

# Recomendaciones de seguridad de Zoom y configuraciones básicas



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

Zoom es una herramienta esencial para realizar reuniones virtuales, clases y conferencias de forma eficiente. Este instructivo está diseñado para ayudar a los usuarios de REUNA a configurar y utilizar Zoom de manera segura, asegurando la protección de las reuniones y el cumplimiento de las mejores prácticas. A continuación, encontrarás recomendaciones clave de seguridad y configuraciones básicas para optimizar tu experiencia en la plataforma.

En este instructivo podrás ver directamente haciendo clic:

- [Recomendaciones Generales](#)
- [Configuración básica de Zoom](#)
- [Recomendaciones de seguridad para reuniones](#)
- [¿Qué es el Zoombing? y consejos adicionales](#)

# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

### RECOMENDACIONES GENERALES

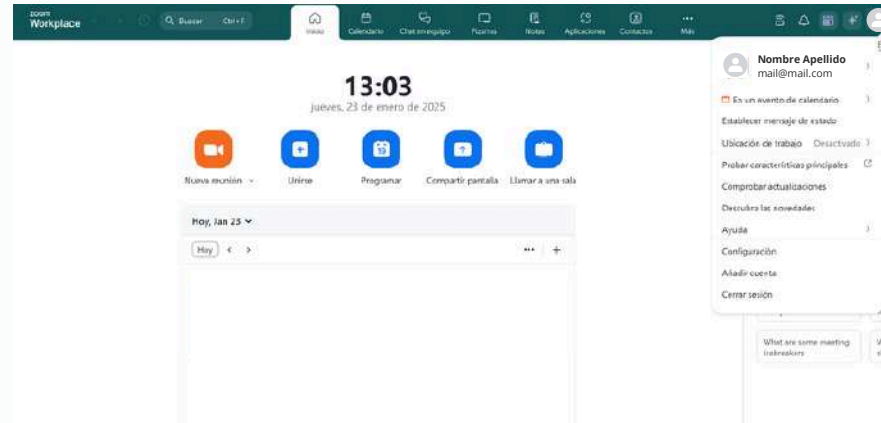
- Mantén tu versión de Zoom **siempre actualizada por canales formales:** Esto te permitirá **corregir posibles errores de seguridad y acceder a las últimas herramientas disponibles de la aplicación.**
- Para actualizar tu aplicación de escritorio debes ir a <https://plaza.reuna.cl/> > **Ir a Zoom**, donde aparecerá un pop up que te dará la opción de ir a la última versión de esta herramienta y la puedas actualizar.



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

- Si quieres realizar la actualización desde la app de Zoom, debes ir a tu foto de perfil y en el menú ir a “comprobar actualizaciones”.



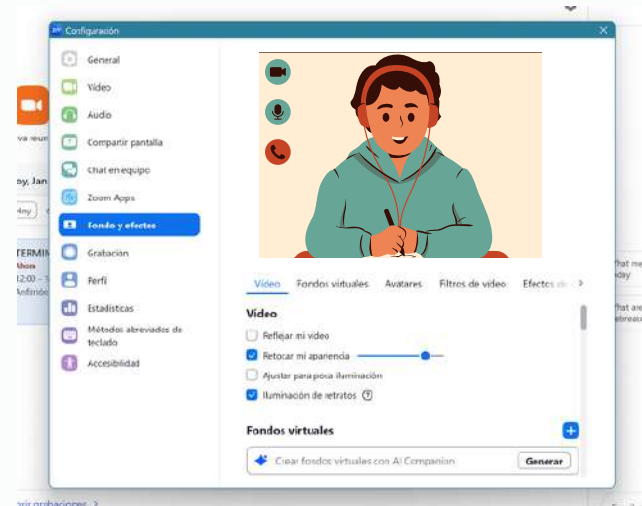
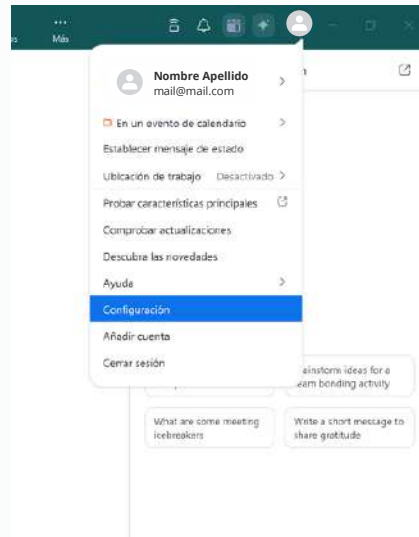
- **No utilices tu ID personal de reunión o sala de reunión personal:** Crea siempre ID aleatorios y no los uses más de una vez.
- **Crea una clave para proteger tu reunión:** Comparte esta clave sólo con los participantes que esperas y no públicamente.
- **No publiques el enlace a tus reuniones en redes sociales:** Comparte esta información por correo electrónico, sólo con los interesados.

# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

### CONFIGURACIONES BÁSICAS DE ZOOM

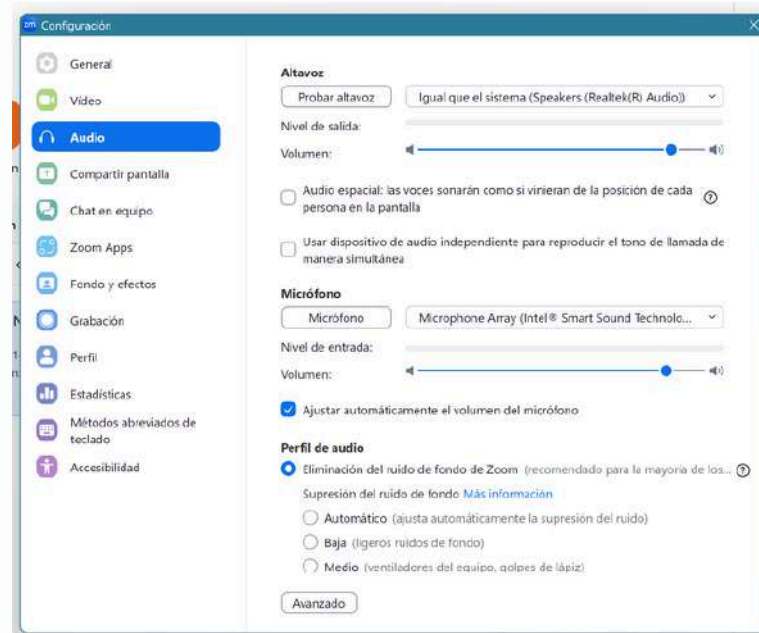
- **Configurar tu perfil:** Personaliza tu perfil con tu nombre y foto. Accede al menú de perfil desde la esquina superior derecha de la aplicación. Aquí en el mismo menú desplegable en: configuración > fondos y efectos, tendrás opciones como: retocar tu apariencia, difuminar el fondo, cambiar el fondo de tu avatar, entre otras utilidades.



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

- **Prueba audio y video:** Antes de unirte a una reunión, prueba tu micrófono y cámara. Ve a "Configuración" > "Audio" y "Video". En esta opción podrás personalizar elementos como el volumen del micrófono, ruido y otras opciones para tus reuniones.

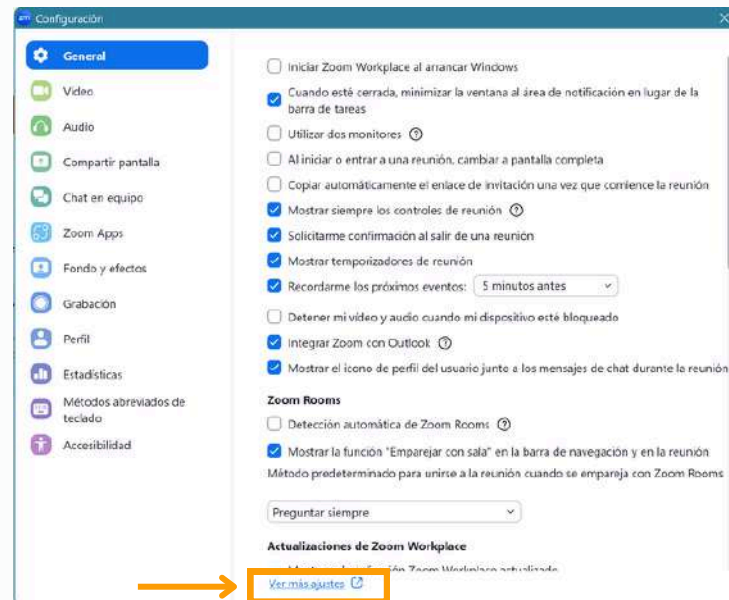


# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

### RECOMENDACIONES DE SEGURIDAD PARA REUNIONES

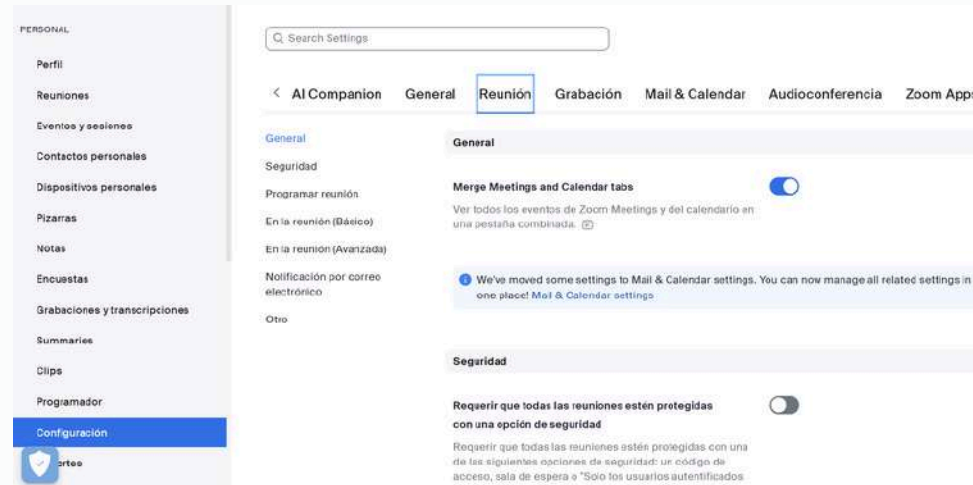
- **Configuración de tus reuniones:** Hay una opción en Zoom para configurar tus reuniones y hacerlas más seguras. Para ello debes ir a: **Tu perfil > Configuraciones > ver más ajustes**. Con esto se desplegará una ventana de configuraciones avanzadas



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

- En la nueva página debes seleccionar en el menú izquierdo configuraciones, y en el menú superior donde dice “Reunión”



- Aquí tendrás una serie de herramientas que puedes habilitar o deshabilitar según tus preferencias, pero en temas de seguridad te sugerimos:



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

- **Utilizar Sala de Espera:** Habilita la sala de espera para verificar a los participantes antes de permitirles ingresar. Aunque tu reunión esté iniciada, quienes vayan ingresando quedan en “espera” hasta tu autorización de ingreso. Así te aseguras quienes ingresan a tu reunión de manera segura.
- **Solicita inscripción obligatoria:** Puedes pedir a los asistentes que se inscriban previamente para acceder al enlace, y además puedes llevar registro de los inscritos, y aceptarlos de forma manual o automática.

*Válido solo para cuentas adscritas a REUNA con cuenta licenciada.*

The image shows two screenshots from the Zoom web interface. The top screenshot displays the 'Seguridad' (Security) settings for a meeting, where the 'Sala de espera' (Waiting Room) toggle is turned on. Below this, the 'Opciones de sala de espera' (Waiting Room Options) are listed, all of which are checked: 'Todos irá a la sala de espera' (Everyone goes to the waiting room), 'Las personas en la sala de espera se clasifican según orden para unirse' (People in the waiting room are ranked by order to join), and 'No permitir que el anfitrión añada un logotipo personalizado' (Do not allow the host to add a custom logo). The bottom screenshot shows the 'PERSONAL' settings sidebar with 'Reuniones' (Meetings) selected. In the main area, the 'Inscripción' (Registration) option is highlighted with an orange box, and the 'Obligatorio' (Required) checkbox is checked. Other visible settings include the meeting topic, date, time, duration, and time zone.

# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

- Puedes silenciar a los participantes y restringir su cámara al momento de ingresar, configurando los ajuste de tus reuniones.
- También puedes evitar que activen su micrófono durante la reunión, para lo cual debes ir al cuadro de Participantes, hacer clic en la opción "Más" y desmarcar la opción "Permitir que los participantes cancelen silenciar ellos mismos".
- Limita el envío de archivos por chat y chat privados y el uso de pantalla compartida en la configuración de ajustes de tu reunión.
- Deshabilita la opción "permitir que los participantes eliminados se vuelvan a unir a la reunión".



# RECOMENDACIONES DE SEGURIDAD DE ZOOM Y CONFIGURACIONES BÁSICAS

## EVITA EL ZOOMBOMBING

### ¿QUÉ ES EL ZOOMBOMBING?

El Zoombombing es un tipo de interrupción no deseada que ocurre en reuniones virtuales o videollamadas, especialmente en plataformas como Zoom. Durante el Zoombombing, personas no autorizadas acceden a una reunión y suelen interrumpirla con comportamientos inapropiados, como compartir contenido ofensivo, pornográfico, racista, o simplemente causando caos.


### CONSEJOS ADICIONALES


- **Desactiva la posibilidad de que los participantes compartan pantalla:** Sólo a menos que sea necesario. Durante la reunión, ve a "Seguridad" y desactiva "Compartir pantalla para los participantes".
- **Grabar reuniones de forma segura:** Si es necesario grabar, informa previamente a los participantes y almacena las grabaciones en ubicaciones seguras.
- **Cierre seguro de reuniones:** Al finalizar, asegúrate de que el anfitrión cierre la reunión correctamente.

## Datos de contacto

En caso de requerir asistencia, puedes contactarnos en:

 [servicios@reuna.cl](mailto:servicios@reuna.cl)

 Tel. +562 2 337 0382 horario de  
lunes a jueves, de 8:30 a 18:00 hrs.  
Viernes de 8:30 a 13:00 hrs.

 Whatsapp +56995384515

## Sitios de interés

Para mayor información, puedes recurrir a:

- <https://plaza.reuna.cl/instructivos/>
- <https://plaza.reuna.cl/videoconferencia/#preguntas-frecuentes>
- <https://plaza.reuna.cl/webinar/#preguntas-frecuentes>
- <https://support.zoom.us/hc/es>
- <https://www.reuna.cl/>

**ROUNA**  
Ciencia y Educación en Red

