

EDUCACIÓN EN LÍNEA/udp

Recomendaciones para un Uso seguro de Zoom

- RECOMENDACIONES EN RELACIÓN A MECANISMOS DE PROTECCIÓN ELABORADAS EN CONJUNTO CON LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.
- CONFIGURACIÓN SEGURA DE ZOOM EN CANVAS.
- USO SEGURO DE ZOOM EN CLASES ACTIVAS.
- SUGERENCIAS ADICIONALES DE SEGURIDAD DESDE PÁGINA ZOOM. US

MacBook

Ante la información relativa a la vulnerabilidad de la herramienta Zoom ligada a los cursos impartidos a través de la plataforma CANVAS, y la inquietud de docentes y estudiantes por la seguridad de reuniones y clases en línea programadas con su uso, le hacemos llegar una serie de recomendaciones para su uso seguro a través de un instructivo.

En éste encontrará:

- A. Recomendaciones en relación a mecanismos de protección elaboradas en conjunto con la Dirección de Tecnologías de la Información.
- B. Configuración segura de Zoom en CANVAS.
- C. Uso seguro de Zoom en clases activas.
- D. Sugerencias adicionales de seguridad desde página Zoom. US

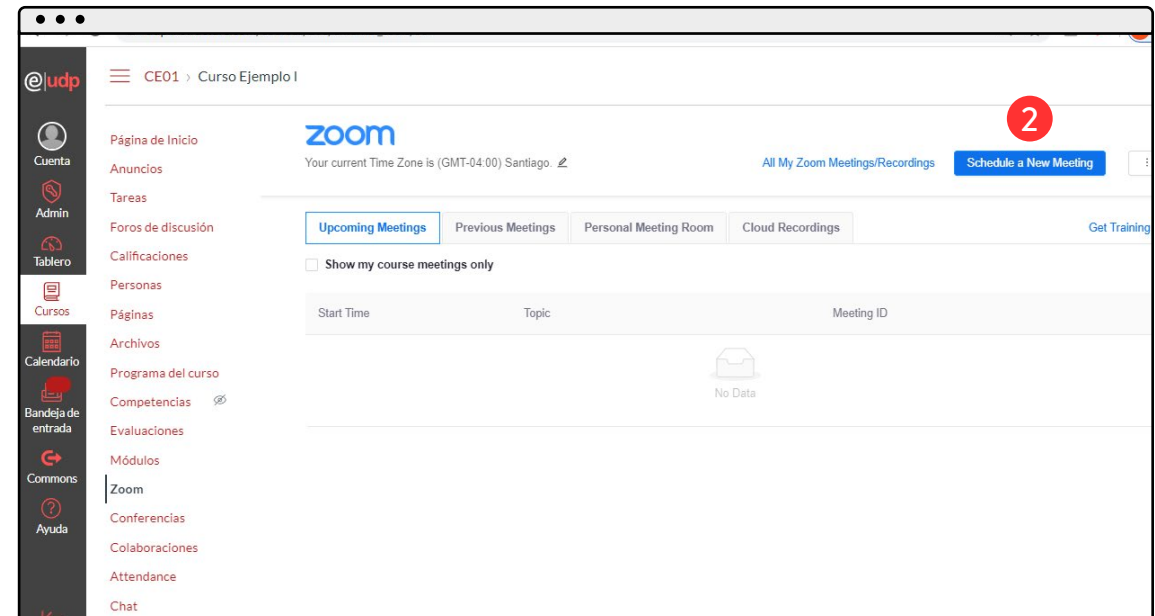
A. Recomendaciones en relación a mecanismos de protección:

- Actualización de Seguridad: Se aconseja revisar que su sistema operativo Windows y Mac. Para Windows puede hacerlo en el siguiente link **<https://support.microsoft.com/es-es/help/15081/windows-turn-on-automatic-app-update>**
- Actualizar versión de Zoom: Es necesario mantener la aplicación actualizado en su última versión, puede revisar el siguiente tutorial haciendo clic en descargar en el enlace **<https://zoom.us>** o directamente desde uno de los siguientes links:
<https://zoom.us/support/download>
<https://zoom.us/download>
<https://zoom.us/download2>
- iOS y Android: Zoom usa notificación móvil cada vez que hay una nueva actualización. Puede hacer clic en AppStore para actualizar y en Android puede descargar la última versión desde Google Play.
- Restringir uso de Zoom a clases: EL uso de herramientas de conversaciones es por lo general en la nube y en línea. Se sugiere no utilizar Zoom para estos efectos, privilegiando el uso de Microsoft Teams, Hangouts, WhatsApp, Facetime, Facebook.

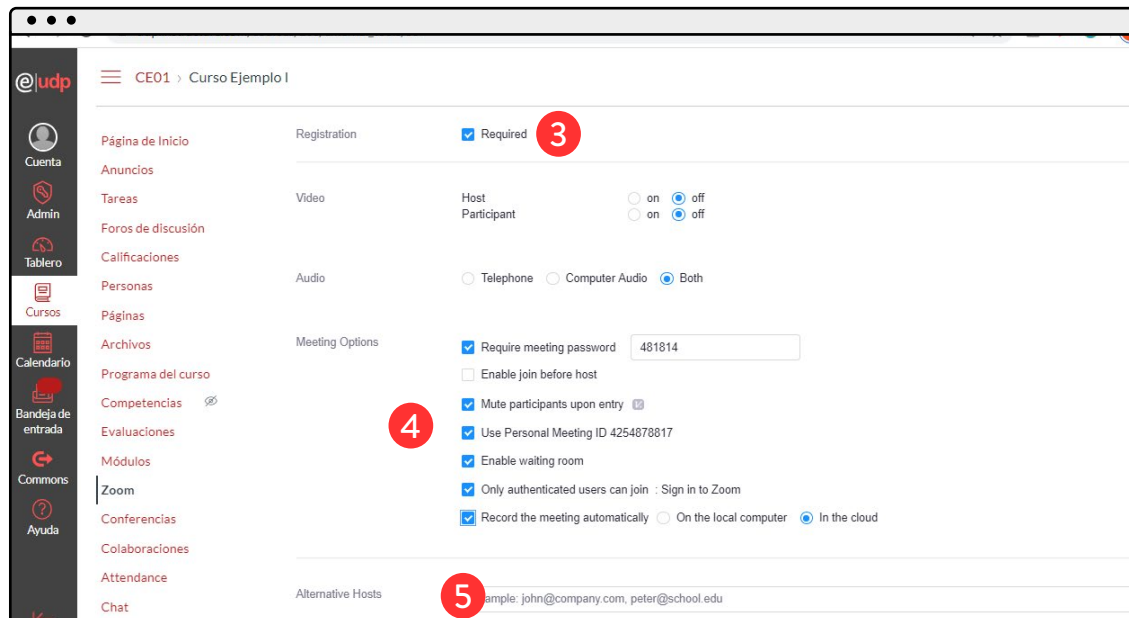
B. Configuración segura de Zoom en CANVAS.



1 Siempre entre a Zoom desde su Aula Virtual en CANVAS

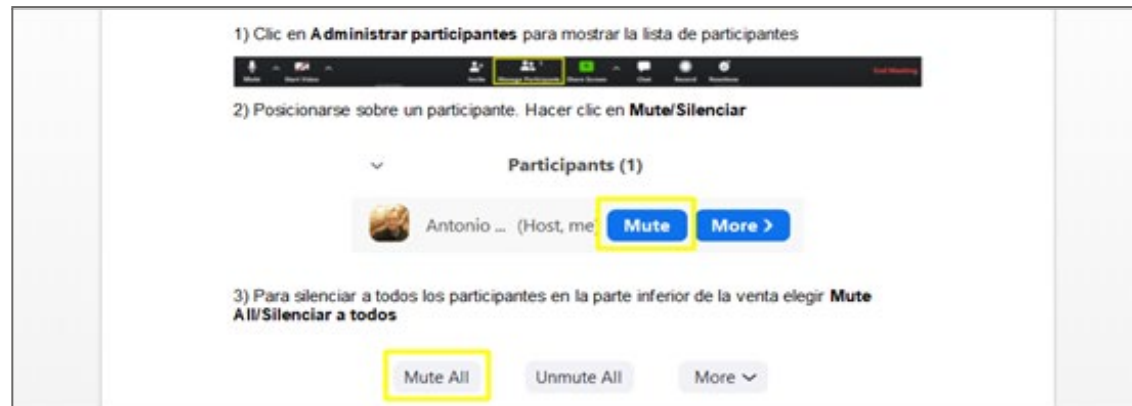


2 Seleccione la opción PROGRAMAR UNA NUEVA REUNIÓN (Schedule a New Meeting)



- 3 Seleccione la opción que indica que sólo pueden unirse usuarios registrados (Registration Required)
- 4 Seleccione las siguientes opciones para la clase (Meeting Options): A. REQUIERE CONTRASEÑA DE REUNIÓN (Require meeting password); B. SILENCIAR PARTICIPANTES AL ENTRAR (Mute participants upon entry), C. USAR EL ID PERSONAL DE REUNIÓN: (Use Personal Meeting ID); D. HABILITAR SALA DE ESPERA (Enable Waiting Room), los participantes tienen que esperar hasta que el anfitrión los admite en la reunión; E. SÓLO USUARIOS AUTENTICADOS EN ZOOM PUEDEN UNIRSE (Only authenticated users can join Sign to Zoom), F. GRABAR LA REUNIÓN AUTOMÁTICAMENTE (Record the meeting automatically), así dejará grabada la clase y las interacciones que se produzcan, se sugiere notificar a los estudiantes antes de habilitar la grabación. Puede grabar en su computador para o en la nube. Aunque es más seguro guardarlo en el computador, desde la nube también puede descargarlo, editarlo y luego subirlo a Canvas.
- 5 Deshabilita la opción de anfitriones alternativos (Alternative Hosts): solo el docente controla las acciones en este espacio virtual.

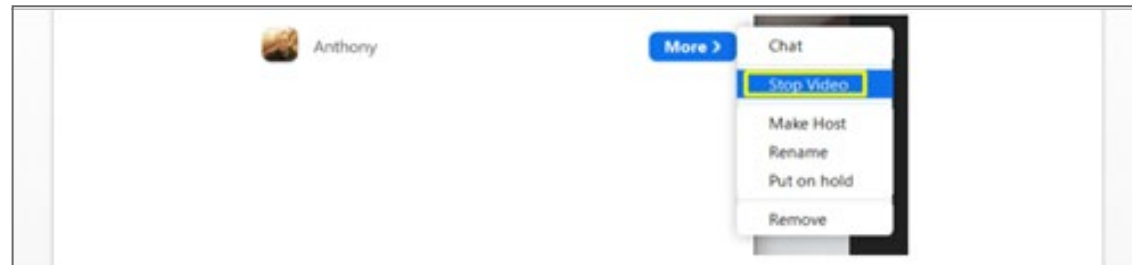
C. Uso seguro de Zoom en clases activas:



Durante la realización de la clase Usted puede silenciar a los participantes



Eliminar participantes

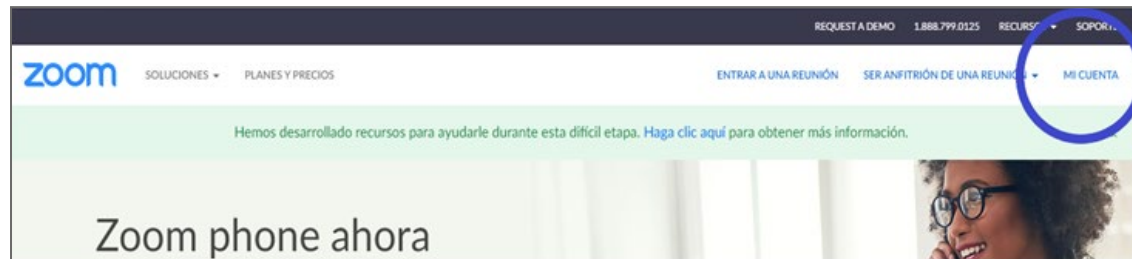


Detener el video de los participantes

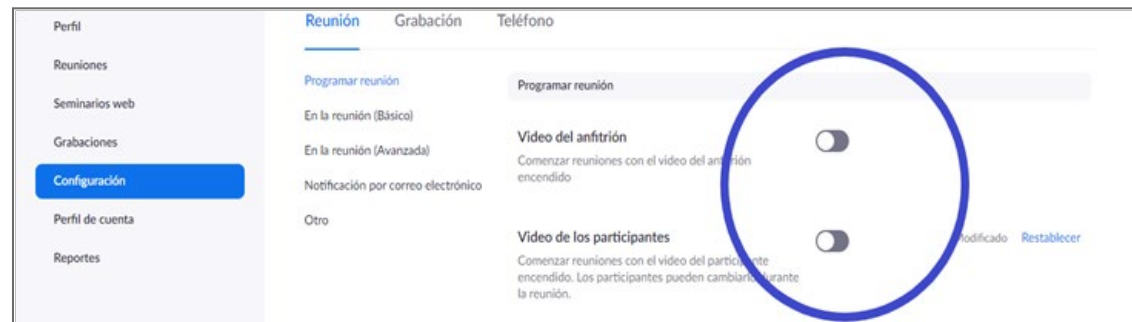


Bloquear el acceso a una clase una vez todos los participantes invitados estén en ella

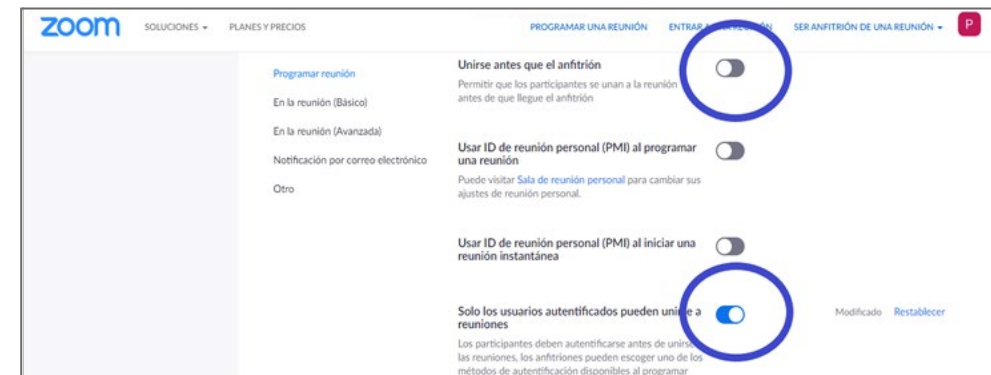
D. Sugerencias adicionales de seguridad desde página Zoom. US



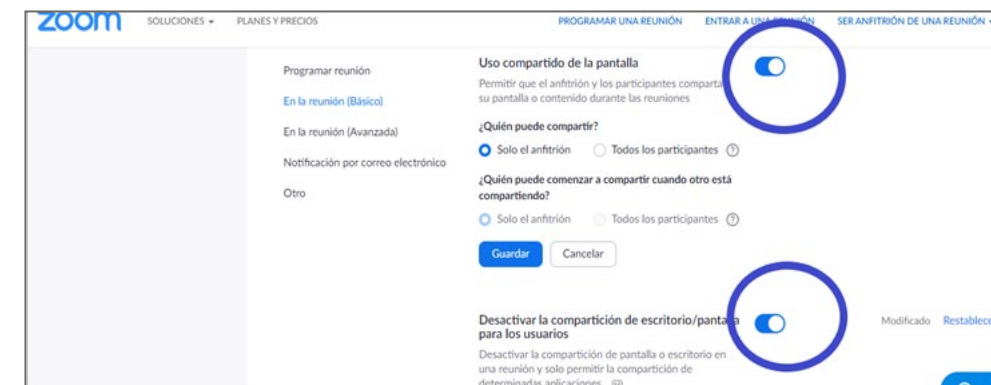
En **www.zoom.us**, pinche “mi cuenta” y entre utilizando tu usuario institucional. Los cambios que haga en esta página, se reflejarán en su Aula virtual en CANVAS.



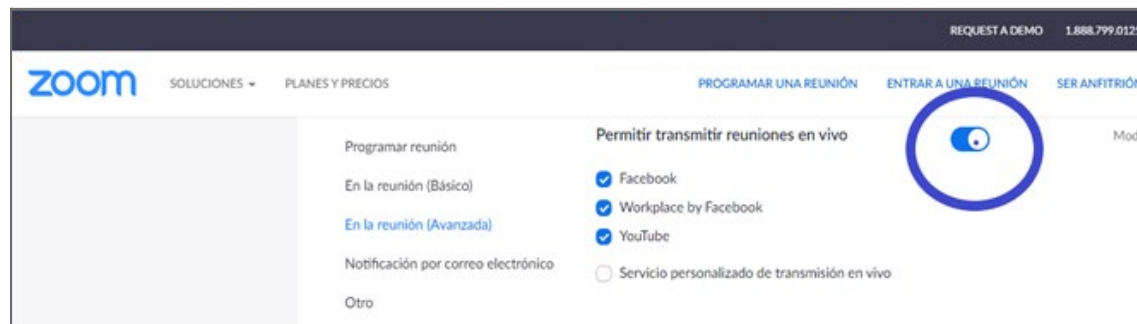
En configuración de la cuenta verá una serie de opciones para incrementar la seguridad y tomar control de Zoom. Las opciones que configure en PROGRAMAR REUNIÓN serán comunes en todas sus clases. Se sugiere inhabilitar la opción de entrar con video prendido.



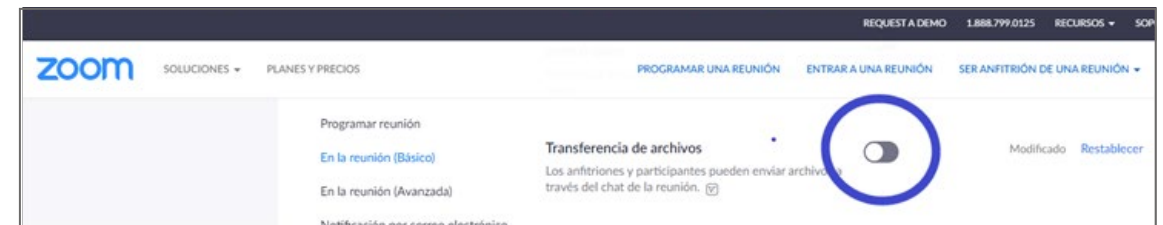
Se sugiere dejar inhabilitado que alguien se una antes que el anfitrión y que sólo los usuarios autenticados puedan hacerlo



-La opción **Uso compartido de la pantalla**, permite que sólo el anfitrión comparta su pantalla o contenido y los estudiantes puedan compartir sólo determinadas aplicaciones



Deshabilitar la opción de permitir a un usuario transmitir por Facebook, Workplace by Facebook, YouTube una reunión en vivo



Deshabilitar la opción de transferencias de archivos durante las reuniones