

# The use of Zoom and its implications for security and privacy. Recommendations and good practices

**Abstract:** in the last few days, the Zoom application has been questioned due to privacy and security issues. The following is an analysis of the reported deficiencies and a set of recommendations and good practices for its use.

## Content:

1	CONTEXT .....	1
2	ZOOM ANALYSIS .....	1
3	RECOMMENDATIONS AND GOOD PRACTICES .....	5
3.1	Schedule a meeting .....	5
3.2	Creating a new meeting from the main menu .....	6
3.3	Creating a new meeting from the secondary menu .....	11
3.4	Recommendations for the education sector .....	13
3.5	Recommendations in general configuration .....	13
4	CONCLUSIONS .....	19

## 1 CONTEXT

The evolution of the COVID-19 pandemic and the associated confinement of citizens, social distancing and quarantine has brought with it the widespread use of video conferencing and chat applications such as Zoom, WebEx, Houseparty, Google Meet or Microsoft Teams.

Cyber-attackers are taking advantage of the opportunities associated with the fear surrounding the pandemic, widespread teleworking, difficulties in patching remotely connected endpoints and the increasing surface area of exposure derived from allowing more fluid operations.

In this context, poorly protected video conferencing sessions and applications are a major vector of attack.

## 2 ZOOM ANALYSIS

Zoom is a video conferencing application with real-time messaging and content sharing that is easy to set up and use, allowing meetings with up to 100 participants and free of charge. Design decisions aimed at providing greater usability, have allowed for unwanted performances.

The Zoom application is being challenged by privacy and security issues in recent days.

- If a host disables waiting rooms and passwords, anyone can join a Zoom meeting if they know the meeting ID. Additionally, if a host broadly shares their meeting

link or ID and password broadly through a public forum such as social media, unwanted guests may join with the intention of disrupting the meeting. These meeting disruptors often use screen sharing to post shocking or inappropriate content or make disturbing sounds.

Zoom has turned on "waiting rooms" and passwords by default and set screen sharing to "Host Only" by default for most accounts to avoid meeting disruptions, and added features to help hosts more easily access in-meeting security controls, including controlling screen sharing, removing and reporting participants, and locking meetings, among other actions.

For larger, public meetings, Zoom offers a Webinar product that allows you to broadcast a Zoom meeting to up to 10,000 view-only attendees. In webinars, only the hosts and pre-selected panelists can appear on video, as well as share content. Attendees do not appear on video, cannot screen share, and cannot speak unless the host chooses to unmute them. This is a safer and more appropriate format to host public meetings in order to avoid meeting disruptors.

- Historically, to minimize the number of clicks from the download of the application to its execution in macOS, the pre-installation checks are incorrectly used by displaying a misleading password message. This was resolved in April.
- Historically, potential leakage of e-mail addresses, photos of users and unjustified calls due to improper settings would automatically add people to a user's contact lists if they both log in with an e-mail address belonging to the same domain. This was resolved in April.
- Historically, Zoom used AES-256 in ECB mode for encrypting communications, which is not advisable since the encrypted information retains possible patterns present in the data in clear, making it easy for a cyber-attacker to break the encryption to capture the traffic. On May 30th, Zoom enabled AES 256-bit GCM encryption for all meetings.

In addition, Zoom encrypts communications, but not content, so MITM (man in the middle) attacks that accept connection with invalid certificates could allow an attacker to access the information. Zoom does plan to offer end-to-end encryption in the very near future. On May 7, Zoom announced the acquisition of Keybase, which will accelerate Zoom's plan to build end-to-end encryption that can reach current Zoom scalability. Following that, Zoom released a draft cryptographic design for an end-to-end-encrypted video communications offering on GitHub on May 22 and after soliciting feedback from the public, the company will publish engineering milestones.

- Due to a temporary misconfiguration in Zoom's global data center routing – which, under normal circumstances, is designed to maintain geo-fencing around China for both primary and secondary data centers – certain meetings may have been able

to connect to Zoom servers in China under extremely limited circumstances, where the authorities in this country with different data protection legislation could oblige service operators to deliver information. This was resolved in April and Zoom has since introduced a feature that gives users the ability to control which data center regions their account can use for its real-time meeting traffic – giving them even more comfort that their data is not being routed through mainland China.

- Although Zoom has integrated anti-sabotage mechanisms, these can be disabled or even replaced by a malicious version that hijacks the application. This is because cybercriminals are taking advantage of the Zoom application boom and the increase in the number of downloads of the app to register domains that offer an executable installer containing malware. Pages created by cybercriminals would distribute the malware by posing as the official page of the application to trick the user. Zoom users should be cautious with emails or links from unknown senders, taking care to only click on authentic links or open attachments from known and trusted service providers. It is strongly recommended to only download the application through Zoom's legitimate distribution channels, including Zoom's website, the Google Play Store and the Apple App Store.

In this scenario, several institutions, organizations and agencies previously advised against the use of Zoom. However, Zoom has actively and quickly addressed privacy and security concerns as they were raised. On March 29, Zoom updated its privacy policy to make it more clear, explicit, and transparent. On April 1, Zoom announced a 90-day plan to double down on its commitment to security and is proactively working to better identify, address, and fix issues. Among other actions, Zoom has:

- Enacted feature freeze and shifting all engineering resources to focus on trust, safety, and privacy.
- Launched a comprehensive review with third-party experts and representative users to understand and ensure the security of all of Zoom's new use cases.
- Begun conducting a series of simultaneous white box penetration tests to further identify and address issues.
- Enhanced its current bug bounty program.
- Launched a CISO council in partnership with leading CISOs from across the industry to facilitate an ongoing dialogue regarding security and privacy best practices.

Furthermore, Zoom is currently working on an end-to-end encryption video communications offering, and the company has plans to publish a transparency report as part of the 90-day plan.

- On March 20, Zoom posted a blog<sup>1</sup> entry to help users prevent meeting disruption incidents, highlighting security features such as waiting rooms, passwords, mute controls and limiting screen sharing.
- Zoom also acknowledged that its claim of end-to-end encryption support is misleading<sup>2</sup>. Zoom clarified that in a meeting where all of the participants are using the Zoom client, and the meeting is not being recorded, Zoom encrypts all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.
- Zoom currently generates and manages encryption keys in the cloud. Importantly, Zoom has implemented robust and validated internal controls to prevent unauthorized access to any content that users share during meetings, including – but not limited to – the video, audio, and chat content of those meetings.
- Zoom also indicated that it has never created a mechanism to decrypt live meetings for lawful interception purposes and that there is no means of including third parties in meetings without being reflected in the list of participants.
- For those who want additional control of their encryption keys, an on-premise solution exists today for the entire meeting infrastructure, and a solution will be available later this year to allow organizations to leverage Zoom's cloud infrastructure but host the key management system within their environment.
- On March 27, Zoom updated its iOS application<sup>3</sup> (iOS privacy violations) to remove the code that sent the user's data to Facebook when the application was opened (time zone and city, details about the device, or if the user did not have a Facebook account).
- On March 29, Zoom updated its privacy policy to make it<sup>4</sup> clearer and more transparent. Zoom emphasized that it does not sell users' data, has never sold user data in the past, and has no intention of selling users' data going forward.
- On April 2, Zoom patched vulnerabilities that allowed the escalation of privileges and the access to recording, meeting and microphone on macOS.
- On April 2, Zoom fixed a vulnerability associated with Windows Zoom client chat that could allow a remote attacker to steal a user's Windows login credentials if the user clicked on a Universal Naming Convention (UNC) type path.
- On April 7, Zoom reported that they had implemented a solution for a serious vulnerability in Zoom that allowed users in the waiting room to obtain the meeting's encryption key.

---

<sup>1</sup> <https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event//>

<sup>2</sup> <https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/>

<sup>3</sup> <https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/>

<sup>4</sup> <https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/>

- Zoom recently removed an "attendee attention tracking" feature that allowed hosts to see if attendees had the Zoom window or another application window focused during a meeting.

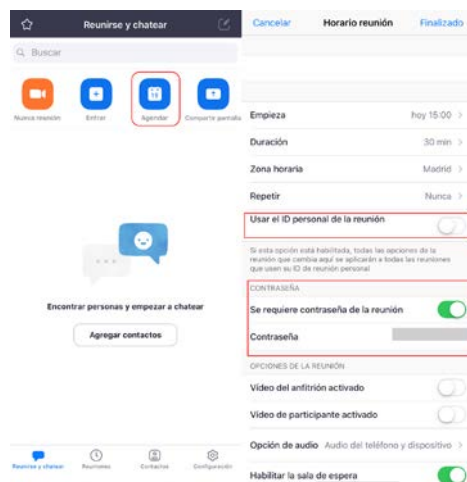
### 3 RECOMMENDATIONS AND GOOD PRACTICES

The best way to avoid meeting disruptions is to not share Zoom meeting IDs except with intended participants. Additionally, participants may be asked to use a password to log in to the meeting.

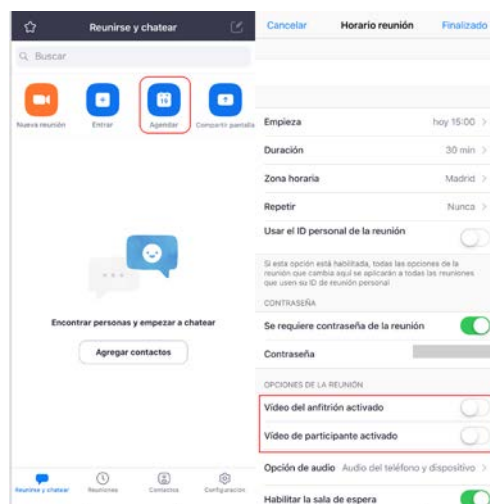
#### 3.1 Schedule a meeting

Zoom allows you to schedule a meeting for a specific time and date. If you are the meeting organizer, you should consider the following recommendations when scheduling your meeting:

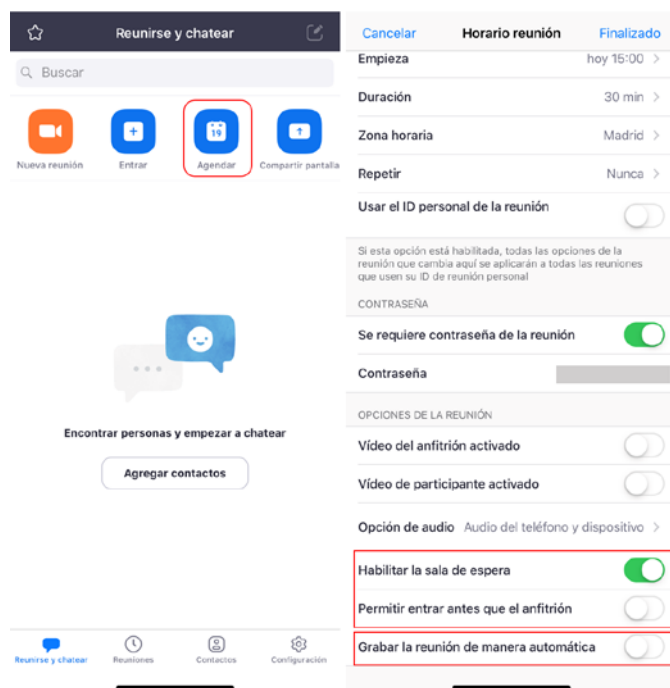
- Generate a random meeting ID and require a password to enter the meeting. If you click on the "Password" option, you can change the default password.
- Configure the meeting so that screen sharing is enabled for host only.



- Configure the meeting so that screen sharing is enabled for host only.



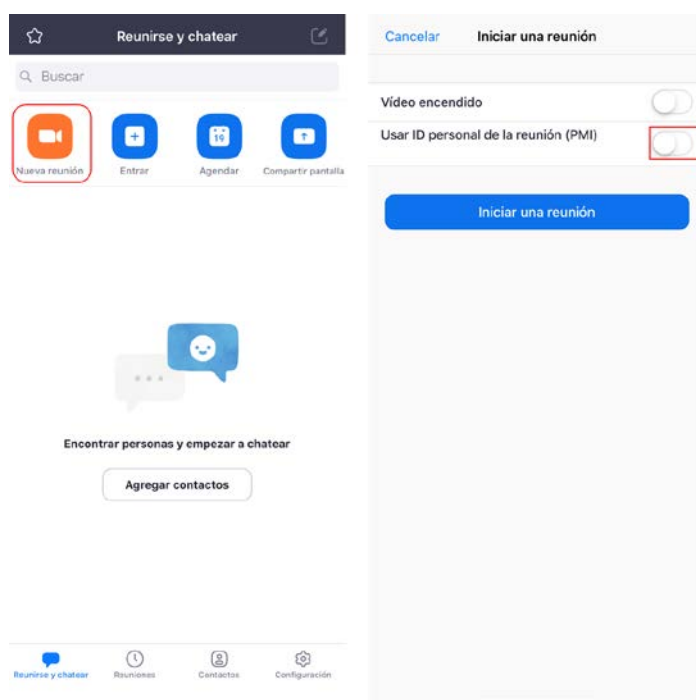
- Enable the waiting room and do not allow guests to enter the meeting before the host (organizer) joins the meeting. Similarly, if it is not strictly necessary to record the meeting, disable this option before the meeting starts.



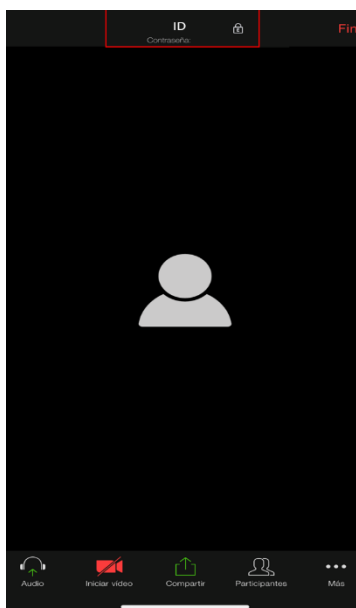
### 3.2 Create a new meeting from the main menu

The Zoom main menu allows you to create a meeting immediately. To do this, click on "New Meeting" and start setting up the room before inviting the participants. To do this:

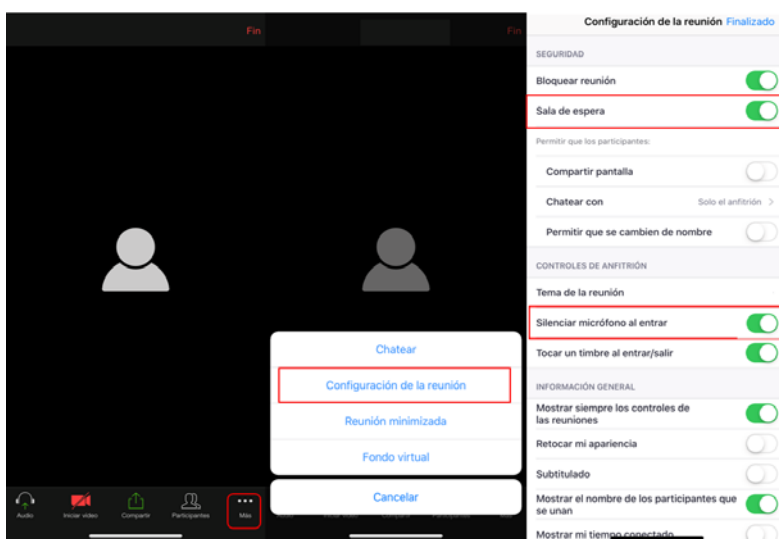
- Once you click on "New Meeting", generate a random meeting ID.



- When you click on the blue "Start a Meeting" button, the screen will display the randomly assigned meeting ID and the password automatically generated when you set up a meeting using this procedure.

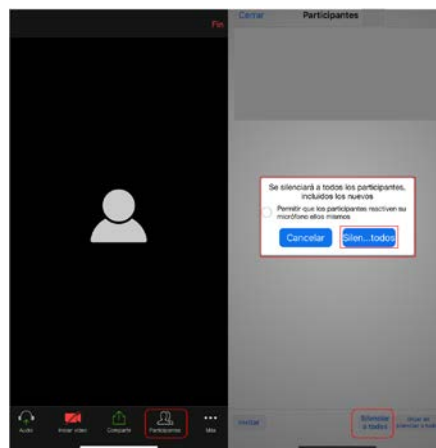
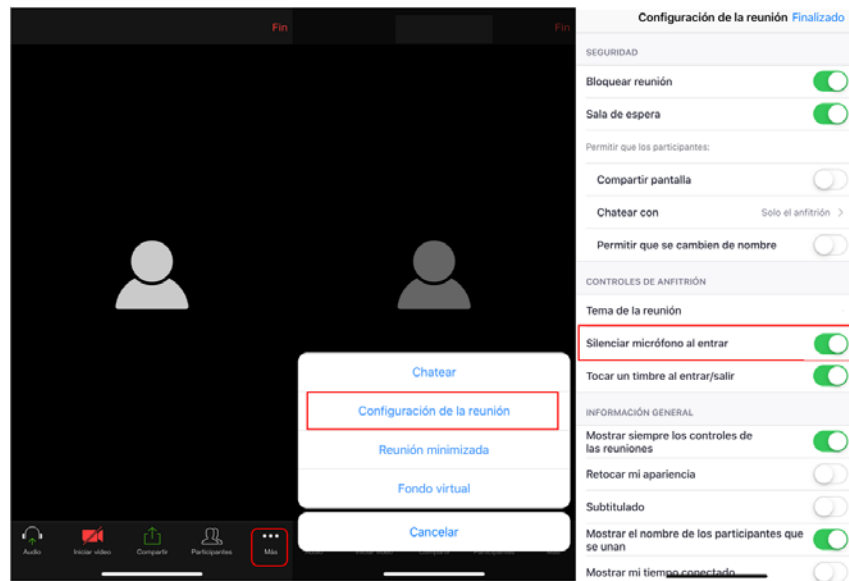


- Enable the waiting room and silence participants upon entry.

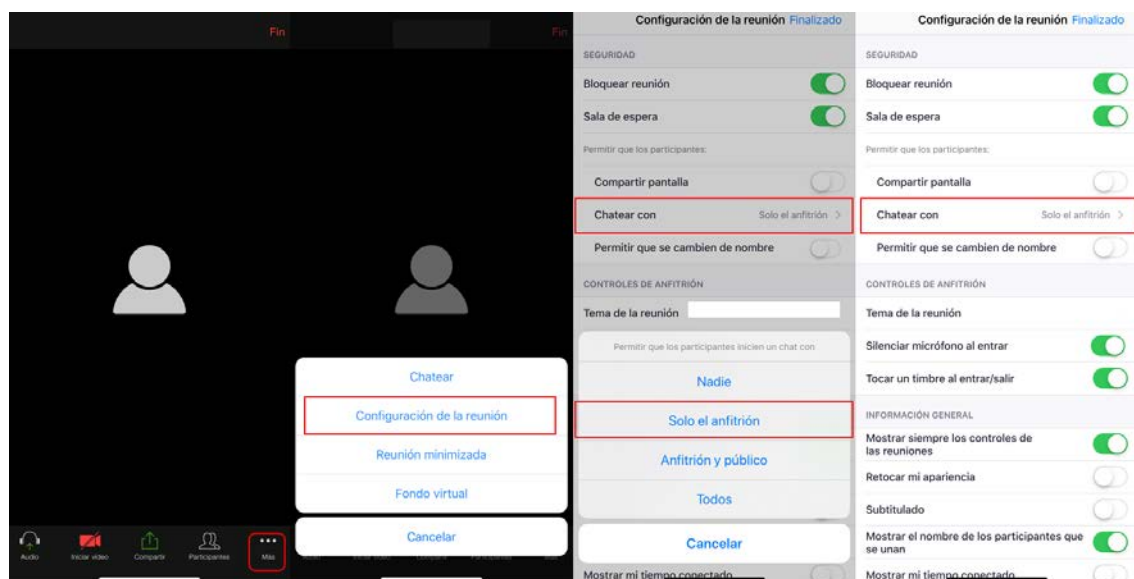


Also, set up the meeting so that:

- It allows only participants who have logged in to Zoom to enter the meeting.
- It disables the inclusion of the password in the meeting invitation link.
- Mute participants when they enter the meeting.

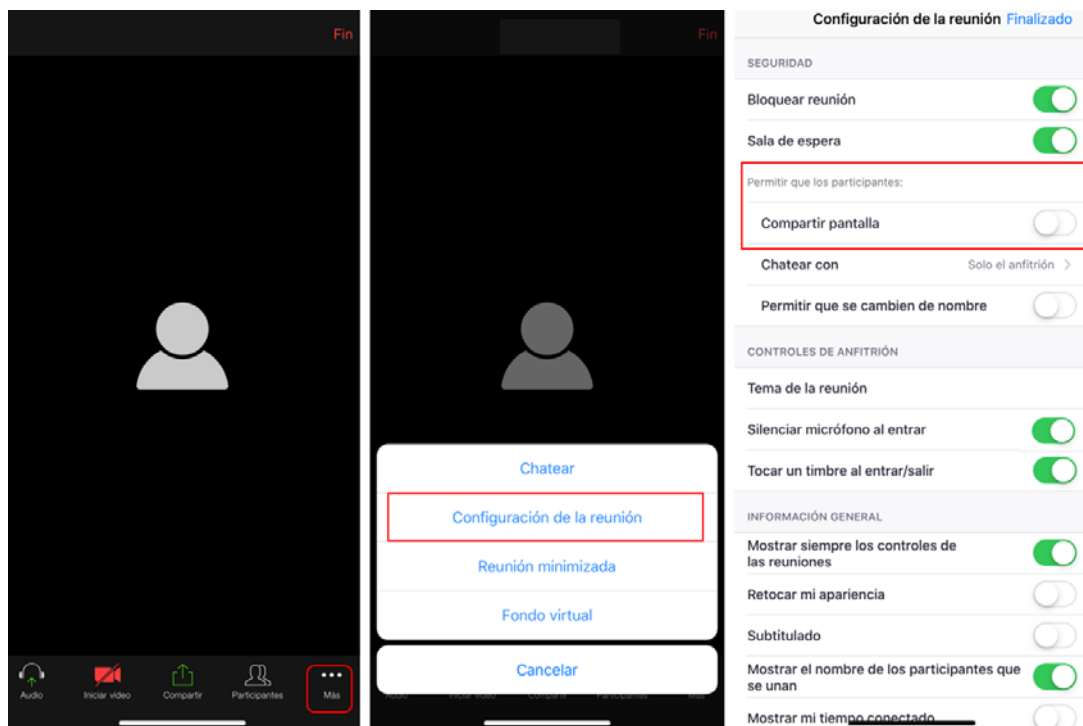


- Disable private chat between attendees.

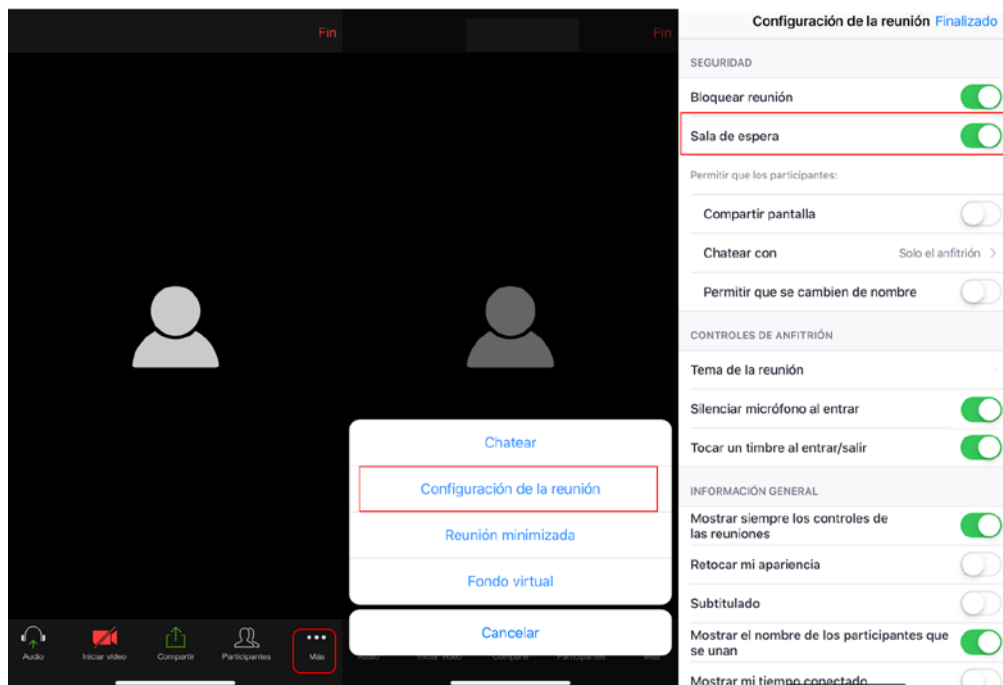


- Disable the automatic saving of chats.
- Set screen sharing for the host only.

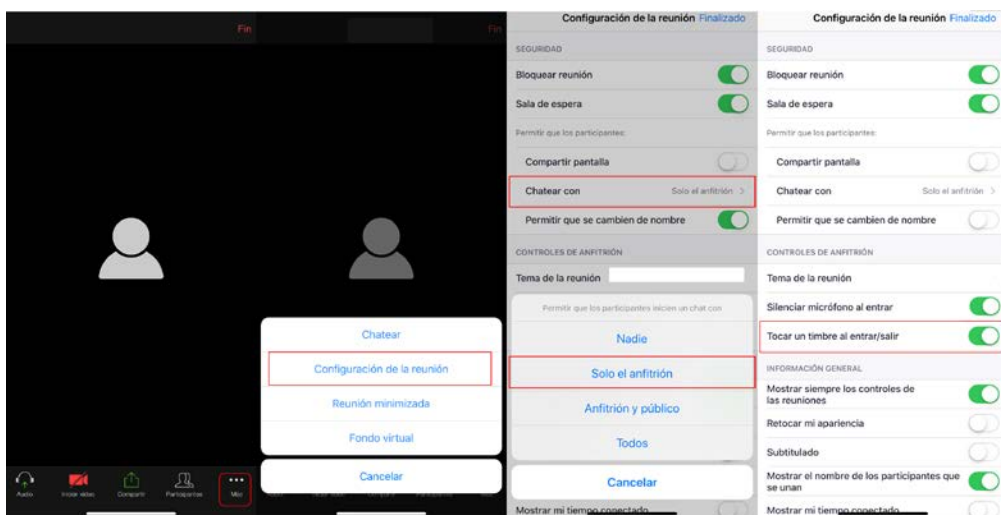




- Enable the waiting room for participants (enabling this option automatically disables the option that allows participants to join the meeting before the host).



- Activate the sound indicator every time a guest enters or leaves the meeting.

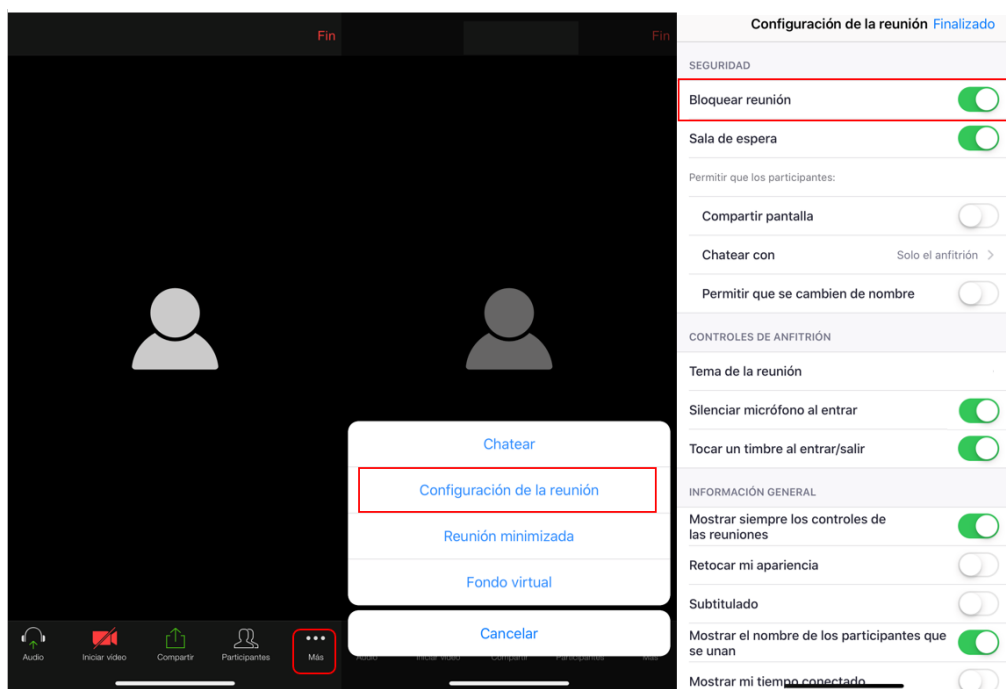


On the other hand, it is up to the host to decide whether to record a meeting and Zoom offers its paying customers the option of storing the recordings on Zoom's own servers.

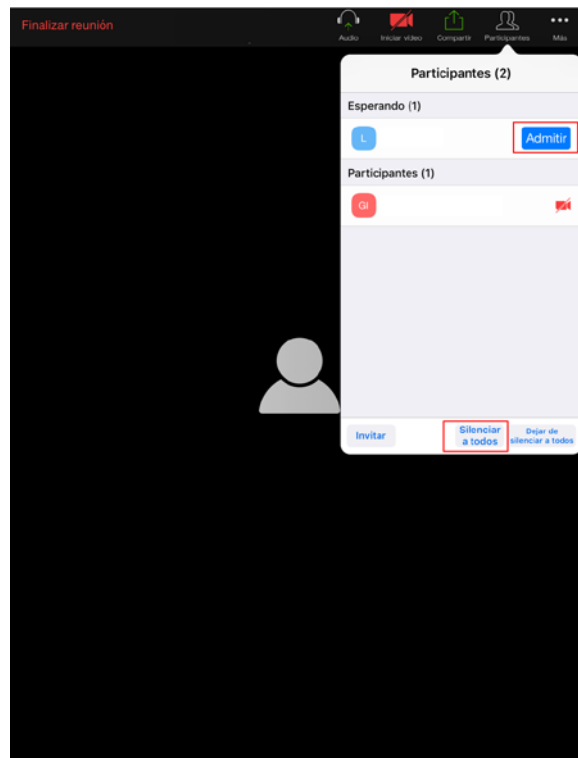
It is also up to the moderator to change the name of the recording file. If you are hosting a Zoom meeting and you decide to record it, make sure you change the default file name after the meeting is over. If you choose to upload your meeting recordings anywhere other than the Zoom cloud or your own machine (e.g. YouTube, a public cloud, etc.) Zoom urges hosts to use extreme caution and be transparent with meeting participants, giving careful consideration to whether the meeting contains sensitive information and to participants' reasonable expectations.

In addition, once participants enter the meeting, as an administrator you must take into account the following issues:

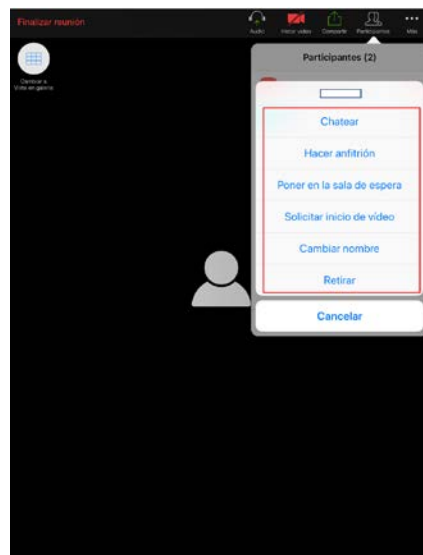
- You can lock the meeting so no new participants can join.



- You can see the list of people who are in the waiting room and decide when they are admitted to the meeting.



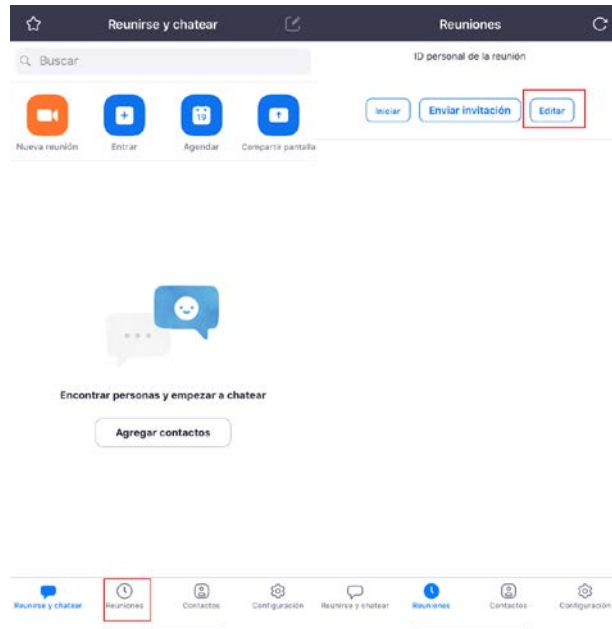
- Once the guests have been accepted, if you click on a specific guest, you can perform different actions. Clicking on "**Remove**" will remove the guest from the meeting.



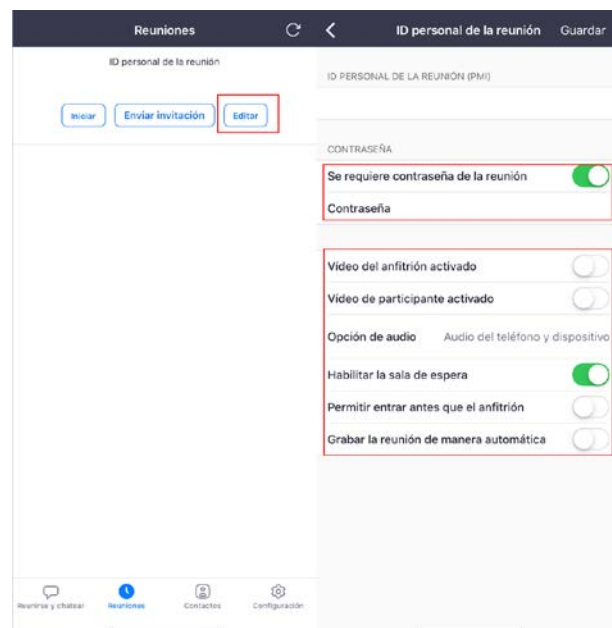
### 3.3 Create a new meeting from the secondary menu

The Zoom application also allows you to create a meeting in another way, which would normally be **inadvisable** as it involves starting the meeting with the **personal ID** and not with a random one.

- If you click on the secondary menu, on the option "Meeting" you can start a new meeting from your personal meeting ID (PMI). First, before starting the meeting or inviting participants, click on the Edit option to start configuring the session settings:



- Require password to access the meeting. If you click on the "Password" option, you can change the default password.
- Disable the video of the guests.
- Set up the waiting room and do not allow guests to enter the meeting before the organizer.
- If it is not strictly necessary to record the meeting, disable the "Record meeting automatically" option.



### 3.4 Recommendations for the educational sector

On the other hand, related to the education sector, Zoom:

- Published an administrator's guide<sup>5</sup> on how to set up a virtual classroom.
- Established a guide<sup>6</sup> on how to improve the security of its virtual classrooms.
- Set up a privacy policy dedicated to children under the age of 17 (K-12)<sup>7</sup>.
- Changed the settings for education users enrolled in the K-12 program so that passwords and virtual waiting rooms are enabled by default, and screen-sharing privileges are set to "Host Only" so teachers by default are the only ones who can share content.

### 3.5 Recommendations in general configuration

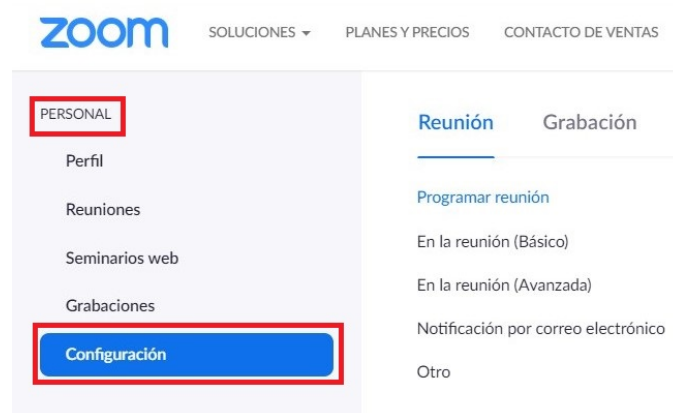
Since Zoom is a highly configurable collaboration tool, there are several customizable features that, while providing great potential in terms of functionality, some of them could compromise the security or confidentiality of your communication and data.

Therefore, it is recommended to thoroughly review the sections found in **PERSONAL->CONFIGURATIONS** and evaluate each of the sections according to the criteria of security vs. functionalities in order to adapt the configuration to the security requirements of the organization.

Some of these points have already been addressed earlier in this document from the point of view of generating meetings.

The following screenshots show an example that puts security above functionalities, having sections that can be varied to enable certain required functionalities according to the characteristics of the session that will be programmed.

- In the personal section, we find configuration.

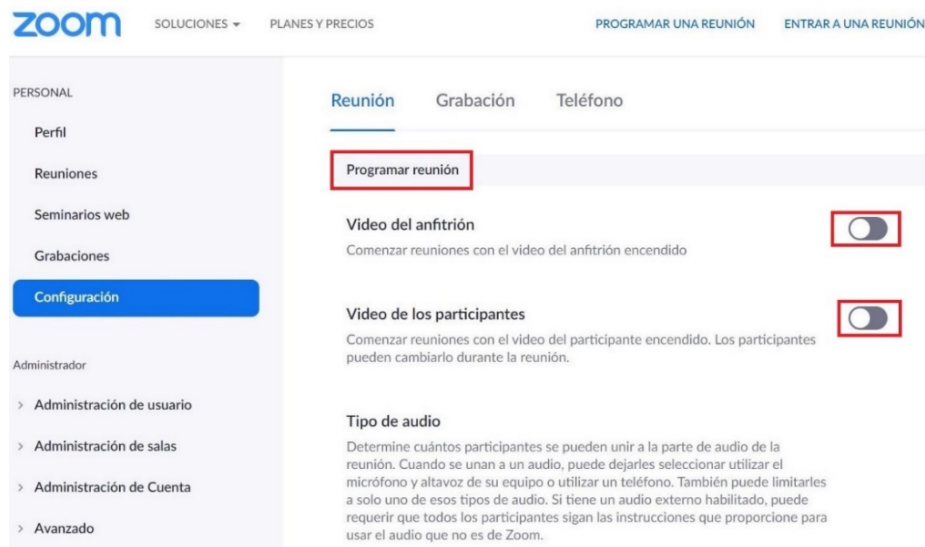


<sup>5</sup> <https://zoom.us/docs/doc/School%20Administrators%20Guide%20to%20Rolling%20Out%20Zoom.pdf?zcid=1231>

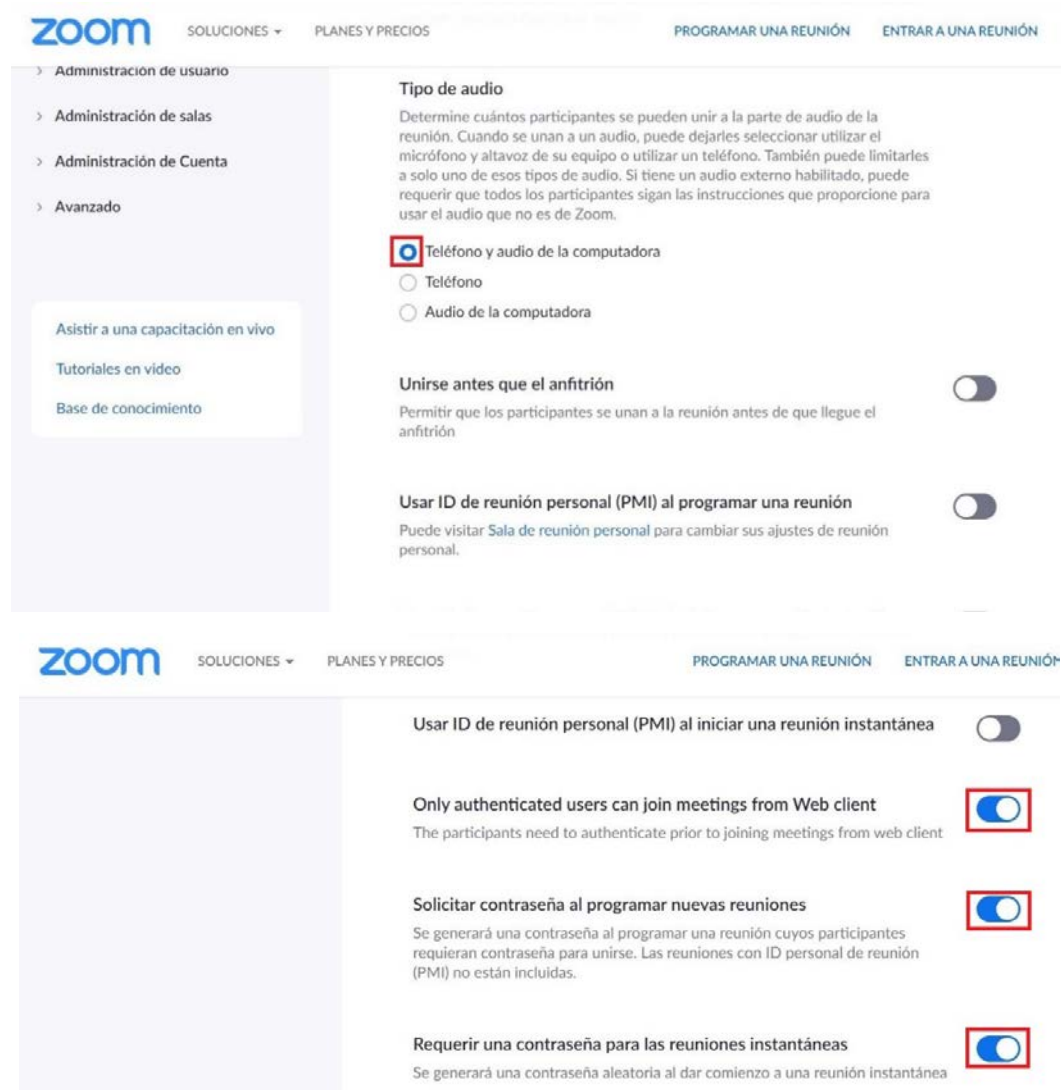
<sup>6</sup> <https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/>

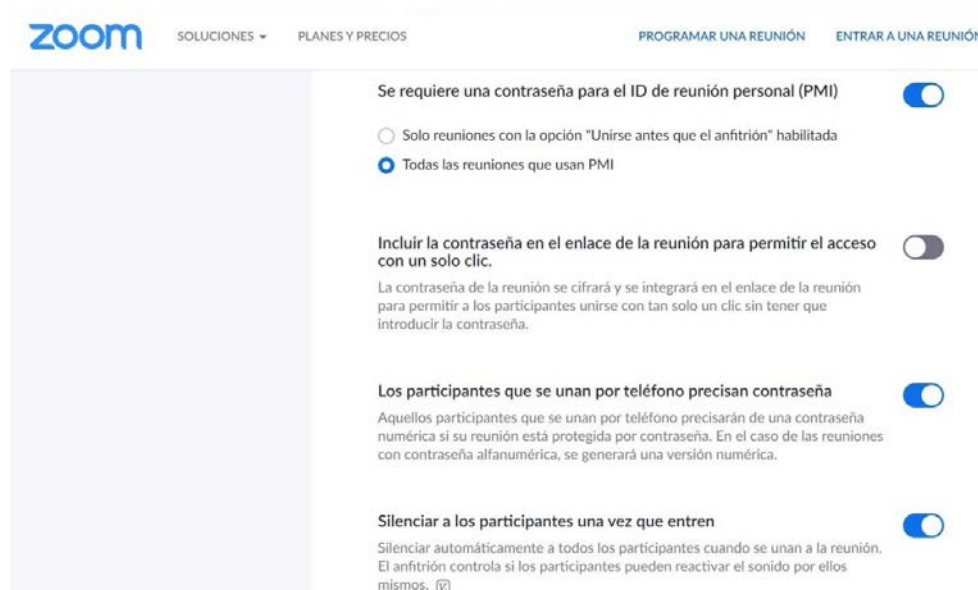
<sup>7</sup> <https://zoom.us/docs/en-us/childrens-privacy.html?zcid=1231>

- In the options of "Program a meeting": If it's gray, the option is deactivated.



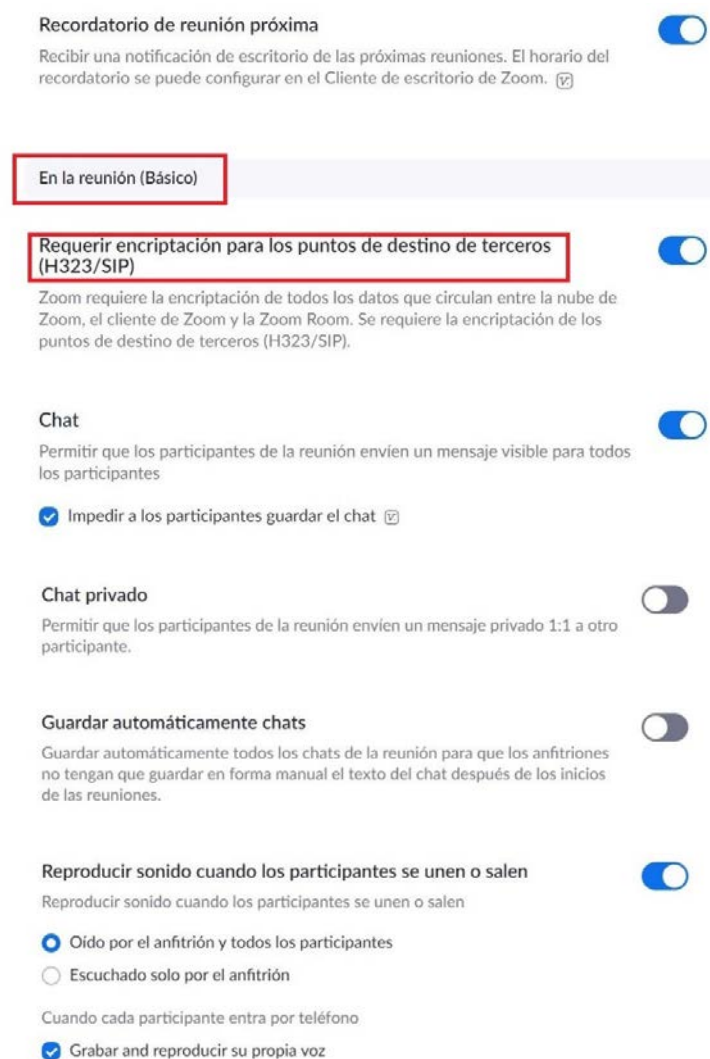
- If it is blue, the option is activated.



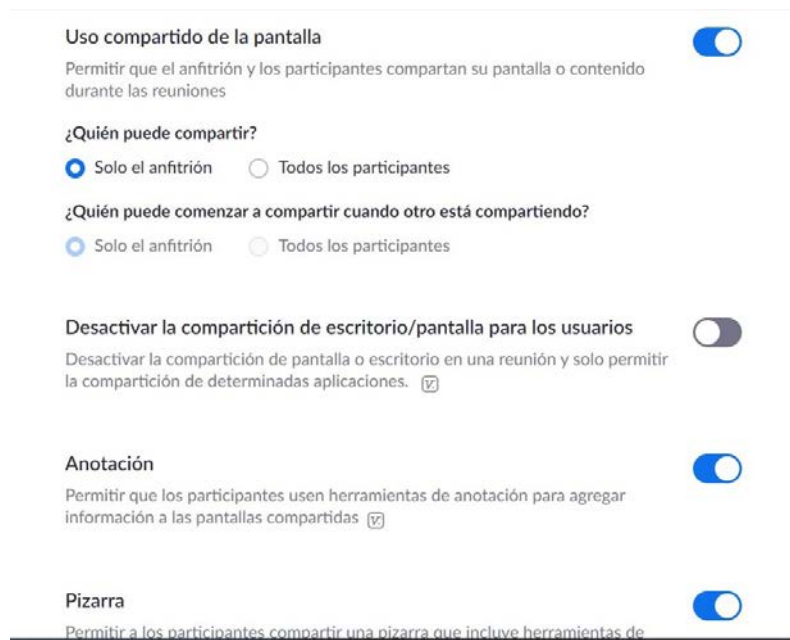



- Basic Meeting Configuration.

**IMPORTANT:** encryption is mandatory for video equipment in the room.







**Uso compartido de la pantalla** 


Permitir que el anfitrión y los participantes compartan su pantalla o contenido durante las reuniones


¿Quién puede compartir?


☒ Solo el anfitrión ☐ Todos los participantes


¿Quién puede comenzar a compartir cuando otro está compartiendo?


☒ Solo el anfitrión ☐ Todos los participantes

**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. 

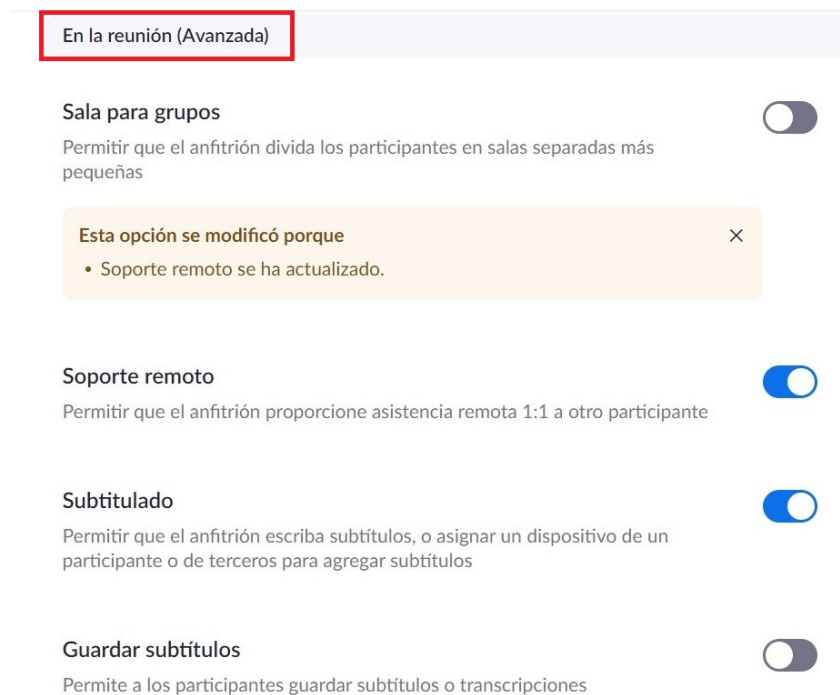
**Anotación** 

Permitir que los participantes usen herramientas de anotación para agregar información a las pantallas compartidas 


**Pizarra** 

Permitir a los participantes compartir una pizarra que incluye herramientas de


- Advanced Meeting Settings.




**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


- The new "Virtual Background" option is recommended to distort the view of the environment of the user.



<b>Control de la cámara más lejana</b> Permitir a otro usuario tomar el control de su cámara durante una reunión	
<b>Fondo virtual</b> 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.	
<b>Identificar a los participantes invitados en la reunión/el seminario web</b> 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. 	
<b>Grupo de respuesta automática en el chat</b> 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.	
<b>Mostrar solamente correo electrónico predeterminado al enviar invitaciones por correo electrónico</b> Permitir que los usuarios inviten a participantes por e-mail solamente mediante el programa predeterminado de e-mail seleccionado en su computadora	
<b>Uso del correo electrónico en formato HTML para el plugin de Outlook</b> Usar el formato HTML en lugar de texto plano para las invitaciones a reuniones programadas con el complemento de Outlook	
<b>Permitir que los usuarios seleccionen audio estéreo en la configuración del cliente</b> Permitir que los usuarios seleccionen el audio en estéreo durante una reunión	
<b>Permitir que los usuarios seleccionen sonido en la configuración del cliente</b> Permitir que los usuarios seleccionen el sonido original durante una reunión	

The "Participate from a web browser" option implies a lower compatibility of functionalities and is more insecure than the option of installing the heavy client, but it is an unavoidable option to enable it if the participants do not have permissions to install software on their devices.

#### 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



- Notification by mail.
- Blurring the snapshot in iOS, avoids showing sensitive information from open applications in 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.



- Recording tab options.

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.




- Telephone Options.
- The option to hide phone numbers is highly recommended.

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 CONCLUSIONS

With the right configuration and appropriate safeguards enabled to protect meetings – such as passwords, waiting rooms and locking meetings – **Zoom** delivers a safe and secure virtual meeting environment, regardless of the fact that this software is currently being targeted by cybercriminals given its recent popularity.

Zoom is releasing security patches, has strengthened the security team, intends to continue improving the product, and is organizing weekly webinars to provide privacy and security updates to the community.

In this sense, if an **adequate implementation is carried<sup>8</sup>out**, respecting **minimum-security requirements in the configuration<sup>9</sup>** and carrying out **good practices<sup>10</sup>**, Zoom can be considered an option to be taken into account in teleworking scenarios such as those currently marked by the COVID-19 crisis where sensitive information is not handled.

In short, given the reactions against Zoom during these days, and in accordance with the previous paragraph, **it is considered acceptable to use Zoom for meetings that are not very sensitive in their content, school classes and situations outside the office on routine matters.**

<sup>8</sup> <https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf>

<sup>9</sup> <https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls>

<sup>10</sup> <https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/206-ciberconsejos-videollamada>



# #CiberCOVID19

## Cybersecurity recommendations for video calls and virtual meetings.

Only download applications from official marketers, such as Google Play or Apple Store, or from the supplier's website (Microsoft, Google, Cisco, etc.).



Keep the video calling applications you use updated.



As far as possible, avoid clicking on links that are shared in the session chat, especially if you do not know the person who has shared it.



Schedule video calls with the exact number of participants. When all users have entered the session, close the access to new participants.



All users must access to the meeting with a password. In public applications, sign up with passwords that you haven't used on other services and do not publicly share the meeting ID.



The moderator of the video call can manage if the call can be recorded. If it is being recorded, a visual and sound indicator must be shown to all the users.



The moderator of the meeting must be able to manage the connection of the participants, close microphones, disable content or video signal. The participants should not access the meeting until the moderator connects.



Consider video calls an insecure communication channel, don't give out sensitive data like passwords.



Set the session so that a visual or audible indicator warns of incoming or outgoing users and disable the automatic answer to incoming calls. Log out of the application if you know no one is going to call.



Do not accept calls/chats from users you do not know. In private conferences all users must enter with a recognizable name/nick-name for the administrator/moderator of the call.