Uso de Cisco Webex, sus implicaciones para la seguridad y privacidad. Recomendaciones y buenas prácticas.

Abstract: ante la incertidumbre creada por los diferentes ataques a diversas plataformas de colaboración y reuniones basadas en la nube, a continuación, se detalla un análisis y recomendaciones de seguridad para el uso de la plataforma Cisco Webex.

Cisco Webex es una plataforma de colaboración que permite la realización de reuniones, eventos, cursos de formación, soporte remoto, mensajería de grupo, con servicios de audio, video y compartición, interoperable con todas las plataformas de video de sala basadas en estándares H323 y SIP. Permite reuniones de hasta 50 participantes en su versión gratuita, y hasta 1.000 participantes en la de pago, incluyendo retransmisiones por *streaming* mediante RTMP y RTMPS.

Contenido:

1 CONTEXTO

En el contexto de estado de alarma decretado por el gobierno de la nación debido a la pandemia de Covid-19 ha provocado una serie de cambios de las rutinas laborales y sociales de los ciudadanos y trabajadores a raíz del confinamiento obligatorio, a las normas de distanciamiento social y el teletrabajo.

Esta situación ha generado una explosión en el uso generalizado de sistemas de videoconferencias y aplicaciones de chat como Zoom, Cisco Webex, Google Meet, Microsoft Teams y aplicaciones de consumo como Houseparty, Jitsi, etc.

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 COMPROMISO DE SEGURIDAD DE CISCO WEBEX

Cisco diseña los productos de acuerdo con el ciclo de vida de desarrollo seguro (SDL – Secure Development Lifecycle) de Cisco que incluye evaluaciones periódicas de impacto de privacidad, pruebas de penetración proactiva y modelado de amenazas. La organización Security and Trust de Cisco supervisa la seguridad y la privacidad de Webex y revela públicamente vulnerabilidades de seguridad.

Son tres (3) los principios de seguridad de Cisco Webex:

- Webex se compromete a respetar la **privacidad** de sus datos.
- Webex es **seguro** de forma predeterminada.
- Webex tiene **gobernanza cibernética** de seguridad y es **transparente** cuando hay problemas de seguridad.

3 BUENAS PRÁCTICAS EN LA ADMINISTRACIÓN Y USO DE REUNIONES WEBEX

Propuesta	Acciones
Evitar que los asistentes no autorizados se unan a las reuniones	• Utilice un enlace único protegido por contraseña para los usuarios con invitación (predeterminado). • Bloquee automáticamente las salas de reuniones para restringir la entrada (predeterminado). • Coloque automáticamente a los asistentes externos o no autenticados en una sala de espera (predeterminado). • Requerir contraseña o inicio de sesión para teléfonos y dispositivos de vídeo.
Evitar interrupciones durante la reunión	• Impedir la posibilidad de unirse a una reunión antes del anfitrión. • Bloquee manualmente su sala de reunión. • Configurar que solo el presentador pueda compartir contenido. • Configure su sala de reunión para que se bloquee automáticamente después de una duración especificada. • Haga que los participantes que se unan a una sala personal que está cerrada sean colocados en el lobby hasta que sean admitidos por el anfitrión.
Limitar las reuniones solo a los usuarios internos	• Aplique inicio de sesión único (SSO) para unirse o entrar a una sala de reuniones personal.

	• Requerir roles de asistente.
Prevenir el reenvío de invitaciones	• Exigir que solo los usuarios invitados puedan unirse a las reuniones.
Habilitar a un anfitrión para administrar de forma segura una reunión de la sala personal	• Diferencia visual en usuarios internos/externos en la lista • Tonos de entrada y salida • Bloquear la sala de reunión • Habilite una notificación por correo electrónico para que se le envíe en caso de que alguien entre en el lobby de su habitación personal mientras usted está fuera • Activar/desactivar las funciones disponibles como chat, vídeo, opciones de voz • Expulsar, bloquear, silenciar, etc.
Administrar el control de compartición de archivos	• El administrador puede optar por habilitar o deshabilitar selectivamente el uso compartido de archivos (Meetings y Teams). • El administrador puede limitar el uso compartido de archivos en función del tipo de cliente (Webex Teams).
Administrar integraciones externas (para Meetings y Teams)	• Un cliente puede permitir o denegar a sus usuarios que utilicen cuentas de Google, cuentas de Microsoft Office 365, cuentas de Facebook y otras aplicaciones de terceros con su cuenta de Cisco Webex. Además, los clientes también pueden asegurarse de que solo se pueden habilitar para sus usuarios aquellas aplicaciones de terceros para Webex Teams (desarrolladas mediante la API disponible en developer.webex.com) que cumplen con sus estándares de seguridad y control de datos. • Los clientes pueden optar por permitir o denegar el acceso a estas aplicaciones de terceros para todos los miembros de la organización o para usuarios específicos.
Administrar bots	• Se puede gestionar bots para espacios de Webex Teams, administrando las integraciones externas, para controlar la salida de información y reducir el riesgo. Los administradores pueden establecer políticas globales para permitir o denegar bots. En caso de "denegación global", se puede configurar una lista blanca de bots soportados.

4 CONTROLES DE SEGURIDAD DE WEBEX

La seguridad de la suite de Webex se gestiona a dos (2) niveles. El primero es un supra-nivel global de la organización gestionado por los administradores de la plataforma y en segundo lugar a nivel de personalización de las salas personales asignadas a cada usuario.

4.1 Controles de seguridad para administradores de Webex

Las funciones de control de seguridad de administración se encuentran disponibles a los administradores a través del Control Hub (admin.webex.com).

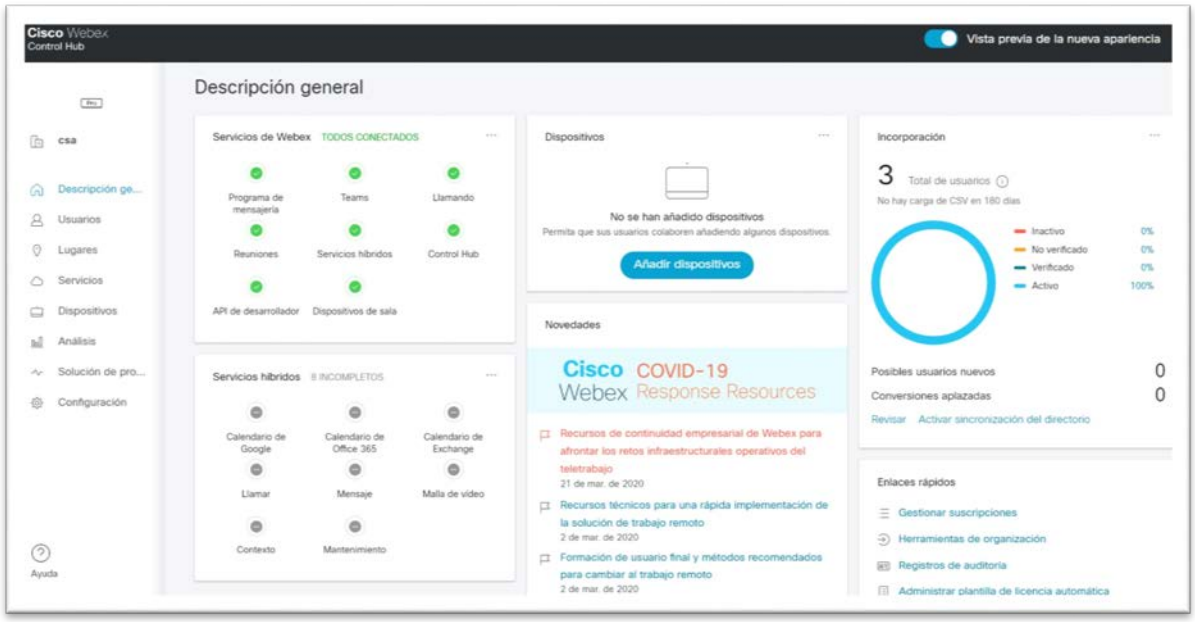


Ilustración 1.- Control Hub (Concentrador de control)

Los siguientes parámetros de seguridad son los recomendados en la pestaña configuración del control hub (https://admin.webex.com/settings).

4.1.1 Seguridad en dispositivos móviles

Deshabilitar la vista previa de mensajes: un cliente puede asegurarse de que las vistas previas de mensajes para las notificaciones móviles siempre estén deshabilitadas para que los usuarios cercanos no puedan observar los mensajes que se recibe en el dispositivo. O si el dispositivo está bloqueado y dejado sin supervisión del usuario, otros usuarios no podrán seguir viendo vistas previas de los mensajes que se envían mirando la pantalla bloqueada del dispositivo.

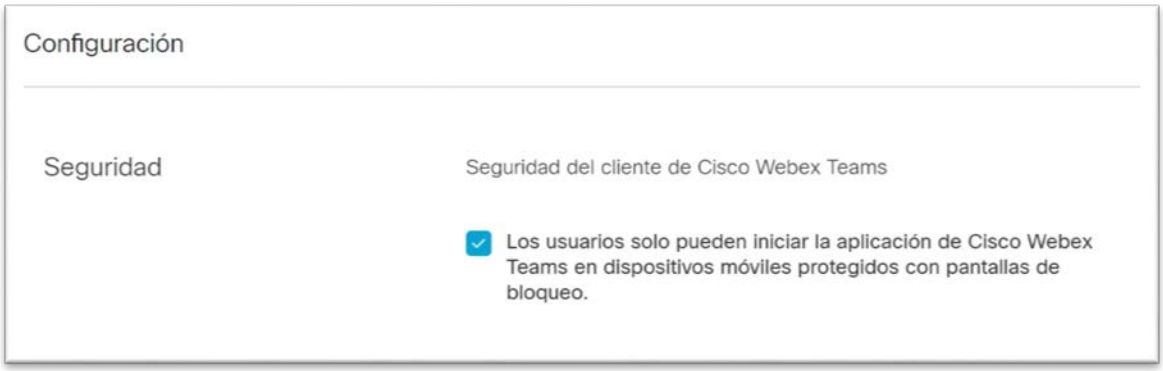


Ilustración 1.- Privacidad vista previa en móviles

4.1.2 Cerrar sesiones de usuario web por inactividad

Tiempo de **inactividad personalizado para las interfaces del navegador.** Un administrador de Cisco Webex usando el concentrador de control (Control Hub), o un

usuario usando la interfaz del navegador, no tiene que preocuparse de dejar su portátil desatendido.

Se establece un tiempo de espera personalizado en el concentrador de control que permite a un administrador reducir el riesgo de seguridad de estos eventos al finalizar sesiones inactivas después de un período de tiempo de espera (opcionalmente entre 10 minutos y 60 minutos). El concentrador de control también tiene un tiempo de espera inactivo predeterminado de 20 minutos.

Estos tiempos de espera se pueden personalizar más para dentro y fuera de la red. Si un usuario está iniciando sesión en el sistema en la seguridad de VPN, el período de tiempo de espera inactivo de la red de la empresa puede ser más largo (o nunca activado), y las duraciones se pueden hacer más cortas si están en una red pública.

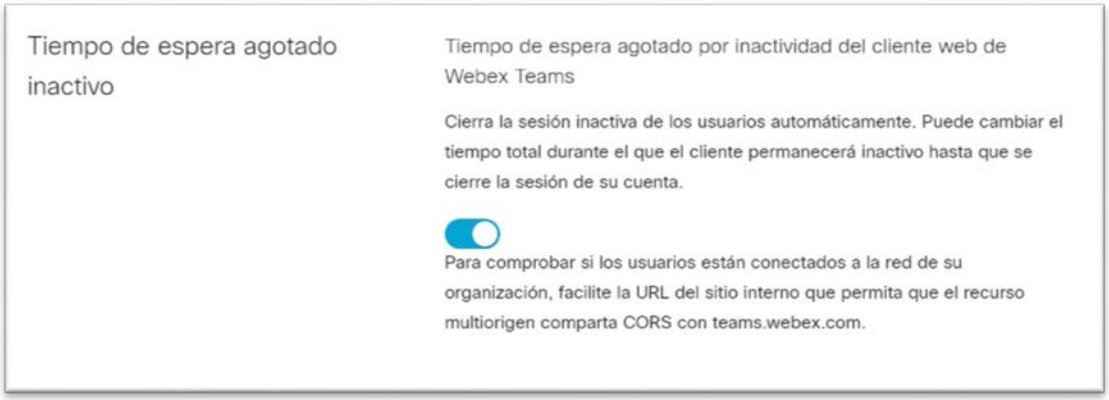


Ilustración 2.- Desconexión por inactividad

4.1.3 Control de comunicaciones externas

La función *Bloquear comunicaciones externas* permite a los administradores controlar la colaboración entre organizaciones de las siguientes maneras:

- Todos los usuarios de su organización tienen restringida la comunicación con cualquier persona perteneciente a organizaciones externas en Webex Teams.
- Los usuarios de la organización no pueden agregar usuarios fuera de los dominios aprobados o unirse a espacios creados por dominios no aprobados en Webex Teams.
- Usar el rol de asistente y el control "Requerir inicio de sesión antes del acceso al sitio" para bloquear a los participantes externos a su sitio de Meetings.

- Habilitar la pestaña de bloqueo de mensajes externo debe ser evaluada cuidadosamente pues implica invitar a usuarios externos a la organización a los grupos de colaboración

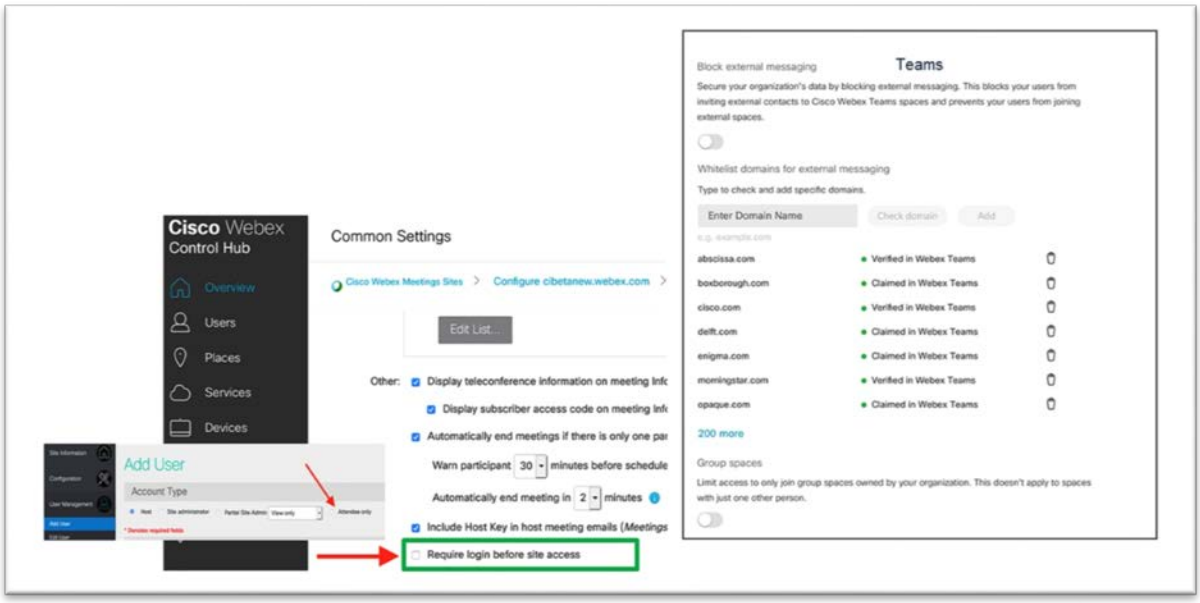


Ilustración 3.- Dominios de terceros permitidos

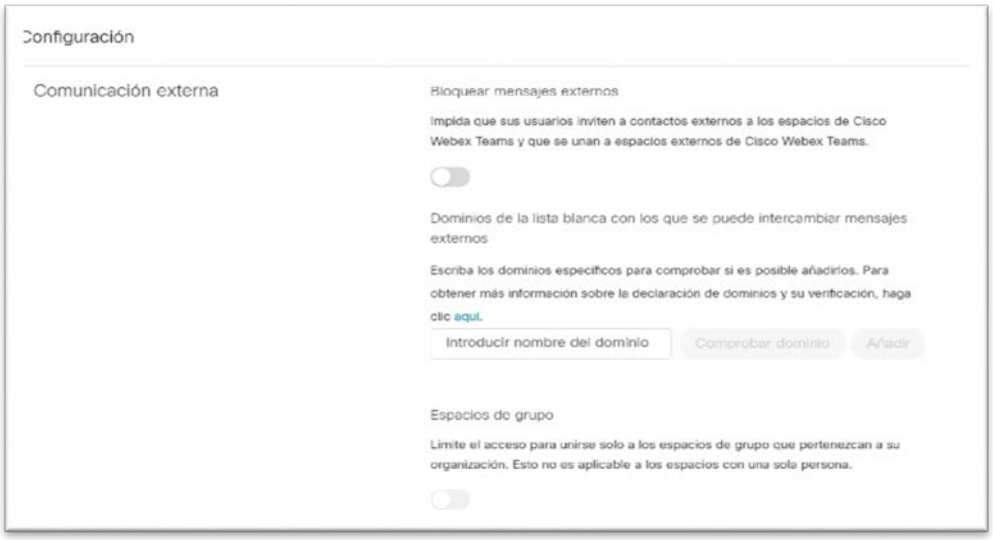


Ilustración 4.- Mensajes externos

4.1.4 Privacidad

La configuración de privacidad permite seleccionar el nivel de detalle de visualización y de intervención que su socio tecnológico o asistente de soporte tenga de su configuración.

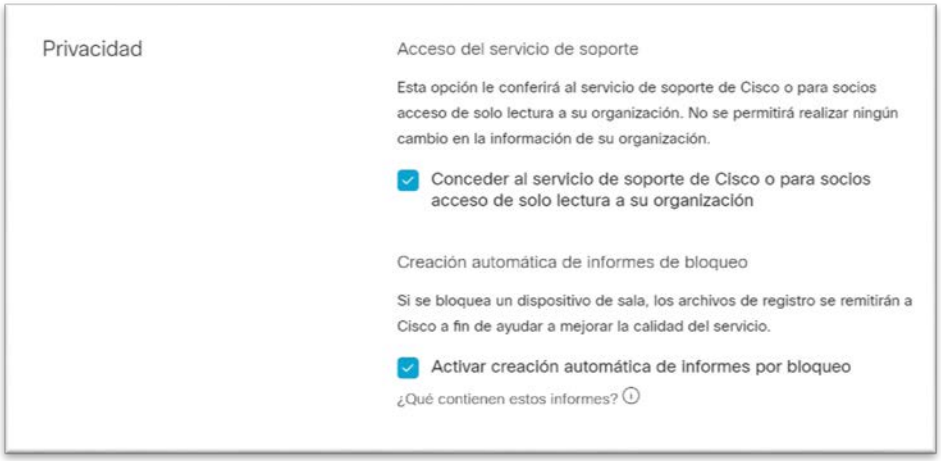


Ilustración 5.- Privacidad

4.1.5 Autenticación de usuarios

Activación del servicio de sesión único (SSO): esta sincronización unidireccional garantiza que los usuarios no solo se aprovisionen cuando se conecten a la empresa, sino que, lo que es más importante, garantiza que a los usuarios se les desprovean de sus datos aprovisionados y que los tokens se revoquen cuando la empresa decida que deben eliminar esa cuenta de usuario.

Prueba de identidad: los administradores comprueban sus dominios para asegurarse de que los usuarios que aprovisionan son quienes dicen ser, de modo que cuando se une a una reunión puede confiar en con quién está colaborando.

Se soporta sistema para el aprovisionamiento de administración de identidades entre dominios (SCIM): incorporación de usuarios a través de integraciones de Okta y Azure AD mediante SCIM, el estándar del sector.

También son compatibles la API People en https://developer.webex.com y CSV.

Ilustración 6.- Inicio de sesión

4.2 Gestión de preferencias de la sala personal del usuario

El usuario tiene acceso a configuraciones particulares de su sala personal de reuniones de Webex meetings a través de un acceso web tipo https://(dominio).webex.com o a través de la pestaña “Sala Personal” de la aplicación.

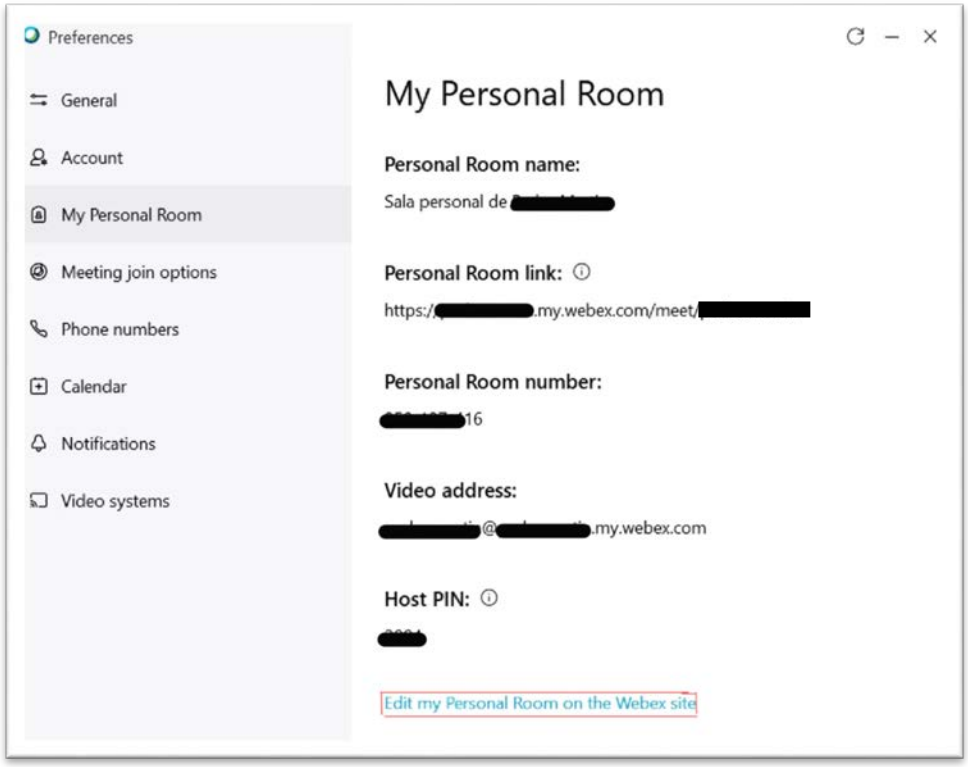


Ilustración 7.- Acceso web vía app

- Personalización del nombre de sala y su enlace.
- Pin del organizador debe cumplir unos requisitos.

Ilustración 8.- personalización de sala y pin

- Bloquear la sala automáticamente tras empezar la reunión, para evitar la intrusión accidental de participantes.

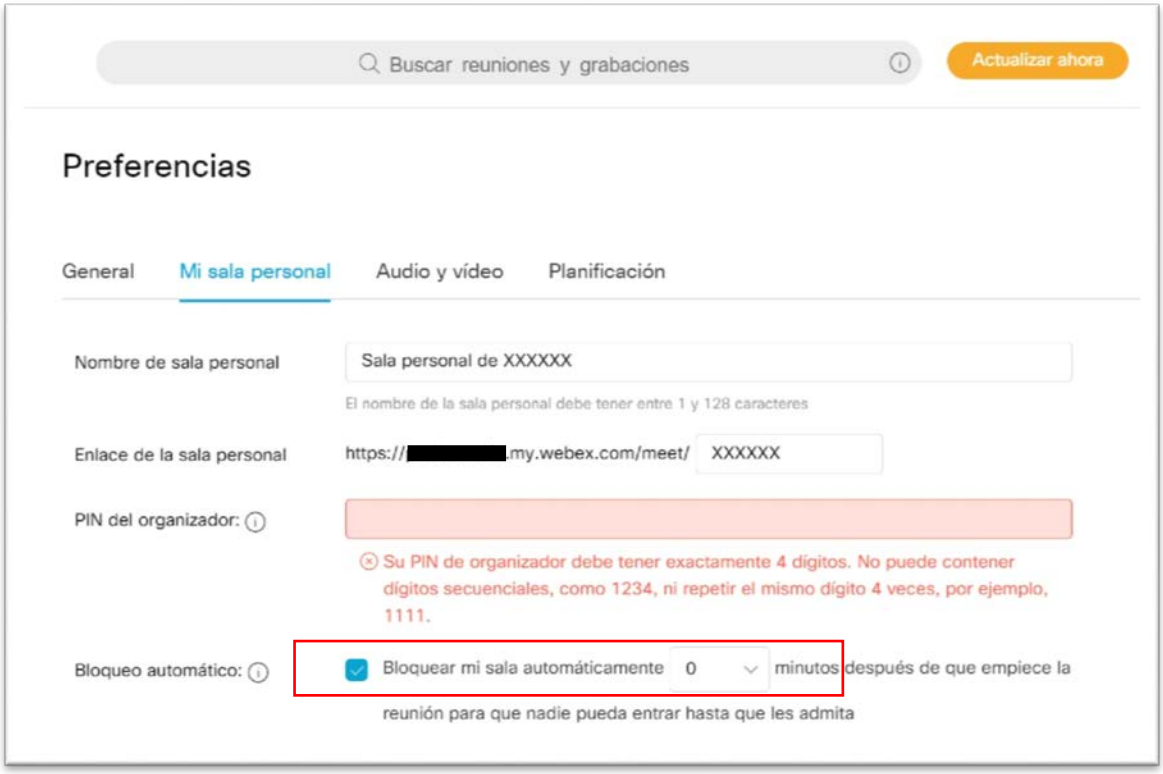


Ilustración 9.- Bloqueo de sala

- Notificación de participantes esperando en Lobby (Sala de espera) al organizador y delegación de permisos a organizadores alternativos.

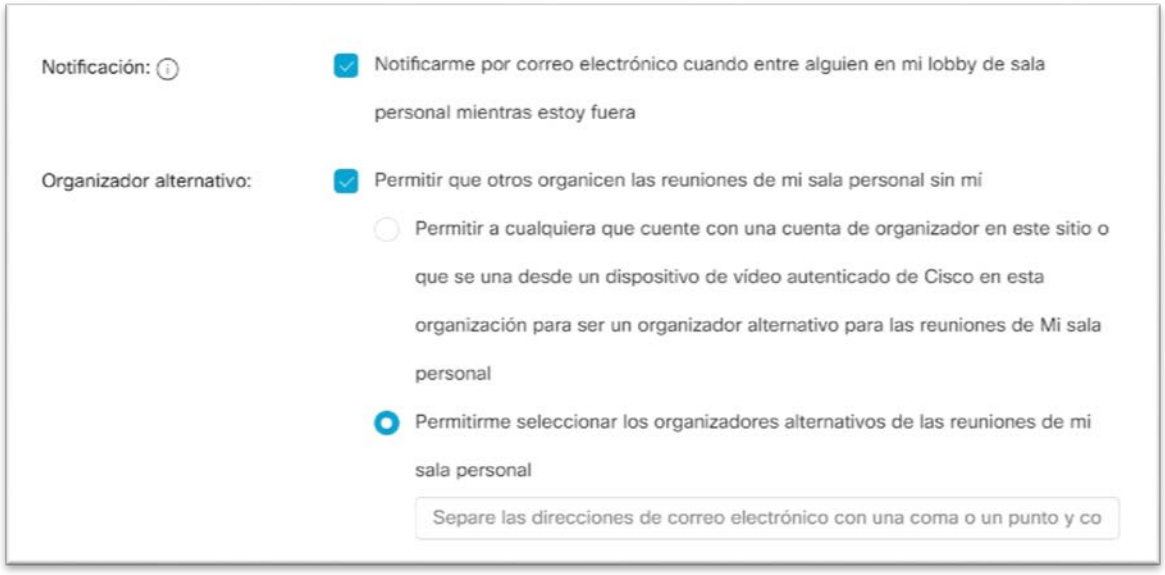


Ilustración 10.- Notificación de participantes en lobby

5 OPERATIVA

Para el acceso a las reuniones, Cisco Webex dispone de salas de reuniones virtuales y salas personales, que permiten que cada usuario disponga de una dirección y código de reunión único, siempre disponible y gestionado por el propio usuario con control de

acceso al bloquear las reuniones automáticamente, según las recomendaciones anteriores.

Existen tres (3) metodologías para la creación de reuniones, a través del portal web, de la aplicación de escritorio o móvil y de un *plugin* para Outlook.

5.1 Crear reunión desde la aplicación de escritorio

- Iniciar una reunión inmediata en la sala personal.

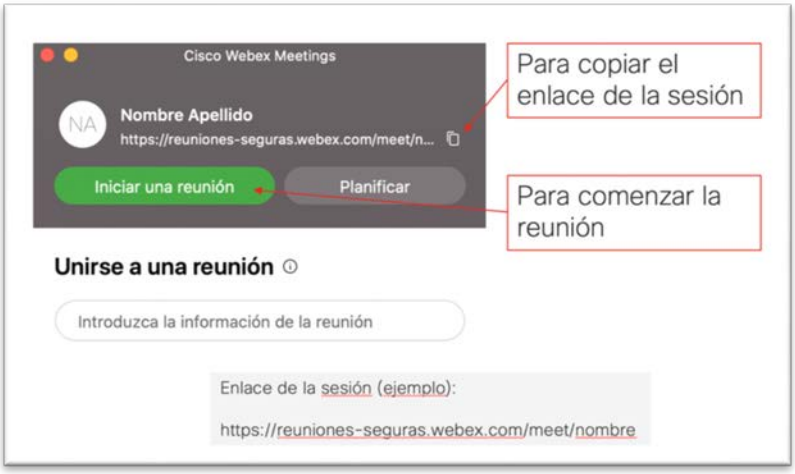


Ilustración 11.- Iniciar reunión

- Planificar una reunión.

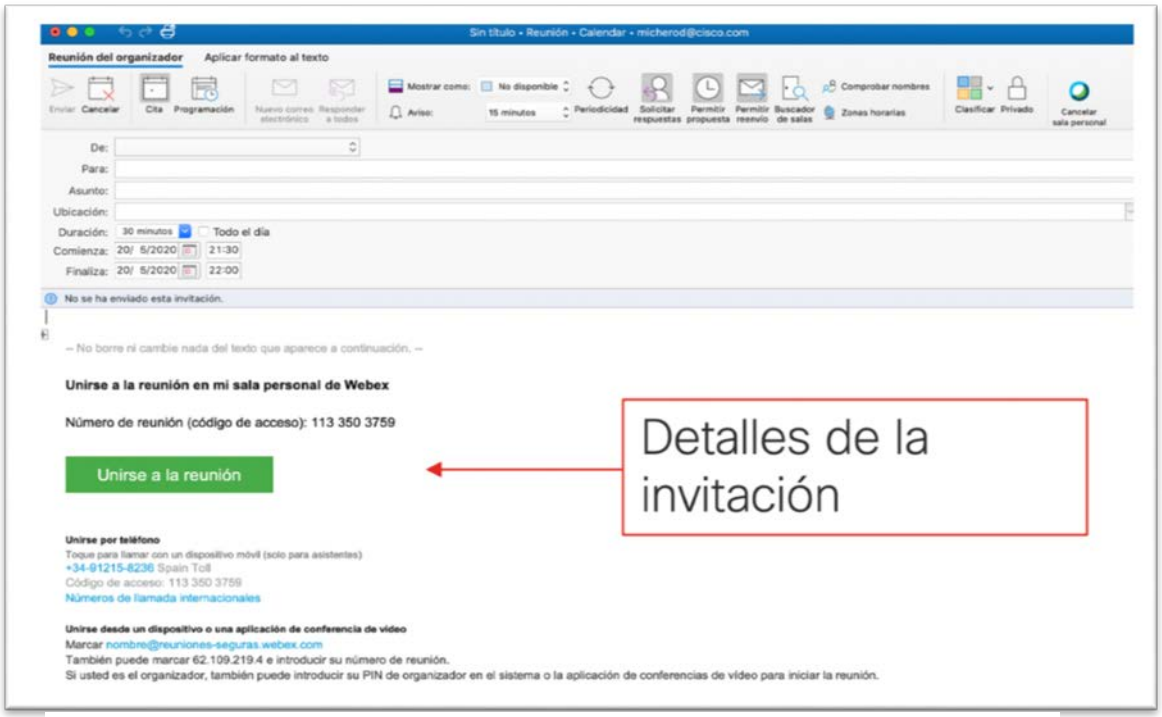


Ilustración 12.- Detalles de la invitación a la reunión

Ilustración 13.- Planificar reunión

5.2 Crear reunión desde el portal Webex

El usuario tiene acceso web a su sala personal de reuniones de Webex meetings a través de un acceso tipo https://(dominio).webex.com .

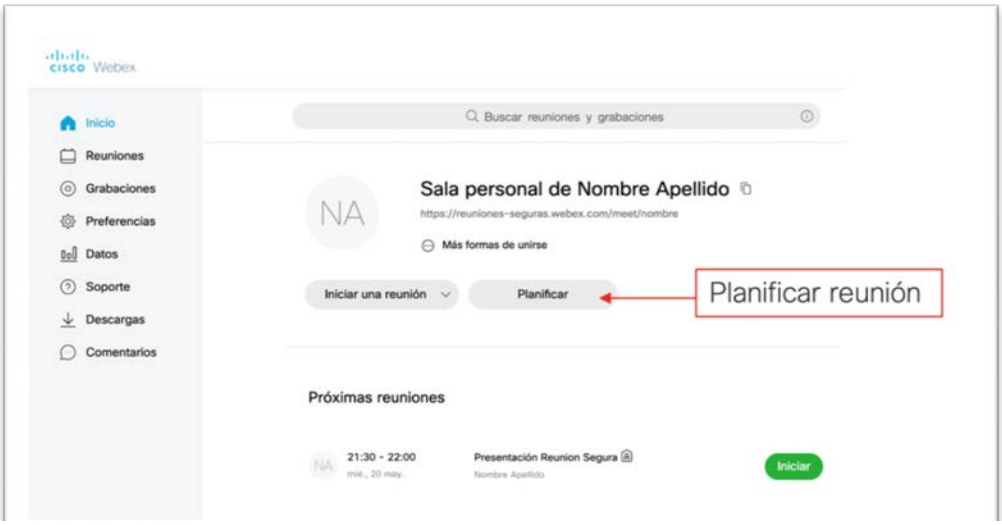


Ilustración 14.- Planificación de reunión

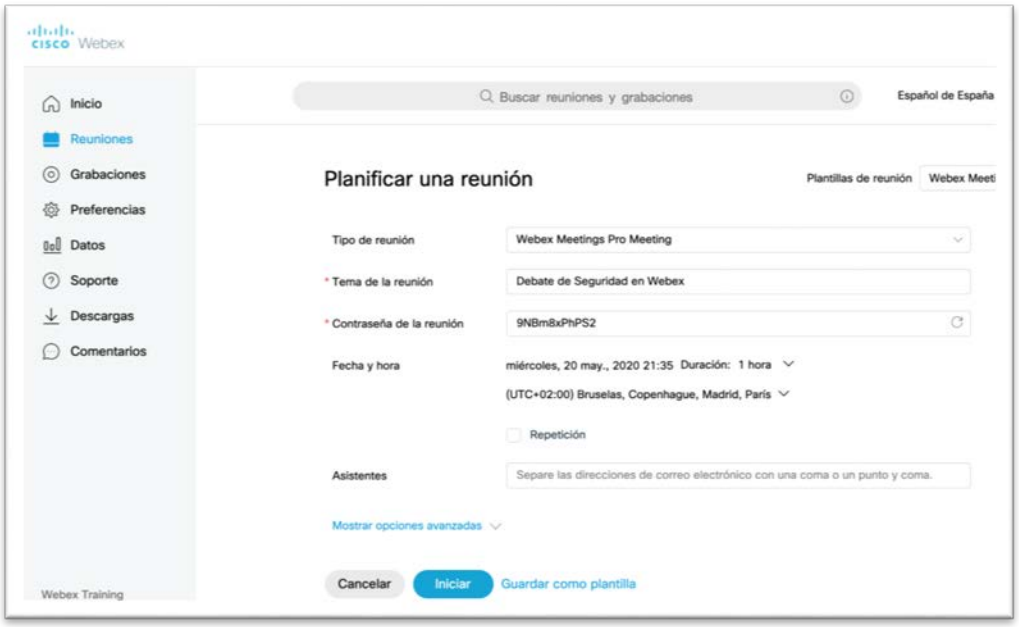


Ilustración 15.- Detalles de reunión

5.3 Crear reunión desde Outlook

Cisco Webex también habilita la inclusión de un *plugin* en el gestor de correo, poniendo a disposición del usuario generar una reunión con un solo clic, con las características de seguridad previamente configuradas.

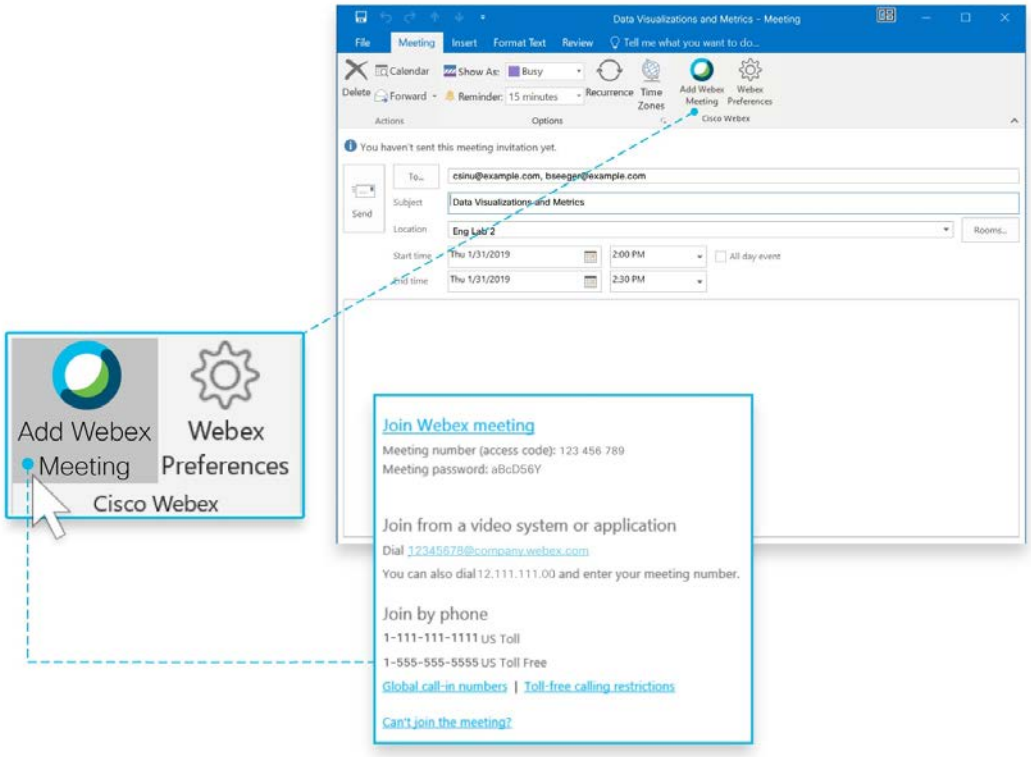


Ilustración 16.- Plugin Outlook

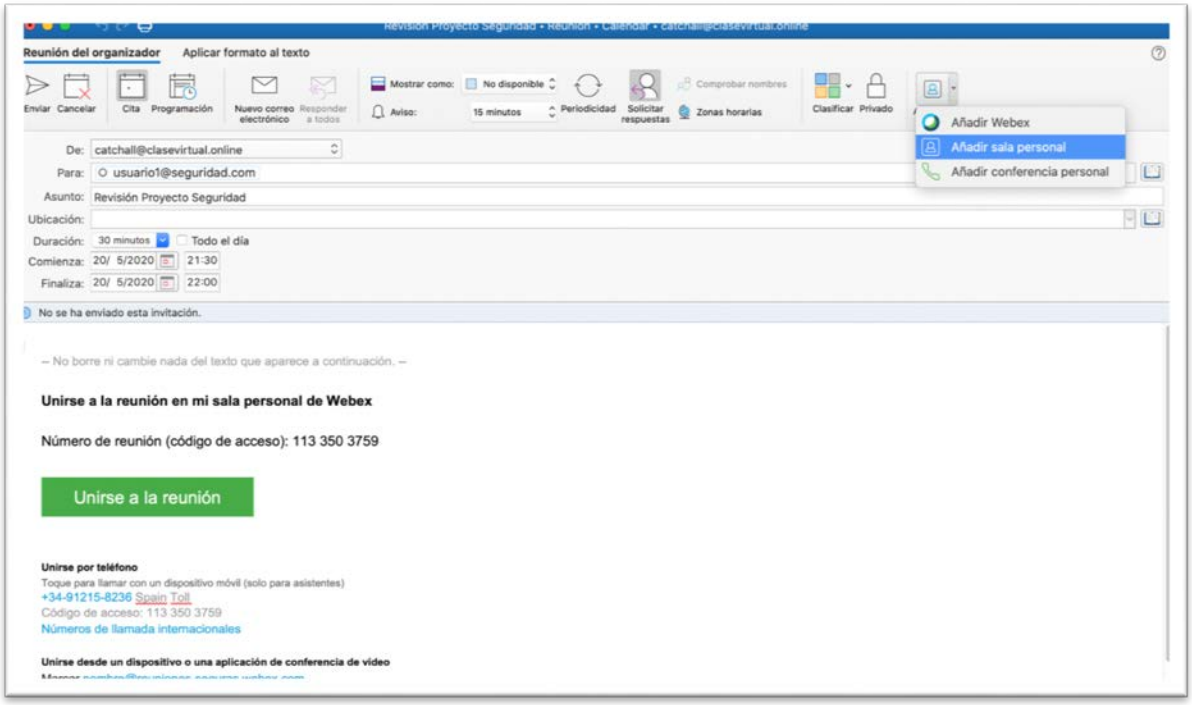


Ilustración 17.- Plugin Webex en Mac

5.4 Recomendaciones para el ámbito educativo

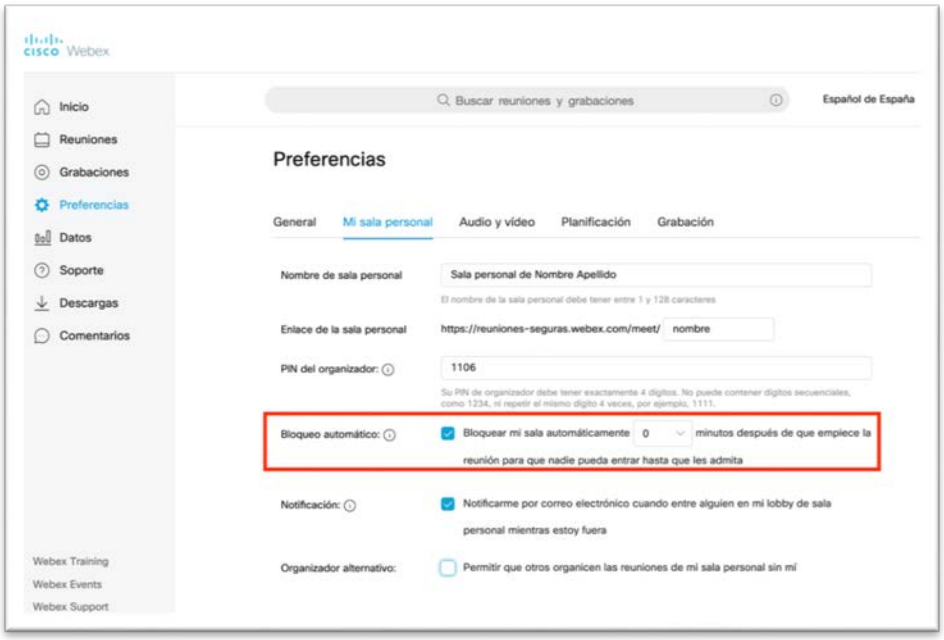


Ilustración 18.- Bloqueo de sala

- **Bloquear la clase virtual**. Desde el sitio web, se puede configurar el bloqueo de la sala después de que comience la clase virtual automáticamente y no dejar que nadie entre sin que el profesor autorice el acceso.
- **Desactivar** la posibilidad de que los estudiantes compartan la pantalla sin permiso.

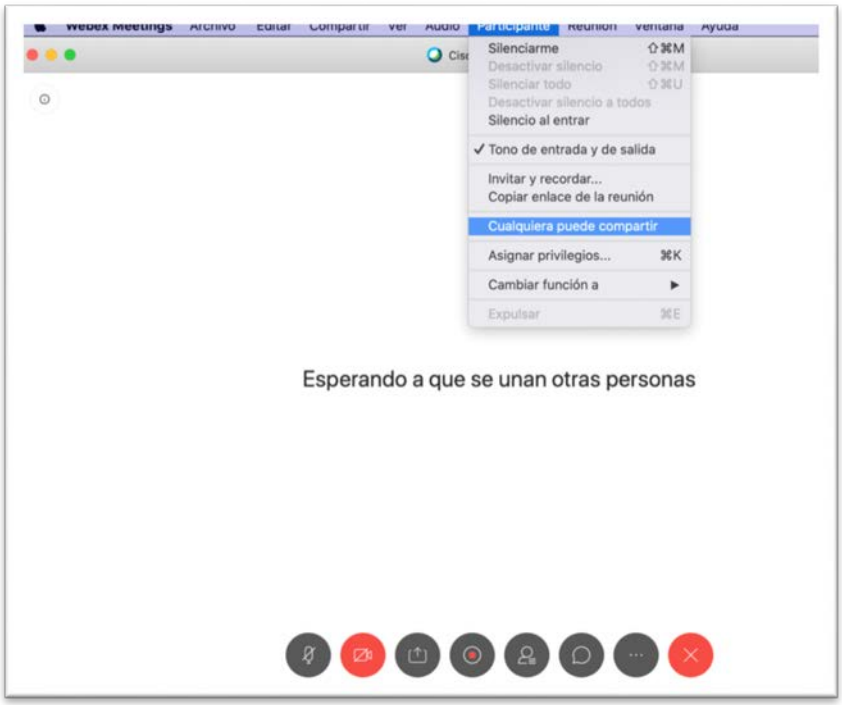


Ilustración 19.- Habilitar compartición de contenido

- Si no se ha configurado automáticamente, **bloquear la sala** cuando comience la clase. Siempre aparecerá una notificación para admitir alumnos que están en la sala de espera.

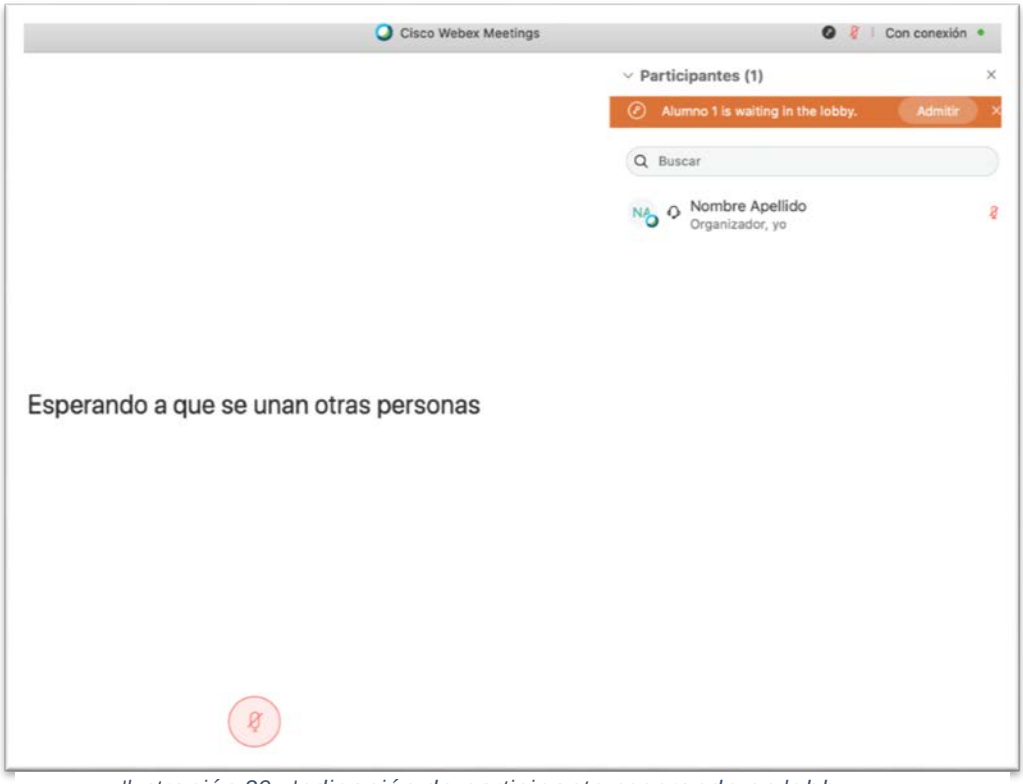


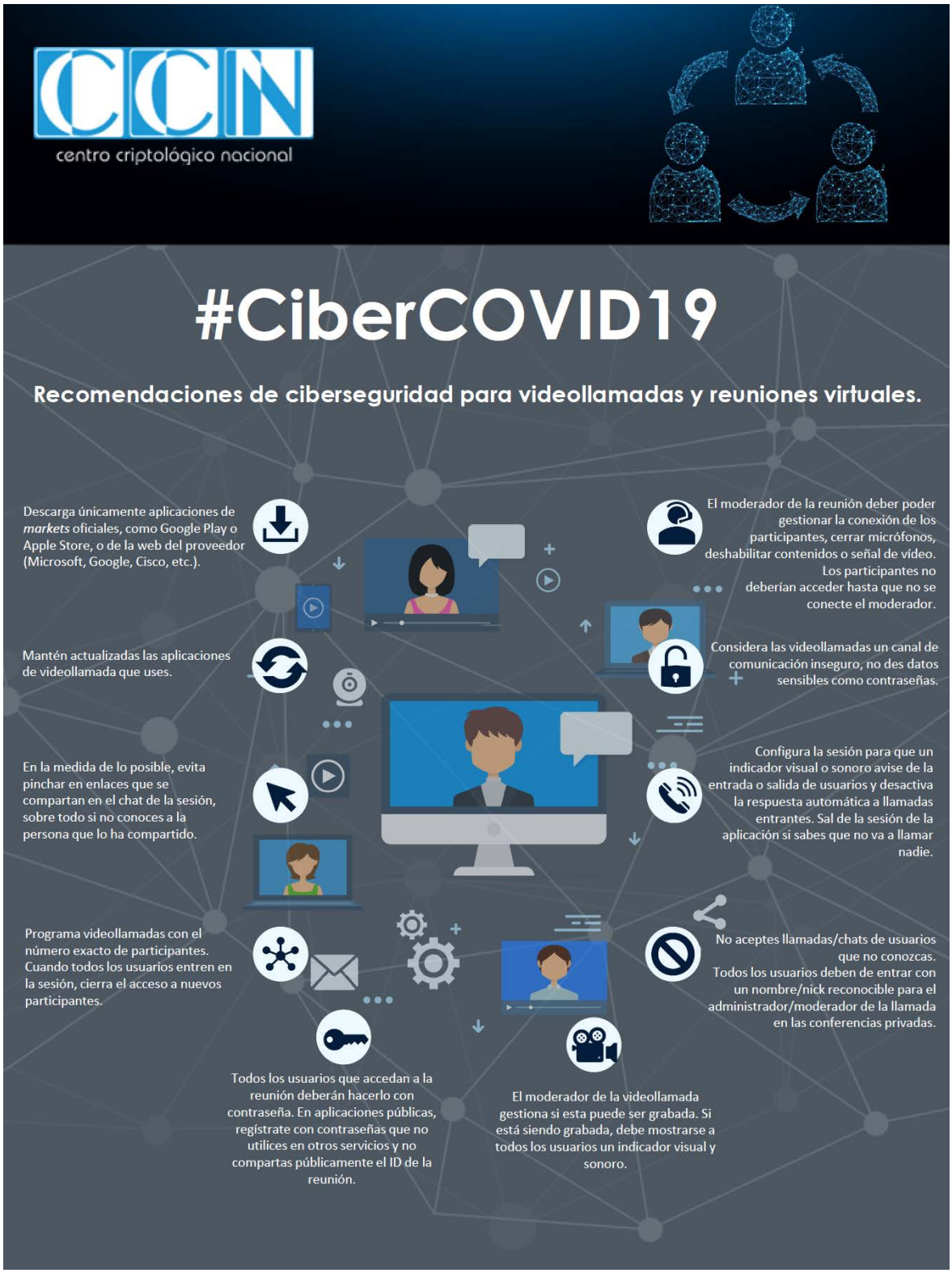
Ilustración 20.- Indicación de participante esperando en lobby

- Solicitar a los que ingresen que se **identifiquen y activen la cámara**. En cualquier caso, es una buena práctica que el profesor active su vídeo.
- **Expulsar o mover** a los alumnos que no se identifican correctamente en la sala de espera.

6 CONCLUSIONES

Cisco ofrece un ecosistema de soluciones extremo a extremo, donde Cisco Webex es la parte de plataforma de colaboración que permite la realización de reuniones, eventos, cursos de formación, soporte remoto, mensajería de grupo, con servicios de audio, video y compartición, interoperable con todas las plataformas de video de sala basadas en estándares H323 y SIP, con posibilidades de ser un servicio puramente en la nube con un licenciamiento flexible por uso o bien un modelo tradicional de servicios alojados en los centros de procesamiento de datos del cliente o bien en una modalidad hibrida entre ambos entornos.

Esto garantiza a los usuarios elegir la mejor modalidad de despliegue de la solución que se ajuste a la normativa de seguridad de su organización.



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
2020.05.22 12:32:16 +02'00'