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

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 ciberdelincuentes[1] 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 blog[2] 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 engañosa[3]. 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 iOS[4] (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 privacidad[5] 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

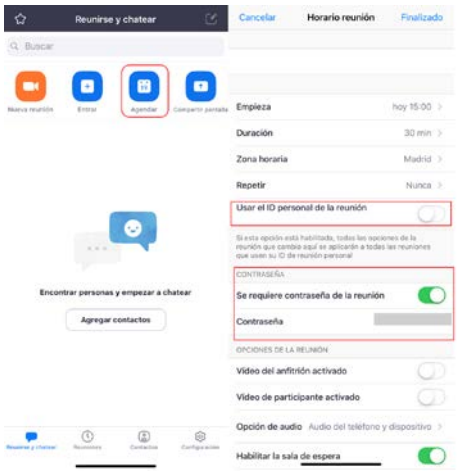
La mejor manera de evitar interrupciones en las reuniones es no compartir las identificaciones de las reuniones de Zoom excepto con los participantes previstos. Además, se puede solicitar a los participantes que utilicen una contraseña para iniciar sesión en la reunión.

3.1 Agendar una reunión

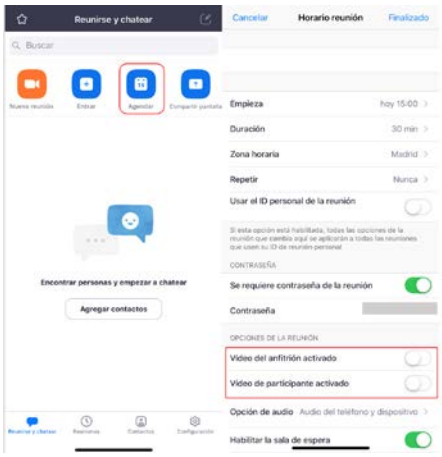
Zoom permite dejar programada una reunión para una hora y fecha concretas. Si usted es el organizador de la reunión, a la hora de agendarla debe tener en cuenta las siguientes recomendaciones:

[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/

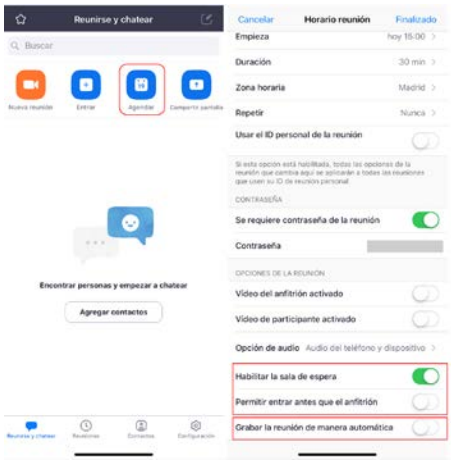
- Genere un ID de reunión aleatorio y requiera contraseña para entrar en la reunión. Si pulsa sobre la opción “Contraseña”, puede cambiar la contraseña por defecto.



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



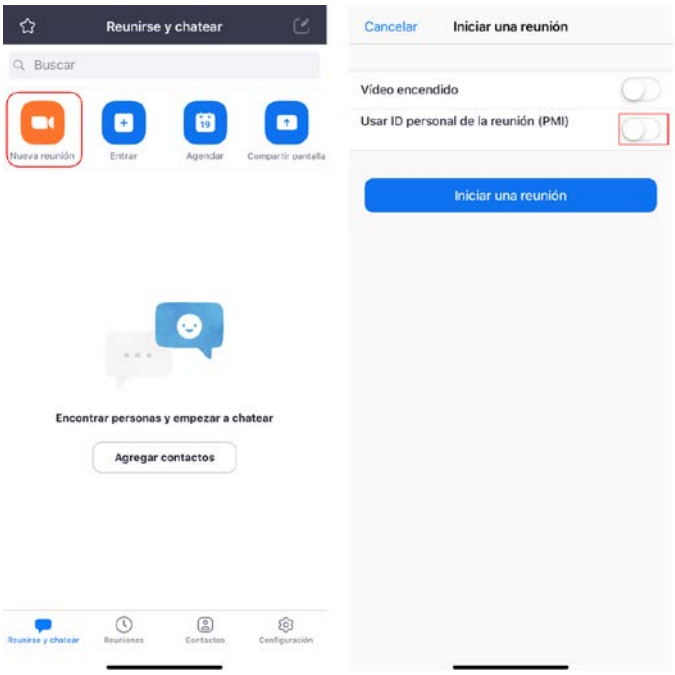
- Habilite la sala de espera y no permita que los invitados entren a la reunión antes que el anfitrión (organizador) se una a la reunión. Del mismo modo, si no es estrictamente necesario grabar la reunión, deshabilite esta opción antes de iniciar la reunión.



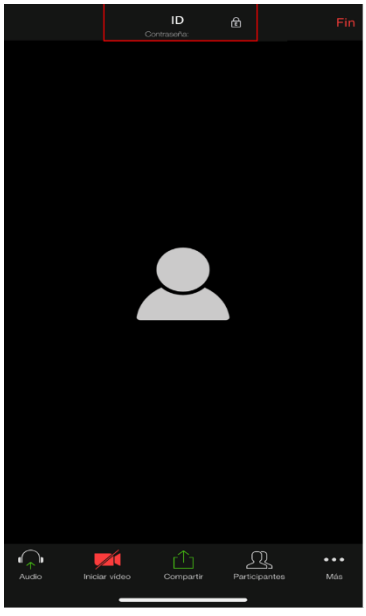
3.2 Crear una nueva reunión desde el menú principal

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:

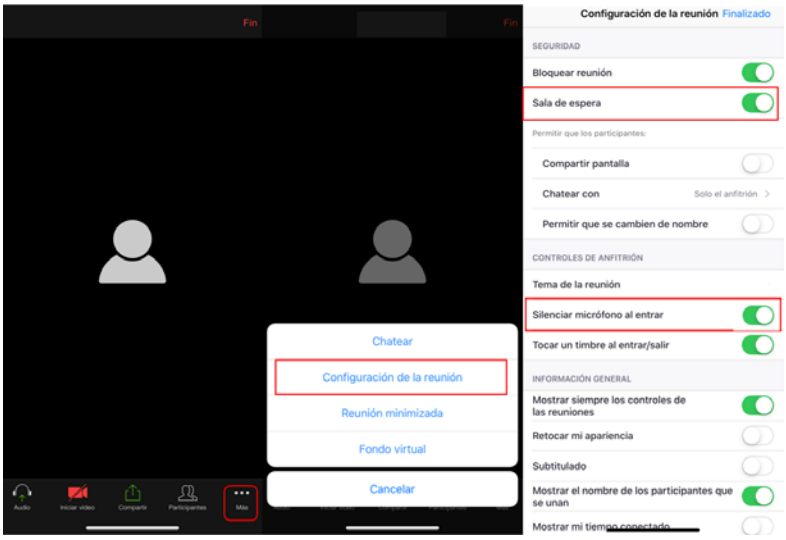
- Una vez pulse sobre “Nueva reunión”, genere una ID de reunión aleatoria.



- 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.

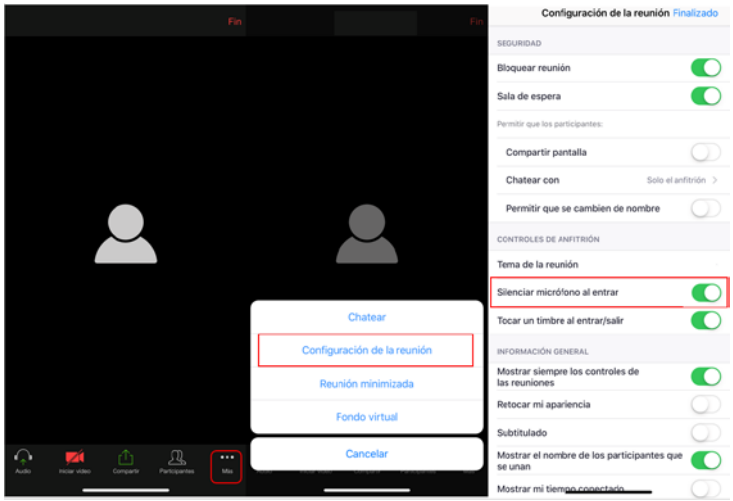


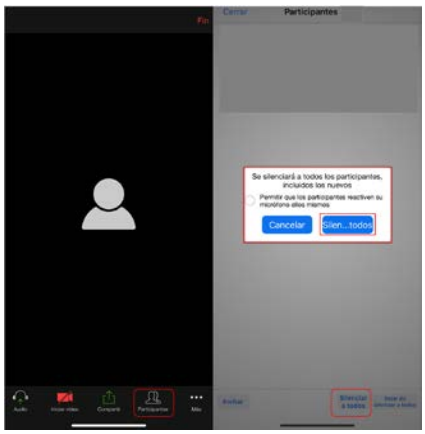
- Habilite la sala de espera y silencie a los participantes al entrar.



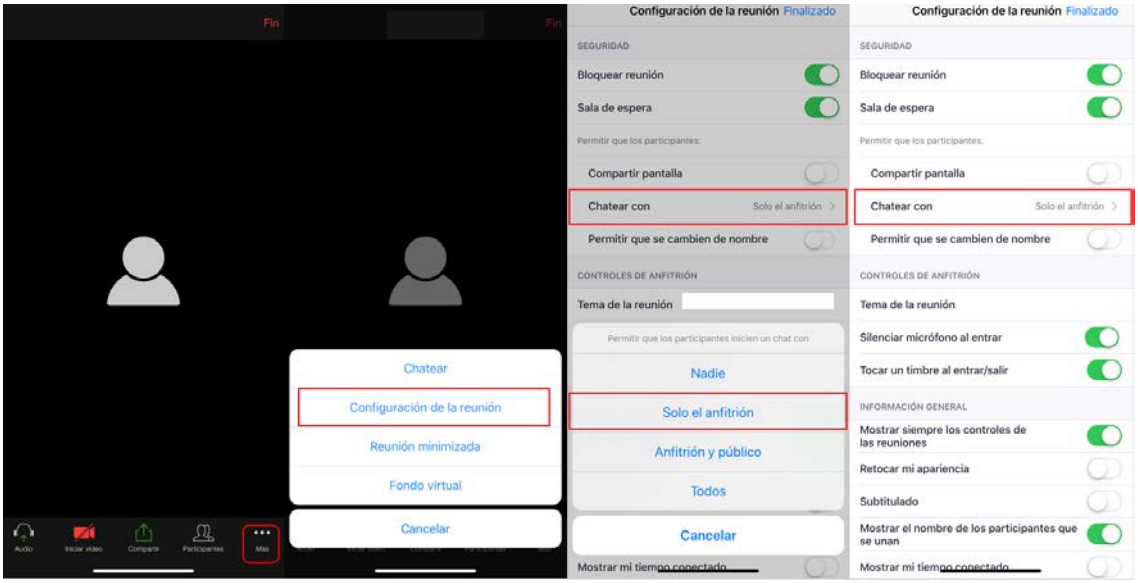
Además, configure la reunión para que:

- 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.

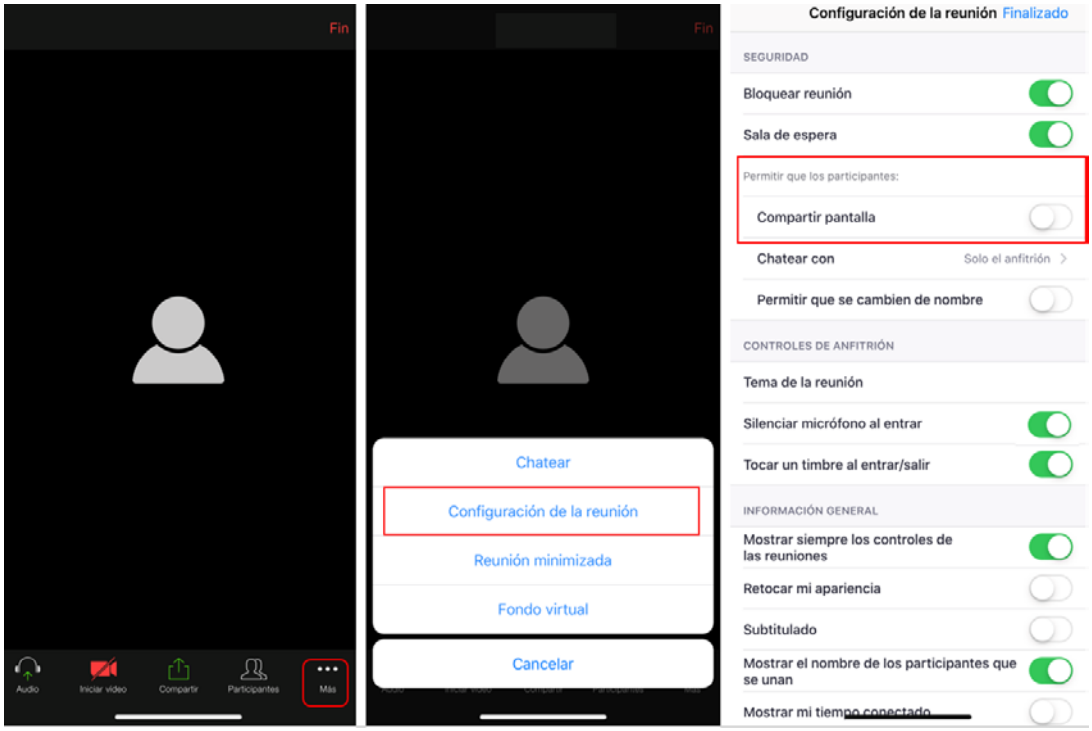




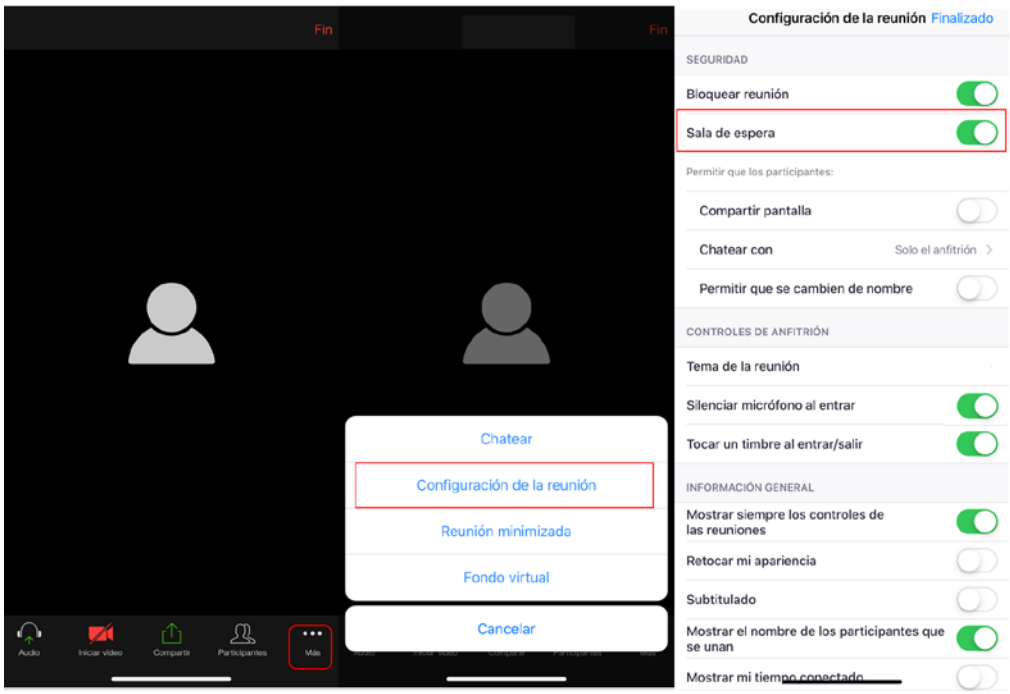
- Desactive el chat privado entre los asistentes.



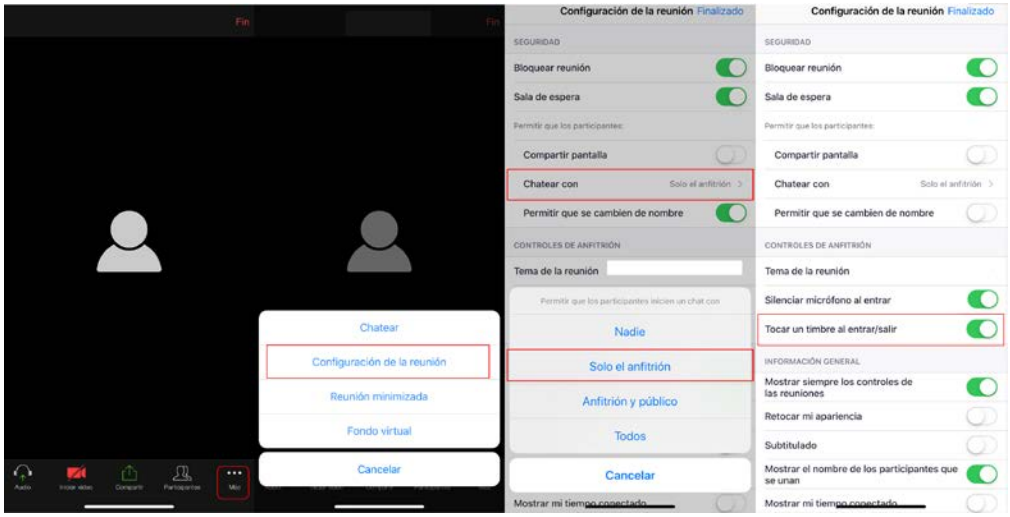
- Desactive el guardado automático de los chats.
- Establezca el uso compartido de pantalla solo para el anfitrión.



- 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.

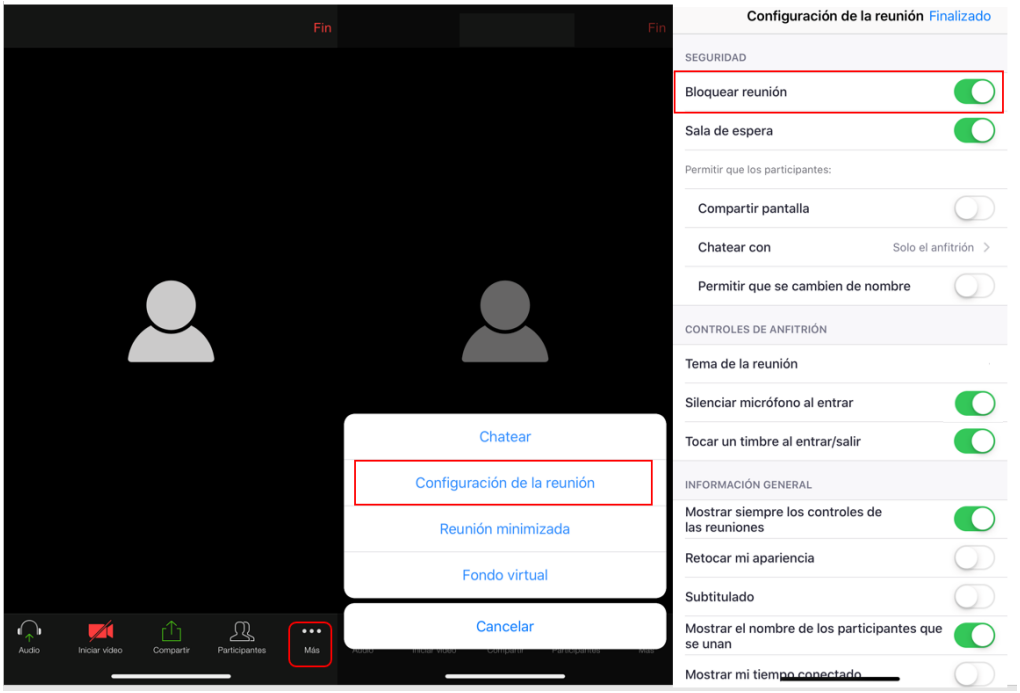


Por otra parte, depende del anfitrión decidir si se graba una reunión, y Zoom ofrece a los clientes de pago la opción de almacenar grabaciones en los propios servidores de Zoom.

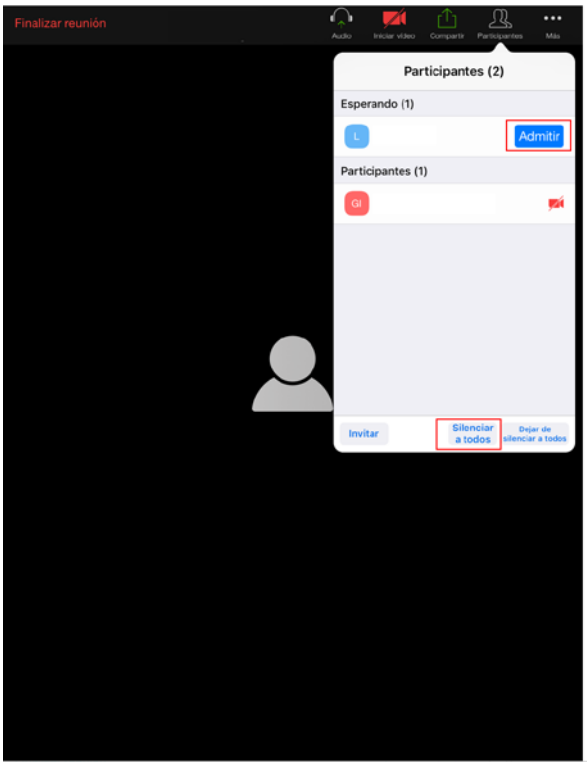
Asimismo, depende del moderador cambiar el nombre del archivo de grabación. Si organiza una reunión de Zoom y decide grabarla, asegúrese de cambiar el nombre de archivo predeterminado una vez que haya terminado. Si decide subir las grabaciones de la reunión a cualquier otro lugar que no sea la nube de 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:

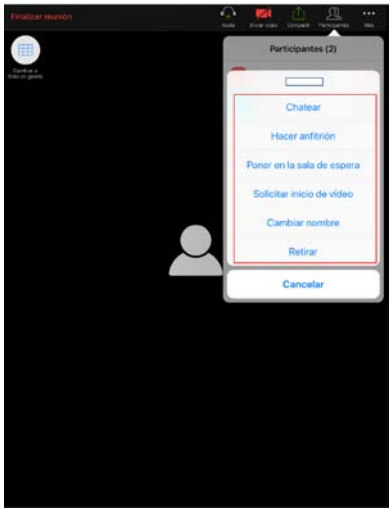
- Puede cerrar la reunión para que no se unan nuevos participantes.



- 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.



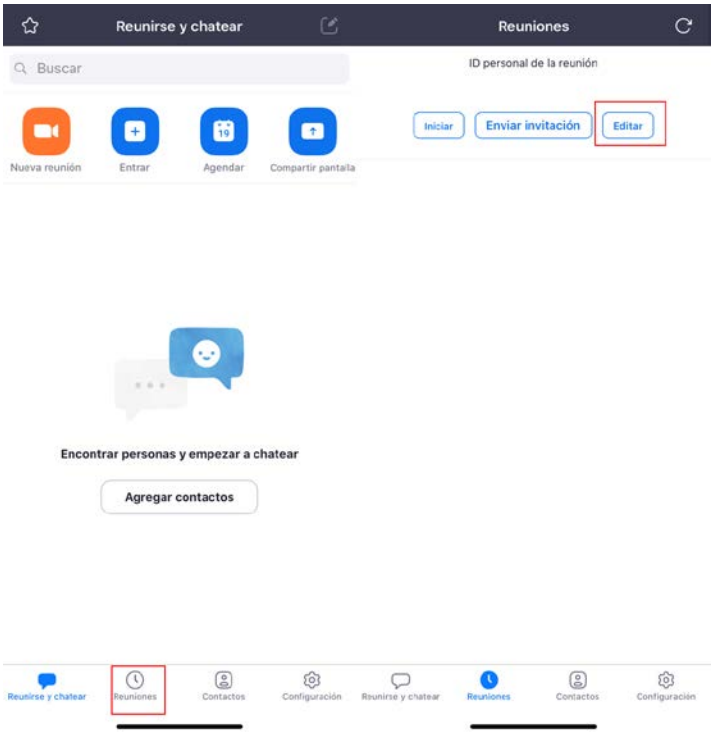
- Una vez aceptados los invitados, si pulsa sobre un invitado concreto, puede realizar diferentes acciones. Si pulsa en "**Retirar**" eliminará de la reunión al invitado.



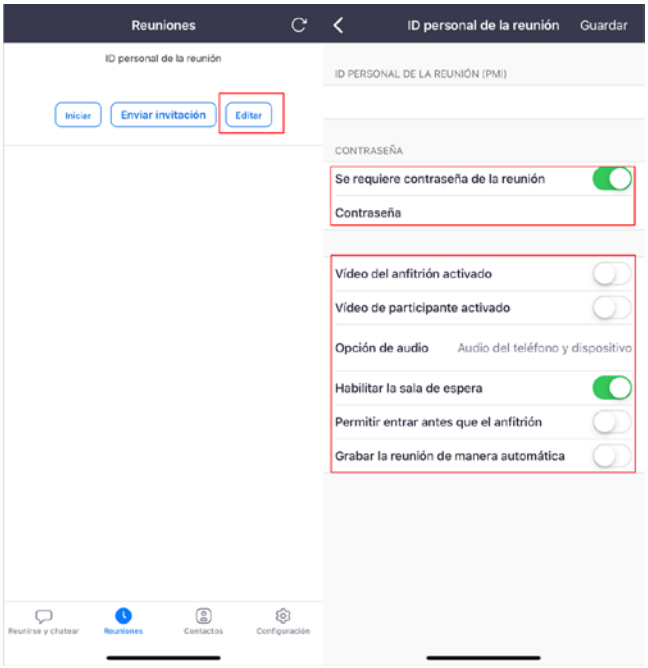
3.3 Crear una nueva reunión desde el menú secundario

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 guía[6] del administrador sobre cómo configurar un aula virtual.
- Estableció una guía[7] 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

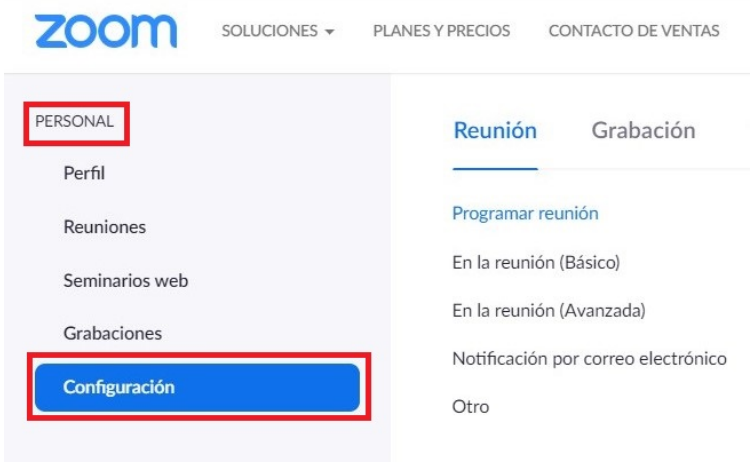
Siendo Zoom una herramienta de colaboración altamente configurable hay una serie de funcionalidades personalizables que, si bien otorgan un gran potencial en cuanto a funcionalidades, algunas de ellas podrían comprometer la seguridad o confidencialidad de su comunicación y datos.

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.

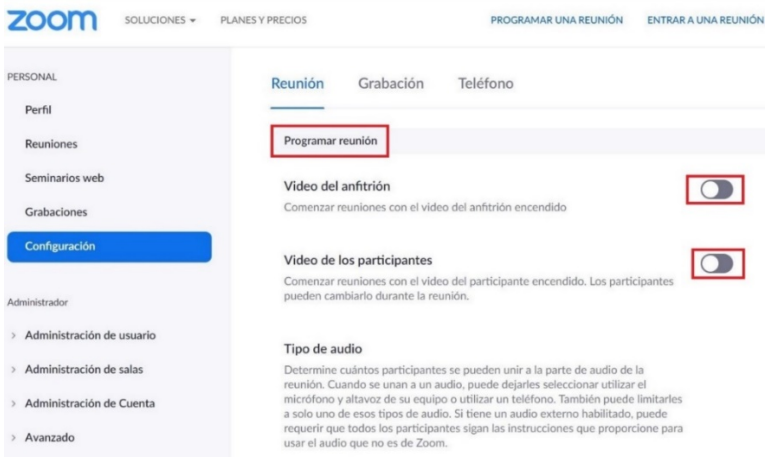
Algunos de estos puntos ya han sido tratados anteriormente en este documento desde el punto de vista de la generación de reuniones.

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.

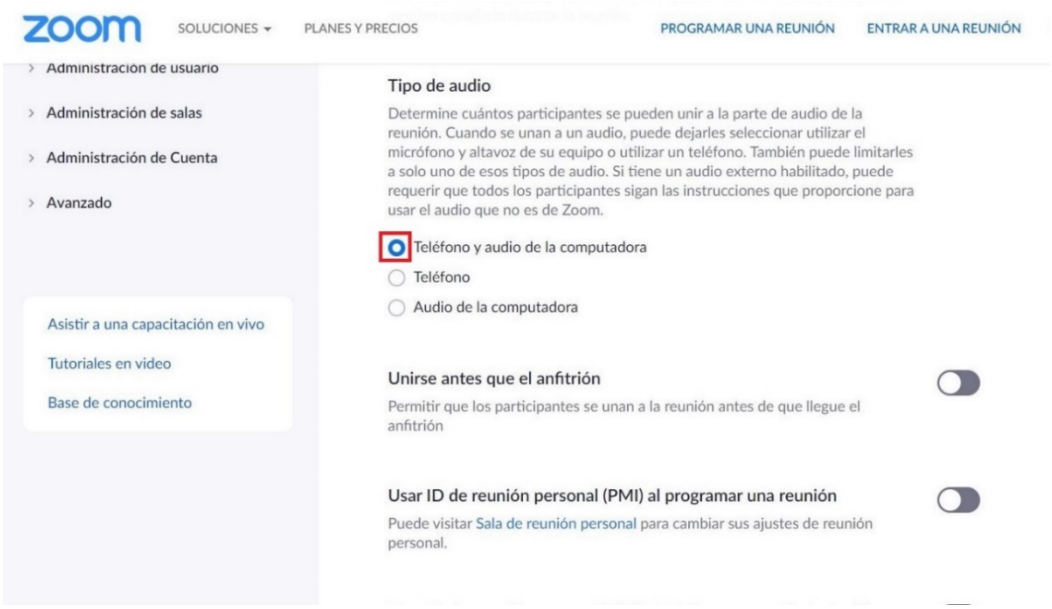
- En el apartado personal encontramos la configuración.

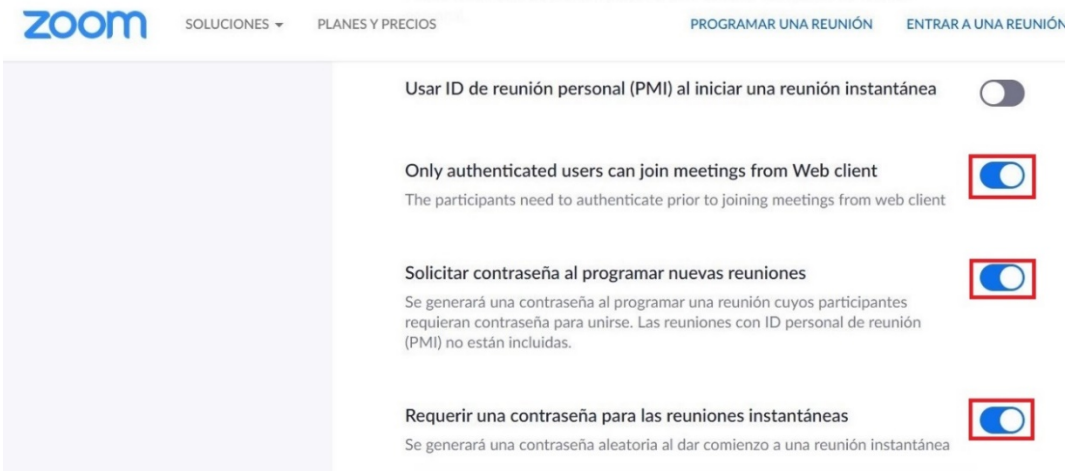


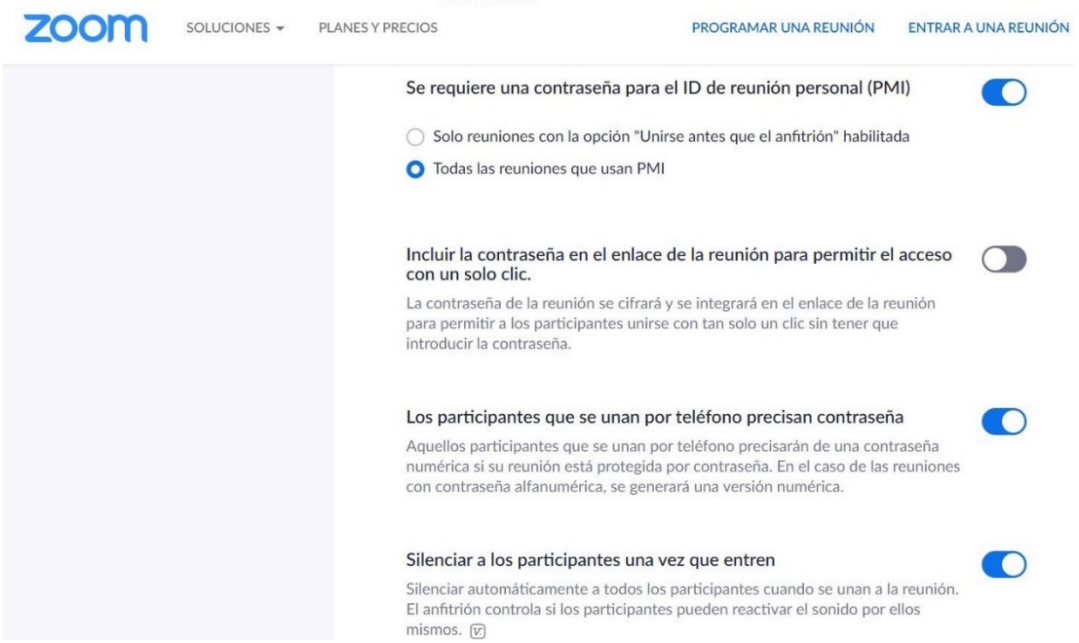
- Opciones “Programar reunión”: En color gris la opción esta activada.



- En color Azul la opción está habilitada

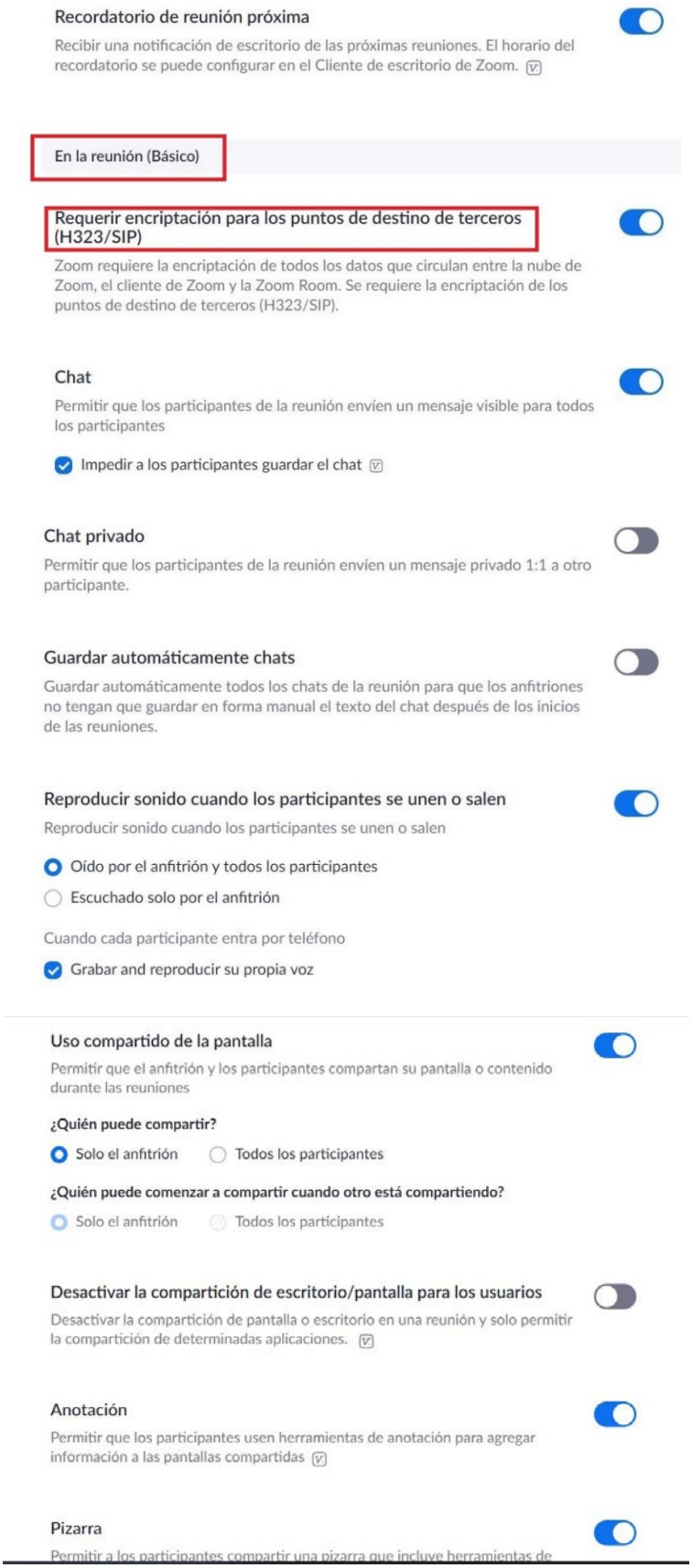




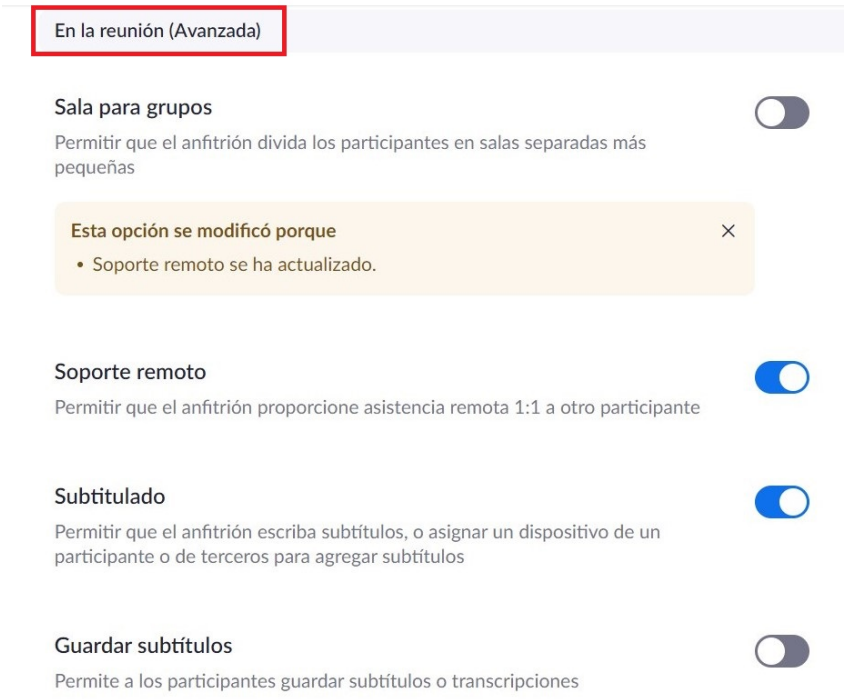


- Configuración de Reunión Básico.

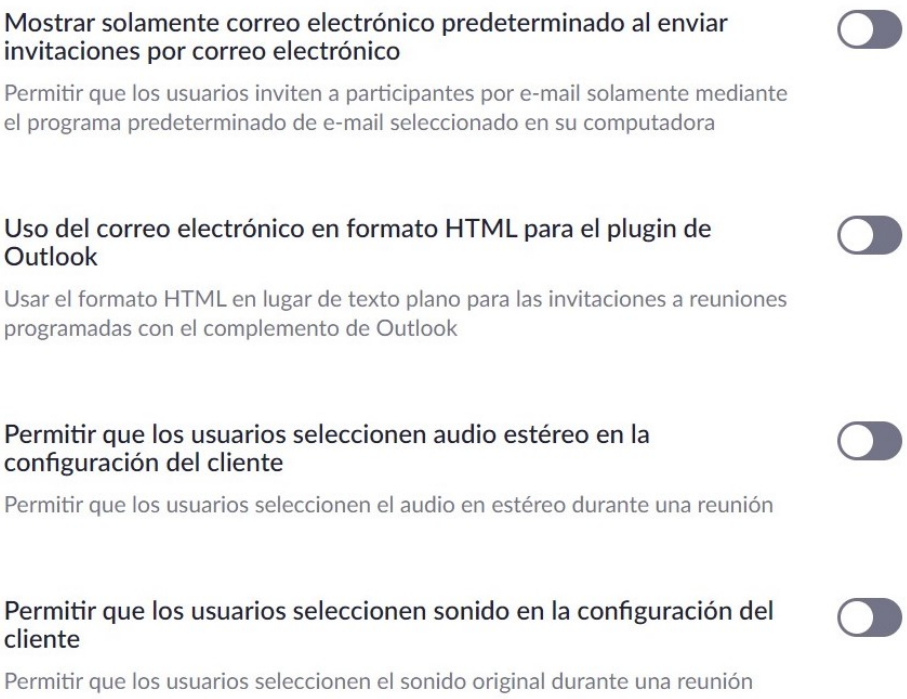
  IMPORTANTE: la encriptación obligatoria para equipos de video de sala.



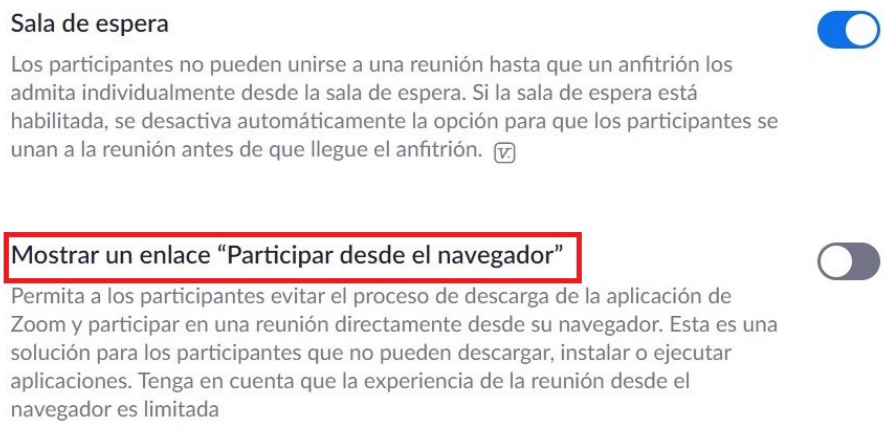
- Configuración de Reunión Avanzada.



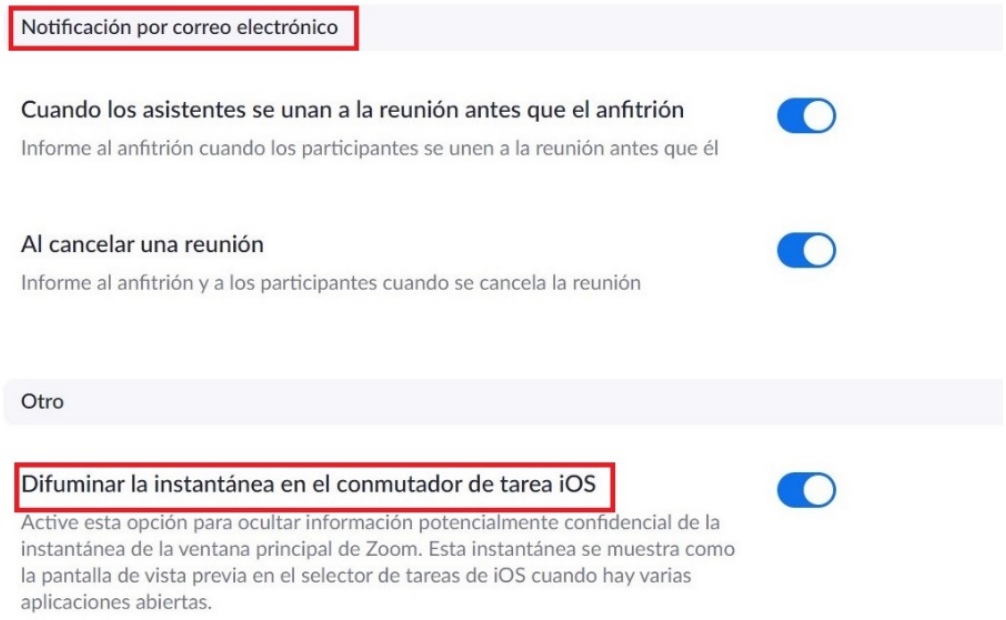
- La nueva opción de “Fondo virtual” es aconsejable para distorsionar la vista del entorno de usuario.



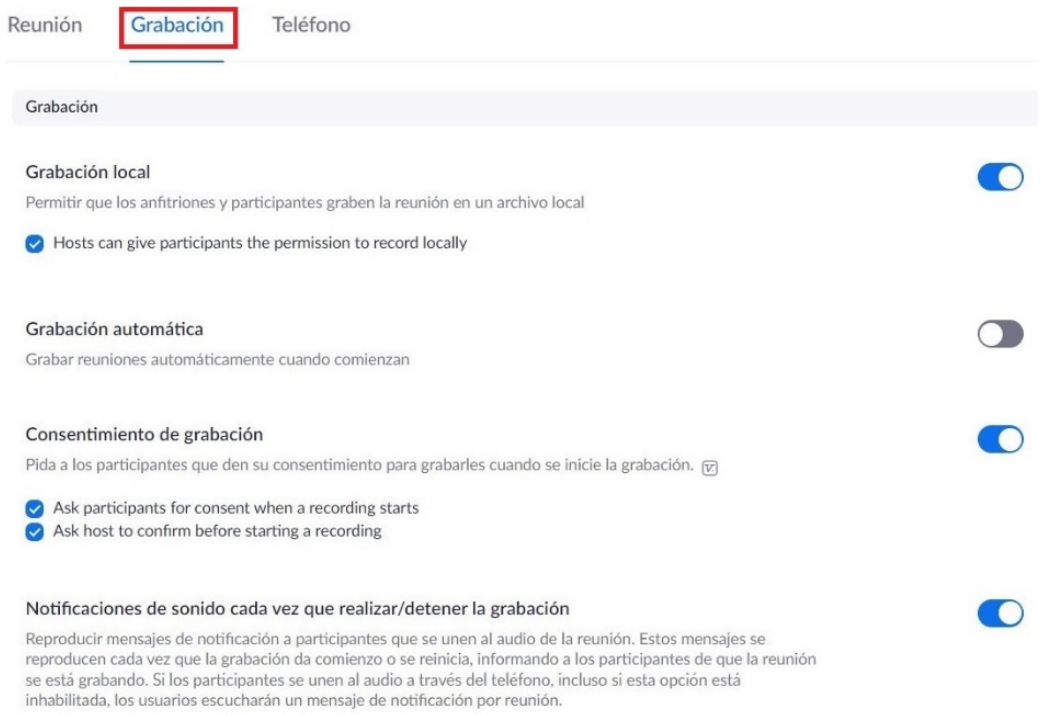
- La opción de "Participar desde un navegador web", implica una menor compatibilidad de funcionalidades y es más insegura que la opción de instalar el cliente pesado, pero es una opción ineludible habilitarla si los participantes no tienen permisos de instalación de software en sus dispositivos.



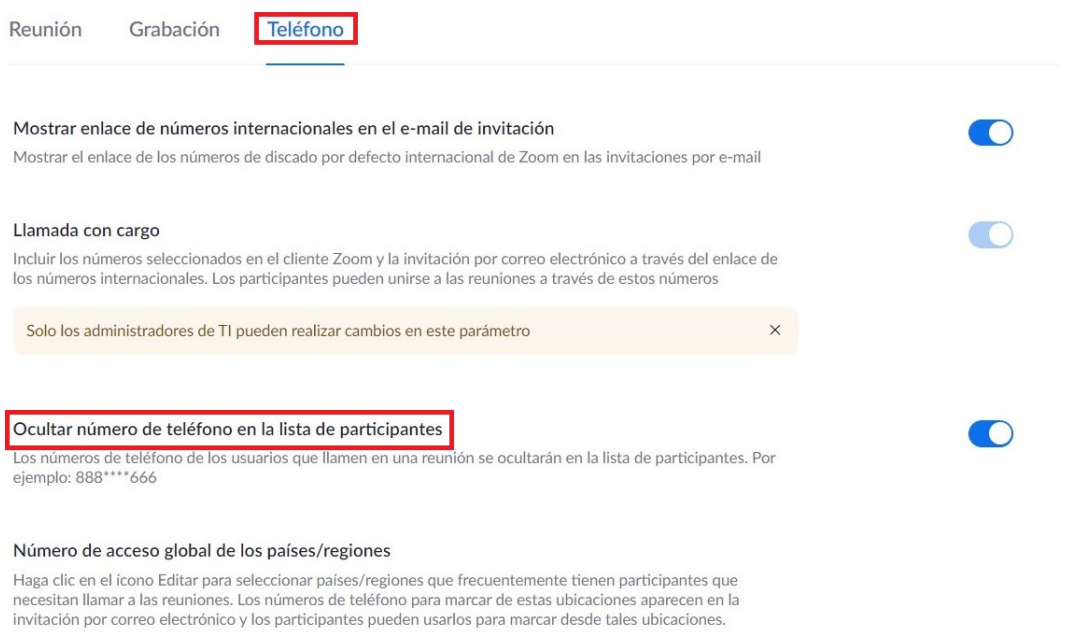
- Notificación por correo.
- Difuminar la instantánea en iOS, evita mostrar información sensible de las aplicaciones abiertas en iOS.



- Opciones de la pestaña de Grabación.



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



4 CONCLUSIONES

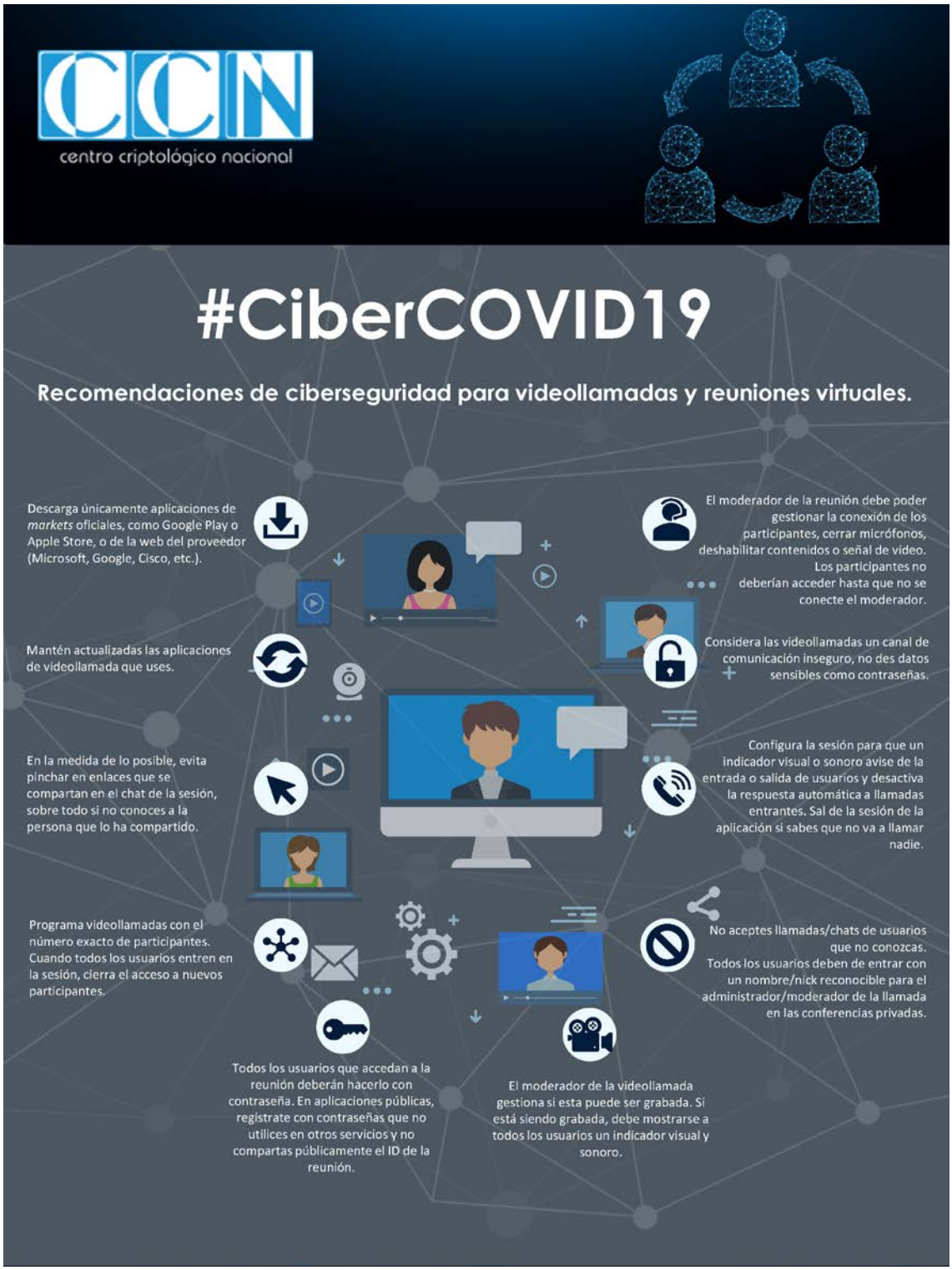
Con la configuración adecuada y las salvaguardias apropiadas habilitadas para proteger las reuniones - como contraseñas, salas de espera y bloqueo de reuniones - **Zoom** ofrece un entorno de reunión virtual seguro y protegido, con independencia de que este software se encuentre actualmente en el objetivo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

Zoom está publicando parches de seguridad, ha reforzado el equipo de seguridad, pretende continuar mejorando el producto[9] y está organizando *webinar* semanales[10] 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


CCN
centro criptológico nacional
#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.
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.
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.
Considera las videollamadas un canal de comunicación inseguro, no des datos sensibles como contraseñas.
El moderador de la reunión debe poder gestionar la conexión de los participantes, cerrar micrófonos, deshabilitar contenidos o señal de vídeo. Los participantes no deberían acceder hasta que no se conecte el moderador.