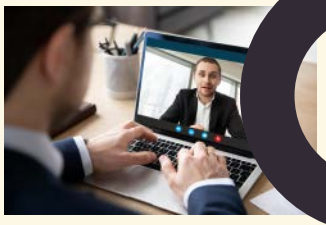
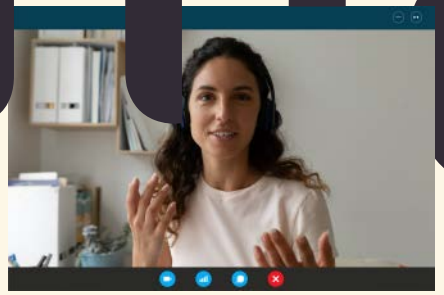
Ministerio del Interior y Seguridad Pública

CONSEJOS DE CIBERSEGURIDAD PARA EL ADMINISTRADOR DE ZOOM





CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ministerio del Interior y Seguridad Pública

PROTEJA SUS REUNIONES,SUS DATOS Y SU PRIVACIDAD

Hace rato quedó claro que el trabajo mantendrá una cuota, quizás incluso creciente, de labores remotas. Y para la coordinación de actividades, es esencial realizar reuniones virtuales, siendo la plataforma más popular para ello Zoom. Por eso queremos entregarte las siguientes recomendaciones para hacer más seguras las reuniones que administres en este programa.

Consejo 1
Habilite la función de sala de espera

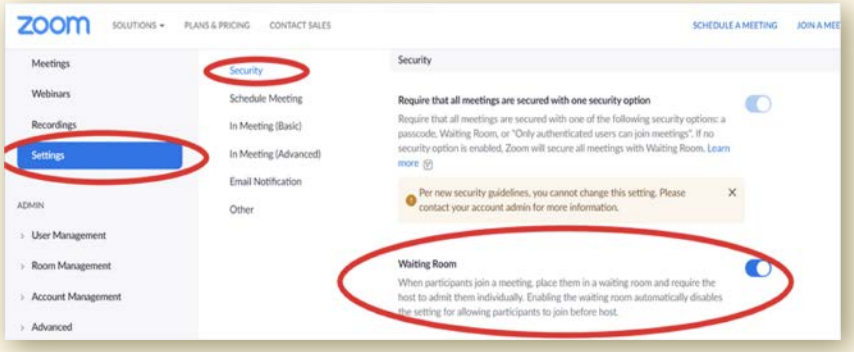
Esta función de seguridad de Zoom brinda a los anfitriones el poder de permitir que solo participantes de confianza entren en sus reuniones. Para configurar la función de sala de espera de forma predeterminada para todas sus reuniones futuras.

Haga clic en **MI CUENTA** en el menú superior del lado derecho

ⓐ Presione Configuración en la barra de navegación de la barra lateral izquierda

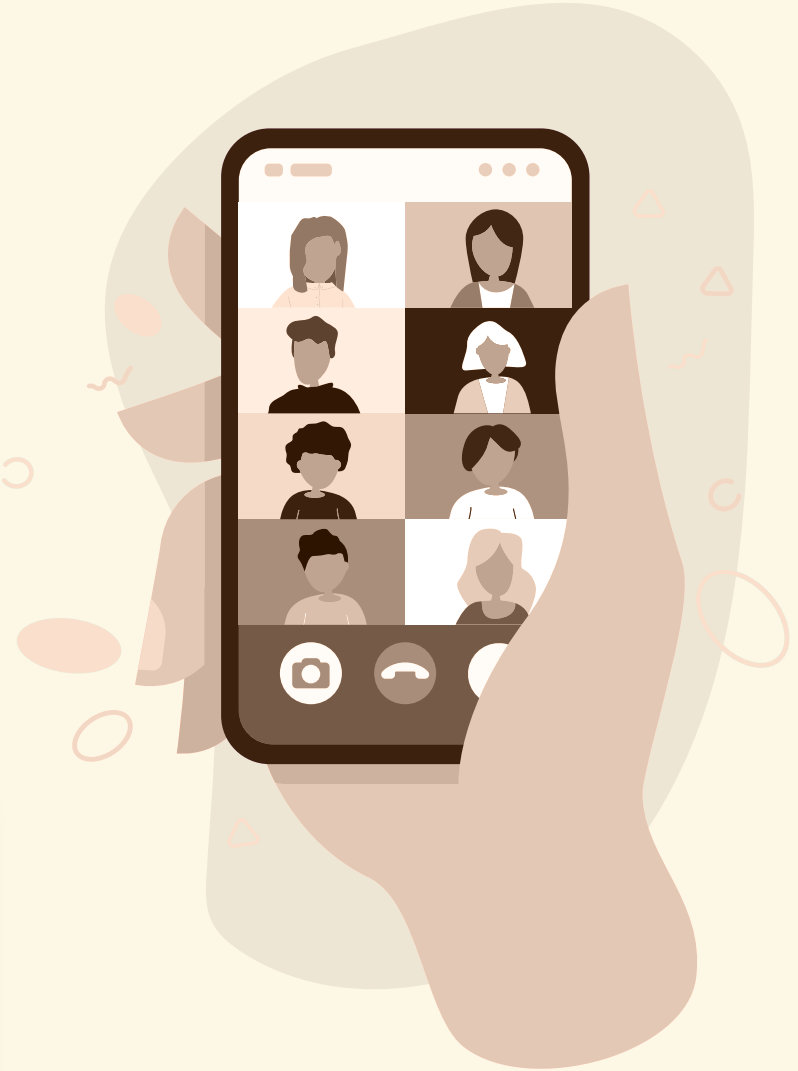
ⓑ Seleccione Seguridad

ⓒ Habilite la sala de espera



Consejo 2
Solicite un código de acceso o un enlace para unirse

Un ID de reunión personal es un número de 10 dígitos que puede compartir con sus participantes. De forma predeterminada, Zoom crea un código de acceso alfanumérico de seis dígitos para cada reunión de Zoom. Sin embargo, puede fortalecerlo o cambiar el código de acceso en la configuración de seguridad de Zoom siguiendo las instrucciones a continuación:



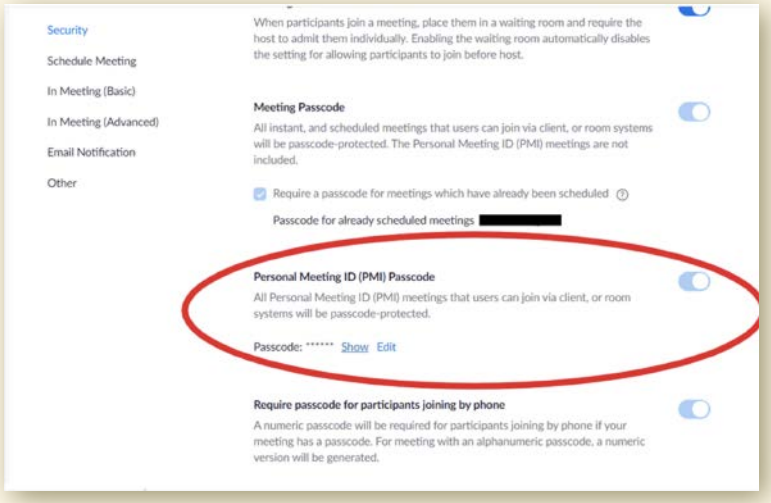
a. Abra Zoom.us en su navegador e inicie sesión

b. Haga clic en MI CUENTA en el menú superior del lado derecho

c. Seleccione Seguridad

d. Busque el código de acceso de la identificación personal de la reunión

e. Haga clic en Editar para hacer un código de acceso más fuerte agregando más letras, números y caracteres especiales



Ministerio del Interior y Seguridad Pública

Consejo 3
Evite la incrustación de código en la url de la invitación

Enviar enlaces de reuniones es una forma insegura de organizar una reunión. Eso es porque la URL de la reunión predeterminada tiene códigos de acceso incrustados. Esto significa que cualquier persona con esta URL puede unirse directamente a la reunión sin conocer el código de acceso. Sin embargo, ahora puede deshabilitar esta configuración y hacer que sea obligatorio que todos los participantes ingresen el código de acceso.

PARA DESHABILITAR
la incrustación del código de acceso en la URL

ⓐ Abra Zoom.us en su navegador e inicie sesión.

ⓑ Luego, haga clic en MI CUENTA en el menú superior del lado derecho.

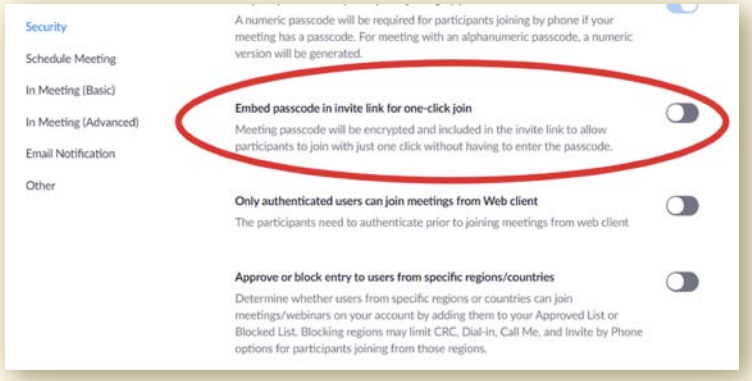
ⓒ Haga clic en Configuración en la barra lateral izquierda.

ⓓ Seleccione Seguridad.

ⓔ Busque Insertar contraseña en el enlace de invitación para unirse con un clic.

ⓕ Por defecto, estaría activado. Desactívelo haciendo clic en la pestaña del lado derecho.

ⓖ Ahora, todos sus participantes deben ingresar un código de acceso incluso si tienen acceso al enlace de la reunión.



Ministerio del Interior y Seguridad Pública

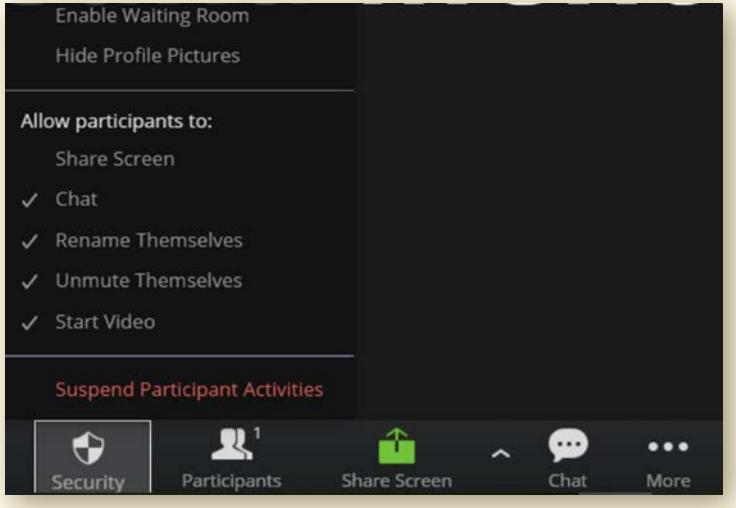
Consejo 4
Habilite la configuración "bloquear reunión"

Otra configuración de seguridad de Zoom que puede habilitar es Bloquear Reunión. Una vez que el reloj llegue a una hora específica o una vez que estén presentes todos los participantes esperados, puede bloquear la reunión para evitar que alguien más se una.

Una vez que inicie una reunión y observe que todos han llegado, vaya a la pestaña Seguridad en la parte inferior de la pantalla. Allí, encontrará la opción Bloquear Reunión.

Consejo 5
suspenda las actividades de los participantes

Si alguien comienza a portarse mal en medio de la reunión, puede suspender todas sus actividades de inmediato. Esta opción:



a. Apaga el audio y el video de todos los participan

b. Deja de compartir la pantalla.

c. Bloquea la reunión.

Lo mejor de esta opción es que no es necesario que finalice la reunión y reprograme todo. Esta función simplemente pausará la reunión para darle tiempo suficiente para expulsar al participante no deseado y reanudar la reunión.

Para pausar una reunión, vaya a la pestaña Seguridad y haga clic en Suspender actividades de los participantes.

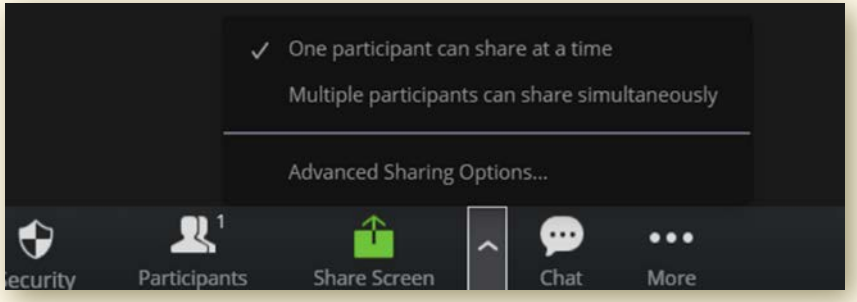
Consejo 6
Limite el uso compartido de la pantalla

En las reuniones donde tiene muchos participantes desconocidos en la reunión, como en clases académicas en línea, reuniones gubernamentales abiertas o eventos de entretenimiento en vivo, debe considerar limitar la opción de compartir pantalla.

Una vez que comience la reunión, haga clic en la opción Compartir pantalla del menú en la parte inferior. Seleccione la opción Uso compartido avanzado. Aquí puedes elegir:

ⓐ Si solo el anfitrión puede compartir su pantalla, o

ⓑ Para permitir que los participantes compartan la pantalla simultáneamente mientras el anfitrión u otros participantes comparten sus pantallas.



Consejo 7
Limite las capacidades para compartir archivos

Otra característica interesante de Zoom es que permite a los usuarios compartir archivos a través de la sala de chat. Pero cuando se trata de una gran cantidad de participantes desconocidos, uno de ellos puede publicar malware o contenido inapropiado en la sala de chat. Se puede restringir fácilmente el uso compartido de archivos siguiendo estos pasos:

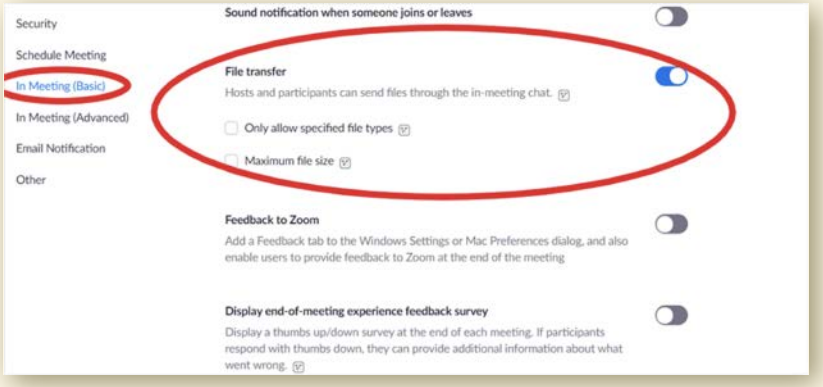
ⓐ Abra Zoom.us en su navegador e inicie sesión.

ⓑ Haga clic en MI CUENTA en el menú superior del lado derecho.

ⓒ Elija Configuración en la barra lateral izquierda.

ⓓ Seleccione En reunión (básico).

ⓔ Busque Transferencia de archivos.

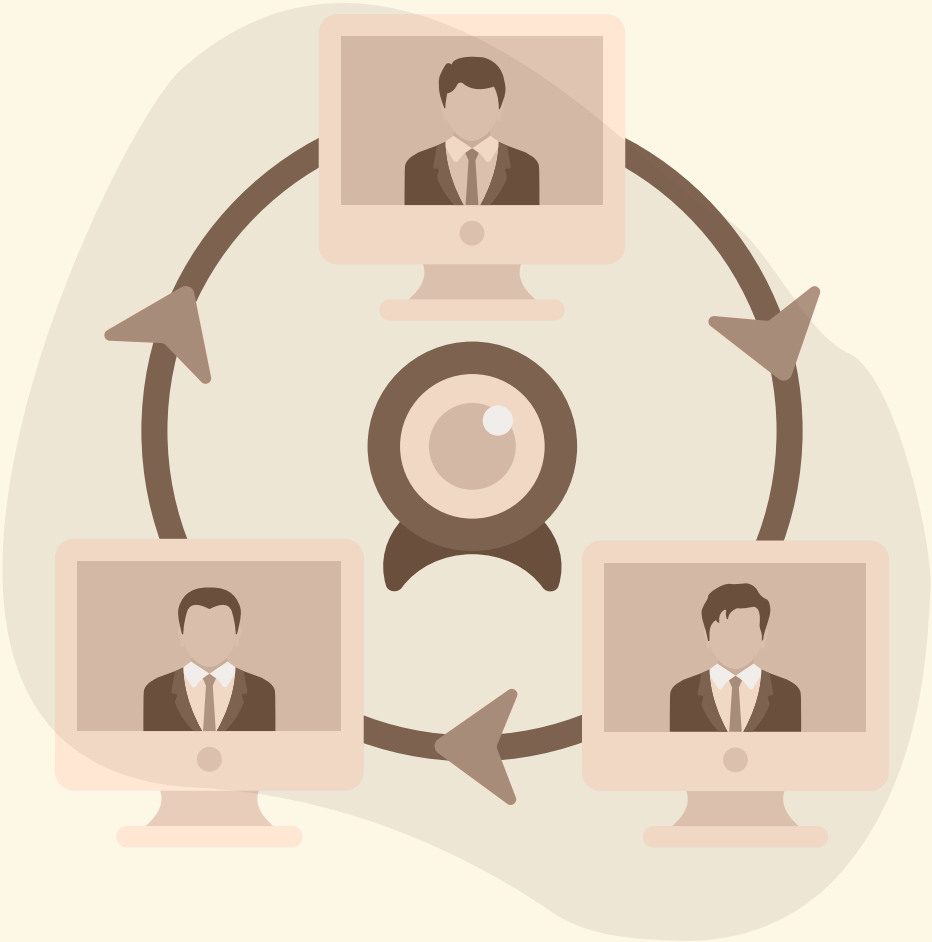


Si no desea que nadie más comparta los archivos durante la reunión, puede desactivar esta función. Si decide habilitarlo, obtendrá opciones para limitar los tipos y tamaños de archivos que los usuarios pueden compartir.

Consejo 8
Habilite la autenticación de dos factores

La autenticación de dos factores agrega otra capa de seguridad de Zoom para las organizaciones que desean que las cuentas de sus funcionarios sean más seguras. La forma en que funciona 2FA es que los usuarios recibirán una contraseña secreta de un solo uso en su teléfono o en una aplicación una vez que habilite esta configuración. Esto requiere que verifiquen que son quienes dicen ser porque tienen acceso al dispositivo o la aplicación registrados.

Para habilitar 2FA en la configuración de seguridad de Zoom, inicie sesión en el panel de control de Zoom:



ⓐ Vaya al menú de navegación y haga clic en Avanzado y luego toque Seguridad.

ⓑ Active la opción " Iniciar sesión con autenticación de dos factores".

ⓒ Verá la opción de si desea configurar 2FA a través de SMS o una aplicación de autenticación de terceros.

ⓓ Si elige emparejar su teléfono, recibirá una contraseña de un solo uso (OTP) cada vez que desee iniciar sesión en Zoom.

Para las aplicaciones, debe descargar aplicaciones como Google Authenticator, Microsoft Authenticator o FreeOTP. Recibirá un código de inicio de sesión único en dichas aplicaciones cuando inicie sesión en Zoom. Si tiene una cuenta comercial, podrá hacer cumplir la 2FA para las cuentas de todos los usuarios o los usuarios que pertenezcan a un grupo en particular o que tengan roles predefinidos.

Ministerio del Interior y Seguridad Pública

Consejo 9
Habilitar el cifrado de extremo a extremo (e2e)

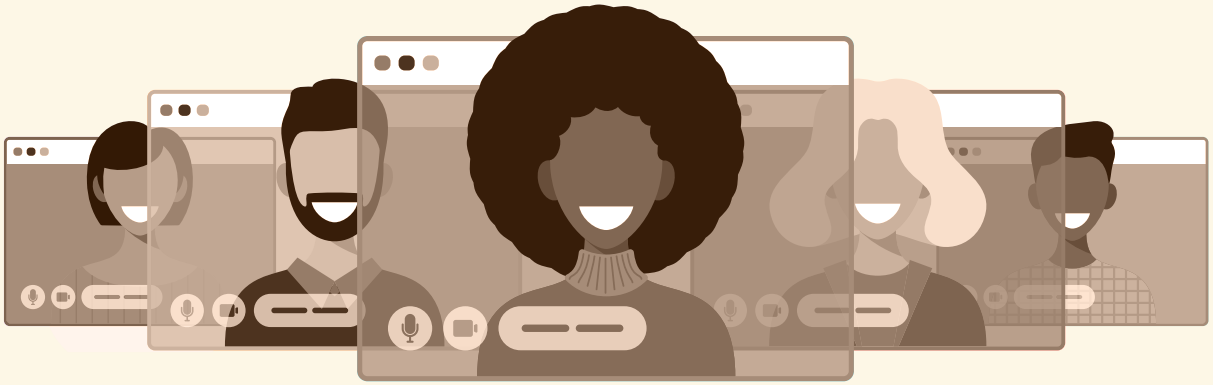
Puede habilitar el cifrado de extremo a extremo (E2E) para agregar otra capa de protección. Para habilitar el cifrado E2E en la configuración de seguridad de Zoom:

ⓐ Abra Zoom.us en su navegador e inicie sesión.

ⓑ Haga clic en MI CUENTA en el menú superior del lado derecho.

ⓒ Seleccione Configuración en la barra lateral izquierda.

ⓓ Busque Permitir el uso del cifrado de un extremo a otro y habilítelo.



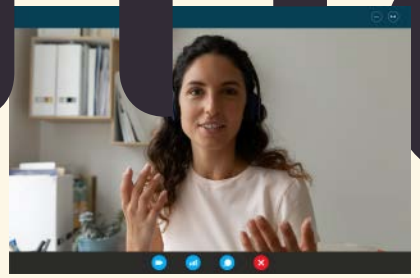
Checklist Resumen: Tenga presente que como administrador puede:

1. Asegurar una reunión con cifrado.
2. Crear salas de espera para los asistentes.
3. Requerir que el anfitrión esté presente antes de que comience la reunión.
4. Expulsar a un participante o a todos los participantes (no identificados o maliciosos).
5. Suspender las actividades de los participantes (para revisar las anomalías).
6. Bloquear una reunión.
7. Marcas de agua para compartir pantalla.
8. Firmas de audio.
9. Activar / desactivar un participante o todos los participantes para grabar.
10. Pausar temporalmente el uso compartido de la pantalla cuando se abre una nueva ventana.
11. Utilizar un código de acceso para proteger una reunión.
12. Solo permitir que se unan personas con un dominio de correo electrónico determinado,

El administrador de la plataforma debe dominar todas las opciones de seguridad que la plataforma ofrece en cuanto a ciberseguridad. Opciones de seguridad durante la reunión:
https://support.zoom.us/hc/en-us/articles/360041848151-In-meeting-security-options
https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

Ministerio del Interior y Seguridad Pública

CONSEJOS DE CIBERSEGURIDAD PARA EL ADMINISTRADOR DE ZOOM



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT: Hernán Espinoza

Diseño y diagramación: Jaime Millán

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile