



# Guía para resguardar la clase virtual en Webex Meeting: Previene el Zoombombing



Centro de Enseñanza y Aprendizaje  
Escuelas de Pregrado  
Facultad de Economía y Negocios  
Universidad de Chile

# GUÍA PARA RESGUARDAR LA CLASE VIRTUAL EN WEBEX MEETING: PREVINIENDO EL ZOOMBOMBING

## PRESENTACIÓN

El modelo de educación online de la Facultad de Economía y Negocios de la Universidad de Chile, invita a abordar algunos desafíos que enfrentan los/as docentes en este nuevo contexto. Uno de ellos tiene que ver con el cuidado de las interacciones en una instancia sincrónica, como una videoconferencia, y cómo se evitan las intervenciones por parte de los/as estudiantes, que tienen como fin interrumpir o "trolea"<sup>1</sup> el desarrollo de la clase. Este fenómeno es el que se denomina Zoombombing.

A continuación, se explica más en detalle qué es el Zoombombing, cómo prevenirlo al utilizar Webex Meeting y otras acciones para su prevención.

## I. ¿Qué es el Zoombombing?

Desde el aumento explosivo de las clases virtuales, ha surgido una nueva forma de trolea una clase en línea. En ella un/a participante usa la función de compartir pantalla o audio, para interrumpir reuniones y clases. El término Zoombombing proviene del nombre de la aplicación de videoconferencia "Zoom" y "bombing" o "bombardeo".

---

<sup>1</sup> Viene de la palabra "trol", utilizada en la jerga de internet, para referirse a una persona que publica mensajes que pueden ser provocadores, molestos o irrelevantes para el tema que se está tratando en un determinado espacio online (blog, chat, foro, etc.). Estos mensajes tienen como fin generar respuestas por parte de los/as otros/as personas, logrando que se enfrenten entre sí o que se enojen por el contenido expuesto en los mensajes.

## II. ¿Cómo configurar y realizar una reunión en Webex para prevenir el Zoombombing?

Para prevenir el Zoombombing, debe revisar estas 5 acciones en la configuración de su sala cada vez que ingrese a ésta:

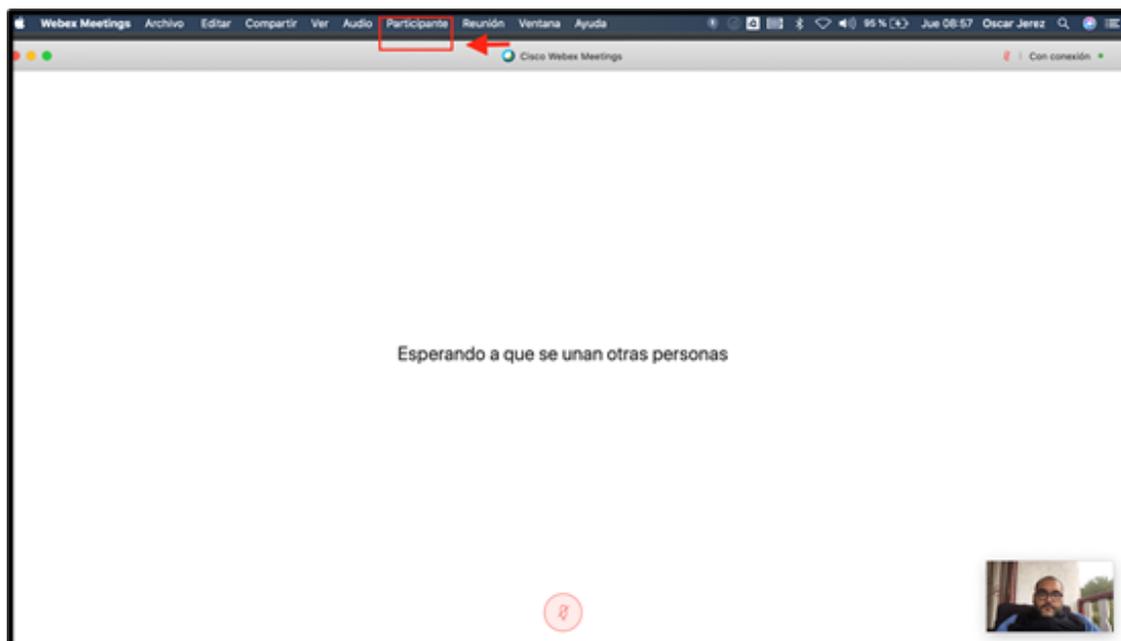
1. Bloquear la opción "Cualquiera puede compartir"
2. Activar las opciones "Silencio al entrar" o "Silenciar todo"
3. Activar la opción de comunicarse sólo de forma pública con "Todo el mundo"
4. Desactivar las opciones de reunión donde pueden "Compartir documentos" o "Controlar aplicaciones compartidas, explorador Webex o pantalla en ordenador remoto"
5. Expulsar a un/a participante de la sala y bloquear su ingreso

A continuación se explica paso a paso cómo realizar cada una de estas acciones.

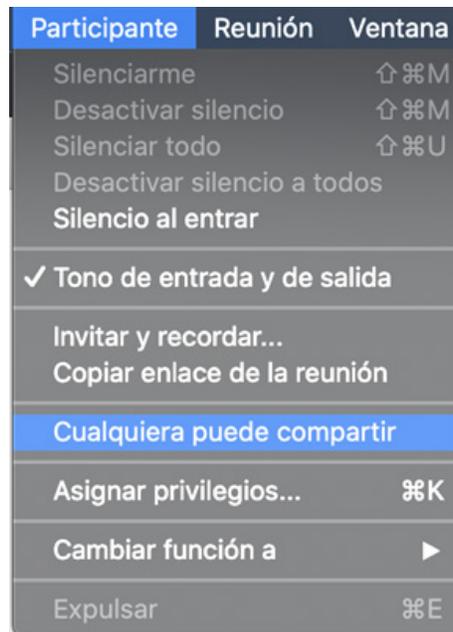
### 1. Bloquear la opción "Cualquiera puede compartir"

Para ello, realice lo siguiente:

a) Entre a la reunión con anterioridad. En el menú de arriba, seleccione la opción "**Participante**"



b) Estando en "Participante", desactive la opción **"Cualquiera puede compartir"**, haciendo un clic sobre el menú. La eliminación del ticket correspondiente, deshabilitará la posibilidad de que los/as estudiantes puedan compartir, sin su permiso, algún tipo de contenido no deseado, que termine interrumpiendo la clase.



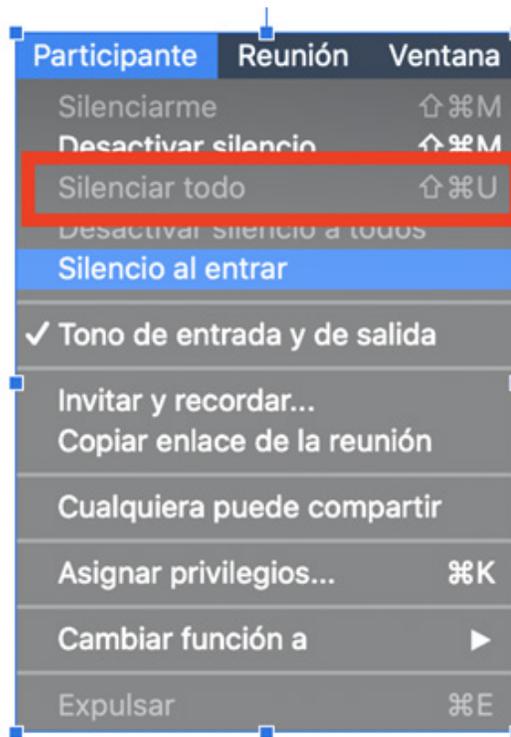
## 2.Activar las opciones **"Silencio al entrar"** o **"Silenciar todo"**

Para ello realice lo siguiente:

a) En el mismo menú "Participante", active **"Silencio al entrar"**. Con ello se asegura que los/as estudiantes al entrar a la sala, entren silenciados/as. Sin embargo, el/a estudiante puede volver a activar su micrófono.



b) Si los/as estudiantes activan su micrófono, la acción más rápida en ese mismo menú es que active la opción **"Silenciar Todo"**, apagando todos los micrófonos de los asistentes.



**IMPORTANTE:** Revise en su sistema operativo cuál es la opción de teclas más eficiente para realizar esta opción de la manera más rápida posible. Acostúmbrese a cada cierto tiempo "Silenciar Todo", para evitar cualquier situación no deseada.

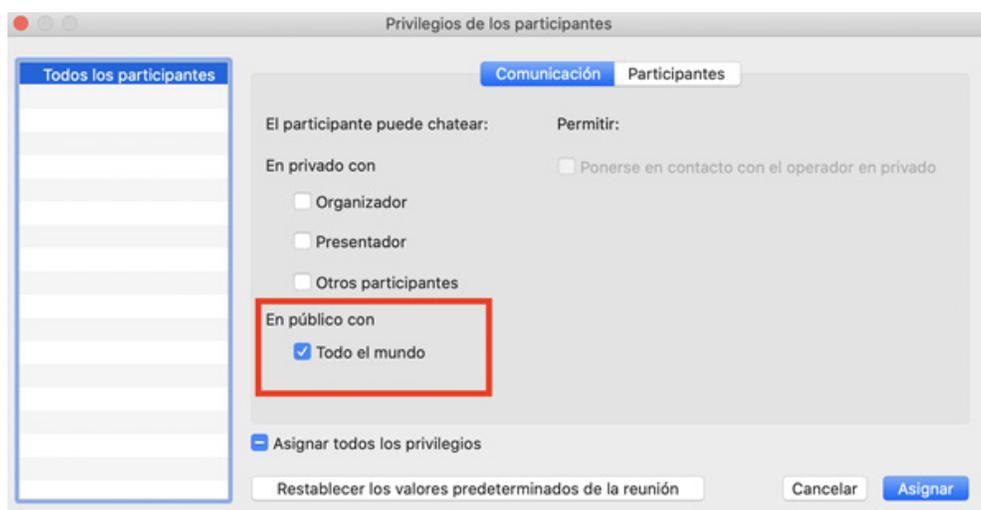
### 3. Activar la opción de comunicarse sólo de forma pública con “Todo el mundo”

Para ello realice lo siguiente:

a) En el mismo menú “Participante” elija la opción **“Asignar Privilegios”**



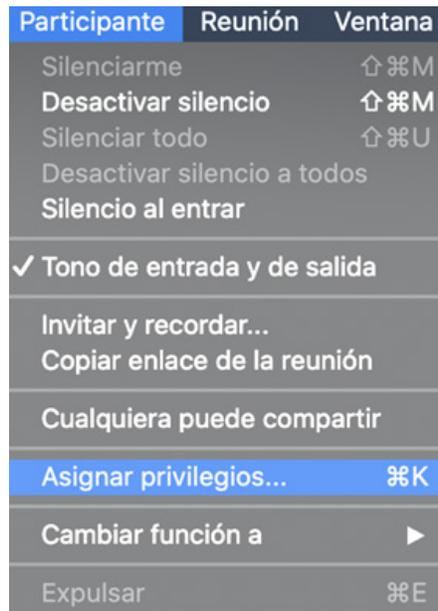
b) En el menú **“Comunicación”** vaya a la subsección “En público con” y seleccione la opción **“Todo el mundo”**, esto permitirá que los/as estudiantes puedan chatear solo de forma pública, es decir que no puedan chatear en privado entre ellos ni con usted. Lo anterior, para evitar la saturación de mensajes privados.



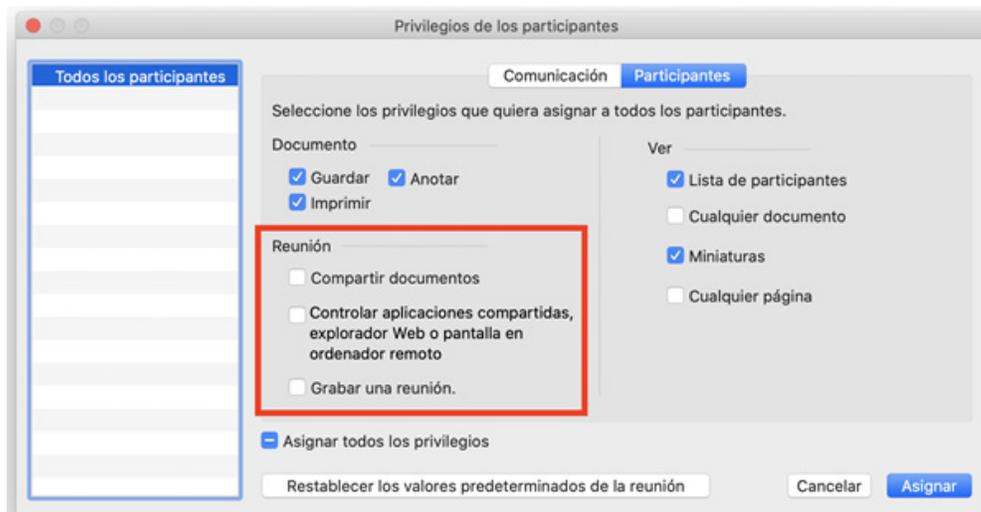
#### 4. Desactivar las opciones de reunión donde pueden “Compartir documentos” o “Controlar aplicaciones compartidas, explorador Webex en pantalla en ordenador remoto”

Para ello realice lo siguiente:

a) En el menú “Participante” elija la opción **“Asignar Privilegios”**



b) En la opción **“Participantes”** encontrará el grupo de opciones **“Reunión”**, identificado en el cuadro rojo de la siguiente imagen. Desmarque las opciones **“Compartir documentos”** y **“Controlar aplicaciones compartidas, explorador Web o pantalla en ordenador remoto”**. Con esto evitará cualquier mal uso de sus aplicaciones. Luego haga clic en **“Asignar”**

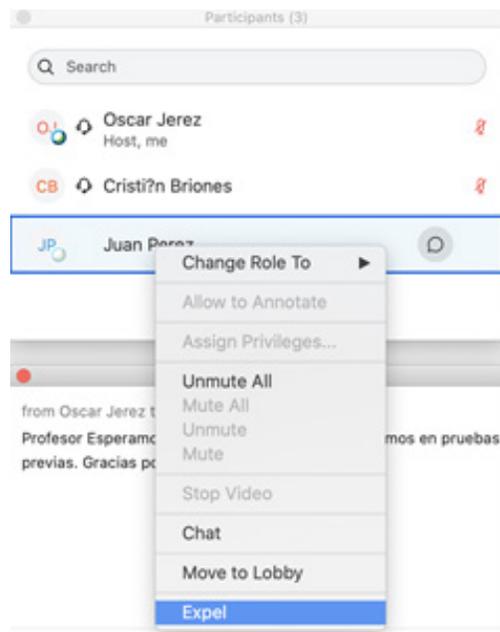


## 5. Expulsar a un/a participante de la sala y bloquear su ingreso

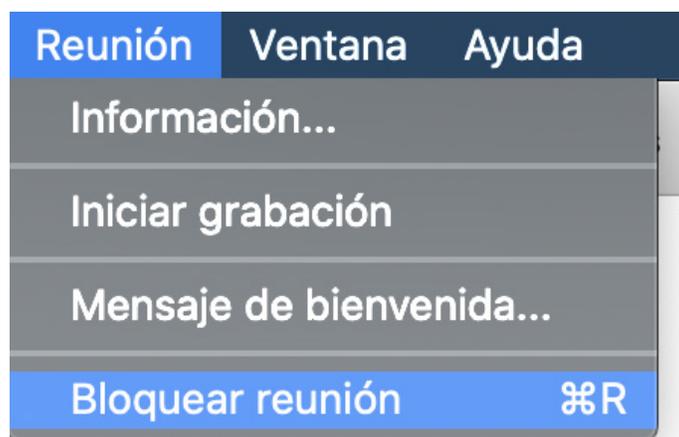
Si un/a participante de la reunión no comprende la dinámica y/o reglas de la clase virtual, usted puede expulsarlo/a de su sala y bloquear el ingreso.

Para ello realice lo siguiente:

a) En el menú desplegado de **“Participantes”** al costado derecho de su pantalla, ubique el nombre del/la participante y haga clic con el botón derecho del mouse. Luego seleccione la opción **“Expulsar”**



b) Enseguida, vaya al menú principal y seleccione la pestaña de “Reunión”. Active la opción “Bloquear reunión”. Con ello, nadie podrá entrar nuevamente si usted no lo/a acepta de manera individual.



### III. ¿Qué otras acciones puedo llevar a cabo como docente para prevenir el Zoombombing?

Además de tener los resguardos de configurar su sala de modo adecuado, se recomienda lo siguiente:

1. Establezca un encuadre o "setting" de trabajo con sus estudiantes al inicio de la clase, por lo menos las primeras semanas. Este encuadre debe orientar a los/as estudiantes respecto de lo que está y lo que no está permitido hacer durante el desarrollo de la clase y por qué.
2. Sea claro/a al indicarles cómo espera que participen de la clase, tanto en el modo de comunicarse como en las funciones de la plataforma Webex que podrán utilizar para ello.
3. Informe a sus estudiantes respecto de las medidas de resguardo que configuró en su sala, de modo que no se extrañen de las funciones que tienen deshabilitadas.
4. Recuerde constantemente a sus estudiantes que un aula virtual exige el mismo nivel de formalidad y respeto que un aula presencial y que un buen desarrollo de la clase depende de la colaboración de todos/as.

Recuerde que cualquier consulta que tenga respecto a este proceso, puede consultar directamente al Centro de Enseñanza y Aprendizaje, a través de su correo electrónico: [\*\*cea@fen.uchile.cl\*\*](mailto:cea@fen.uchile.cl), un/a profesional le responderá a la brevedad.

