Universidad Veracruzana
Secretaría de Desarrollo Institucional
Dirección General de Tecnología de Información

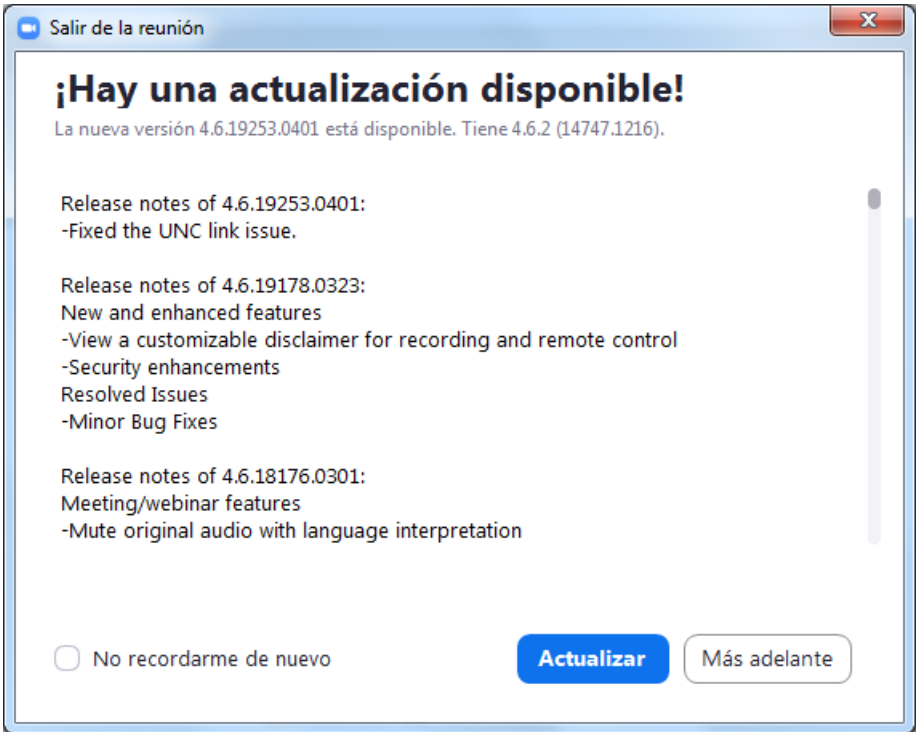
Cómo mejorar la seguridad de sus reuniones con Zoom

El objetivo de este documento es proveer a los usuarios de la comunidad universitaria, recomendaciones de buenas prácticas que les permitan organizar clases y reuniones que resulten seguras y satisfactorias.

Recuerde que el ingreso a Zoom para usuarios de la comunidad UV es a través del portal https://uveracruzana.zoom.us usando sus credenciales del correo electrónico institucional. Por lo tanto, la primera y más importante recomendación, es no prestar sus credenciales del correo electrónico de UV, para mantener segura su identidad institucional y sus reuniones de Zoom, entre otras plataformas que se acceden a través del mecanismo de *single sign-on* (SSO).

1. Mantenga su cliente actualizado

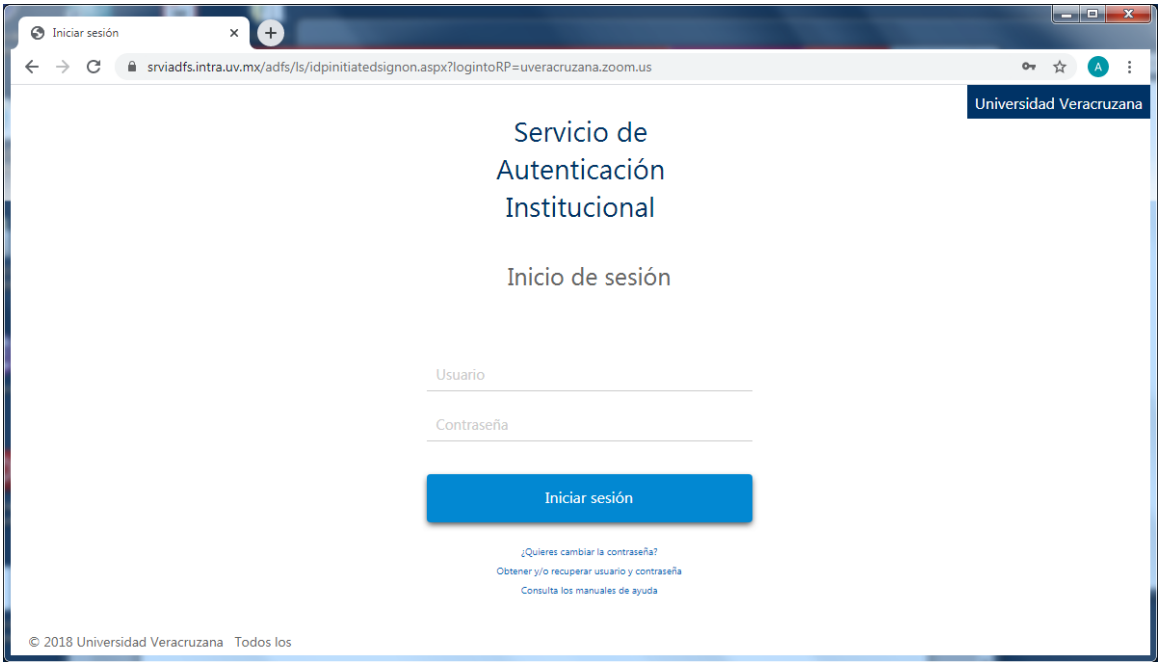
Al igual que cualquier sistema informático, el cliente de Zoom puede sufrir vulnerabilidades de seguridad; sin embargo, la compañía las arregla con gran celeridad. De modo que es fundamental que Ud. aplique en su computadora las actualizaciones del cliente de Zoom, tan pronto como éste lance los "parches" o actualizaciones, los cuales se notifican de manera automática a los usuarios.



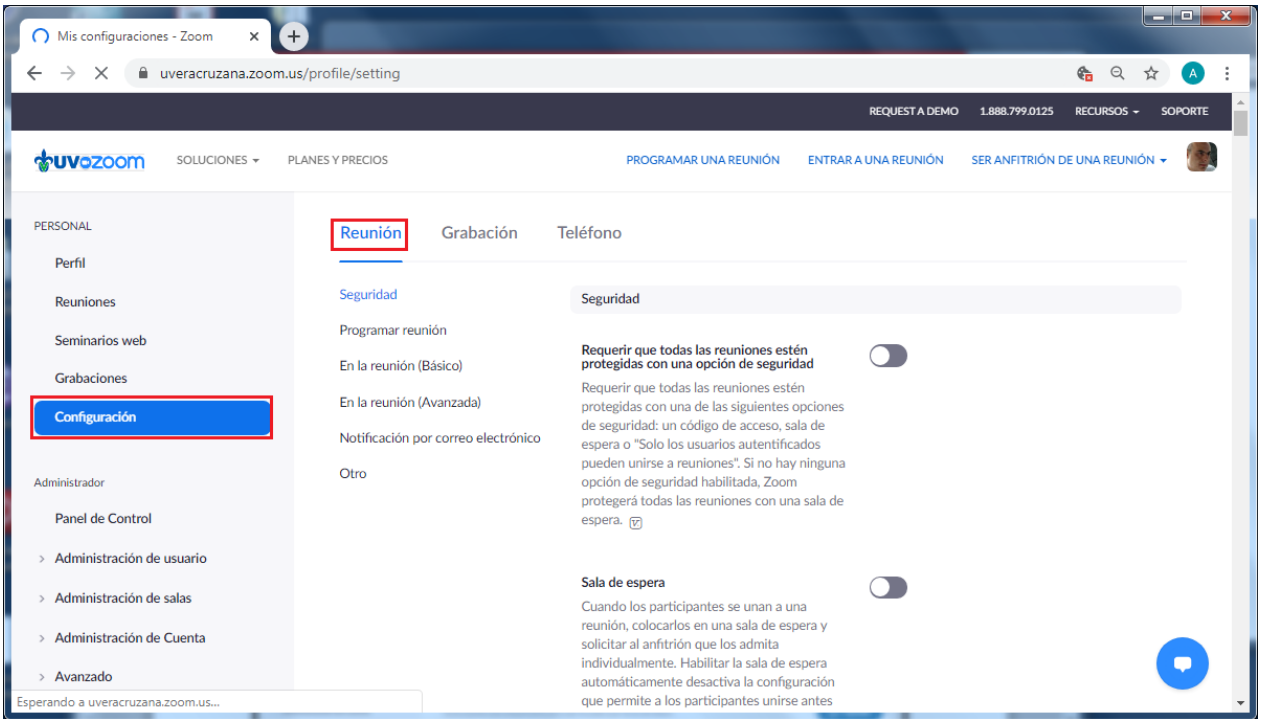
2. Use contraseña para proteger sus reuniones

Algunos de nosotros hemos escuchado noticias de “Zoom bombing” o “party-crashers”, es decir, personas no invitadas que ingresan a la sala virtual con la intención de arruinar las reuniones o eventos. ¿Cómo evitarlo? ¡Sencillo! Proteja sus reuniones con contraseña.

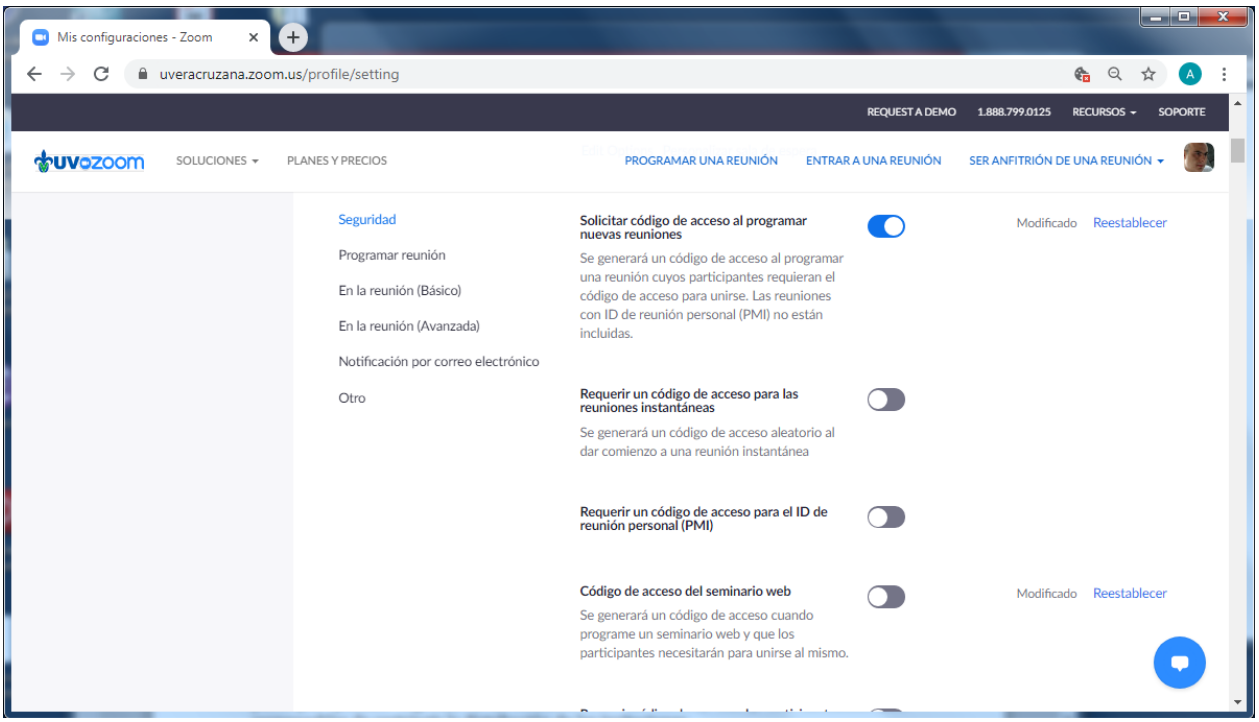
Para ello, ingrese a Zoom desde el portal https://uveracruzana.zoom.us y seleccione el botón de “Ingresar”, esto le llevará a la pantalla de inicio de sesión.



Ingrese usando sus credenciales del correo electrónico de UV. En el marco izquierdo de la interfaz, ubique la sección de “Configuración”.



En sus ajustes de configuración de reunión, descienda (scroll down) hasta encontrar el control “Solicitar código de acceso al programar nuevas reuniones”, y habilítelo, como se muestra en la ilustración.



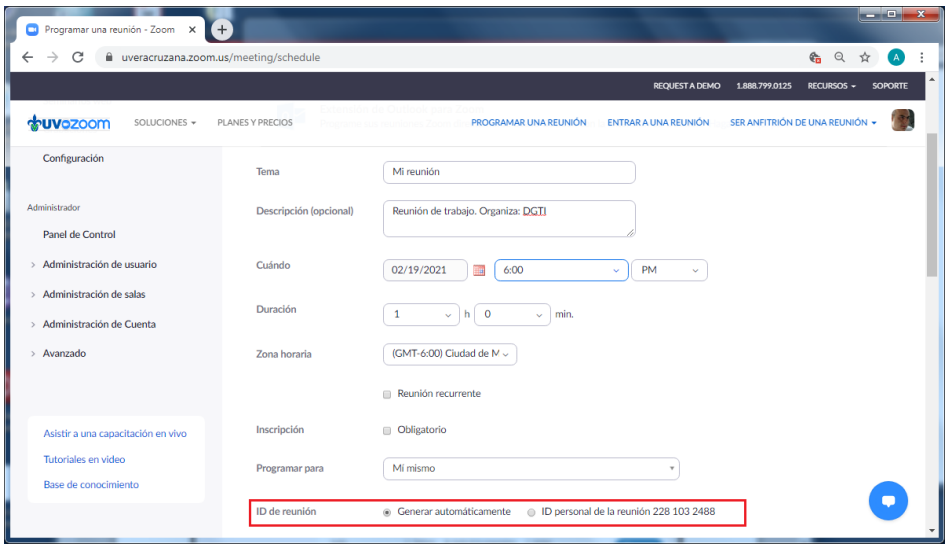
Evidentemente, si en la invitación de correo electrónico Ud. publica la contraseña, y ésta es distribuida de manera libre, se abre la posibilidad de que personas que no deben participar puedan ingresar a la reunión. Por tal motivo, Ud. y sus invitados son responsables de **restringir la distribución de las invitaciones** hacia únicamente los auténticos destinatarios de la invitación.

3. No comparta su ID de reunión

Su ID de reunión es una cadena numérica de 10 dígitos que corresponde a su sala virtual.

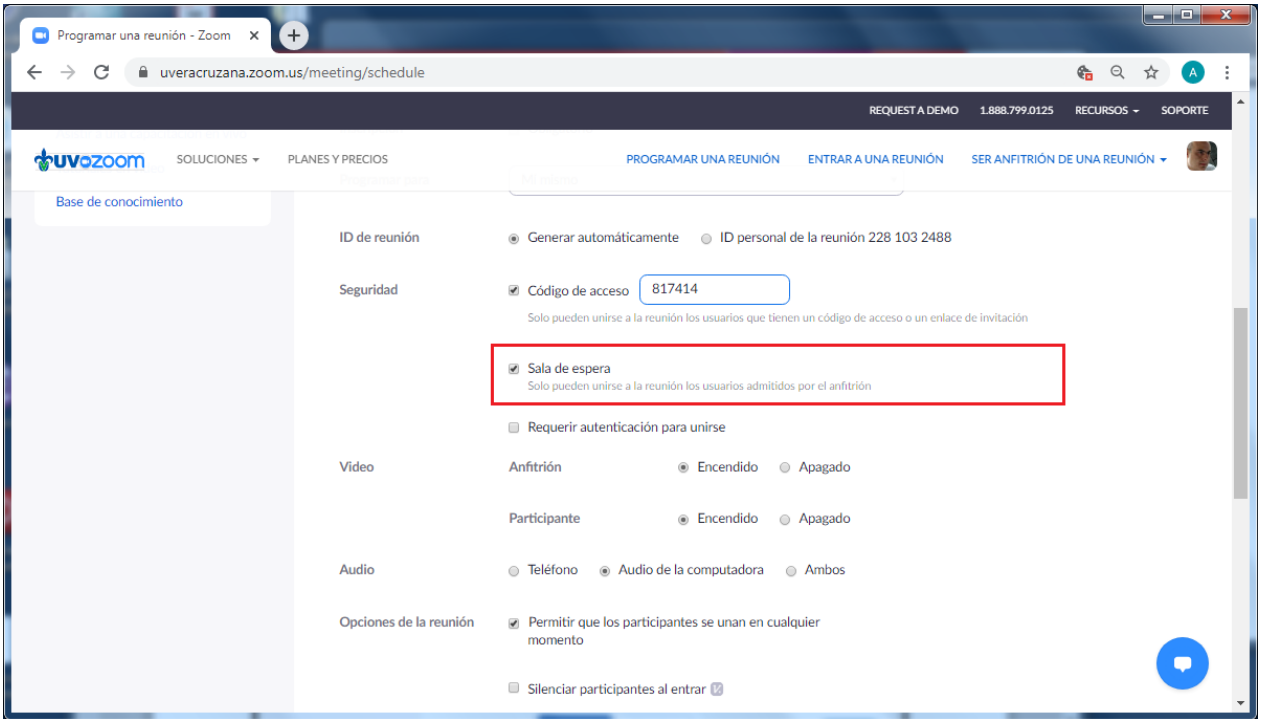
Compartir su ID de reunión es análogo a compartir su número de teléfono celular: éste debe conservarse privado, y darlo únicamente a sus contactos de confianza.

Zoom ofrece la funcionalidad de generar un ID aleatorio para cada reunión. Cuando Ud. programa una nueva reunión, elija siempre la característica “Generar ID automáticamente” en vez de usar su ID de reunión.



4. Use la sala de espera

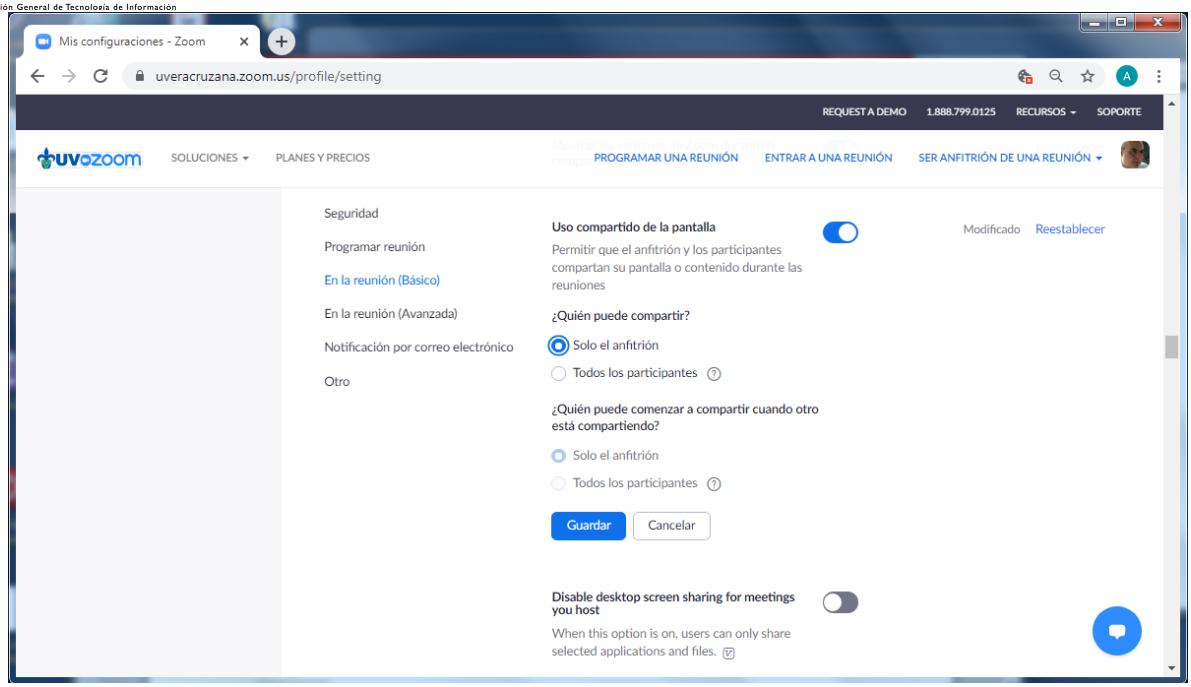
La sala de espera es una funcionalidad de Zoom que permite a Ud. identificar y filtrar a sus participantes en la sala virtual, **antes** de permitirles ingresar. Use esta funcionalidad como anfitrión, para asegurar que sólo los invitados tengan acceso a la reunión.



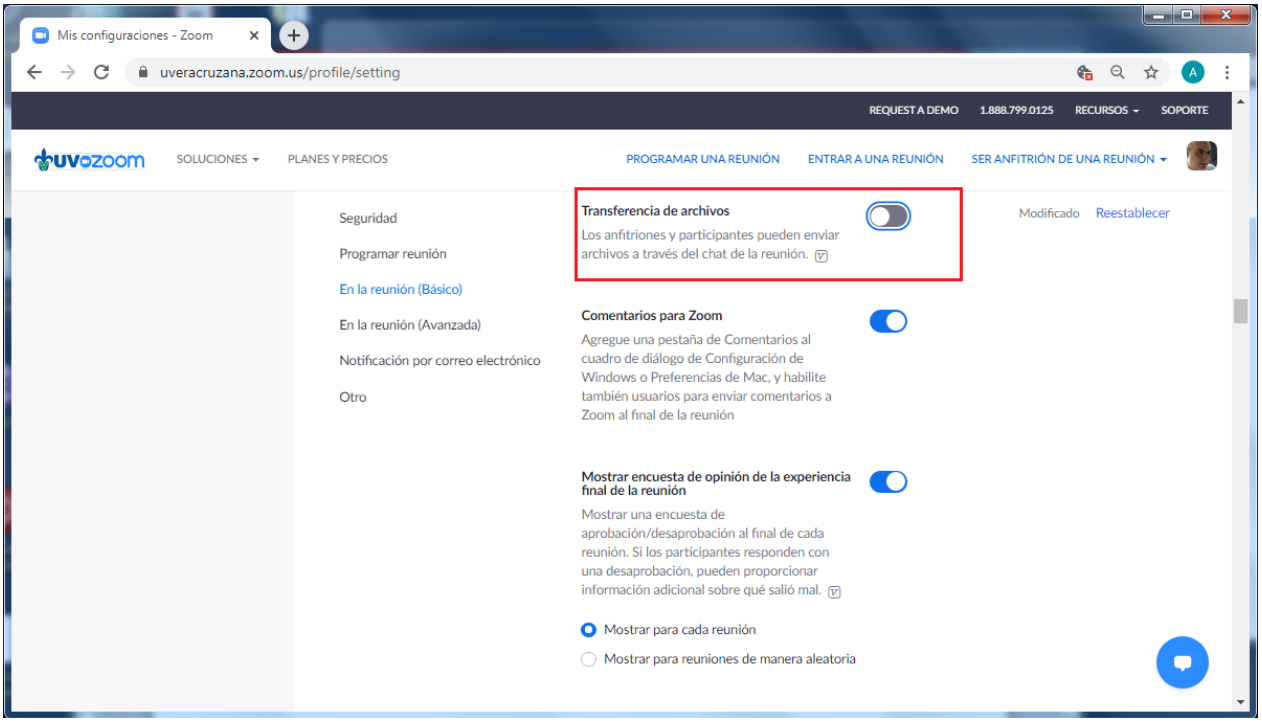
Cuando los usuarios ingresen a la reunión, incluso los invitados, deberán aguardar a que Ud. como anfitrión, les autorice el acceso a la sala virtual.

5. Restrinja quién puede compartir presentaciones y archivos

En su panel de configuración de su reunión, Ud. puede indicar que sólo el anfitrión pueda compartir contenidos, esto como precaución adicional para evitar que aparezcan en pantalla contenidos no autorizados.



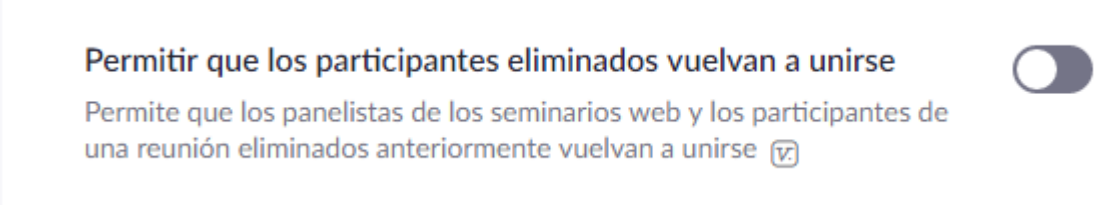
Como precaución adicional, Ud. puede evitar que los participantes compartan archivos a través del chat. Para ello, deshabilite la opción de "Transferencia de archivos" en su panel de configuración de la reunión:



Esto evitará que usuarios envíen archivos animados u otros contenidos que podrían ser distractores.

6. Administre a los participantes

Como organizador de la reunión, Ud. tiene varios recursos para administrar a los participantes. Ud. puede, desde la interfaz de su reunión, "apagar" el video de la cámara de sus participantes, "mutear" (cancelar el audio de) los micrófonos remotos, e incluso, en el caso de un participante invitado pero indeseable, sacarlo de la reunión (colgar su llamada). Si la opción de "permitir que los participantes eliminados vuelvan a unirse" está deshabilitada, aquellos participantes que Ud. retire de la reunión no podrán volver a ingresar.



No tratamos aquí de que Ud. emplee **todas** estas recomendaciones en la misma reunión. Más bien, la idea es contribuir a que tenga Ud. los elementos necesarios para asegurar sus reuniones y por ende, brindar mayores garantías de seguridad y confiabilidad a sus invitados para su trabajo.

Recuerde Ud. que la plataforma de Zoom de la Universidad Veracruzana está licenciada, es decir, se tiene un soporte por parte del proveedor del servicio, que permite a la UV solicitar y dar respuesta a incidentes que pudiesen detectarse.

En caso de dudas o dificultades que Ud. experimente o haya experimentado, no dude en establecer comunicación con el Departamento de Videoconferencias, a través del correo electrónico videoconferencias@uv.mx, donde se le brindará soporte para la utilización de la plataforma de videoconferencias.

Adicionalmente, ponemos a su disposición la sección de Guías Rápidas que podrá localizar en el sitio web https://www.uv.mx/video

©Dirección General de Tecnología de Información. Fecha de revisión: Febrero 19, 2021