Use of Cisco Webex, its implications for security and privacy. Recommendations and good practices.

Abstract: given the uncertainty created by different attacks on various cloud-based collaboration and meeting platforms, here is an analysis and security recommendations for the use of the Cisco Webex platform.

Cisco Webex is a collaboration platform that enables meetings, events, training courses, remote support, group messaging, with audio, video and sharing services, interoperable with all video room platforms based on H323 and SIP standards. It allows meetings of up to 50 participants in its free version, and up to 1,000 participants in the paid one, including *streaming* transmissions via RTMP and RTMPS.

Content:

1 CONTEXT

In the context of the state of alarm decreed by the government of the nation due to the COVID-19 pandemic has led to a series of changes in the work and social routines of citizens and workers because of mandatory confinement, social distancing rules and teleworking.

This situation has generated an explosion in the widespread use of video conferencing systems and chat applications such as Zoom, Cisco Webex, Google Meet, Microsoft Teams and consumer applications such as Houseparty, Jitsi, etc.

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 increased surface area of exposure resulting from allowing operations that are more fluid.

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

2 CISCO WEBEX SECURITY COMMITMENT

Cisco designs products according to the Cisco Secure Development Lifecycle (SDL), which includes periodic privacy impact assessments, proactive penetration testing, and threat modeling. Cisco's Security and Trust organization monitors Webex security and privacy and publicly discloses security vulnerabilities.

There are three (3) Cisco Webex security principles:

- Webex is committed to respecting the **privacy** of your data.
- Webex is **secure** by default.
- Webex has **cyber** security **governance** and is **transparent** when there are security issues.

3 GOOD PRACTICES IN THE ADMINISTRATION AND USE OF WEBEX MEETINGS

Proposal	Actions
Preventing unauthorized attendees from joining meetings	• Use a unique password-protected link for invited users (default). • Automatically lock meeting rooms to restrict entry (default). • Automatically place external or unauthenticated attendees in a waiting room (default) • Require password or login for phones and video devices
Avoiding interruptions during the meeting	• Prevent the possibility of joining a meeting before the host. • Manually lock your meeting room. • Configure that only the presenter can share content. • Set your meeting room to lock automatically after a specified duration. • Have participants who join a closed personal room placed in the lobby until they are admitted by the host.
Limit meetings to internal users only	• Apply Single Sign-On (SSO) to join or enter a personal meeting room. • Require assistant roles.
Preventing the resending of invitations	• Require that only invited users can join meetings.

Enable a host to securely manage a personal room meeting	• Visual difference in internal/external users in the list. • Entry and exit tones. • Blocking the meeting room. • Enable an e-mail notification to be sent to you in case someone enters the lobby of your personal room while you are out. • Enable/disable available functions such as chat, video, voice options. • Eject, block, mute, etc.
Manage file sharing control	• The administrator can choose to selectively enable or disable file sharing (Meetings and Teams). • The administrator can limit file sharing depending on the client type (Webex Teams).
Manage external integrations (for Meetings and Teams)	• A client can allow or deny its users to use Google accounts, Microsoft Office 365 accounts, Facebook accounts, and other third-party applications with their Cisco Webex account. In addition, clients can also ensure that only those third-party applications for Webex Teams (developed through the API available at developer.webex.com) that meet their security and data control standards can be enabled for their users. • Clients can choose to allow or deny access to these third-party applications for all members of the organization or for specific users.
Manage bots	• You can manage bots for Webex Teams spaces, managing external integrations, to control the output of information and reduce risk. Administrators can establish global policies to allow or deny bots. In the case of "global denial", a white list of supported bots can be configured.

4 WEBEX SECURITY CONTROLS

The security of the Webex suite is managed on two (2) levels. The first is a global supra level of the organization managed by the administrators of the platform and secondly at the level of customization of the personal rooms assigned to each user.

4.1 Security controls for Webex administrators

Security management control features are available to administrators through the Control Hub (admin.webex.com).

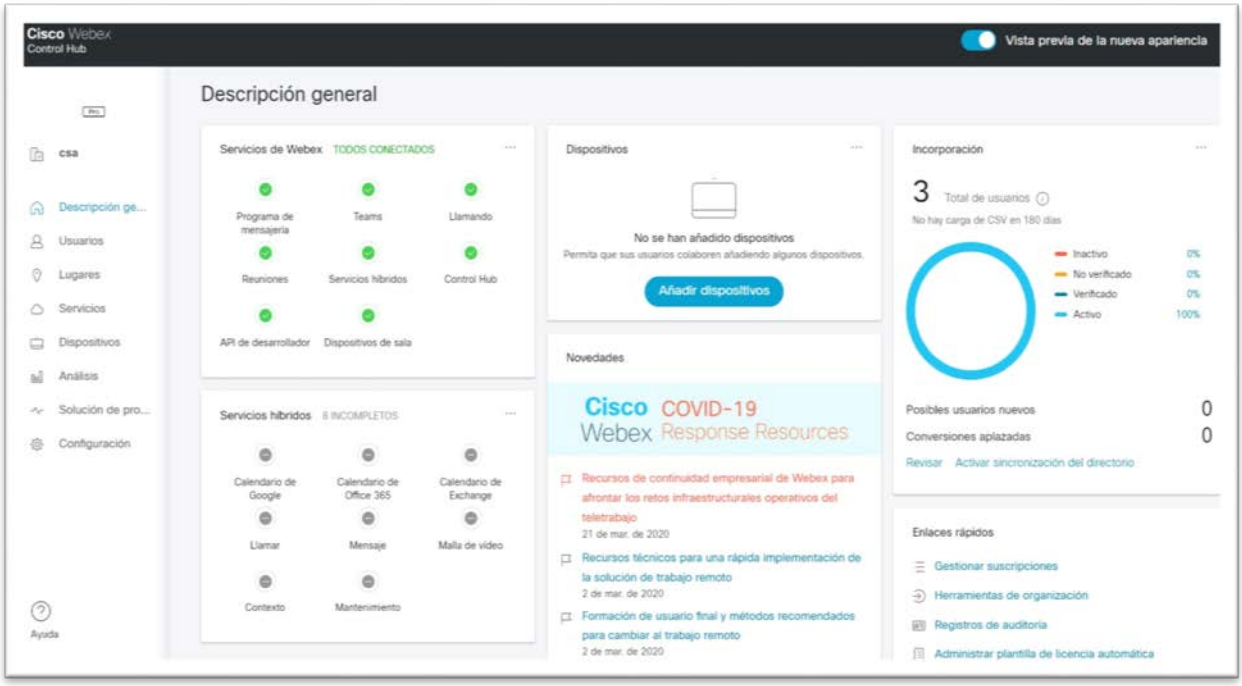


Figure 1.- Control Hub

The following security parameters are recommended in the configuration tab of the hub control (https://admin.webex.com/settings).

4.1.1 Security in mobile devices

To disable message previews: a client can ensure that message previews for mobile notifications are always disabled so that users nearby cannot see the incoming messages on the device. Alternatively, if the device is locked and left unattended by the user, other users will no longer be able to preview the messages on the locked screen on the device.

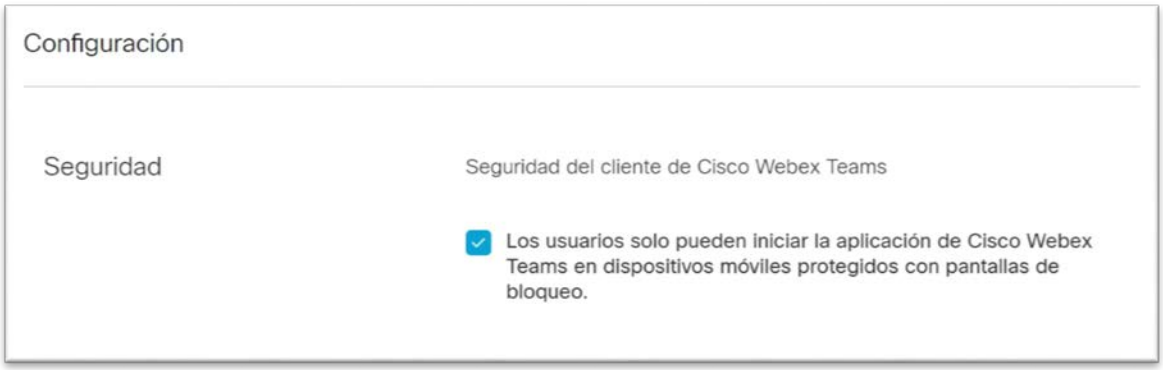


Illustration 1.- Privacy preview on mobiles

4.1.2 Close web user sessions due to inactivity

Customized downtime for browser interfaces. A Cisco Webex administrator using the Control Hub, or a user using the browser interface, does not have to worry about leaving his laptop unattended.

A custom timeout is set in the control hub allowing an administrator to reduce the security risk of these events by ending idle sessions after a period of timeout (optionally between 10 minutes and 60 minutes). The control hub also has a default inactive timeout of 20 minutes.

These timeouts can be further customized for in and out of the network. If a user is logging into the system on the VPN security, the inactive timeout period of the company network can be longer (or never activated), and the durations can be shortened if they are on a public network.

Figure 2.- Inactivity shutdown

4.1.3 Control of external communications

The *Block External Communications* function allows managers to control collaboration between organizations in the following ways:

- All the users of your organization are restricted from communicating with anyone belonging to external organizations on Webex Teams.
- The organization's users cannot add users outside the approved domains or join spaces created by non-approved domains on Webex Teams.
- Use the attendee role and "Require Login Before Site Access" control to block participants from outside the Meetings site.
- Enabling the external message-blocking tab should be carefully evaluated as it involves inviting users from outside the organization to collaboration groups.

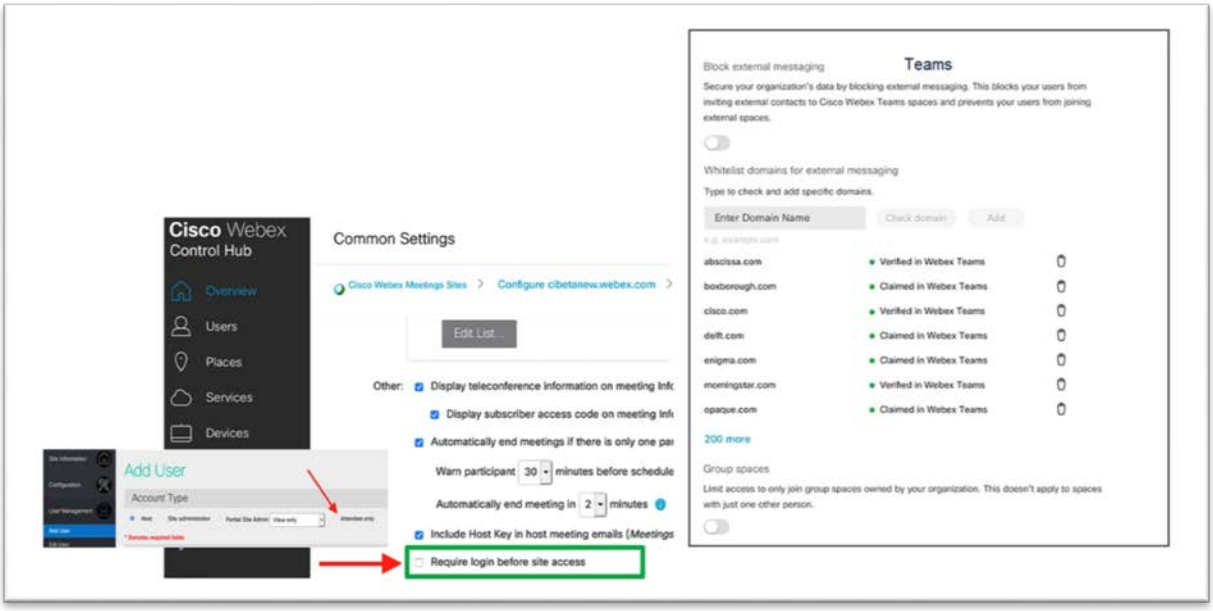


Illustration 3.- Third party domains allowed

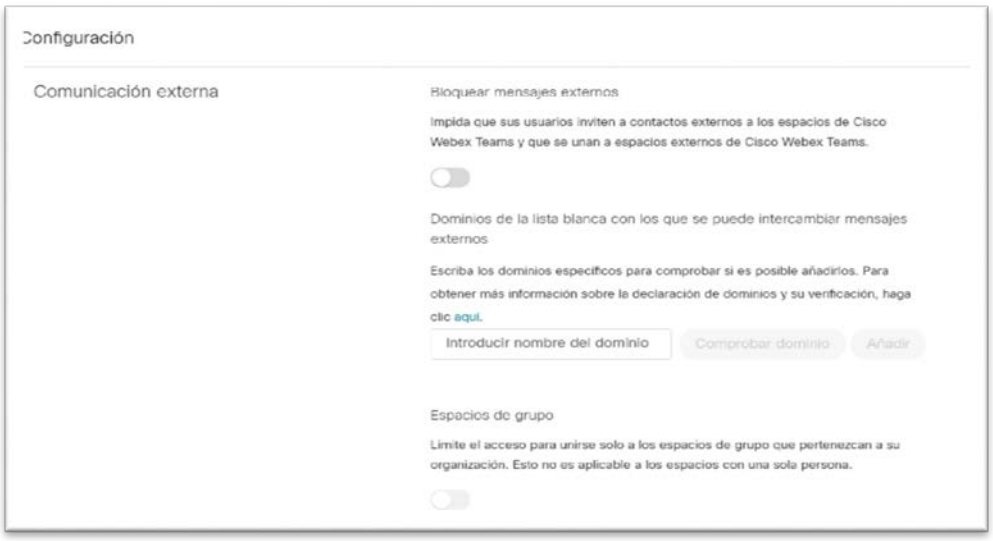


Illustration 5.- External messages

4.1.4 Privacy

Privacy settings allow selecting the level of viewing detail and intervention that your technology partner or support assistant has from your configuration.

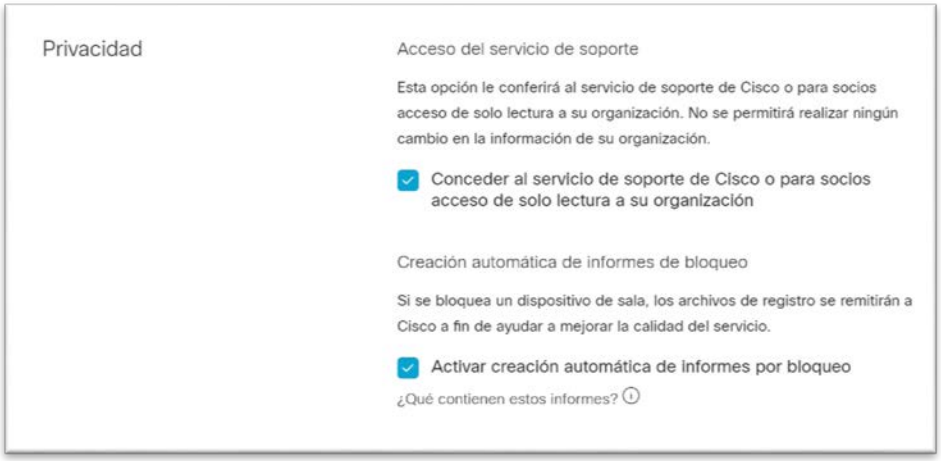


Illustration 4.- Privacy

4.1.5 User authentication

Enable Single Session Service (SSO): This one-way synchronization ensures that users are not only provisioned when they connect to the company, but more importantly, ensures that users are stripped of their provisioned data and that tokens are revoked when the company decides that they should delete that user account.

Proof of identity: Administrators check their domains to ensure that the users they provision are who they claim to be, so when you join a meeting you can trust who you are collaborating with.

System for Cross-Domain Identity Management (SCIM) provisioning is supported: incorporation of users through Okta and Azure AD integrations using SCIM, the sector standard.

The People API at https://developer.webex.com and CSV are also supported.

Illustration 5.- Login

4.2 Manage user's personal room preferences

The user has access to particular configurations of his Webex meetings personal room through a web access such as https://(domain).webex.com or through the "Personal Room" tab of the application.

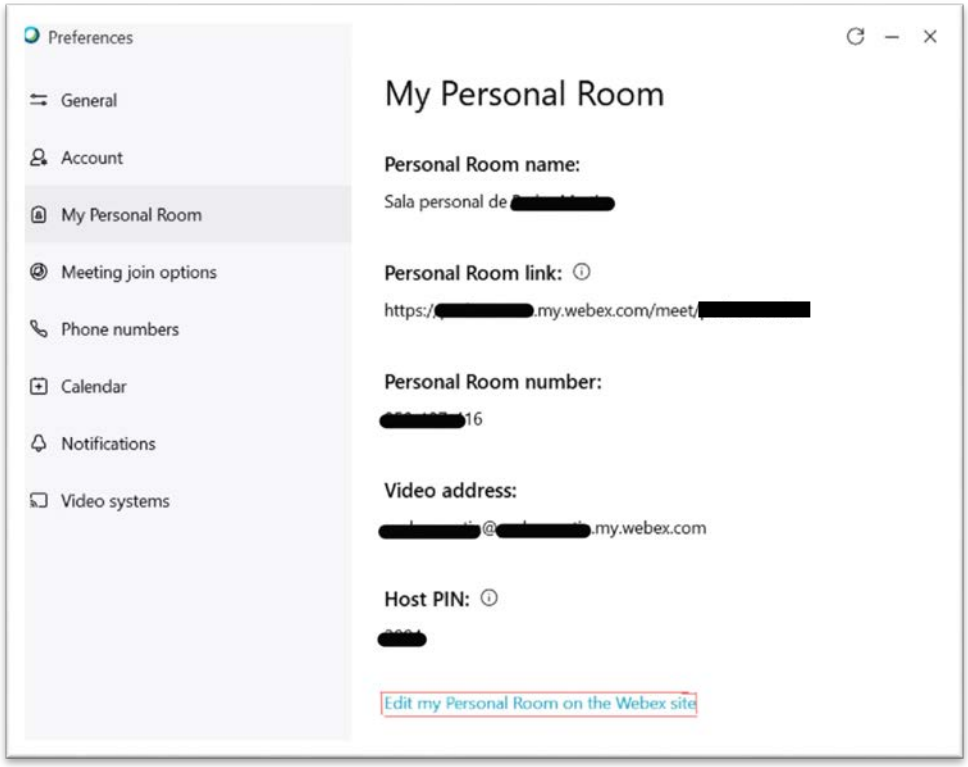


Illustration 6.- Web access via app

- Customization of the room's name and its link.
- The organizer's pin must meet certain requirements.

Illustration 7.- Room and pin customization

- Block the room automatically after the meeting has started, to prevent accidental intrusion of participants.

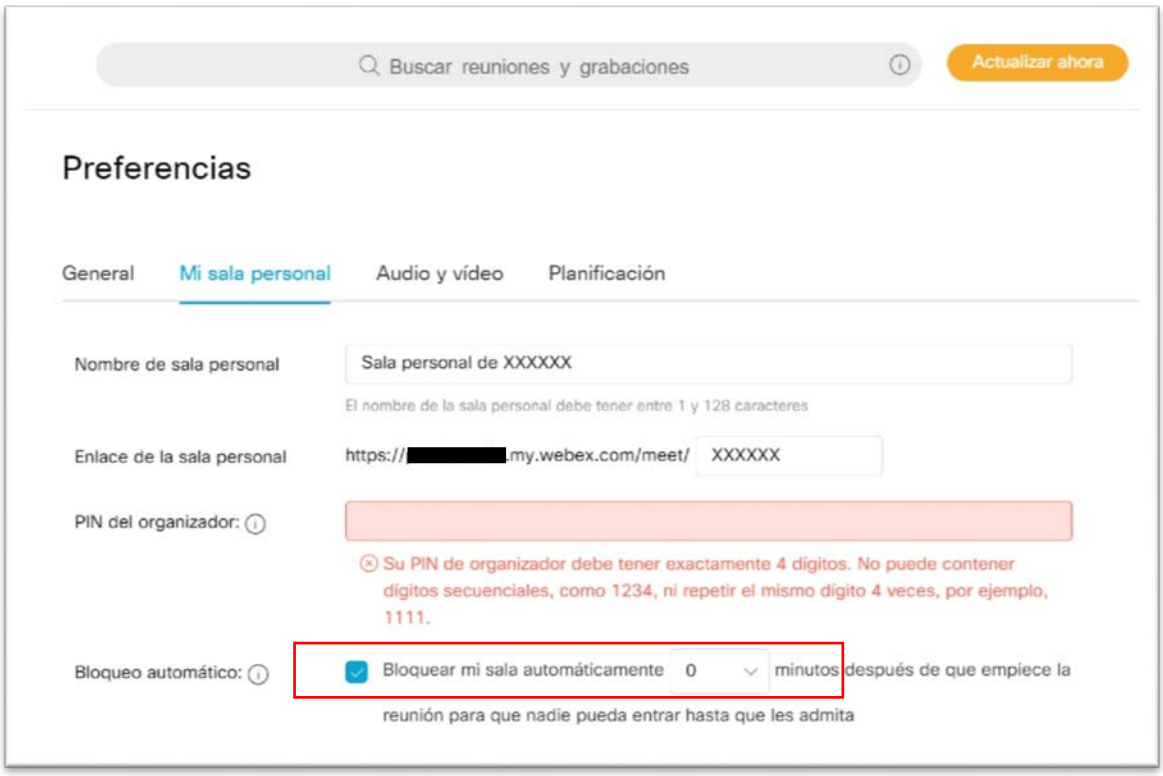


Illustration 8.- Room lock

- Notification of participants waiting in the lobby to the organizer and delegation of permits to alternative organizers.

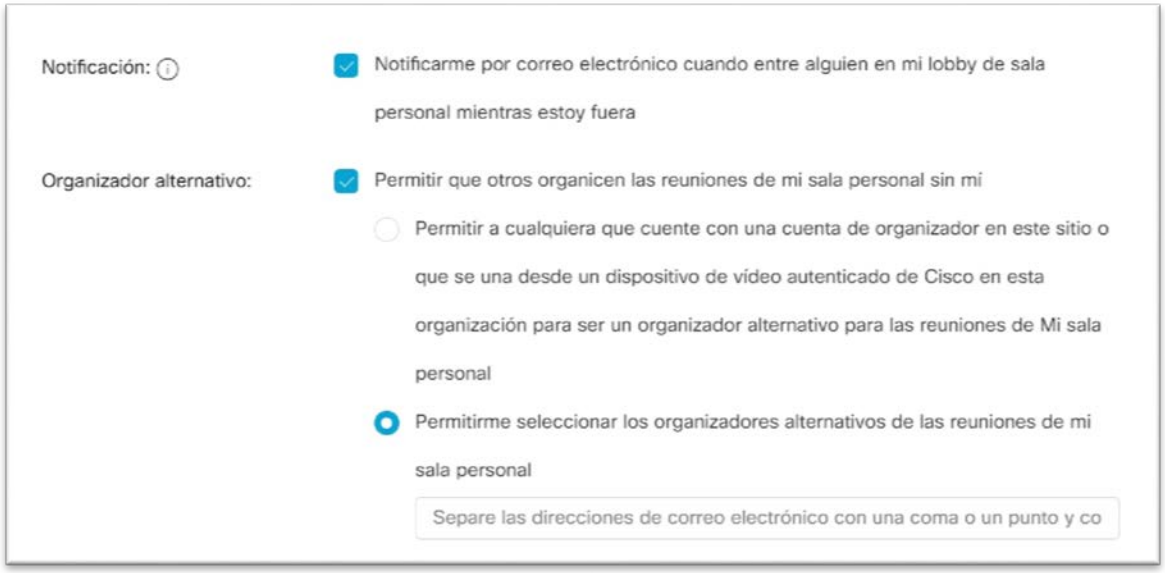


Illustration 9.- Notification of participants in the lobby

5 OPERATIVE

For accessing the meetings, Cisco Webex has virtual meeting rooms and personal rooms, which allow each user to have a unique address and meeting code, always available and managed by the user himself with access control by automatically locking the meetings, as recommended above.

There are three (3) methodologies for creating meetings, via the web portal, desktop or mobile application and an Outlook *plug-in.*

5.1 Creating a meeting from desktop application

- Start an immediate meeting in the personal room.

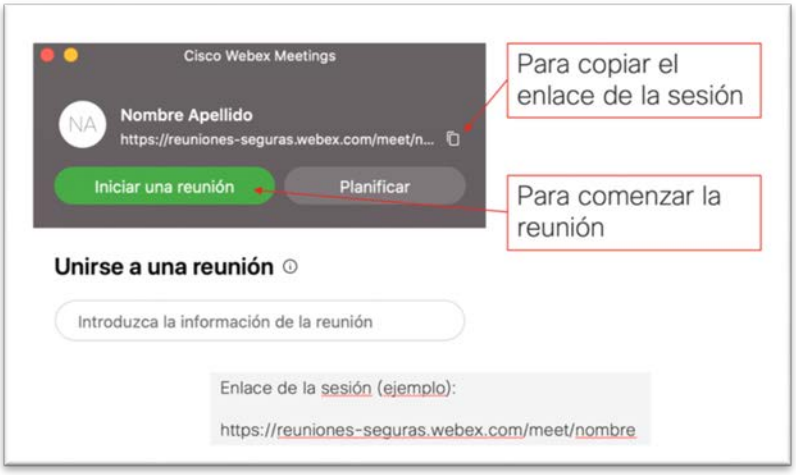


Illustration 10.- Starting a meeting

- Planning a meeting.

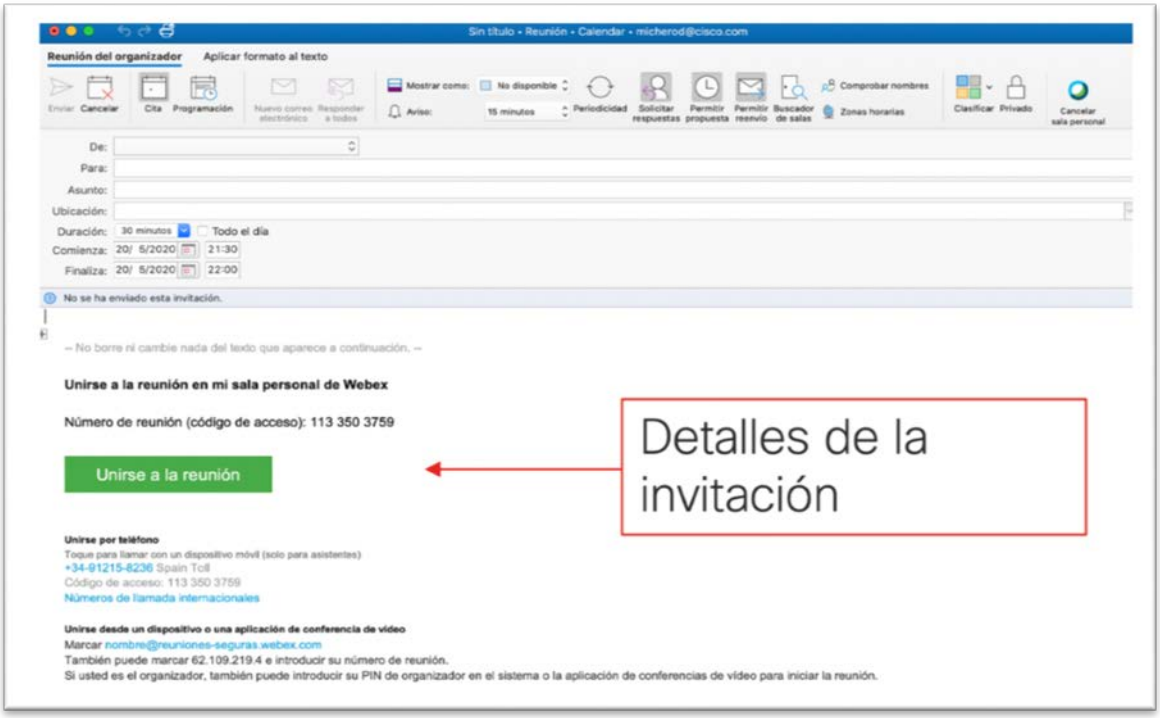


Figure 11.- Details of the meeting invitation

Figure 12.- Planning a meeting

5.2 Creating a meeting from Webex portal

The user has web access to his personal Webex meetings room through a https://(domain).webex.com type access.

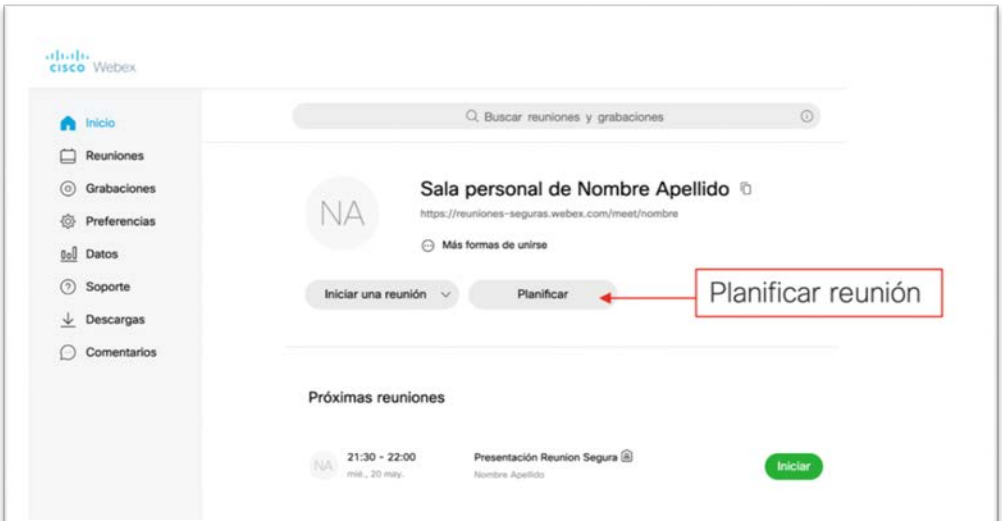


Illustration 13.- Meeting planning

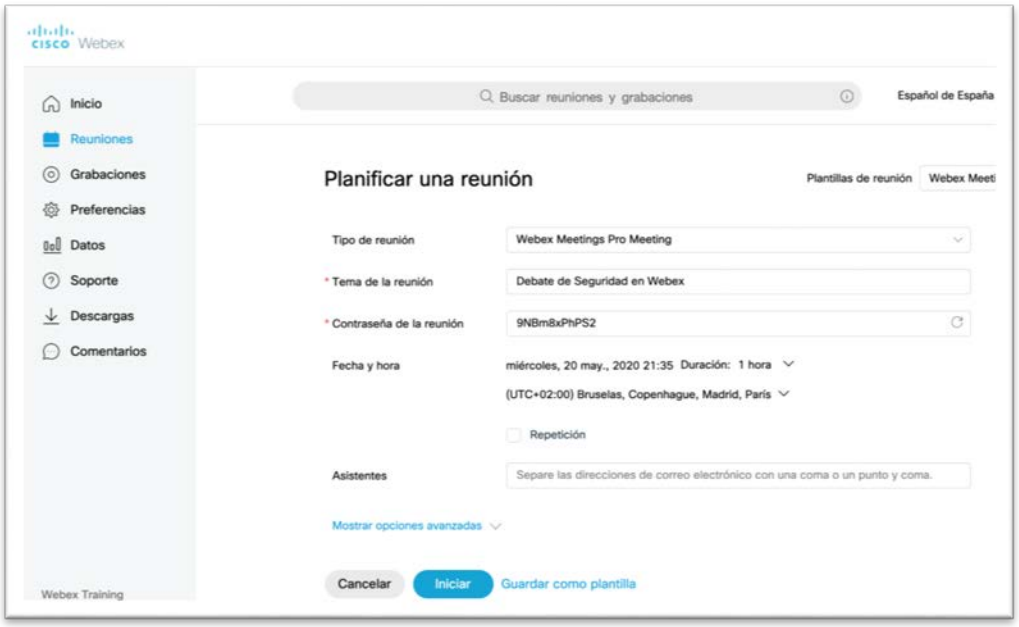


Illustration 14.- Meeting details

5.3 Creating a Meeting from Outlook

Cisco Webex also enables the inclusion of a *plug-in* in the mail manager, making it available to the user to generate a meeting with a single click, with the security features previously configured.

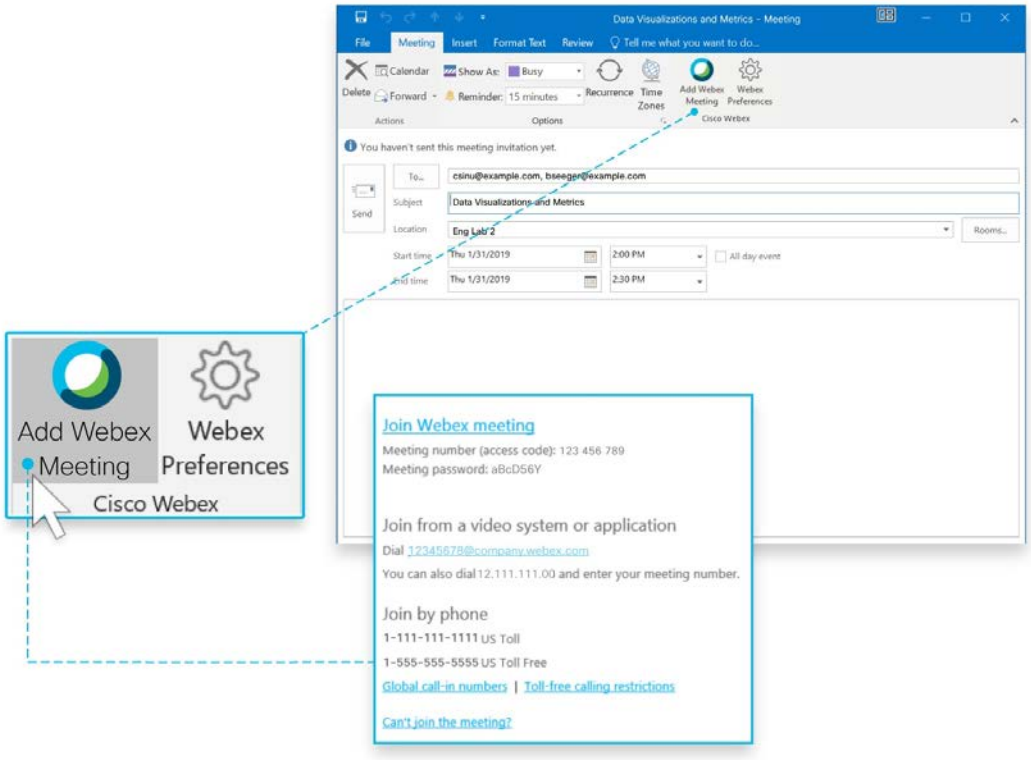


Illustration 15.- Outlook Plug-in

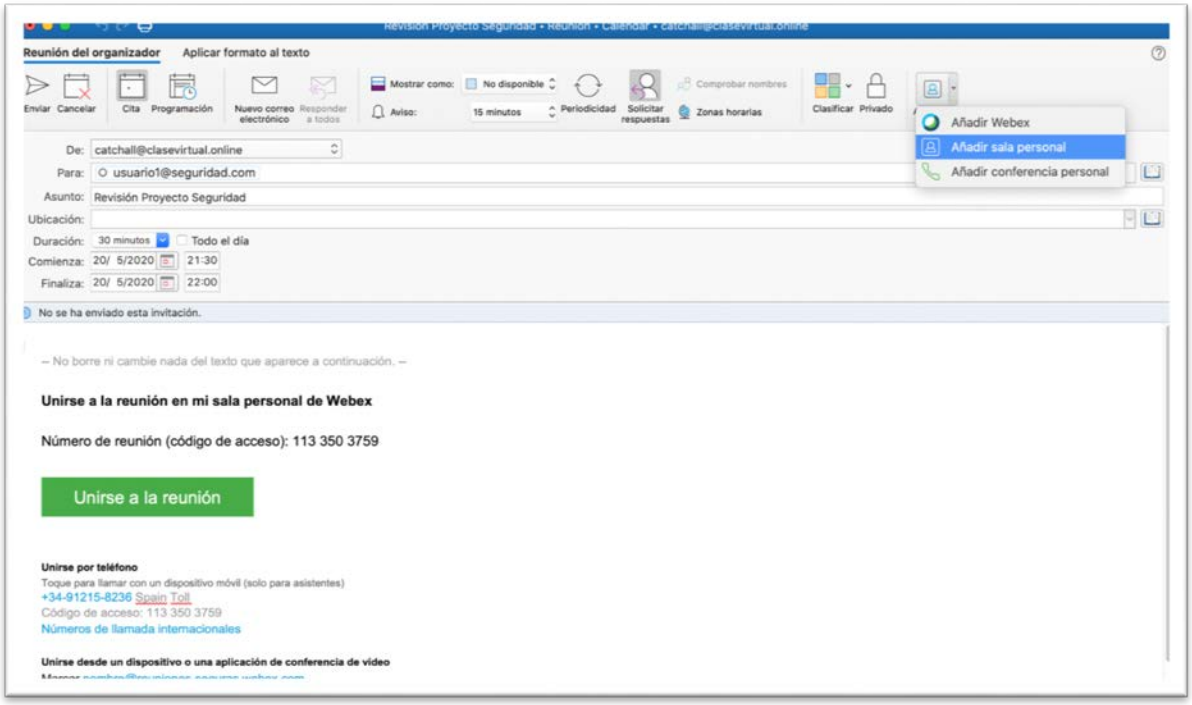


Illustration 16.- Webex Plug-in on Mac

5.4 Recommendations for the education sector

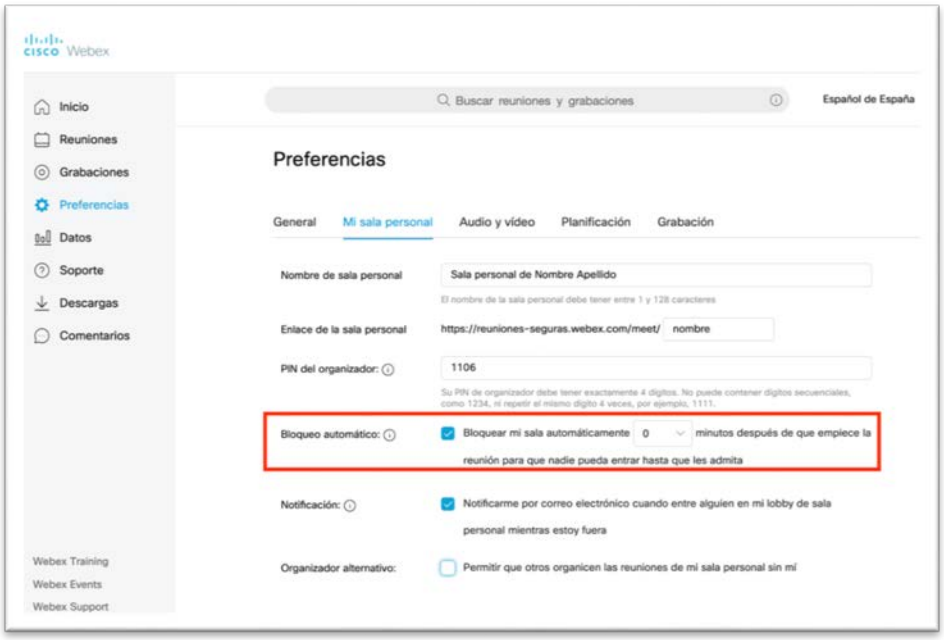


Illustration 17.- Room lock

- **Block the virtual classroom**. From the website, you can set up the locking of the room automatically after the virtual class starts, not letting anyone in without the teacher authorizing access.
- **Disable** screen sharing by students without permission.

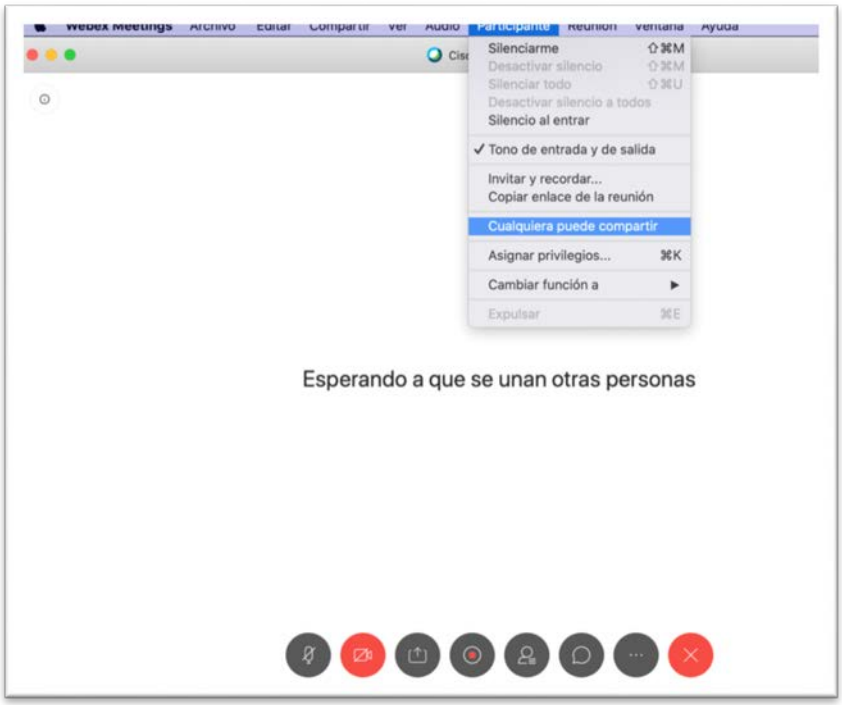


Figure 18.- Enable content sharing

- If it is not configured automatically, **lock the room** when the class starts. A notification will always appear to admit students who are in the waiting room.

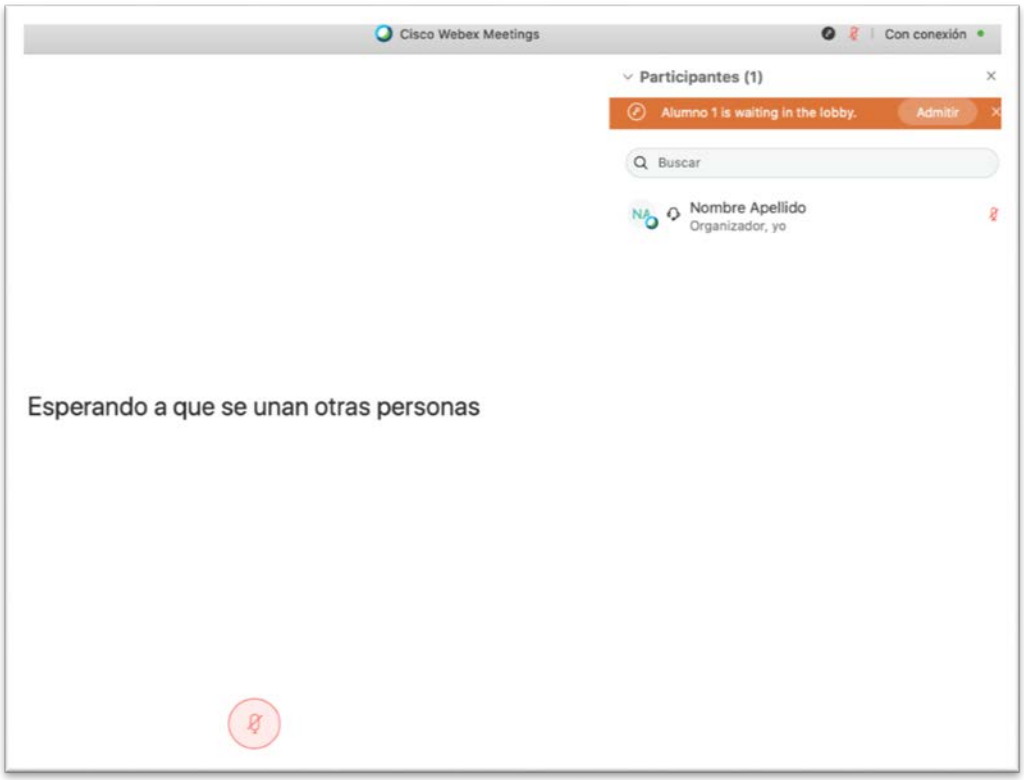


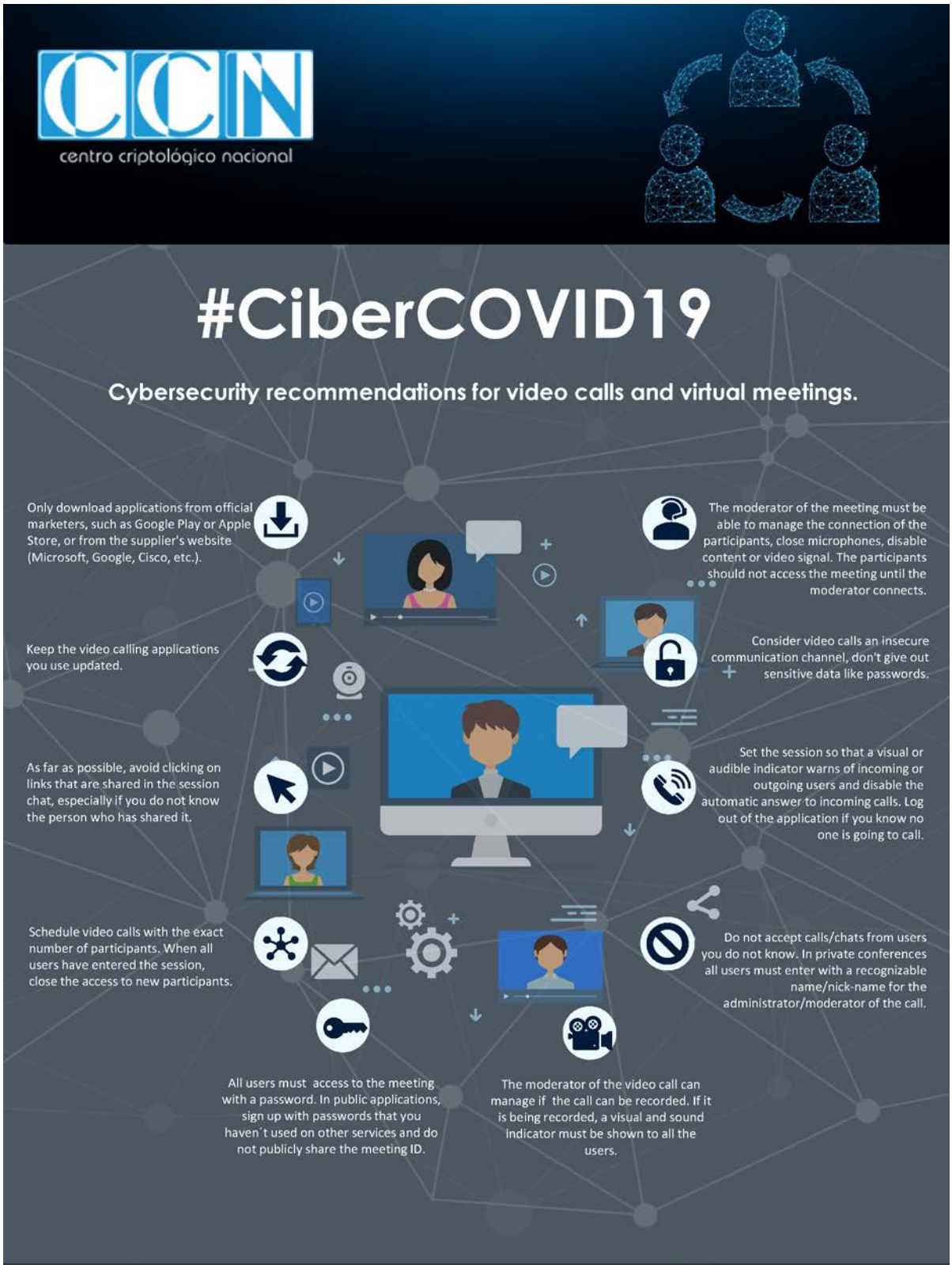
Figure 19.- Indication of participant waiting in the lobby

- Ask those entering to **identify** themselves **and activate the camera**. In any case, it is good practice for the teacher to activate his or her video.
- **Eject or move** students who do not identify themselves correctly in the waiting room.

6 CONCLUSIONS

Cisco offers an ecosystem of end-to-end solutions, where Cisco Webex is the collaboration platform that enables meetings, events, training courses, remote support, group messaging, with audio, video and sharing services, interoperable with all video room platforms based on H323 and SIP standards, with the possibility of being a cloud service with flexible licensing per use or a traditional model of services hosted in the customer's data processing centers or in a hybrid mode between both environments.

This ensures that users can choose the best mode of deployment for the solution that meets their organization’s security standards.



centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.05.28 12:48:25 +02'00'