Manuales Web. Zoom

Medidas de Seguridad para un uso seguro de Zoom

SSH TEAM CONSULTING

Presentación

Debido a la pandemia ocasionada por el COVID-19 y el estado de alarma decretado, el software de videoconferencia Zoom se ha convertido en una de las soluciones más populares y utilizadas para seguir en contacto con amigos y familiares, seguimiento de clases de deporte impartidas en línea e incluso para el teletrabajo.

Sin embargo, con el aumento de la popularidad de Zoom, ha crecido como objetivo ante ciberataques. Estos han descubierto algunas vulnerabilidades (donde no vamos a entrar en detalles) pero que ya han sido corregidas en la última versión de la herramienta.

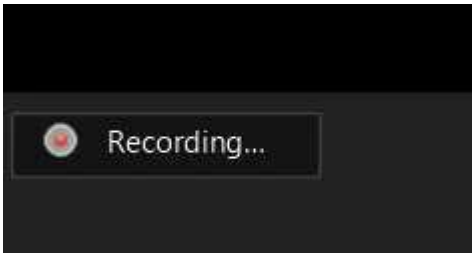
Debido a este aumento de ciberataques y un desconocimiento de la propia herramienta, ocasionado en gran medida por la irrupción del servicio, queremos dar algunos consejos de seguridad a la hora de configurar la herramienta o incluso, crear una nueva videoconferencia.

Consideraciones previas de privacidad al usar Zoom

Antes de comenzar a aprender a usar Zoom, es importante tener en cuenta las ramificaciones de privacidad al participar en reuniones de Zoom.

Una de las cosas más importantes para recordar, es que un Anfitrión puede grabar una sesión, incluido el video y el audio, en su equipo local. Por lo tanto, hay que tener cuidado al hablar de temas personales o confidenciales.

Los participantes de la reunión sabrán cuándo se está grabando una reunión, ya que se mostrará un indicador “Grabando...” en la esquina superior izquierda de la reunión, como se muestra a continuación.



También es importante recordar que ZOOM permite usar otras características como compartir archivos, realizar chats de grupo o privados (1 to 1) e incluso un usuario puede descargar sus registros de chat antes de abandonar una reunión.

Estas características anteriores, no se recomiendan debido a la privacidad del servicio, por lo que hay que tratar que al usar ZOOM sea solamente para un único propósito, videollamada.

Asegurar las reuniones de Zoom

Ahora que conocemos los riesgos potenciales de privacidad del uso de Zoom, antes de programar una reunión con amigos o compañeros de trabajo, puede familiarizarse con las diversas formas en que puede asegurar las reuniones de Zoom a través de los siguientes pasos.

Vamos a partir de la base que queremos asegurar la privacidad al completo, esto implicará configurar ZOOM para que, por defecto, ningún usuario que acceda a una reunión lo haga ya con el vídeo compartido, se pueda chatear e incluso compartir pantalla. De esta forma, nos aseguraremos de que el anfitrión, tiene plenos poderes sobre estas características.

Configuración perfil Zoom

Se va a tratar de resumir como configurar un perfil de Zoom de la forma más segura y privada posible. Para ello, vamos a tratar que cuando se realice una videollamada, sólo se trate de ello, es decir, desactivaremos cualquier tipo de chat, compartición de archivos, compartición de pantalla por parte de los invitados, etc.

Para configurar un perfil, hay que entrar a la cuenta de ZOOM a través de Internet, y en el menú superior pulsar en la opción "**Mi Cuenta**"

Acto seguido, vamos a la pestaña "**Configuración**" del menú lateral izquierdo.

Menú Reuniones

Reuniones próximas o Programar una reunión nueva

Apartado asistente para programar en un día y hora concreto una reunión.

Al programar una nueva reunión, se abrirá un formulario para elegir las opciones de configuración que creamos oportunas. Como puntos importantes, queremos destacar los siguientes:

1. **Generar un ID de reunión automáticamente**. Hay que tratar de no compartir nunca nuestro ID personal de reunión (PMI). 2.
2. Habilitar "**Requerir contraseña de reunión**". Se puede poner una manualmente, pero es aconsejable dejarla por defecto, ya que, mezclas mayúsculas, minúsculas y números y para cada reunión es diferente.

   Nunca utilizar una contraseña fácil del estilo: 123456, qwerty, asdfgh, etc.

3. **Vídeo apagado para anfitrión y participante.** Por defecto, las reuniones se inician con vídeo apagado. Debe ser el propio usuario quien configure manualmente si quiere iniciar el vídeo.

   Esta opción se puede activar más tarde desde dentro de la propia reunión.

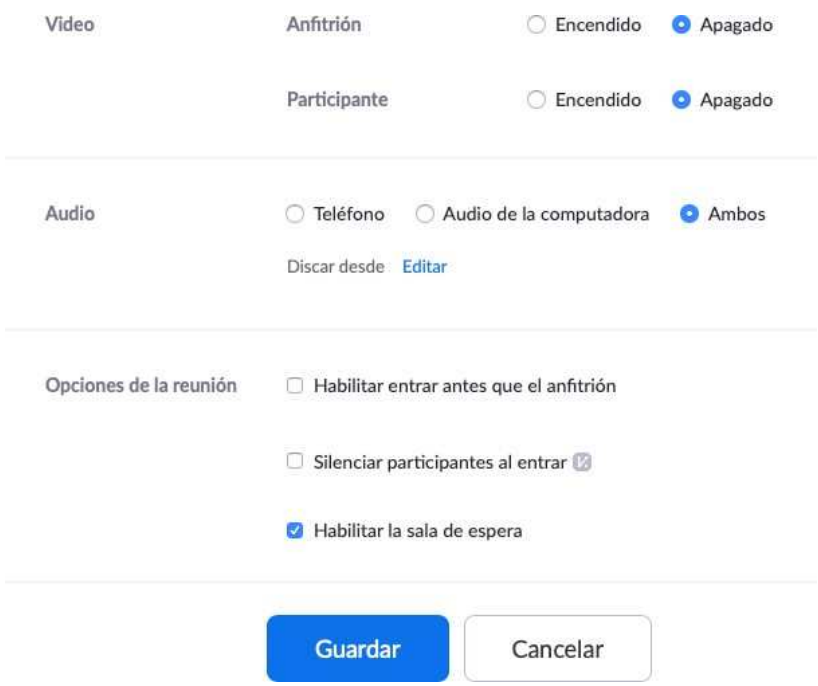
4. Opciones de la reunión:
   a. Deshabilitar "**entrar antes que el anfitrión**".
   b. Habilitar "**sala de espera**".

Como ya hemos comentado anteriormente, la función **"**sala de espera**"** impide que los usuarios ingresen a la reunión sin ser admitidos previamente por el organizador.

Cuando está habilitada, cualquier persona que se una a la reunión se colocará en una sala de espera donde se mostrará un mensaje que dice "Espere, el anfitrión de la reunión lo dejará entrar pronto".

El anfitrión de la reunión recibirá una alerta cuando alguien se una a la reunión para "quitar o admitir" y puede ver a los que esperan haciendo clic en el botón "Participantes" en la barra de herramientas de la reunión.

Las opciones 2 y 3 quedarán configuradas de la siguiente forma:



Sala de reunión personal

Muy parecido al apartado anterior, pero en este caso, la reunión se compartirá mediante el identificador de reunión personal (PMI).

Las medidas de configuración son iguales que en el apartado anterior con algún matiz:

1. **Requerir contraseña de reunión.**

   Por defecto, cualquier reunión implementa una contraseña aleatoria de 6 dígitos.

   A diferencia que su punto homólogo en el apartado anterior, esta contraseña siempre será la misma para estas reuniones personales, por lo que se recomienda cambiarla para cada reunión.

2. **Vídeo apagado para anfitrión y participante.**
3. **Desmarcar opción "Habilitar entrar antes que el anfitrión" y marcar "habilitar la sala de espera".**

Menú Configuración

Reunión

Este apartado recoge todas las opciones de configuración de cómo debe comportarse ZOOM ante una nueva reunión.

En ella, podemos configurar el comportamiento de vídeo, audio, la forma en la que los participantes se unen a una reunión, como compartir los enlaces de una reunión con otras personas, etc.

Se van a enumerar los puntos más importantes:

Programar reunión

1. Deshabilitar "**Video del anfitrión y participantes**"
2. Deshabilitar "**Unirse antes que el anfitrión**".
3. Habilitar "**Solicitar contraseña al programar nuevas reuniones**" y "**Requerir una contraseña para las reuniones instantáneas**"
4. Habilitar "**Se requiere una contraseña para el ID de reunión personal (PMI)**"
5. Deshabilitar "**Incluir la contraseña en el enlace de la reunión para permitir el acceso con un solo clic**". Hay que tratar de pasar por distintos medios de comunicación, el enlace y la contraseña de acceso, de este modo, añadimos más seguridad a los accesos
6. Habilitar "**Los participantes que se unan por teléfono precisan contraseña**". **En la reunión (Básico)**
7. Habilitar "**Requerir encriptación para los puntos de destino de terceros (H323/SIP)**"
8. Deshabilitar los chats tanto grupales como privados
9. Deshabilitar "**Guardar automáticamente chats**"
10. Deshabilitar "**Transferencia de archivos**"
11. Habilitar "**Uso compartido de la pantalla**", sólo para el anfitrión. Para evitar que otras personas secuestren su reunión, debe evitar que otros participantes que no sean el Anfitrión compartan su pantalla.
    También se puede cambiar la configuración desde dentro de una reunión

12. Habilitar "**Desactivar la compartición de escritorio/pantalla para los usuarios**"
13. Deshabilitar "**Control remoto**"
14. Deshabilitar "**Permitir que los participantes eliminados vuelvan a unirse**"
15. Deshabilitar "**Permitir que los participantes puedan renombrarse**

En la reunión (Avanzada)

16. Deshabilitar "**Soporte remoto**"
17. Habilitar "**Sala de espera**"

Grabación

1. Deshabilitar "**Grabación local**"
2. Deshabilitar "**Grabación automática**"
3. Habilitar "**Consentimiento de grabación**"
    a. Habilitar "**Preguntar a los participantes para su consentimiento**"
    b. Habilitar "**Preguntar al anfitrión para que confirme que se va a comenzar a grabar**".

Teléfono

1. Habilitar "**Mostrar enlace de números internacionales en el e-mail de invitación**"
2. Habilitar "**Ocultar número de teléfono en la lista de participantes**"

Una vez realizada la configuración de seguridad y privacidad interna de ZOOM, vamos a pasar a comentar algunos otros aspectos de seguridad para tener en cuenta:

a) Mantener actualizado el cliente ZOOM
b) No comparta su ID de reunión
c) Bloquear "unirse" cuando todos los participantes hayan accedido a la reunión
d) No publicar fotos de reuniones de Zoom en RRSS u otros medios compartidos con personas que no deben participar en dicha reunión
e) No publique enlaces "públicos" a sus reuniones

Mantener actualizado el cliente ZOOM

Las últimas actualizaciones de Zoom, habilitan las contraseñas de reunión de forma predeterminada y agregan protección contra las personas que escanean en busca de ID de reunión.

No comparta su ID de reunión

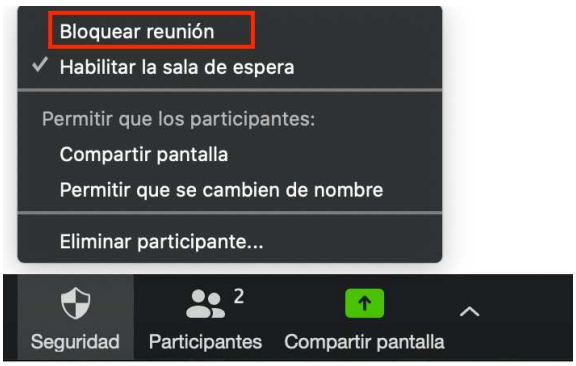
Cada usuario de Zoom recibe una "Identificación de reunión personal" (PMI) permanente que está asociada con su cuenta. Si le da su PMI a otra persona, siempre podrá verificar si hay una reunión en curso y potencialmente unirse si no se configura una contraseña.

En lugar de compartir su PMI, cree nuevas reuniones cada vez que comparta con los participantes según sea necesario.

Bloquear "unirse" cuando todos los participantes hayan accedido a la reunión

Si todos los participantes ya se han unido a su reunión y no está invitando a nadie más, debe bloquear la reunión para que nadie más pueda unirse.

Para hacer esto, haga clic en el botón "Seguridad" en la barra de herramientas Zoom y seleccione "Bloquear reunión".



No publicar fotos de reuniones de Zoom en RRSS u otros medios compartidos con personas que no deben participar en dicha reunión

Si toma una foto de su reunión de Zoom, cualquiera que vea esta foto podrá ver su ID de reunión asociada. Esto puede ser utilizado por personas no invitadas para intentar acceder a la reunión.

No publique enlaces “públicos” a sus reuniones

Al crear reuniones de Zoom, nunca debe publicar públicamente un enlace a su reunión. Al hacerlo, los motores de búsqueda como Google indexarán los enlaces y los hará accesibles para cualquiera que los busque.

Como la configuración predeterminada en Zoom es incrustar contraseñas en los enlaces de invitación, una vez que una persona tiene su enlace Zoom puede bombardear su reunión con Zoom.