Recomendaciones de ciberseguridad **para videoconferencias usando ZOOM**

Mantén siempre el software actualizado

Actualiza siempre Zoom a su última versión. También verifica las actualizaciones en tu sistema operativo, navegador y antivirus. Así te proteges de eventuales ciberataques.

Controla el envío y/o apertura de archivos o links a través de chat

Durante tu clase, puedes impedir o evitar que se envíen o abran links y archivos externos, que podrían ser maliciosos y dañar tu información.

Permitir solo participantes registrados

Con inscripción previa, puedes tener control de los asistentes y evitar el **"zoombombing"** (ingreso de terceros con intención de interrumpir reuniones virtuales)

Utiliza formas seguras de invitar a los participantes

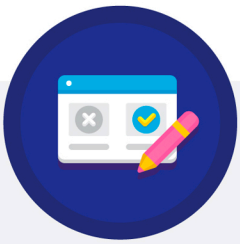
No publiques el ID de tu reunión en redes sociales o canales públicos. Usa siempre el sitio del curso o el correo institucional de tus estudiantes.

Gestionar el acceso de los participantes

Puedes habilitar una sala de espera, para revisar y aceptar manualmente a cada alumno de la clase, tarea que puede ser delegada a un ayudante o coanfitrión.

No entregues el control de la pantalla compartida

Al habilitar esta funcionalidad, evitarás que los participantes compartan contenidos no deseados. Además, como anfitrión puedes silenciar micrófonos y deshabilitar cámaras de los asistentes.



Deshabilita la opción "unirse antes del anfitrión"

De este modo, evitarás perder el control de los asistentes a la clase.

Remueve a personas del evento si causan algún tipo de incidente

Restringe o elimina a quienes generen desorden o no respeten las recomendaciones de seguridad. Para reincorporarlos, debes verificar la opción "permitir que los participantes eliminados se vuelvan a unir".

UCHILE, FRENTE AL CORONAVIRUS
¡PREVENGAMOS JUNTOS EL COVID-19!

UNIVERSIDAD DE CHILE

STI.uchile