Reglas para el uso más seguro de ZOOM

Este documento presenta una seria de reglas básicas para mitigar los problemas de seguridad relacionados con el uso de la aplicación de videoconferencia Zoom. Estas reglas no mitigan los problemas de privacidad de Zoom.

La empresa Zoom Comunications ha corregido la falla que afecta a la aplicación Zoom para Windows y que permitía robar las credenciales de los usuarios via el chat. Si tiene instalado el cliente Zoom para Windows, debe actualizar lo antes posible esta versión con la última versión disponible en el sitio web de Zoom. En caso de duda, es mejor usar Zoom a través de su navegador (Brave Browser de preferencia).
El cliente Zoom para MacOS ha sido también corregid. si están usando el cliente para Mac, tienen también que actualizarlo a la última versión disponible.

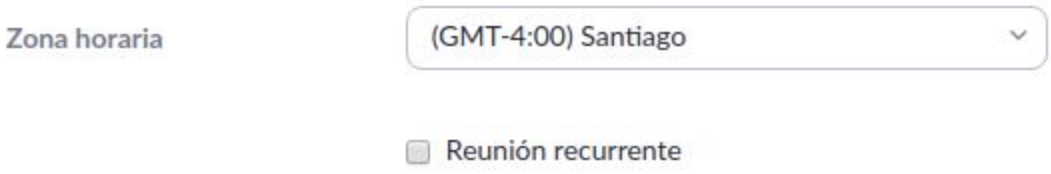
Regla 1

No usar nunca su identificador personal como identificador de una reunión Zoom. Se debe siempre usar un número diferente (generado por Zoom) para una reunión.

Esta regla permite evitar que sea demasiado fácil para un atacante inferir el número de la sesión Zoom.

Regla 2

No usar la funcionalidad de reuniones recurrentes. Hay que crear un nuevo identificador para cada reunión. Si tienen cada semana la misma clase el mismo día a la misma hora, deben crear una instancia diferente para cada clase.



La razón es la misma que para la regla 1. Permite evitar que un atacante pueda deducir fácilmente el Identificador de la reunión.

Regla 3

Es imperativo poner una contraseña a cada reunión que se crea.

Esta contraseña, debe ser entregada a los participantes:

- Por un medio seguro de transmisión de información (por ejemplo Whatapps, Signal, Telegram u otro), si se transmite se forma separada con el identificador de la reunión.
- Como enlace (URL) Zoom si se transmite por un medio de comunicación inseguro (como el email).

La contraseña permite evitar que cualquier persona que conoce o que pudo inferir el identificador de la reunión pueda colgarse en esta reunión sin haber sido invitada. Existen numerosos casos en EE.UU. y en Chile de reuniones donde aparecieron personas no invitadas que insultan o despliegan imágenes de pornografía.

Regla 4

No publicar nunca las invitaciones a reuniones en redes sociales.
Por la misma razón que la regla 3, con el fin de evitar que aparezcan personas no deseadas en una reunión.

Reglas 5

Activar la opción de compartir pantalla solamente par el profesor (anfitrión), y no para los otros participantes.

Permite evitar que una persona no invitada, pero que logró entrar a la reunión, sea capaz de difundir su pantalla a los otros.

Regla 6

Es importante usar la función de Sala de Espera para una reunión. Los participantes pueden entrar solamente cuando el anfitrión lo autoriza.

Permite aún más controlar las personas que pueden entrar en una reunión. Sin embargo, es bastante complicado en reuniones con muchos participantes (por ejemplo cursos masivos).

Regla 7

Desactivar la opción que permite re-entrar en una reunión cuando un participante salió o fue expulsado por el anfitrión.

Regla 8

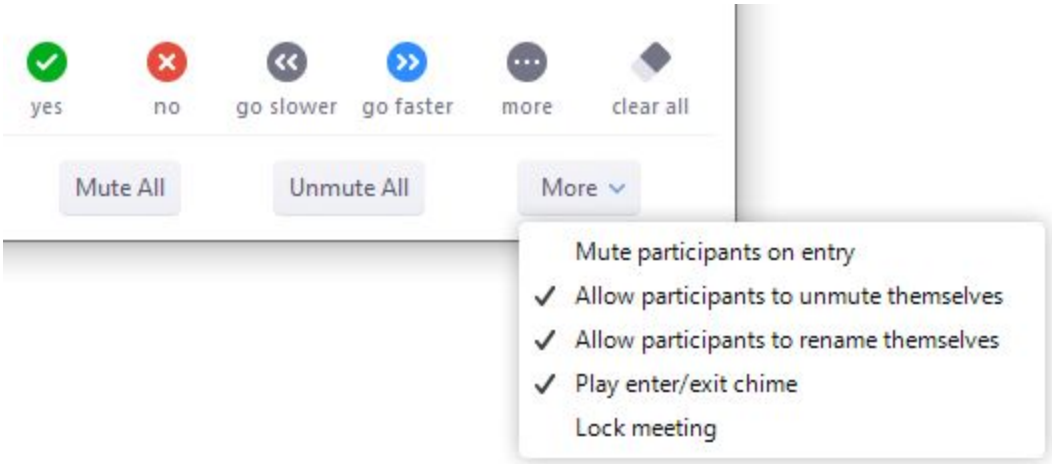
No usar la sala de reunión personal. La sala de reunión personal usa su identificador de usuario como ID de la reunión. Ver comentarios de la regla 1.

Regla 9

Desactivar la opción que permite a los invitados unirse a la reunión antes que el anfitrión.

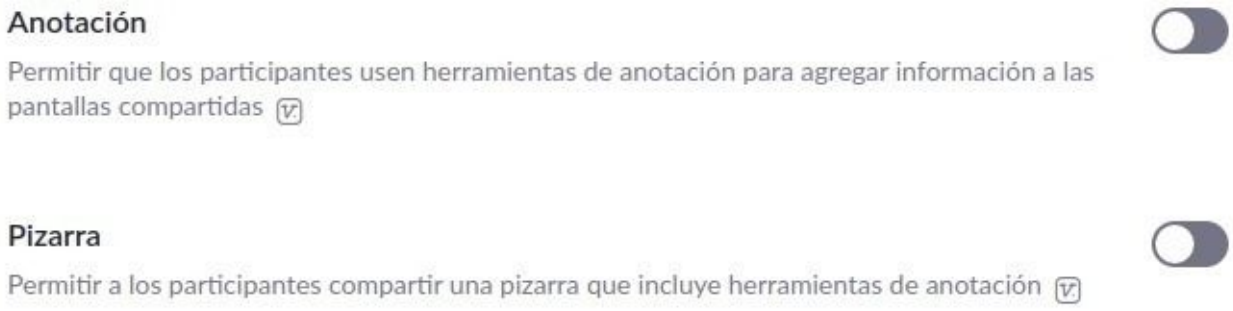
Regla 10

Deshabilitar la posibilidad de unirse a la reunión cuando ya llegaron todos los participantes. Eso se puede hacer en la ventana con la lista de participantes usando la opción More-->Lock meeting.



Regla 11

Desactivar la opción de poder usar una herramienta de anotación para agregar informaciones a las pantallas compartidas, y la que permite a los participantes compartir una pizarra con herramientas de anotación.



Regla 12

Instalar y actualizar siempre el cliente Zoom (Linux, Windows, MacOS) desde la página web De Zoom (https://zoom.us/) y no desde otro sitio. Existen una gran cantidad de clientes hackeados dando vueltas en Internet.

De la misma forma, las versiones para celulares deben ser instaladas desde el Play Store de Google o el App Store de Apple y no desde un sitio alternativo.

Acuérdense, que según las condiciones generales de uso de Zoom, la empresa Zoom Comunications Inc. puede entregar a terceros a fines de marketing los contenidos de las reuniones incluyendo el contenido del chat. Como Zoom no implementa un cifrado de tipo End-to-End, eso significa que Zoom tiene acceso y puede usar toda la información que pasa por sus servidores, incluyendo las partes video y audio.