Seguridad en Conferencias utilizando Zoom

Con el objetivo de tener una videoconferencia segura a través de Zoom a continuación se listan las recomendaciones para el presentador (host) y para clientes (clients) de este servicio.

RECOMENDACIONES

1. ASIGNAR UNA CLAVE DE ACCESO A LA REUNIÓN

Esta clave de acceso puede ser distinta para cada reunión según la documentación de Zoom para cuentas de paga, en caso de cuenta gratis se puede asignar una clave y cambiarla cuando se desee.

2. AUTENTIFICAR USUARIOS

Cuando se crea una reunión es recomendable solo dejar entrar a los usuarios que se encuentren registrados con cuenta de Zoom gratis o de paga.

3. NO DEJAR INICIAR SIN EL PRESENTADOR (HOST)

No permitir que la reunión empiece sin que el presentador haya entrado. Esto se puede definir en los ajustes de la reunión.

4. BLOQUEAR LAS REUNIONES

Una vez iniciada la reunión y con todos los asistentes esperados en la misma es recomendable bloquear (lock) la reunión para evitar que usuarios no deseados se conecten.

5. DESHABILITAR A LOS PARTICIPANTES EL COMPARTIR LA PANTALLA

En caso de que solo el presentador (host) sea el único que muestre pantalla se recomienda que se deshabilite la función de compartir pantalla a los asistentes.

6. UTILIZAR UN IDENTIFICADOR DE REUNIÓN ALEATORIO

Tratar de evitar el identificador personal de Zoom para las reuniones y generar uno aleatorio siempre.

7. UTILIZAR CUARTO DE ESPERA (WAITING ROOMS)

Zoom tiene una función de cuarto de espera y es una forma de verificar a un usuario antes de dejarlo entrar a la reunión.

8. EVITAR COMPARTIR ARCHIVOS

Evitar el compartir archivos desconocidos de los participantes que no sean confiables. Se recomienda deshabilitar esta opción de Zoom.

9. ELIMINAR ASISTENTES MOLESTOS

Estar atento de los usuarios que estén entrando a la reunión para identificar algún usuario intruso en la reunión y eliminarlo con la opción de patear (kick) asistentes.

10. REVISAR ACTUALIZACIONES

Estar atento de las actualizaciones de Zoom para los parches de seguridad oficiales de Zoom.

11. EVITAR CONEXIONES DESDE SMARTPHONES O TABLETS

Nota: Los puntos de 1 a 7 son configurados por el responsable de la cuenta institucional. Para el caso de cuentas no institucionales, el usuario puede controlar estos puntos.