

El uso de Zoom y sus implicaciones para la seguridad y privacidad. Recomendaciones y buenas prácticas

Resumen: en los últimos días se ha cuestionado la aplicación Zoom por problemas de privacidad y seguridad. A continuación, se analizan las deficiencias reportadas y se recogen una serie de recomendaciones y buenas prácticas para su uso.

Contenido:

1	CONTEXTO	1
2	ANÁLISIS DEL ZOO	1
3	RECOMENDACIONES Y BUENAS PRÁCTICAS	5
3.1	Programe una reunión	5
3.2	Crear una nueva reunión desde el menú principal	7
3.3	Crear una nueva reunión desde el menú secundario	12
3.4	Recomendaciones para el sector de la educación	13
3.5	Recomendaciones en la configuración general	14
4	CONCLUSIONES	20

1 CONTEXTO

La evolución de la pandemia marcada por COVID-19 y el confinamiento asociado de los ciudadanos, el distanciamiento social y la cuarentena ha traído consigo el uso generalizado de videoconferencias y aplicaciones de chat como Zoom, Webex, Houseparty, Google Meet o Microsoft Teams.

Los ciberatacantes están aprovechando las oportunidades asociadas con el miedo en torno a la pandemia, el teletrabajo ampliamente implantado, las dificultades para parchear puntos finales conectados remotamente y el incremento de la superficie de exposición derivada de permitir operativas más fluidas.

En este contexto, las sesiones y aplicaciones de videoconferencia deficientemente protegidas son un magnífico vector de ataque.

2 ANÁLISIS DE ZOOM

Zoom es una aplicación de videoconferencia con mensajería en tiempo real e intercambio de contenido fácil de configurar y usar, que permite reuniones con hasta 100 participantes de forma gratuita. Decisiones de diseño orientadas a ofrecer una mayor usabilidad han permitido realizar actuaciones no deseadas.

La aplicación Zoom está siendo cuestionada por problemas de privacidad y seguridad en los últimos días.

- Si un anfitrión deshabilita las salas de espera y las contraseñas, cualquiera puede unirse a una reunión de Zoom si conoce el ID de la reunión. Además, si un anfitrión comparte ampliamente su enlace de reunión o su ID y contraseña a través de un foro público como las redes sociales, los invitados no deseados pueden unirse con la intención de interrumpir la reunión. Estos a menudo utilizan el uso compartido de la pantalla para publicar contenido chocante o inapropiado o hacer sonidos molestos.

Zoom ha activado las "salas de espera" y las contraseñas de forma predeterminada y ha establecido el uso compartido de pantalla en "Solo para anfitriones" de forma predeterminada para la mayoría de las cuentas a fin de evitar interrupciones en las reuniones, y ha añadido funciones para ayudar a los anfitriones a acceder más fácilmente a los controles de seguridad de las reuniones, incluido el control del uso compartido de pantalla, la eliminación y la notificación de los participantes y el bloqueo de las reuniones, entre otras acciones.

Para reuniones más grandes y públicas, Zoom ofrece un producto de *webinar* que le permite transmitir una reunión de Zoom a hasta 10.000 asistentes de solo lectura. En los seminarios web, solo los anfitriones y los panelistas preseleccionados pueden aparecer en vídeo, así como compartir contenido. Los asistentes no aparecen en el vídeo, no pueden compartir la pantalla y no pueden hablar a menos que el anfitrión así lo decida. Se trata de un formato más seguro y apropiado para acoger reuniones públicas, a fin de evitar trastornos en la reunión.

- Para minimizar el número de clics desde la descarga de la aplicación hasta su ejecución en macOS, las comprobaciones previas a la instalación se utilizaban incorrectamente mostrando un mensaje de contraseña engañoso. Este fue resuelto en abril.
- Fugas de direcciones de correo electrónico, fotos de usuarios y llamadas injustificadas debido a una configuración inadecuada que agregaría automáticamente personas a las listas de contactos de un usuario si ambos inician sesión con una dirección de correo electrónico perteneciente al mismo dominio. Esto se resolvió en abril.
- Zoom utilizaba el AES-256 en modo ECB para cifrar las comunicaciones, lo que no resulta aconsejable ya que la información cifrada conserva posibles patrones presentes en los datos en claro facilitando romper el cifrado para un ciberatacante que capture el tráfico. El 30 de mayo, Zoom habilitó la encriptación AES de 256 bits GCM para todas las reuniones.

Además, Zoom encripta las comunicaciones, pero no el contenido, por lo que los ataques MITM (man in the middle) que aceptan la conexión con certificados no válidos podrían permitir a un atacante acceder a la información. Zoom planea ofrecer encriptación de extremo a extremo en un futuro muy cercano. El 7 de

mayo, Zoom anunció la adquisición de Keybase, lo que acelerará el plan de Zoom de construir una encriptación de extremo a extremo que pueda alcanzar la actual escalabilidad de Zoom. A continuación, Zoom publicó un borrador de diseño criptográfico para una oferta de comunicaciones de video encriptadas de extremo a extremo en GitHub el 22 de mayo y, tras de solicitar la opinión del público, la compañía publicará hitos de ingeniería.

- Debido a una mala configuración temporal en el enrutamiento de los centros de datos mundiales de Zoom - que, en circunstancias normales, está diseñado para mantener el geo-cercado alrededor de China tanto para los centros de datos primarios como para los secundarios - ciertas reuniones pueden haber sido capaces de conectarse a los servidores de Zoom en China en circunstancias extremadamente limitadas, donde las autoridades de este país con diferente legislación de protección de datos podrían obligar a los operadores de servicios a entregar información. Esto se resolvió en abril y, desde entonces, Zoom también ha introducido una función que permite a los usuarios controlar qué regiones de centros de datos puede utilizar su cuenta para su tráfico de reuniones en tiempo real, lo que les da aún más comodidad de que sus datos no se están encaminando a través de la China continental.
- Aunque Zoom ha integrado mecanismos antisabotaje, estos pueden ser desactivados o incluso reemplazados por una versión maliciosa que secuestre la aplicación. Esto se debe a que los ciberdelincuentes¹ están aprovechando el auge de la aplicación Zoom y el aumento del número de descargas de la aplicación para registrar dominios que ofrecen un instalador ejecutable que contiene malware. Las páginas creadas por los ciberdelincuentes distribuirían el malware haciéndose pasar por la página oficial de la aplicación para engañar al usuario. Los usuarios de Zoom deben tener cuidado con los correos electrónicos o los enlaces de remitentes desconocidos, teniendo cuidado de hacer clic solo en los enlaces auténticos o de abrir los archivos adjuntos de proveedores de servicios conocidos y de confianza. Se recomienda encarecidamente que solo descarguen la aplicación a través de los canales de distribución legítimos de Zoom, incluyendo el sitio web de Zoom, Google Play Store y Apple App Store.

En este escenario, varias instituciones, organizaciones y organismos aconsejaron previamente que no se utilizara Zoom. Sin embargo, Zoom ha abordado activa y rápidamente las preocupaciones sobre la privacidad y la seguridad a medida que se iban planteando. El 29 de marzo, Zoom actualizó su política de privacidad para hacerla más clara, explícita y transparente. El 1 de abril, Zoom anunció un plan de 90 días para duplicar su compromiso con la seguridad y está trabajando proactivamente para

¹ [un artículo que recogía las investigaciones de la empresa Check Point Research](#)

identificar, abordar y solucionar mejor los problemas. Entre otras acciones, Zoom ha hecho lo siguiente:

- Promulgar la congelación de características y el cambio de todos los recursos de ingeniería para centrarse en la confianza, la seguridad y la privacidad.
- Iniciar un examen exhaustivo con expertos de terceros y usuarios representativos para comprender y garantizar la seguridad de todos los nuevos casos de uso de Zoom.
- Comenzar a realizar una serie de pruebas de penetración de caja blanca simultáneas para seguir identificando y abordando los problemas.
- Mejorar su actual programa de recompensas por errores.
- Crear un consejo de CISO en asociación con los principales CISO de toda la industria para facilitar un diálogo permanente sobre las mejores prácticas en materia de seguridad y privacidad.

Además, Zoom está trabajando actualmente en una oferta de comunicaciones de vídeo cifradas de extremo a extremo, y la empresa tiene previsto publicar un informe de transparencia como parte del plan de 90 días.

- El 20 de marzo, Zoom publicó en su blog² una entrada para ayudar a los usuarios a evitar incidentes de interrupción de reuniones, destacando características de seguridad como salas de espera, contraseñas, controles de silencio y limitación del uso compartido de pantallas.
- Zoom también reconoció que su afirmación de apoyo a la encriptación de extremo a extremo es engañosa³. Zoom aclaró que en una reunión en la que todos los participantes están usando el cliente de Zoom y la reunión no está siendo grabada, Zoom encripta todo el contenido de vídeo, audio, pantalla compartida y chat en el cliente emisor, y no lo descifra hasta que llega a los receptores.
- Zoom actualmente genera y gestiona las claves de cifrado en la nube. Es importante señalar que Zoom ha puesto en práctica controles internos sólidos y validados para impedir el acceso no autorizado a cualquier contenido que los usuarios compartan durante las reuniones, incluidos, entre otros, los contenidos de vídeo, audio y chat de esas reuniones.
- Zoom también indicó que nunca ha creado un mecanismo para descifrar las reuniones en vivo con fines de interceptación legal y que no hay forma de incluir a terceros en las reuniones sin que ello quede reflejado en la lista de participantes.
- Para aquellos que deseen un control adicional de sus claves de cifrado, existe hoy una solución in situ para toda la infraestructura de reuniones, y a finales de este

² <https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event//>

³ <https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/>

año estará disponible una solución que permitirá a las organizaciones aprovechar la infraestructura en la nube de Zoom.

- El 27 de marzo, Zoom actualizó su aplicación iOS⁴ (violaciones de la privacidad de iOS) para eliminar el código que enviaba los datos del usuario a Facebook cuando se abría la aplicación (zona horaria y ciudad, detalles sobre el dispositivo o si el usuario no tenía una cuenta en Facebook).
- El 29 de marzo, Zoom actualizó su política de privacidad⁵ para que fuese más clara y transparente. Zoom hizo hincapié en que no vende datos de usuarios, nunca ha vendido datos de usuarios en el pasado y no tiene intención de vender datos de usuarios en el futuro.
- El 2 de abril, Zoom parcheó las vulnerabilidades que permitían la escalada de privilegios y el acceso a la grabación, reunión y micrófono en macOS.
- El 2 de abril, Zoom corrigió una vulnerabilidad asociada con el chat del cliente Zoom de Windows que podría permitir a un atacante remoto robar las credenciales de inicio de sesión de Windows de un usuario si este hacía clic en una ruta de tipo Universal Naming Convention (UNC).
- El 7 de abril, Zoom informó de que habían implementado una solución para una vulnerabilidad grave en Zoom que permitía obtener la clave de cifrado de la reunión a usuarios en la sala de espera.
- Zoom eliminó recientemente una función de "*seguimiento de la atención de los asistentes*" que permitía a los anfitriones ver si los asistentes tenían la ventana de Zoom u otra ventana de la aplicación enfocada durante una reunión.

3 RECOMENDACIONES Y BUENAS PRÁCTICAS

La mejor manera de evitar interrupciones en las reuniones es no compartir las identificaciones de las reuniones de Zoom excepto con los participantes previstos. Además, se puede solicitar a los participantes que utilicen una contraseña para iniciar sesión en la reunión.

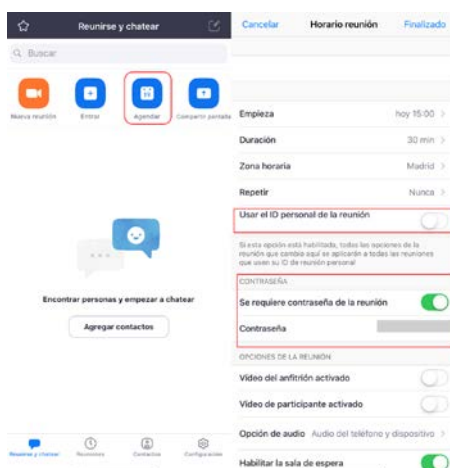
3.1 Agendar una reunión

Zoom permite dejar programada una reunión para una hora y fecha concretas. Si usted es el organizador de la reunión, a la hora de agendarla debe tener en cuenta las siguientes recomendaciones:

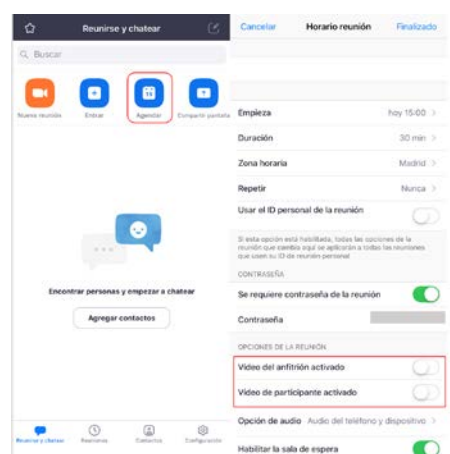
⁴ <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/>

⁵ <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/>

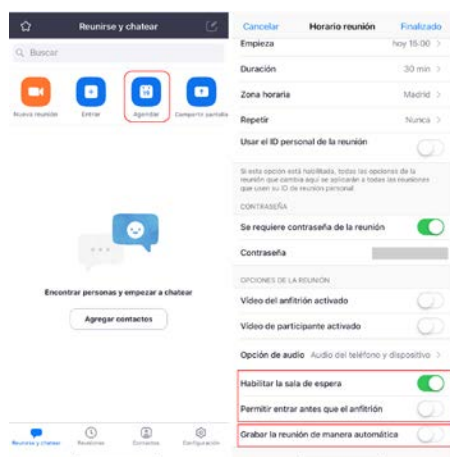
- Genere un ID de reunión aleatorio y requiera contraseña para entrar en la reunión. Si pulsa sobre la opción “Contraseña”, puede cambiar la contraseña por defecto.



- Configure la reunión de modo que el uso compartido de la pantalla esté habilitado sólo para el anfitrión.



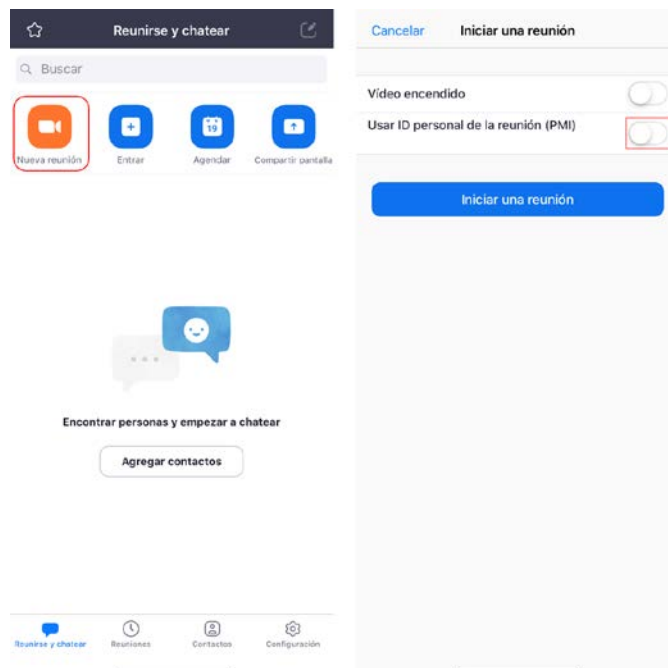
- Habilite la sala de espera y no permita que los invitados entren a la reunión antes que el anfitrión (organizador) se una a la reunión. Del mismo modo, si no es estrictamente necesario grabar la reunión, deshabilite esta opción antes de iniciar la reunión.



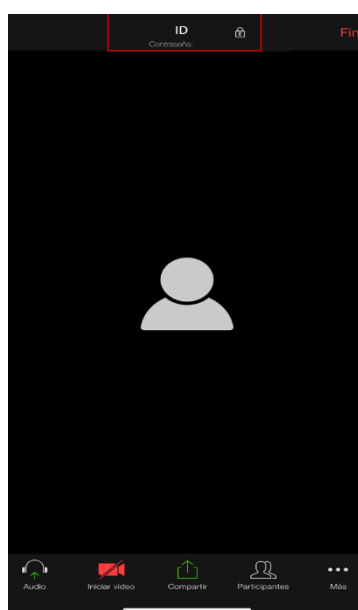
3.2 Crear una nueva reunión desde el menú principal

El menú principal de Zoom, también permite crear una reunión de forma inmediata. Para ello, habría que pulsar sobre “Nueva reunión” y comenzar a configurar la sala antes de invitar a los participantes. Para ello:

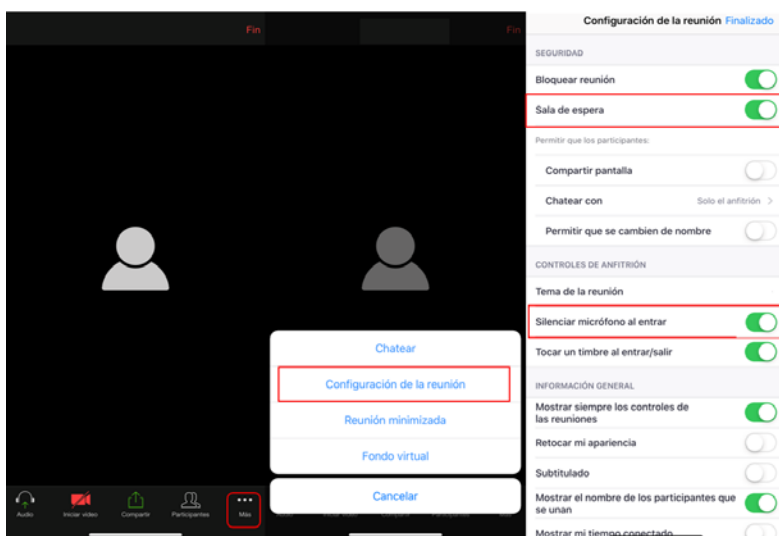
- Una vez pulse sobre “Nueva reunión”, genere una ID de reunión aleatoria.



- Cuando pinche sobre el botón azul “Iniciar una reunión”, le aparecerá en la pantalla el ID de la reunión asignado de manera aleatoria y la contraseña generada de manera automática al organizar una reunión siguiendo este procedimiento.

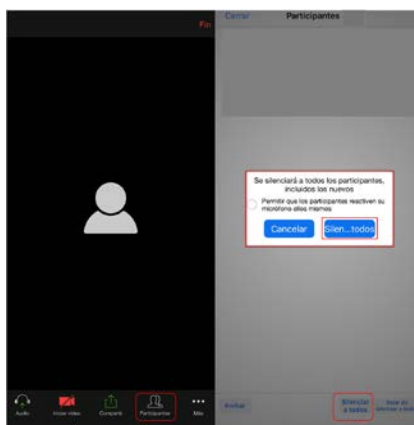
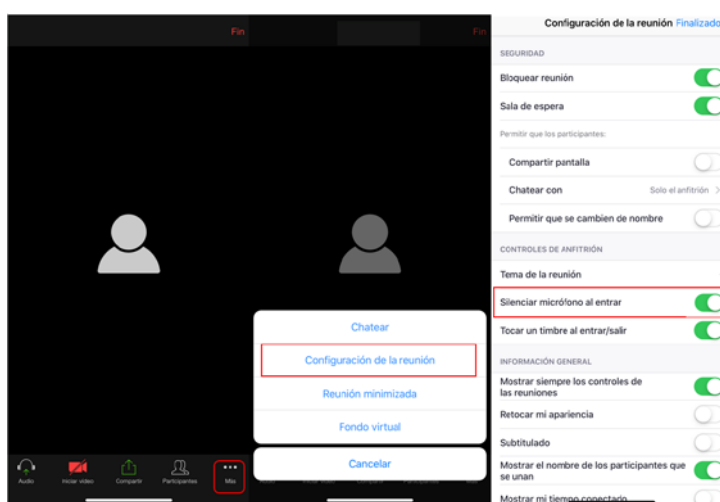


- Habilite la sala de espera y silencie a los participantes al entrar.

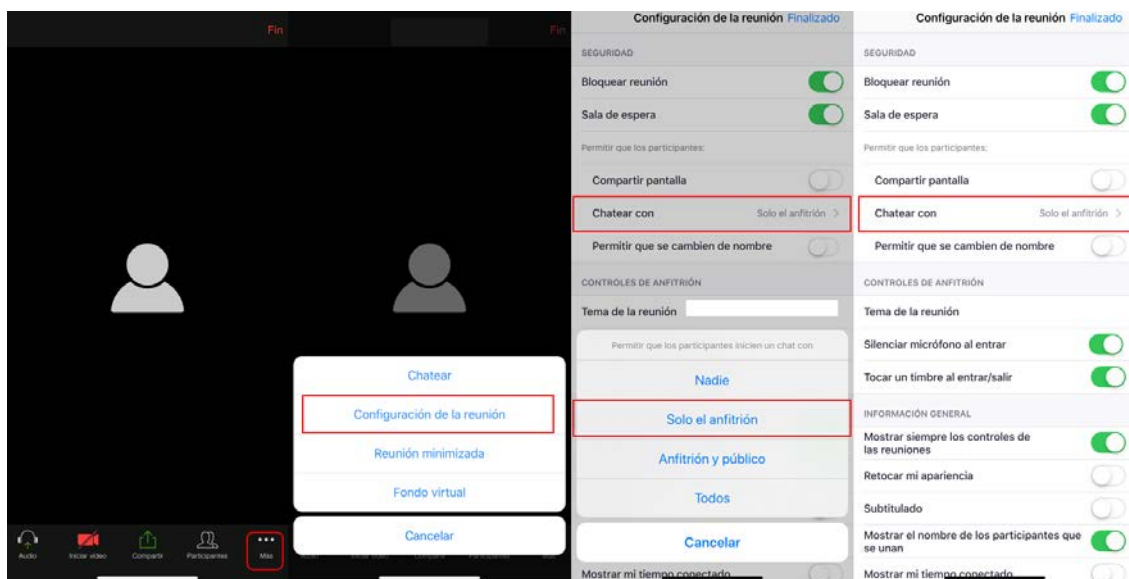


Además, configure la reunión para que:

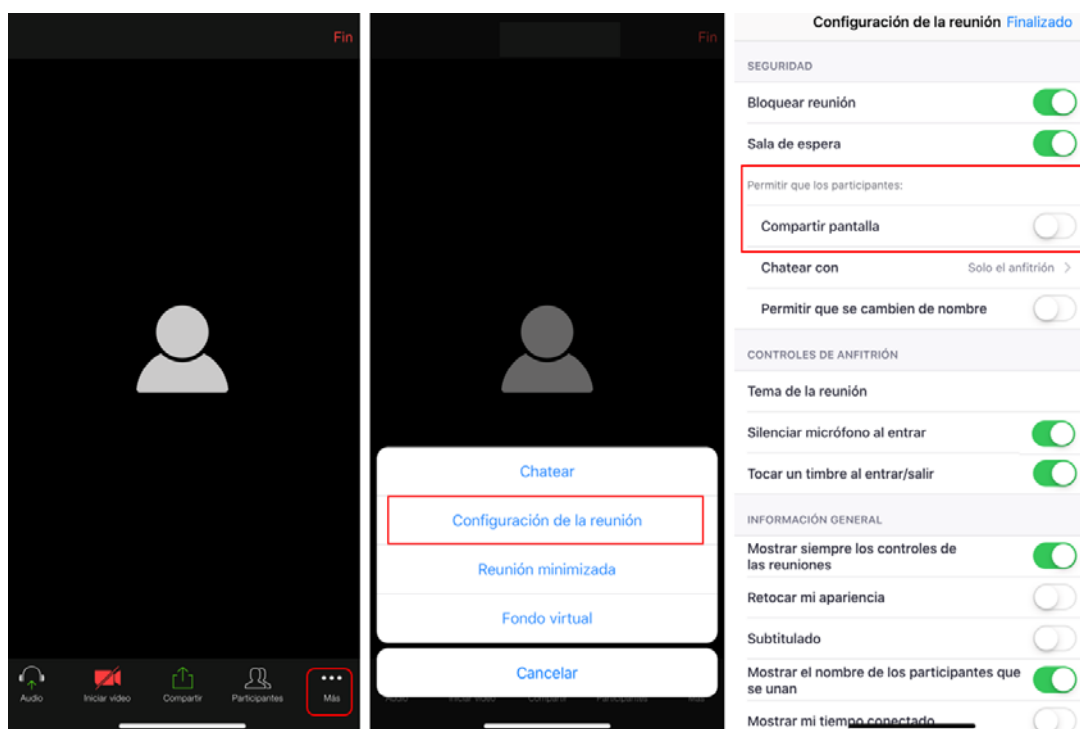
- Permita que solo los participantes que hayan iniciado sesión en Zoom ingresen a la reunión.
- Deshabilite la inclusión de contraseña en el enlace de invitación a la reunión.
- Silencie a los participantes cuando ingresen a la reunión.



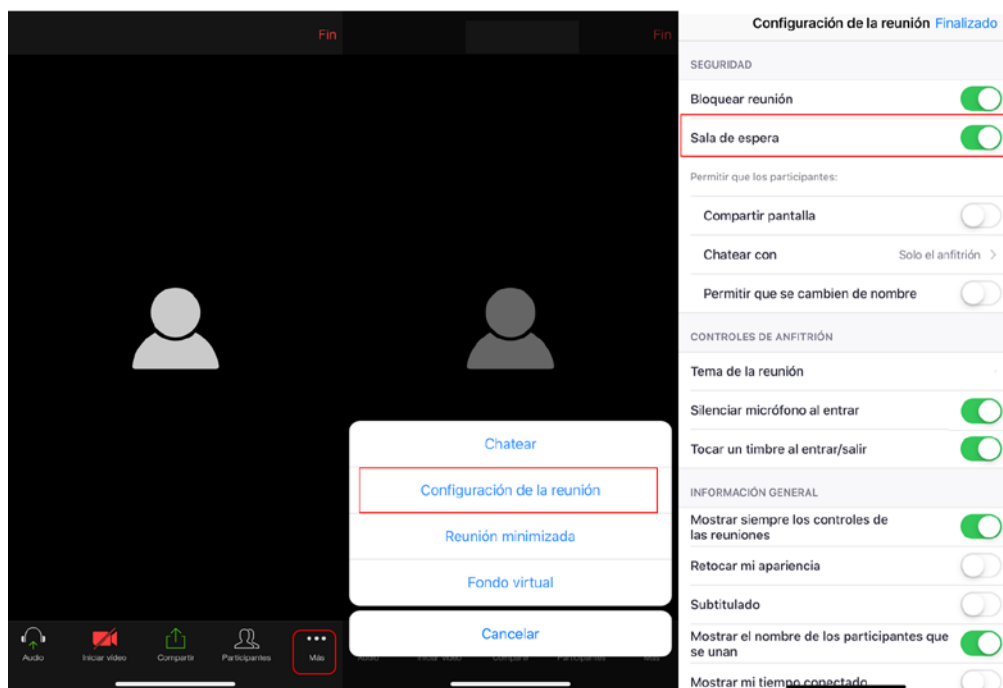
- Desactive el chat privado entre los asistentes.



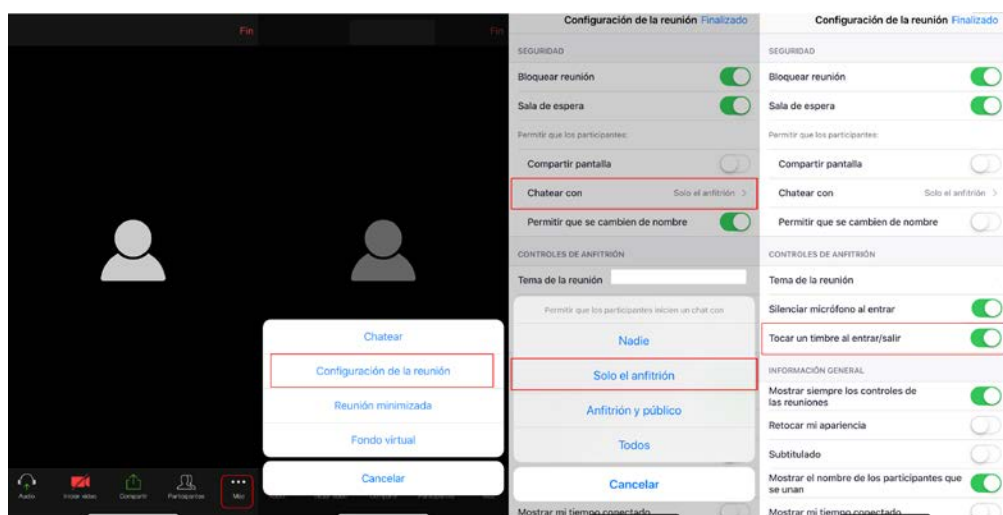
- Desactive el guardado automático de los chats.
- Establezca el uso compartido de pantalla solo para el anfitrión.



- Active la sala de espera para los participantes (al activar esta opción, se desactiva automáticamente la opción que permite a los participantes unirse a la reunión antes que el anfitrión).



- Active el indicador sonoro cada vez que un invitado entre o salga de la reunión.

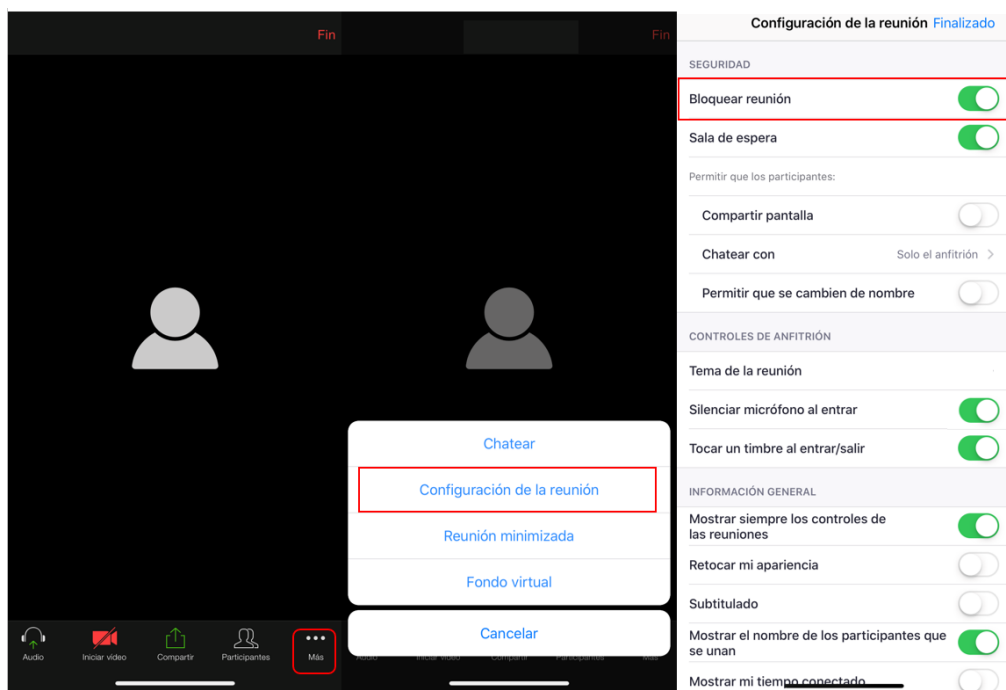


Por otra parte, depende del anfitrión decidir si se graba una reunión, y Zoom ofrece a los clientes de pago la opción de almacenar grabaciones en los propios servidores de Zoom.

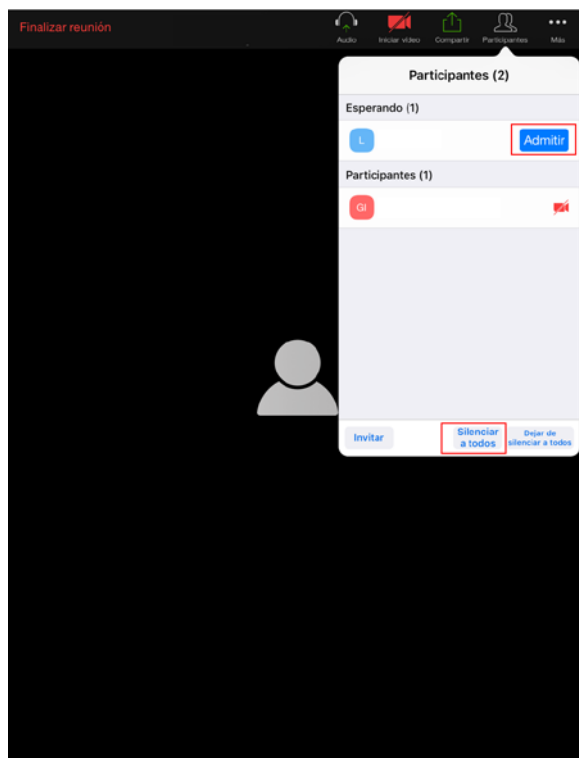
Asimismo, depende del moderador cambiar el nombre del archivo de grabación. Si organiza una reunión de Zoom y decide grabarla, asegúrese de cambiar el nombre de archivo predeterminado una vez que haya terminado. Si decide subir las grabaciones de la reunión a cualquier otro lugar que no sea la nube de Zoom o su propio equipo (por ejemplo, YouTube, una nube pública, etc.), Zoom insta a los anfitriones a que actúen con extrema cautela y sean transparentes con los participantes de la reunión, considerando detenidamente si la reunión contiene información confidencial y las expectativas razonables de los participantes.

Adicionalmente, una vez ingresan los participantes en la reunión ha de tener en cuenta como administrador las siguientes cuestiones:

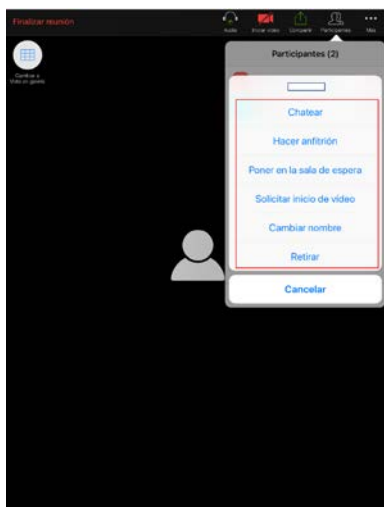
- Puede cerrar la reunión para que no se unan nuevos participantes.



- Puede ver el listado de personas que se encuentran en la sala de espera y decidir el momento en el que se admiten a la reunión.



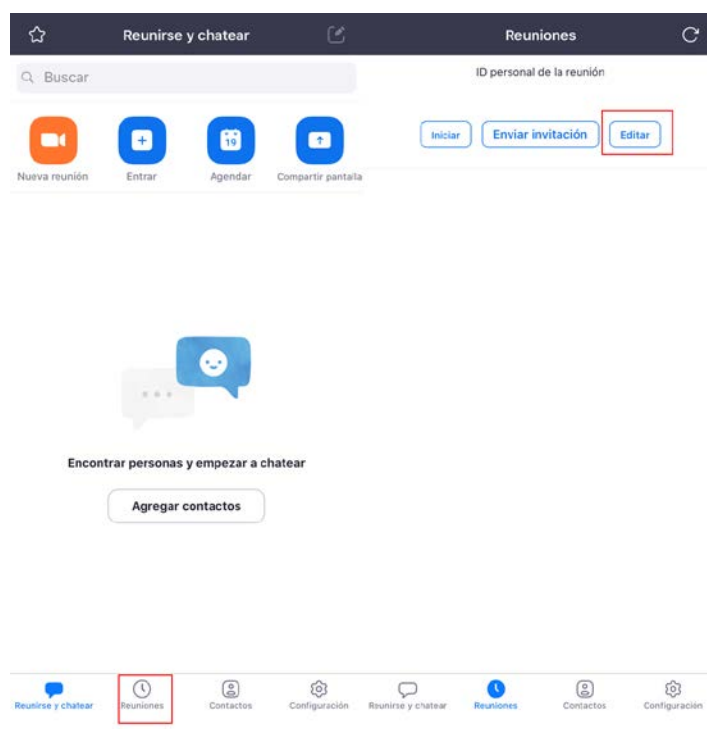
- Una vez aceptados los invitados, si pulsa sobre un invitado concreto, puede realizar diferentes acciones. Si pulsa en “Retirar” eliminará de la reunión al invitado.



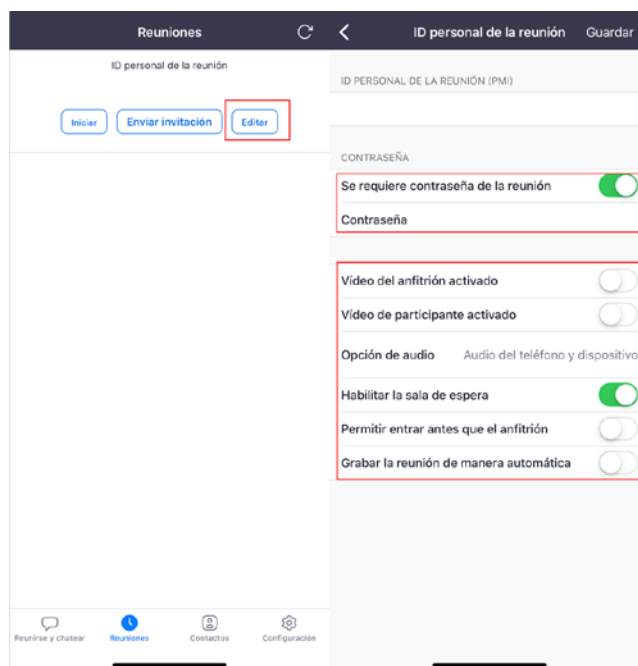
3.3 Crear una nueva reunión desde el menú secundario

La aplicación Zoom también permite crear de una tercera forma una reunión que, en principio, **se desaconsejaría puesto que implica iniciar la reunión con el ID personal y no con uno aleatorio.**

- Si se pulsa sobre el menú secundario, sobre la opción “Reunión” puede iniciar una nueva reunión a partir de su ID personal de reunión (PMI). En primer lugar, antes de iniciar la reunión o invitar a participantes, pulse sobre la opción Editar para comenzar a configurar los ajustes de la sesión:



- Requiera contraseña para acceder a la reunión. Si pulsa sobre la opción “Contraseña” puede modificar la que establecida por defecto.
- Desactive el video de los invitados.
- Habilite la sala de espera y no permita que los invitados accedan a la reunión antes que el organizador.
- Si no es estrictamente necesario grabar la reunión, desactive la opción “Grabar la reunión de forma automática”.



3.4 Recomendaciones para el ámbito educativo

Por otro lado, relacionado con el sector de la educación, Zoom:

- Publicó una guía⁶ del administrador sobre cómo configurar un aula virtual.
- Estableció una guía⁷ sobre cómo mejorar la seguridad de sus aulas virtuales.
- Configuró una política de privacidad dedicada a los menores de 17 años (K-12)⁸.
- Cambió la configuración para los usuarios de educación inscritos en el programa K-12 para que las contraseñas y las salas de espera virtuales estén habilitadas de forma predeterminada, así como los privilegios para compartir la pantalla estén configurados en "Sólo Anfitrión", de forma que los profesores, de forma predeterminada, sean los únicos que puedan compartir el contenido.

⁶ <https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf?zcid=1231>

⁷ <https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/>

⁸ <https://zoom.us/docs/en-us/childrens-privacy.html?zcid=1231>

3.5 Recomendaciones en configuración general

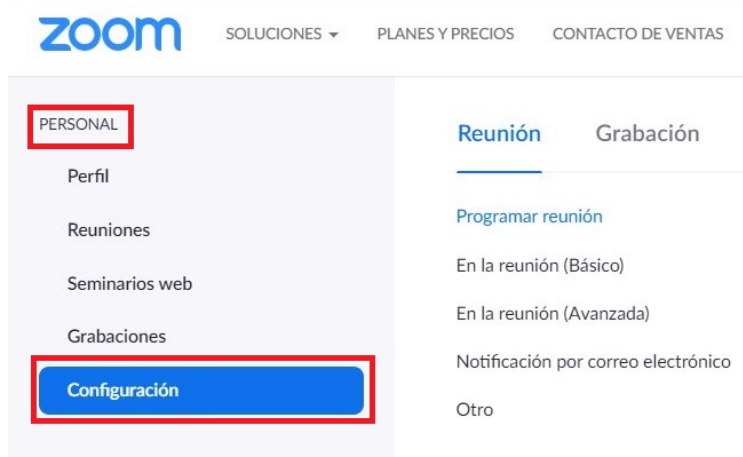
Siendo Zoom una herramienta de colaboración altamente configurable hay una serie de funcionalidades personalizables que, si bien otorgan un gran potencial en cuanto a funcionalidades, algunas de ellas podrían comprometer la seguridad o confidencialidad de su comunicación y datos.

Por tanto, se recomienda revisar exhaustivamente los apartados que se hallan en **PERSONAL->CONFIGURACIONES** y evaluar según los criterios de seguridad versus funcionalidades cada uno de los apartados para adecuar la configuración a los requerimientos de seguridad de la organización.

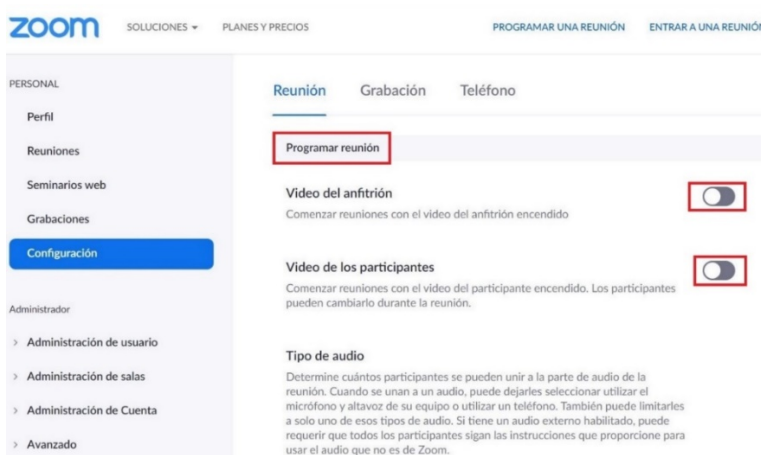
Algunos de estos puntos ya han sido tratados anteriormente en este documento desde el punto de vista de la generación de reuniones.

Los siguientes pantallazos muestran un ejemplo que prima la seguridad sobre las funcionalidades habiendo apartados que son susceptibles de ser variados para habilitar determinadas funcionalidades requeridas según las características de la sesión que se vaya a programar.

- En el apartado personal encontramos la configuración.



- Opciones “Programar reunión”: En color gris la opción esta activada.



- En color Azul la opción está habilitada

zoom SOLUCIONES ▾ PLANES Y PRECIOS PROGRAMAR UNA REUNIÓN ENTRAR A UNA REUNIÓN

> Administración de usuario
> Administración de salas
> Administración de Cuenta
> Avanzado

Asistir a una capacitación en vivo
Tutoriales en video
Base de conocimiento

Tipo de audio

Determine cuántos participantes se pueden unir a la parte de audio de la reunión. Cuando se unan a un audio, puede dejarles seleccionar utilizar el micrófono y altavoz de su equipo o utilizar un teléfono. También puede limitarles a solo uno de esos tipos de audio. Si tiene un audio externo habilitado, puede requerir que todos los participantes sigan las instrucciones que proporcione para usar el audio que no es de Zoom.

☒ Teléfono y audio de la computadora
☐ Teléfono
☐ Audio de la computadora

Unirse antes que el anfitrión ☐
Permitir que los participantes se unan a la reunión antes de que llegue el anfitrión

Usar ID de reunión personal (PMI) al programar una reunión ☐
Puede visitar [Sala de reunión personal](#) para cambiar sus ajustes de reunión personal.

zoom SOLUCIONES ▾ PLANES Y PRECIOS PROGRAMAR UNA REUNIÓN ENTRAR A UNA REUNIÓN

Usar ID de reunión personal (PMI) al iniciar una reunión instantánea ☐

Only authenticated users can join meetings from Web client ☒
The participants need to authenticate prior to joining meetings from web client

Solicitar contraseña al programar nuevas reuniones ☒
Se generará una contraseña al programar una reunión cuyos participantes requieran contraseña para unirse. Las reuniones con ID personal de reunión (PMI) no están incluidas.

Requerir una contraseña para las reuniones instantáneas ☒
Se generará una contraseña aleatoria al dar comienzo a una reunión instantánea

zoom SOLUCIONES ▾ PLANES Y PRECIOS PROGRAMAR UNA REUNIÓN ENTRAR A UNA REUNIÓN

Se requiere una contraseña para el ID de reunión personal (PMI) ☒
☐ Solo reuniones con la opción "Unirse antes que el anfitrión" habilitada
☒ Todas las reuniones que usan PMI

Incluir la contraseña en el enlace de la reunión para permitir el acceso con un solo clic. ☐
La contraseña de la reunión se cifrará y se integrará en el enlace de la reunión para permitir a los participantes unirse con tan solo un clic sin tener que introducir la contraseña.

Los participantes que se unan por teléfono precisan contraseña ☒
Aquellos participantes que se unan por teléfono precisarán de una contraseña numérica si su reunión está protegida por contraseña. En el caso de las reuniones con contraseña alfanumérica, se generará una versión numérica.

Silenciar a los participantes una vez que entren ☒
Silenciar automáticamente a todos los participantes cuando se unan a la reunión. El anfitrión controla si los participantes pueden reactivar el sonido por ellos mismos. ☒


- Configuración de Reunión Básico.


IMPORTANTE: la encriptación obligatoria para equipos de video de sala.


Recordatorio de reunión próxima Recibir una notificación de escritorio de las próximas reuniones. El horario del recordatorio se puede configurar en el Cliente de escritorio de Zoom. [?]	<input checked="" type="checkbox"/>
En la reunión (Básico)	
Requerir encriptación para los puntos de destino de terceros (H323/SIP) Zoom requiere la encriptación de todos los datos que circulan entre la nube de Zoom, el cliente de Zoom y la Zoom Room. Se requiere la encriptación de los puntos de destino de terceros (H323/SIP).	<input checked="" type="checkbox"/>
Chat Permitir que los participantes de la reunión envíen un mensaje visible para todos los participantes <input checked="" type="checkbox"/> Impedir a los participantes guardar el chat [?]	<input checked="" type="checkbox"/>
Chat privado Permitir que los participantes de la reunión envíen un mensaje privado 1:1 a otro participante.	<input type="checkbox"/>
Guardar automáticamente chats Guardar automáticamente todos los chats de la reunión para que los anfitriones no tengan que guardar en forma manual el texto del chat después de los inicios de las reuniones.	<input type="checkbox"/>
Reproducir sonido cuando los participantes se unen o salen Reproducir sonido cuando los participantes se unen o salen <input checked="" type="radio"/> Oído por el anfitrión y todos los participantes <input type="radio"/> Escuchado solo por el anfitrión Cuando cada participante entra por teléfono <input checked="" type="checkbox"/> Grabar and reproducir su propia voz	<input checked="" type="checkbox"/>
Uso compartido de la pantalla Permitir que el anfitrión y los participantes compartan su pantalla o contenido durante las reuniones ¿Quién puede compartir? <input checked="" type="radio"/> Solo el anfitrión <input type="radio"/> Todos los participantes ¿Quién puede comenzar a compartir cuando otro está compartiendo? <input checked="" type="radio"/> Solo el anfitrión <input type="radio"/> Todos los participantes	<input checked="" type="checkbox"/>
Desactivar la compartición de escritorio/pantalla para los usuarios Desactivar la compartición de pantalla o escritorio en una reunión y solo permitir la compartición de determinadas aplicaciones. [?]	<input type="checkbox"/>
Anotación Permitir que los participantes usen herramientas de anotación para agregar información a las pantallas compartidas [?]	<input checked="" type="checkbox"/>
Pizarra Permitir a los participantes compartir una pizarra que incluye herramientas de	<input checked="" type="checkbox"/>


- Configuración de Reunión Avanzada.


En la reunión (Avanzada)

Sala para grupos 
Permitir que el anfitrión divida los participantes en salas separadas más pequeñas


Esta opción se modificó porque 
• Soporte remoto se ha actualizado.


Soporte remoto 
Permitir que el anfitrión proporcione asistencia remota 1:1 a otro participante



Subtitulado 
Permitir que el anfitrión escriba subtítulos, o asignar un dispositivo de un participante o de terceros para agregar subtítulos


Guardar subtítulos 
Permite a los participantes guardar subtítulos o transcripciones

- La nueva opción de “Fondo virtual” es aconsejable para distorsionar la vista del entorno de usuario.

Control de la cámara más lejana 
Permitir a otro usuario tomar el control de su cámara durante una reunión

Fondo virtual 
Permitir a los usuarios reemplazar su fondo con cualquier imagen seleccionada. Seleccionar o cargar una imagen en la configuración de la aplicación de escritorio de Zoom.

Identificar a los participantes invitados en la reunión/el seminario web 
Los participantes que pertenezcan a su cuenta pueden ver si hay un invitado (alguien que no pertenece a su cuenta) participando en la reunión/el seminario web. La lista de participantes indica qué asistentes son invitados. Los invitados no ven que aparecen como invitados en la lista. 

Grupo de respuesta automática en el chat 
Permitir que los usuarios vean y agreguen contactos al 'grupo de respuesta automática' en la lista de contactos en el chat. Cualquier llamada de los miembros de este grupo será respondida automáticamente.

Mostrar solamente correo electrónico predeterminado al enviar invitaciones por correo electrónico



Permitir que los usuarios inviten a participantes por e-mail solamente mediante el programa predeterminado de e-mail seleccionado en su computadora

Uso del correo electrónico en formato HTML para el plugin de Outlook



Usar el formato HTML en lugar de texto plano para las invitaciones a reuniones programadas con el complemento de Outlook

Permitir que los usuarios seleccionen audio estéreo en la configuración del cliente



Permitir que los usuarios seleccionen el audio en estéreo durante una reunión

Permitir que los usuarios seleccionen sonido en la configuración del cliente



Permitir que los usuarios seleccionen el sonido original durante una reunión

- La opción de “Participar desde un navegador web”, implica una menor compatibilidad de funcionalidades y es más insegura que la opción de instalar el cliente pesado, pero es una opción ineludible habilitarla si los participantes no tienen permisos de instalación de software en sus dispositivos.

Sala de espera



Los participantes no pueden unirse a una reunión hasta que un anfitrión los admita individualmente desde la sala de espera. Si la sala de espera está habilitada, se desactiva automáticamente la opción para que los participantes se unan a la reunión antes de que llegue el anfitrión.

Mostrar un enlace “Participar desde el navegador”



Permita a los participantes evitar el proceso de descarga de la aplicación de Zoom y participar en una reunión directamente desde su navegador. Esta es una solución para los participantes que no pueden descargar, instalar o ejecutar aplicaciones. Tenga en cuenta que la experiencia de la reunión desde el navegador es limitada

- Notificación por correo.
- Difuminar la instantánea en iOS, evita mostrar información sensible de las aplicaciones abiertas en iOS.

Notificación por correo electrónico

Cuando los asistentes se unan a la reunión antes que el anfitrión

Informe al anfitrión cuando los participantes se unen a la reunión antes que él



Al cancelar una reunión

Informe al anfitrión y a los participantes cuando se cancela la reunión



Otro

Difuminar la instantánea en el conmutador de tarea iOS

Active esta opción para ocultar información potencialmente confidencial de la instantánea de la ventana principal de Zoom. Esta instantánea se muestra como la pantalla de vista previa en el selector de tareas de iOS cuando hay varias aplicaciones abiertas.



- Opciones de la pestaña de Grabación.

Reunión

Grabación

Teléfono

Grabación

Grabación local

Permitir que los anfitriones y participantes graben la reunión en un archivo local



☒ Hosts can give participants the permission to record locally

Grabación automática

Grabar reuniones automáticamente cuando comienzan



Consentimiento de grabación

Pida a los participantes que den su consentimiento para grabarles cuando se inicie la grabación. 



☒ Ask participants for consent when a recording starts

☒ Ask host to confirm before starting a recording

Notificaciones de sonido cada vez que realizar/detener la grabación

Reproducir mensajes de notificación a participantes que se unen al audio de la reunión. Estos mensajes se reproducen cada vez que la grabación da comienzo o se reinicia, informando a los participantes de que la reunión se está grabando. Si los participantes se unen al audio a través del teléfono, incluso si esta opción está inhabilitada, los usuarios escucharán un mensaje de notificación por reunión.



- Opciones de Teléfono.

- La opción de ocultar números de teléfono es altamente recomendable.

Reunión Grabación **Teléfono**

Mostrar enlace de números internacionales en el e-mail de invitación

Mostrar el enlace de los números de discado por defecto internacional de Zoom en las invitaciones por e-mail



Llamada con cargo

Incluir los números seleccionados en el cliente Zoom y la invitación por correo electrónico a través del enlace de los números internacionales. Los participantes pueden unirse a las reuniones a través de estos números



Solo los administradores de TI pueden realizar cambios en este parámetro



Ocultar número de teléfono en la lista de participantes

Los números de teléfono de los usuarios que llamen en una reunión se ocultarán en la lista de participantes. Por ejemplo: 888****666



Número de acceso global de los países/regiones

Haga clic en el ícono Editar para seleccionar países/regiones que frecuentemente tienen participantes que necesitan llamar a las reuniones. Los números de teléfono para marcar de estas ubicaciones aparecen en la invitación por correo electrónico y los participantes pueden usarlos para marcar desde tales ubicaciones.

4 CONCLUSIONES

Con la configuración adecuada y las salvaguardias apropiadas habilitadas para proteger las reuniones - como contraseñas, salas de espera y bloqueo de reuniones - **Zoom** ofrece un entorno de reunión virtual seguro y protegido, con independencia de que este software se encuentre actualmente en el objetivo de los ciberatacantes dada su reciente popularidad.

Zoom está publicando parches de seguridad, ha reforzado el equipo de seguridad, pretende continuar mejorando el producto⁹ y está organizando *webinar* semanales¹⁰ para proporcionar actualizaciones sobre privacidad y seguridad a la comunidad.

En este sentido, si se realiza una **adecuada implementación**¹¹, respetan unos **mínimos requisitos de seguridad en la configuración**¹² y llevan a cabo **buenas prácticas**¹³ se puede considerar Zoom una opción a tener en cuenta en escenarios de teletrabajo como los actuales marcados por la crisis del COVID-19 donde no se maneje información sensible.

En definitiva, ante las reacciones en contra de Zoom durante estos días, y de acuerdo con el párrafo anterior **se considera asumible el riesgo de usar Zoom para reuniones que no sean muy sensibles en su contenido, clases escolares y situaciones fuera de la oficina sobre asuntos rutinarios.**

⁹ <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>

¹⁰ https://zoom.us/webinar/register/WN_9jdr63uuRuSRBX-yEJ2zVQ?zcid=1231

¹¹ <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>

¹² <https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls>

¹³ <https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/206-ciberconsejos-videollamada>



#CiberCOVID19

Recomendaciones de ciberseguridad para videollamadas y reuniones virtuales.

Descarga únicamente aplicaciones de *markets* oficiales, como Google Play o Apple Store, o de la web del proveedor (Microsoft, Google, Cisco, etc.).

Mantén actualizadas las aplicaciones de videollamada que uses.

En la medida de lo posible, evita pinchar en enlaces que se compartan en el chat de la sesión, sobre todo si no conoces a la persona que lo ha compartido.

Programa videollamadas con el número exacto de participantes. Cuando todos los usuarios entren en la sesión, cierra el acceso a nuevos participantes.

Todos los usuarios que accedan a la reunión deberán hacerlo con contraseña. En aplicaciones públicas, regístrate con contraseñas que no utilices en otros servicios y no compartas públicamente el ID de la reunión.

El moderador de la videollamada gestiona si esta puede ser grabada. Si está siendo grabada, debe mostrarse a todos los usuarios un indicador visual y sonoro.

El moderador de la reunión debe poder gestionar la conexión de los participantes, cerrar micrófonos, deshabilitar contenidos o señal de video. Los participantes no deberían acceder hasta que no se conecte el moderador.

Considera las videollamadas un canal de comunicación inseguro, no des datos sensibles como contraseñas.

Configura la sesión para que un indicador visual o sonoro avise de la entrada o salida de usuarios y desactiva la respuesta automática a llamadas entrantes. Sal de la sesión de la aplicación si sabes que no va a llamar nadie.

No aceptes llamadas/chats de usuarios que no conozcas. Todos los usuarios deben de entrar con un nombre/nick reconocible para el administrador/moderador de la llamada en las conferencias privadas.