contraseña**. Activa el uso de contraseña para ingresar a la reunión. Esto también lo puedes activar desde la solapa "Programa una reunión". Recuerda, existen buscadores automatizados que están escaneando internet para ingresar a salas Zoom que estén sin contraseña. Por eso hay ataques en reuniones difundidas pero también reuniones no publicitadas.



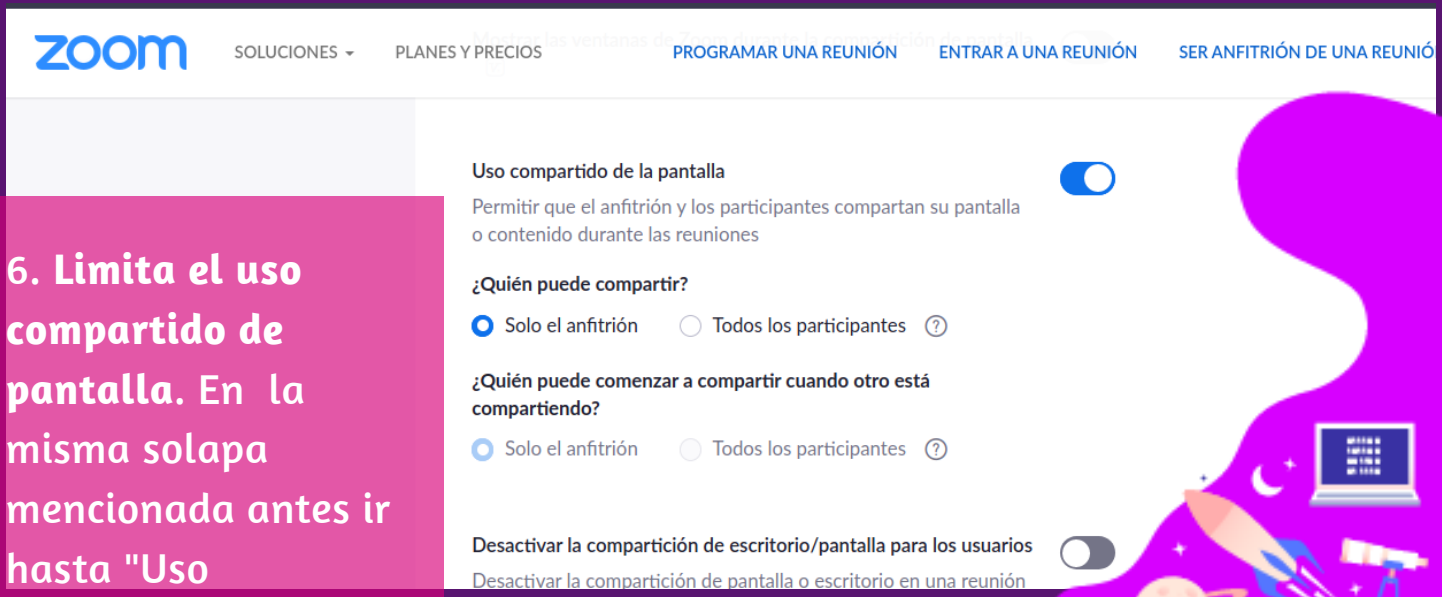
3. Habilita la opción sala de espera. Para habilitar la entrada a la sala de espera la "anfitriona" tiene que estar con su panel de control de Zoom abierto, no debe entrar en la reunión como cualquier participante. Es necesario conservar el rol de anfitriona durante la reunión para, sobre esa base, decidir abrir el ingreso o no a otras personas.



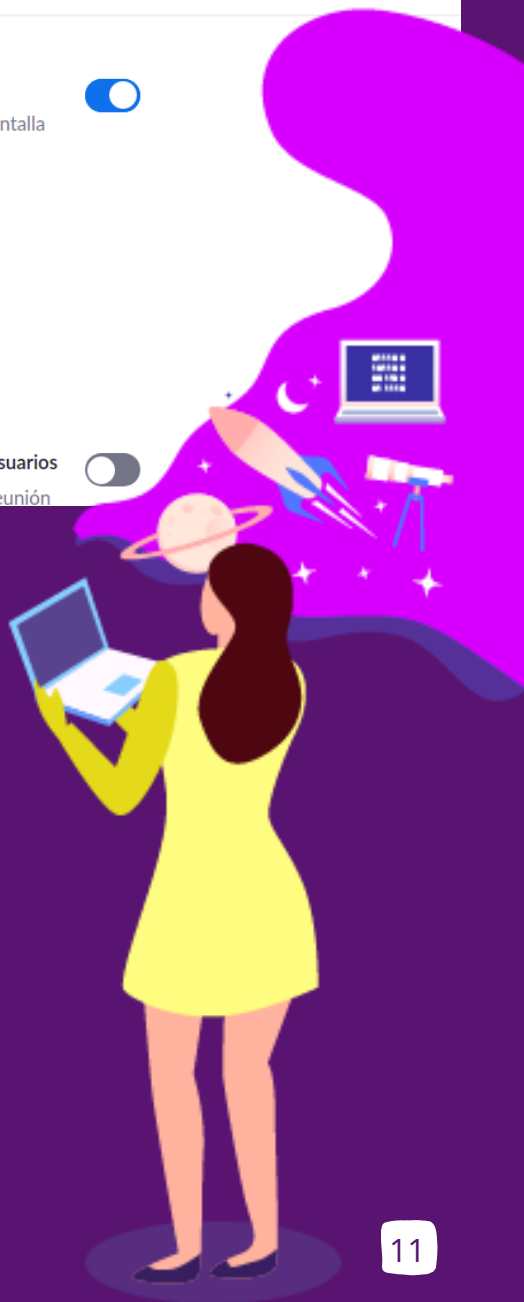
4. **Silencia a las/los/les participantes cuando ingresen a la reunión.** Esta opción también se encuentra dentro de Programar reunión, activa la opción que dice “Silenciar a los participantes al entrar”.

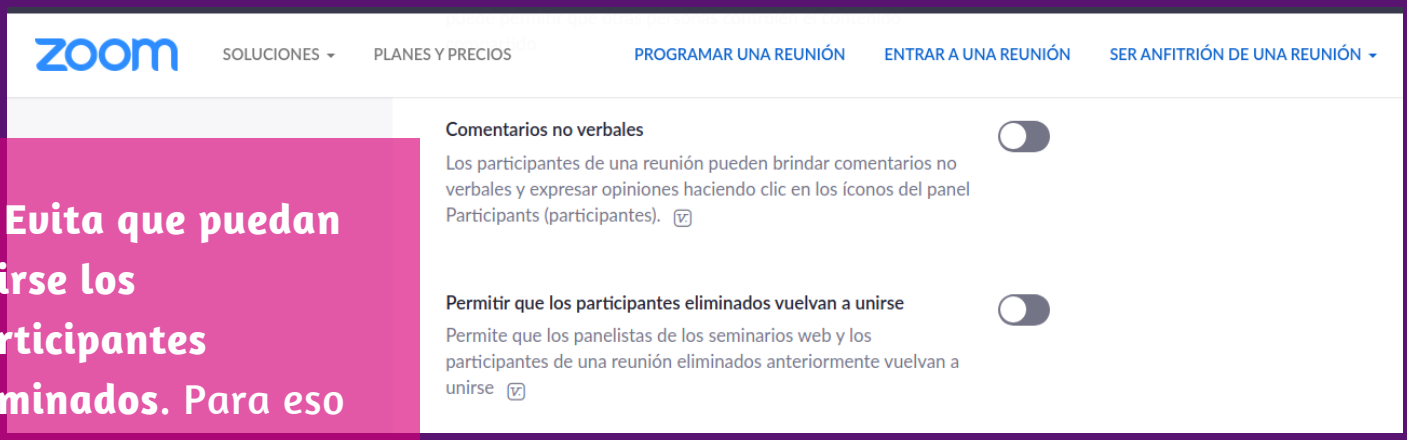


5. Impide chats privados dentro de la reunión. Dentro de la solapa "Reunión/En la reunión (básico)" busca "Chat privado" y desactívalo.

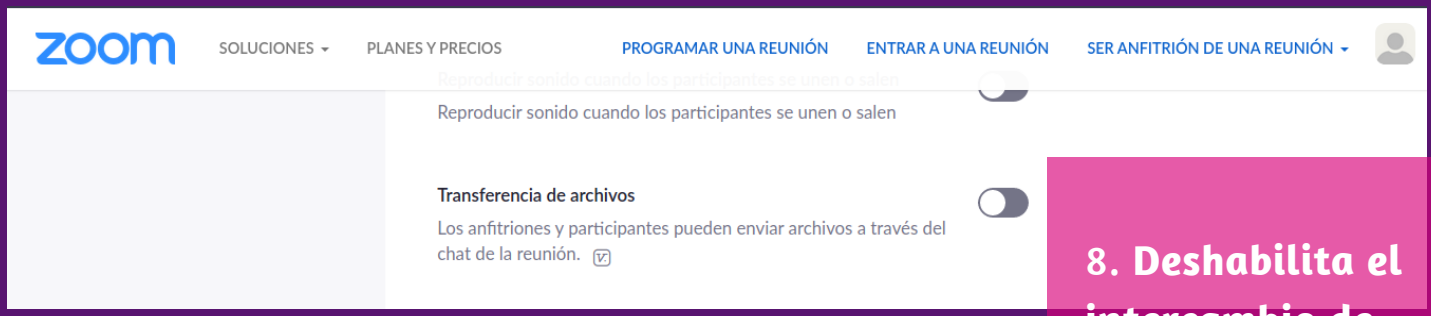


6. Limita el uso compartido de pantalla. En la misma solapa mencionada antes ir hasta "Uso compartido de la pantalla" y deshabilita la opción que permite que todos los participantes compartan pantalla.



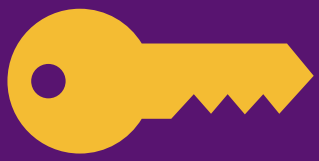


7. Evita que puedan unirse los participantes eliminados. Para eso hay que deshabilitar la opción que dice "Permitir que los participantes eliminados puedan volver a unirse".



8. Deshabilita el intercambio de archivos para participantes. Desconecta esta función para evitar que el chat sea bombardeado con fotos no solicitadas, GIFs, memes y otros contenidos, en "Reunión/Básico".

Consejos para antes, durante y después de las reuniones



Algunas buenas prácticas para concebir un espacio seguro son:

- Asegúrate de saber **quién va a estár conectada/o** (si es necesario revisa su perfil y chequea el trabajo de su colectiva)

- Acuerda las **reglas del espacio:** si van a mantener las cámaras encendidas o las van a tener apagadas, mantener el micrófono encendido y apagado cuando no se habla, designar cuándo los participantes quieren hablar, quién presidirá la reunión, quién tomará notas. También es importante decidir dónde y cómo se escribirán y, a posteriori, se distribuirán esas notas, si está bien hacer capturas de pantalla de una videollamada, si están de acuerdo en grabar la llamada, etc.

- En tiempos de sobreabundancia de reuniones **acordar agendas y duración de las reuniones no es menor.** Si el seminario web dura más de una hora, probablemente sea mejor dividirlo en sesiones de una hora separadas por algún tiempo acordado con las participantes, para que tengan tiempo de relajarse y responder a otras cosas. Puedes aprovechar el tiempo en sala de espera para postear reglas de convivencia en la reunion, o compartir información relevante.

Fuentes consultadas para la redacción de esta guía:

Así que necesitas hacer una videollamada (Derechos Digitales)

Guide to Secure Group Chat and Conferencing Tools (Frontline Defenders)

Más cerca que nunca (Asociación para el Progreso de las Comunicaciones)

dominemos la tecnología

INICIATIVA MESOAMERICANA de mujeres defensoras DE DERECHOS HUMANOS