Recomendaciones y buenas prácticas para el uso de la aplicación Jitsi

Abstract: ante la generalización del empleo de plataformas de videoconferencias y reuniones virtuales, se realiza en este documento un análisis de la aplicación Jitsi, al tiempo que se ofrecen recomendaciones y buenas prácticas para un uso más seguro de la plataforma.

Contenido:

1. INTRODUCCIÓN

Jitsi (antes SIP Communicator) es una aplicación de videoconferencia, VoIP y mensajería instantánea con aplicaciones nativas para iOS y Android, y con soporte para MS Windows, Linux y macOS a través de la web. Se distribuye bajo los términos de la licencia Apache, por lo que es software libre y de código abierto.

Con el crecimiento de WebRTC, el enfoque del equipo del proyecto se trasladó a Jitsi Videobridge para permitir videollamadas múltiples basadas en la web. Más tarde, el equipo agregó Jitsi Meet, una aplicación de videoconferencia completa que incluye clientes web, Android e iOS.

Jitsi también opera meet.jit.si, una versión de Jitsi Meet alojada por Jitsi para uso gratuito. Cuenta con diferentes módulos y librerías para implementar servicios y funcionalidades como SIP Gateway e integraciones en terceras soluciones.

Actualmente se disponen de 73 repositorios de código abierto relativos a Jitsi en Github. Los principales proyectos incluyen:

- **Jitsi Meet**: servidor de videoconferencia diseñado para una instalación rápida en servidores Debian/Ubuntu.
- **Jitsi Videobridge**: motor de unidad de reenvío selectivo WebRTC para impulsar conferencias multipunto.
- **Jigasi**: aplicación del lado del servidor que permite a los clientes SIP habituales unirse a las conferencias JitMeet organizadas por Jitsi Videobridge.
- **lib-jitsi-meet**: una API de JavaScript de bajo nivel para proporcionar un interfaz de usuario personalizada para Jitsi Meet.
- **Jidesha**: una extensión de Chrome y Firefox para Jitsi Meet.
- **Jitsi**: un comunicador de audio, video y chat que admite protocolos como SIP, XMPP/Jabber, AIM ICQ e IRC.

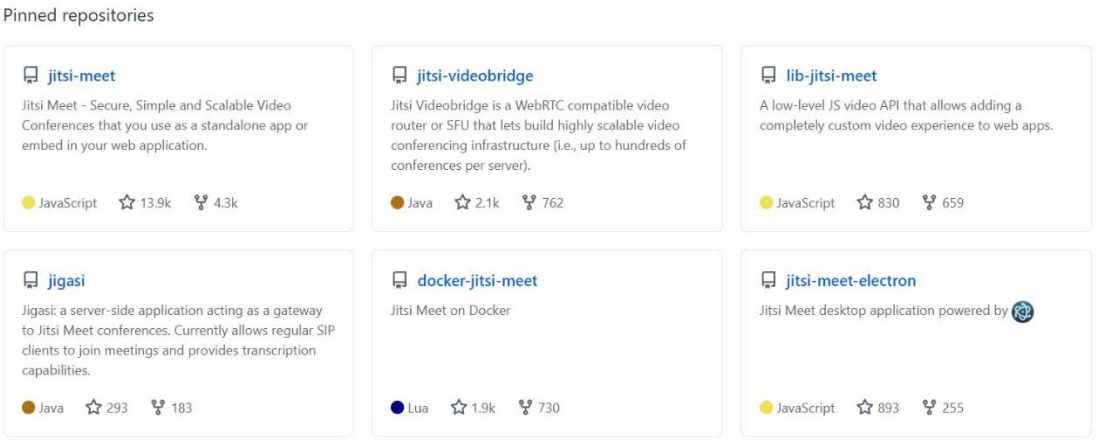


Ilustración 1.- Repositorios más relevantes de Jitsi en: https://github.com/jitsi

Jitsi comenzó su andadura en 2003 en el marco de un proyecto estudiantil de Emil Ivov, en la Universidad de Estrasburgo. Originalmente, el proyecto se utilizó sobre todo como una herramienta de experimentación debido a su soporte de IPv6.

Jitsi ha recibido apoyo de diversas instituciones como la Fundación NLnet, la Universidad de Estrasburgo y la región de Alsacia, y ha participado en varias ocasiones en el Google Summer of Code.

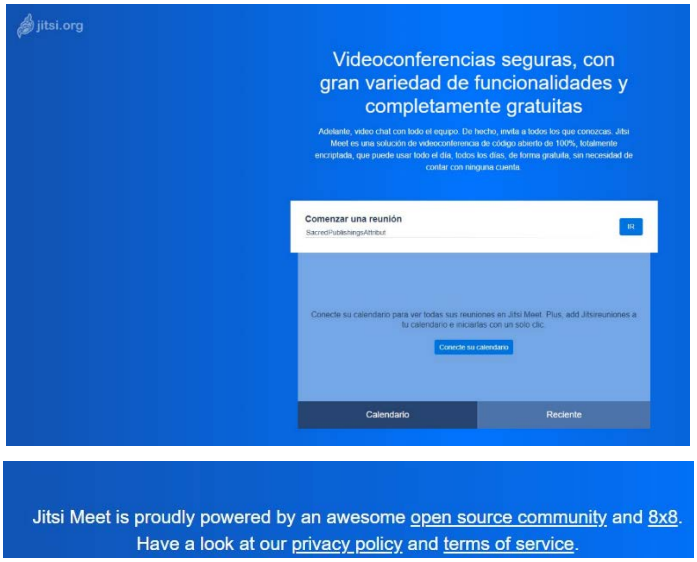
Atlassian adquirió BlueJimp (Jitsi) el 5 de abril de 2015. Después de la adquisición, el nuevo equipo Jitsi de Atlassian dejó de realizar nuevos trabajos de desarrollo en el proyecto Jitsi Desktop y amplió sus esfuerzos en los proyectos relacionados con Jitsi Videobridge y Jitsi Meet.

En octubre de 2018, 8x8, compañía con sede en California y cotizada en bolsa (NYSE, S&P 600), compró Jitsi. 8x8 ofrece servicios comerciales de videoconferencia y comunicaciones bajo su marca con tecnología Jitsi. Asimismo, soporta y provee los servicios para Meet.jit.si gratuitos en la nube.

2. MODELOS DE LA PLATAFORMA

2.1 Meet.Jit.Si

Meet.jit.si es un servicio Cloud gratuito basado en navegador web bajo el protocolo WebRTC, alojado en servidores de internet mantenidos por Jitsi.org con el apoyo de la compañía matriz 8x8.



2.2 Jitsi Meet

Jitsi Meet es el cliente o aplicación WebRTC de JavaScript de código abierto y puede utilizarse para videoconferencias. Es compatible con Android, macOS, MS Windows y Linux. Además, permite compartir escritorio y presentaciones y con solo un enlace puede invitar a nuevos miembros a videoconferencias. Adicionalmente, se puede utilizar directamente en un navegador o descargar la aplicación.

Ilustración 1.- Interfaz web

Se usa indistintamente como App o Cliente desktop para meet.jit.si y también permite cambiar la dirección de la instancia (Servidor Videobridge) a un servidor particular con instalación on-premise.

2.3 Jitsi Videobridge

Jitsi Videobridge es un servidor XMPP de videoconferencia, compatible con WebRTC, que permite la comunicación de vídeo multipunto. Es una instancia desplegable on-premise que permite una configuración y personalización bajo demanda del gestor e implementación con otros módulos y soluciones.

A diferencia de las costosas MCU de hardware dedicado, Jitsi Videobridge no mezcla los canales de vídeo en un flujo de vídeo compuesto, sino que solo transmite los canales de vídeo recibidos a todos los participantes de la llamada. Por lo tanto, si bien debe ejecutarse en un servidor con gran ancho de banda de red, la potencia de la CPU no es tan crítica para el rendimiento, abaratando los costos en servidores y licencias de virtualización.

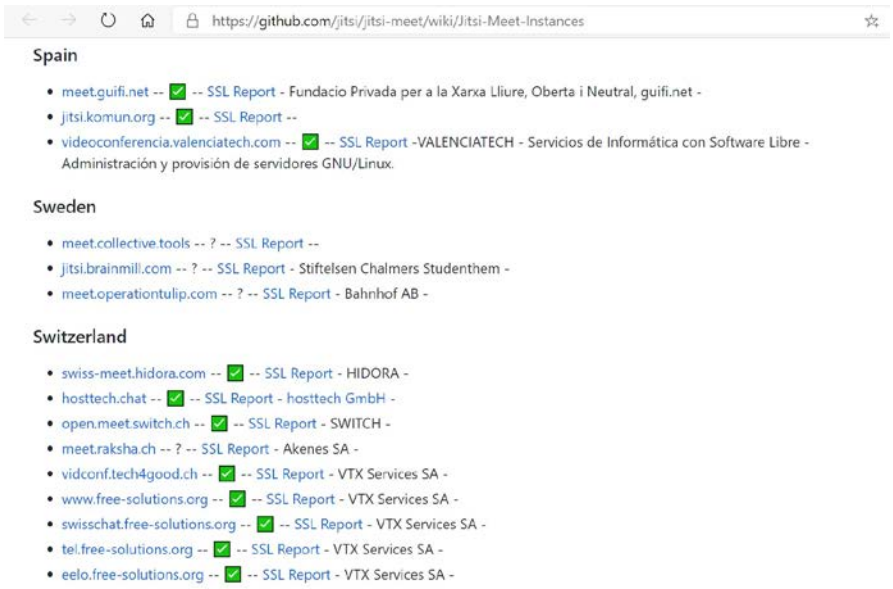


Ilustración 2.- Ejemplo de instancias públicas y gratuitas, alojadas por organizaciones o empresas privadas

3. PRIVACIDAD Y SEGURIDAD

Jitsi Meet es un proyecto de código abierto, lo que significa que cualquiera puede descargar y examinar el proyecto, hecho que a nivel de seguridad tiene ventajas e inconvenientes, ya que la comunidad puede acceder al código abierto y participar en la búsqueda de brechas y cualquier vulnerabilidad o exploits, que le permita ganar acceso a las máquinas o datos.

En el momento de escribir este documento, no hay advertencias de seguridad relacionadas con el envío de datos de Jitsi Meet a fuentes externas o la filtración de

información privada en otros lugares. Tampoco hay ningún tipo de aviso sobre la **propagación de malware** usando la App de Jitsi Meet.

La recomendación siempre es instalar las App desde fuentes confiables y no aceptar vía chat u otros medios hipervínculos sospechosos o dudosos que pudieran derivar en la ejecución de código malicioso en los dispositivos.

3.1 Vulnerabilidades

Actualmente hay publicados tres (3) avisos de vulnerabilidades relativos a Jitsi, aunque ninguno de ellos conlleva un riesgo, pues están referidos a tres (3) casos específicos de implementación con otros módulos de desarrollo como Docker, implementaciones incorrectas de servicios en versiones antiguas o módulos adicionales como Jitsi Electron.

Name	Description
CVE-2020-25019	jitsi-meet-electron (aka Jitsi Meet Electron) before 2.3.0 calls the Electron shell.openExternal function without verifying that the URL is for an http or https resource, in some circumstances.
CVE-2020-11878	The Jitsi Meet (aka docker-jitsi-meet) stack on Docker before stable-4384-1 uses default passwords (such as passw0rd) for system accounts.
CVE-2017-5603	An incorrect implementation of "XEP-0280: Message Carbons" in multiple XMPP clients allows a remote attacker to impersonate any user, including contacts, in the vulnerable application's display. This allows for various kinds of social engineering attacks. This CVE is for Jitsi 2.5.5061 - 2.9.5544.

3.2 Privacidad

En el momento de la redacción de este informe, la empresa 8x8 y Jitsi.org, como proveedor del servicio meet.jit.si, no ofrecen ninguna respuesta clara sobre el cumplimiento del Reglamento General de Protección de Datos (RGPD). Tampoco hay información relativa a la ubicación geográfica de las instancias que dan soporte a meet.jit.si.

El **cumplimiento del RGPD** en el caso de instancias privadas de Jitsi Videobridge on-premise quedan sujetas a la normativa de aplicación en el alojamiento del propietario de la instancia.

En cuanto a la privacidad, cabe destacar que en Jitsi se emplea Google Analytics para evaluar el uso de funciones y posibles errores, existiendo la posibilidad de código

desarrollado por terceros que permite desactivar esta opción desde el cliente que habilita al equipo como servidor.

También cabe destacar que debido a que la solución WebRTC no requiere de registro, se garantiza que determinados datos personales nunca serán proporcionados a la plataforma.

¿Qué información personal procesa el servicio en la nube meet.jit.si?

Para proporcionar el servicio meet.jit.si, 8 × 8 procesa la red y la información de uso, incluidas las direcciones IP de los participantes de la reunión, la URL especificada por el usuario utilizada para organizar la reunión e información sobre los números de teléfono que se conectan a la reunión (si se trata de audio la conexión se realiza mediante una llamada telefónica).

En algunos casos, el contenido relacionado con la reunión, que puede contener información personal, se almacena temporalmente para habilitar la funcionalidad del usuario en una videoconferencia de meet.jit.si.

Ejemplos:

- Si se utiliza la función de chat, el contenido del chat se almacena durante la reunión.
- Si se graba una reunión, la grabación de la reunión se almacena temporalmente hasta que se carga en su servicio de alojamiento de archivos (por ejemplo, Dropbox).
- Si se transmite en vivo su reunión, el contenido de vídeo se almacena temporalmente para almacenar en búfer la transmisión en vivo.
- Además, los usuarios de meet.jit.si tienen la opción de proporcionar el nombre, la dirección de correo electrónico y el enlace a una imagen que se mostrará a los participantes en la reunión.

Métodos de recopilación de analíticas usado por Meet.jit.si

Jitsi publicita en sus documentos sobre privacidad su compromiso con la privacidad y la seguridad. Actualmente, usan Amplitude, Datadog y Crashlytics para cubrir varios aspectos de las aplicaciones y la infraestructura en meet.jit.si.

La información que se rastrea incluye un identificador anónimo (se puede ejecutar en modo "incógnito"), tasa de bits, ancho de banda disponible, ofertas y respuestas de SDP, eventos de utilización de productos o volcado de caída de aplicaciones móviles.

Lo más importante es que una vez que finaliza la reunión, no se guardaría nombre alguno, dirección de correo electrónico o foto de perfil. Esta información solo se transmite a los demás participantes de la reunión.

¿Cómo se usa esta información?

Según indica 8 × 8, se utilizaría la información de los usuarios para ofrecer el servicio meet.jit.si, identificar y solucionar problemas con el servicio meet.jit.si y mejorar el servicio meet.jit.si. Además, 8 × 8 podría utilizar esta información para investigar fraudes o abusos.

3.3 Cifrado

El nivel de cifrado de la aplicación es un aspecto que preocupa a la comunidad. Jitsi Meet por defecto no utiliza cifrado de extremo a extremo (E2EE), como FaceTime o WhatsApp. En estos momentos están **trabajando en una BETA** la posibilidad de cifrado de extremo a extremo sobre WebRTC, utilizando una nueva API de Chrome WebRTC llamada "Flujos insertables" para agregar una segunda capa de cifrado de extremo a extremo a los flujos de medios de una manera que los haría inaccesibles para el Videobridge de Jitsi.

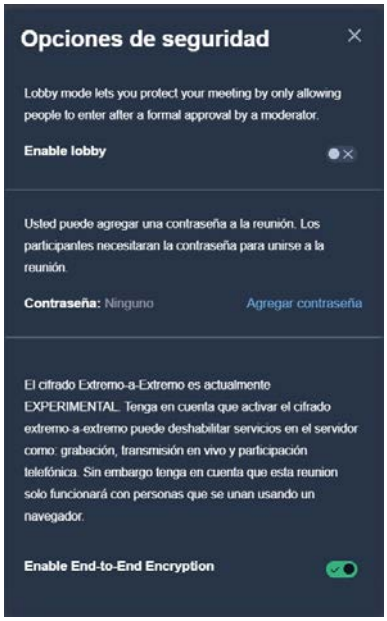


Ilustración 3.- Opciones de seguridad y cifrado de E2EE

En este momento, el modelo estándar de cifrado en Jitsi es el **cifrado de salto a salto,** lo que significa que cada etapa de la videollamada se cifra en parte. La videollamada al servidor va cifrada, el servidor descifra la videollamada, luego la vuelve a cifrar y la reenvía a los participantes del vídeo.

El cifrado de salto a salto no es perfecto y esto significa que la seguridad podría verse comprometida. La forma de evitar este hecho es alojar un servidor Jitsi Meet para lograr así una total privacidad.

Cuando se usa WebRTC, se emplea el cifrado WebRTC de facto: DTLS-SRTP con claves efímeras. Con los flujos insertables, se cifra el payload que va dentro de los paquetes cifrados DTLS-SRTP. Por lo tanto, cuando el puente de vídeo descifra los paquetes SRTP, no podrá ver la media, ya que está cifrada con un cifrador con flujos insertables.

Actualmente, Jitsi usa AES-GCM con claves de 128 bits generadas por una contraseña proporcionada por el usuario usando passphrase de PKDF2. Este aspecto se encuentra en vías de cambio, ya que Jitsi está en proceso de introducir claves por participante e implementar el algoritmo Double Ratchet para la señalización segura de estas claves.

Este modelo de cifrado de salto a salto no significa que Jitsi Meet sea inseguro, pero existe un punto débil definido en el proceso de privacidad y es el cifrado-descifrado de datos en un servidor Jitsi Meet.

La solución a este punto débil, como ya se ha mencionado, sería instalar el software Jitsi Meet en un servidor privado que controle la organización o empresa, de forma que todos los datos permanecerían seguros.

4. RECOMENDACIONES PARA COMUNICACIONES SEGURAS EN JITSI

Jitsi Meet es un software gratuito de videoconferencia cifrada. Jitsi Meet es de código abierto y utiliza por defecto cifrado de extremo a servidor, mediante el cual la comunicación se cifra antes de salir de su dispositivo, se descifra en el servidor, se procesa y se vuelve a cifrar antes de ser enviada a las personas destinatarias.

Es importante utilizar Jitsi Meet en un servidor de confianza o propietario on-premise, debido a que puede ayudar a reducir la superficie de exposición y el riesgo de vigilancia, la interferencia en las llamadas y la venta y/o mal manejo de la información privada de los participantes.

4.1 No requerir registro

Cuando se utiliza un equipo, se recomienda conectarse a una llamada utilizando los navegadores Firefox o Chrome (es posible que otros navegadores no funcionen). También existe la opción de usar un programa de escritorio para Linux, macOS, en MS Windows es Jitsi Desktop.

Cuando utilice teléfono móvil inteligente, se recomienda descargar la aplicación Jitsi de los markets oficiales, disponible para Android e iPhone, y preferentemente emplear la aplicación sobre la opción de navegador.

4.2 Comienzo de una reunión

A la "sala de reunión" (chat room) se puede acceder a través de un enlace, que debe ser compartido de antemano por la persona que organiza la reunión. En relación con las

sesiones de videoconferencia, todas las salas de reuniones son efímeras: solo existen mientras la reunión tiene lugar.

Es decir, las reuniones se crean cuando se une el primer participante y se destruyen cuando se va el último. Si alguien vuelve a unirse a la misma sala, se crea una nueva reunión con el mismo nombre y no hay conexión con ninguna reunión anterior que se haya celebrado con el mismo nombre.

4.3 Generación del link

Para la organización de una reunión, en Jitsi Meet se genera un enlace a través del nombre que se le da a la sala. Este enlace lo puede generar directamente la plataforma de manera aleatoria, aunque también permite que el organizador genere uno personalizado.

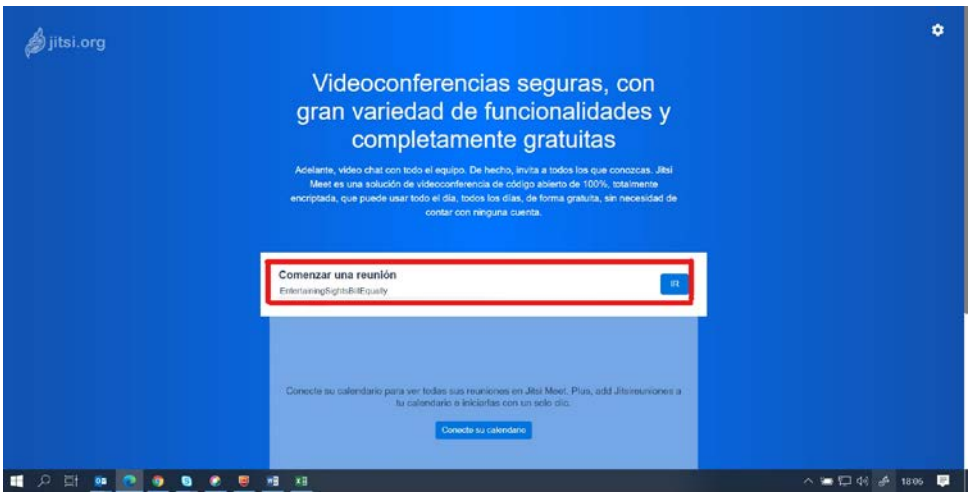


Ilustración 4.- Cómo crear una reunión, generación automática de nombre de sala

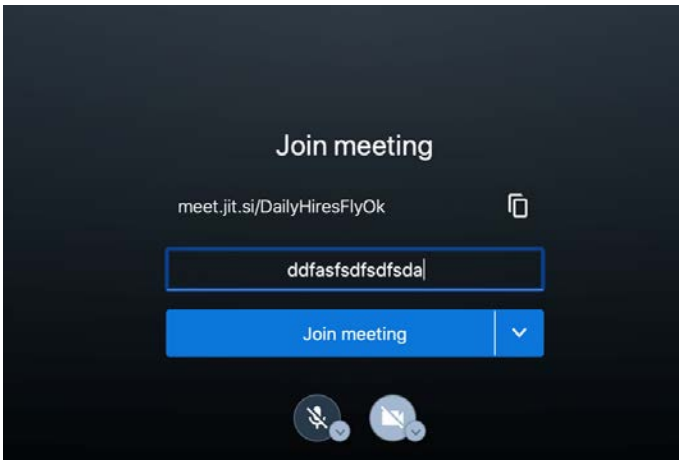


Ilustración 5.- Ejemplo de enlace que se compartiría con el resto de participantes de una reunión. En este caso, el nombre de la sala ha sido autogenerado

El enlace que se genera en cada sala es “meet.jit.si/” seguido del nombre de la sala autogenerado o creado por el organizador. En este último caso, si el organizador escoge un nombre de sala demasiado común, usuarios desconocidos podrían intentar tener

acceso a una reunión a la que no han sido invitados. La propia plataforma avisa a los usuarios de este aspecto.

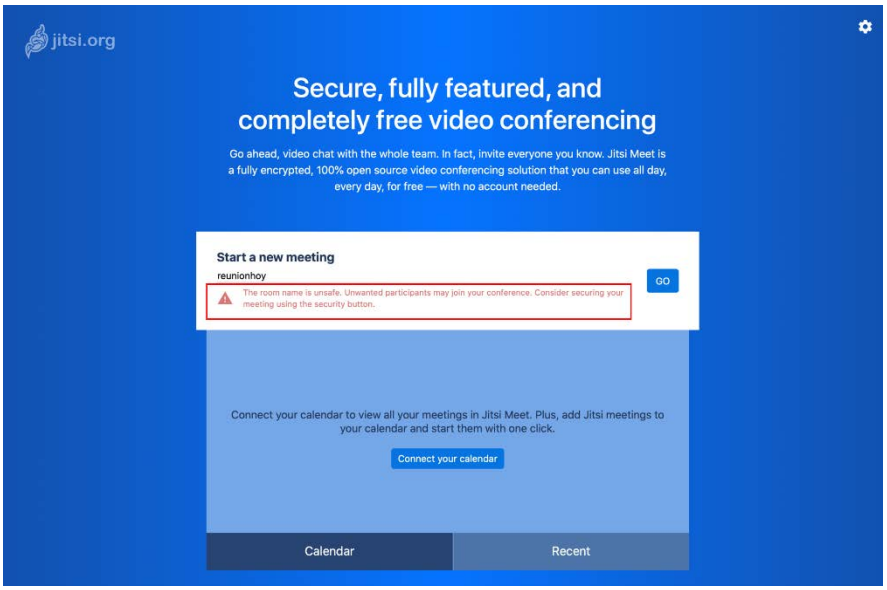


Ilustración 6.- Aviso de Jitsi de generación de enlace poco seguro

Un nombre de sala podría ser todo lo que un usuario necesita para acceder a una reunión y por ello la propia plataforma avisa al usuario. Si se inicia una reunión con el nombre "Test", "Yoga" o "Reuniondetrabajo", por ejemplo, las posibilidades de que se unan algunas personas no invitadas al azar son muy altas.

El generador de nombres de reuniones al azar es una opción disponible. Ofrece nombres aleatoriamente (en inglés) que son fáciles de recordar y leer en voz alta en una llamada telefónica, que además provienen de un conjunto de más de un billón de combinaciones posibles. Para utilizar los enlaces generados automáticamente, hay que hacer clic en "Ir/Go", junto a la opción "Iniciar una nueva reunión".

Por último, y como la plataforma advierte en su aviso, es altamente recomendable establecer una contraseña para la reunión. En este sentido, es importante considerar que si establece una contraseña se debe tener en cuenta que esta, al igual que las estadísticas de chat y oradores, se restablecerán una vez que la última persona salga de la sala. Por lo tanto, hay que asegurarse de que la contraseña se ha establecido nuevamente, si termina la reunión y luego vuelve a unirse.

4.4 Uso de contraseñas para acceder a la reunión

Para acceder a la reunión y para mayor seguridad, en la parte inferior derecha de la pantalla, en el icono "i" o en el menú de aplicaciones, se **puede añadir una contraseña** para entrar en la reunión (que debe compartirse con los participantes a través de un canal seguro, como SMS o correo electrónico cifrado). Además, en las opciones de seguridad, Jitsi permite al organizador de la reunión habilitar el modo Lobby, de forma que únicamente los usuarios aprobados por un “Moderador” podrían acceder a la sala de reunión.

Ilustración 7.- Botón para establecer medidas de seguridad en la reunión

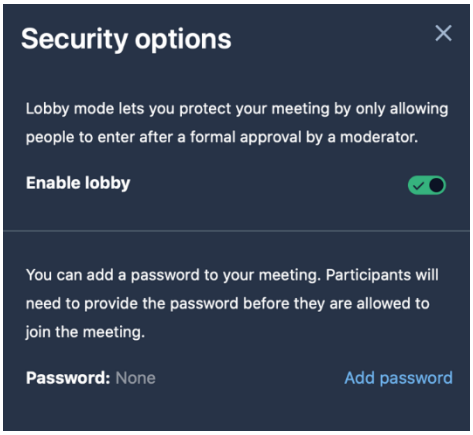


Ilustración 8.- Opciones de seguridad de la sala de reunión, contraseña y modo Lobby

Asimismo, es preferible evitar el uso de la función integrada de «Iniciar grabación», ya que la grabación de la reunión podría cargarse en la nube. Si necesita grabar la reunión, es preferible utilizar un software de grabación en su ordenador o equipo portátil. Del mismo modo, se recomienda habilitar la opción de cifrado extremo a extremo (modo Beta) siempre que sea posible y no afecte al normal trascurso de la conferencia.

4.5 Funciones

El micrófono y el vídeo pueden ser activados y desactivados en la parte inferior de la pantalla. En la esquina inferior izquierda de la pantalla hay un icono para abrir el chat de texto, que puede ser utilizado por todas las personas participantes. Junto a él o en el menú de aplicaciones, se encuentra la opción de "levantar la mano".

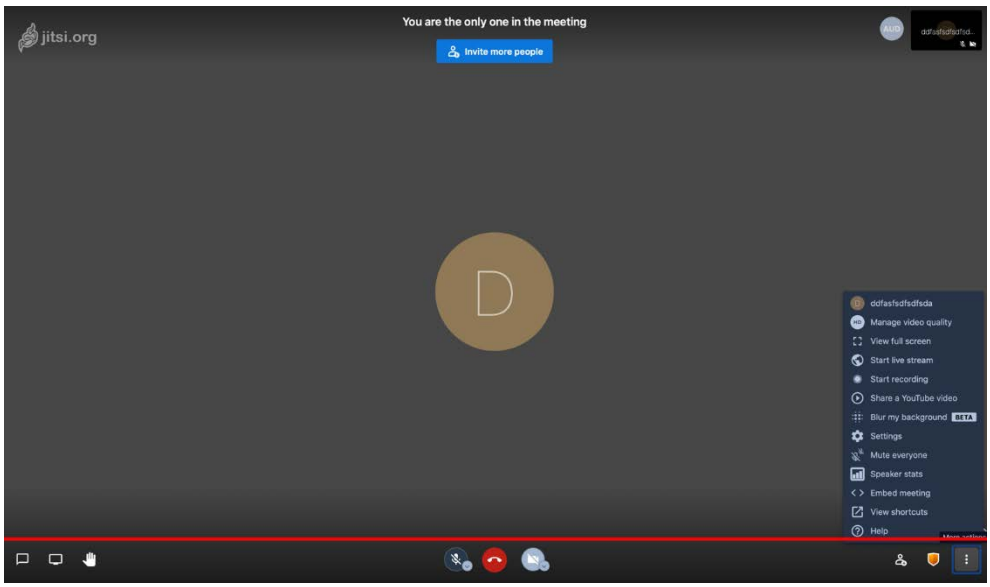


Ilustración 9.- De izquierda a derecha, se muestran los botones de iniciar chat, compartir pantalla, pedir la palabra, silenciar audio, cortar llamada, desconectar cámara, añadir participantes, botón de preferencias de seguridad y botón de más opciones

Las personas participantes pueden compartir su pantalla para mostrar presentaciones o documentos. En el botón "Más opciones", se desglosan distintas opciones configurables, desde la grabación de la reunión y la posibilidad de silenciar a todos los participantes, entre otras cuestiones.

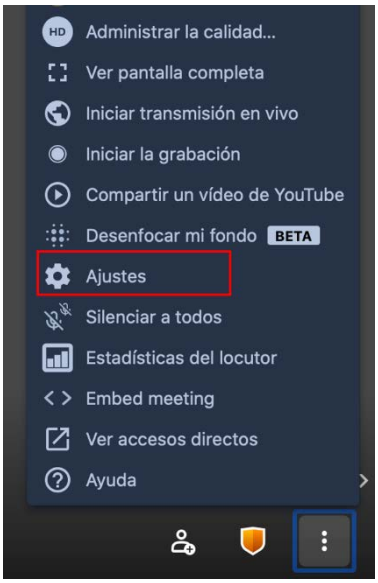


Ilustración 10.- Más opciones de configuración de reunión

En la opción "Ajustes", del botón "más opciones", la plataforma permite configurar el micrófono y la cámara del moderador, así como establecer el modo de conexión de los usuarios a la hora de acceder a la reunión.

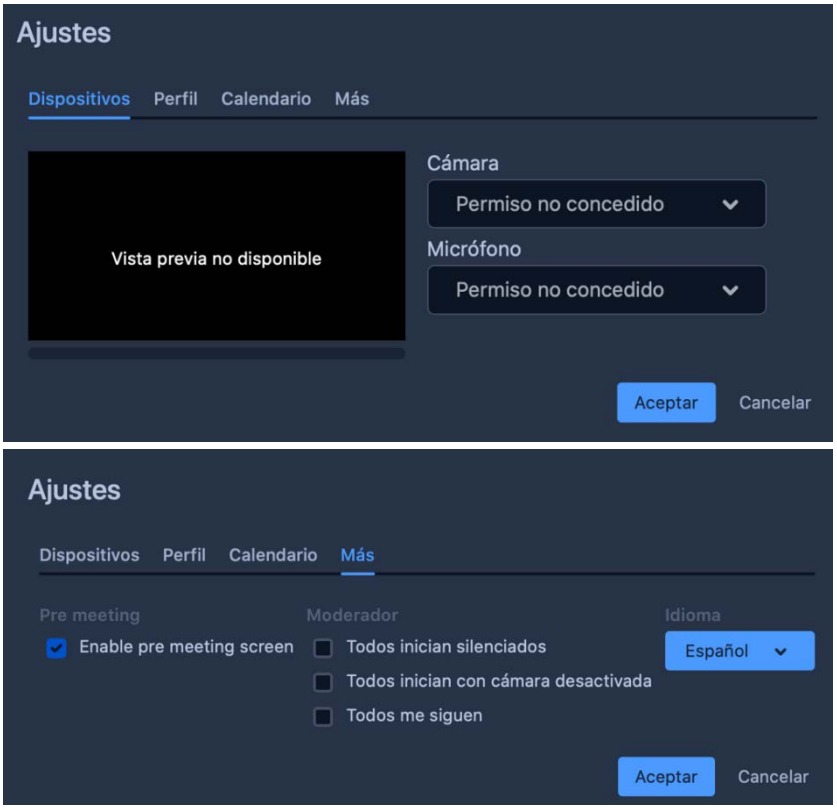


Ilustración 11.- Opciones de configuración de la reunión

Una vez abierta la reunión y configurados los aspectos más relevantes, el moderador y organizador podrán invitar a la reunión, compartiendo los detalles de la sala.

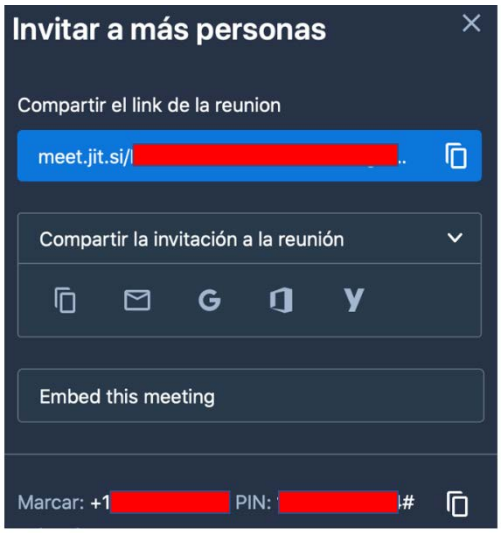


Ilustración 12.- Invitar a más personas a la reunión

4.6 Identificación de participantes

Se recomienda que todas las personas participantes en la reunión accedan con un nombre de usuario, que permita al resto de asistentes identificar su identidad.

Para evitar suplantaciones, los participantes pueden usar una cámara para ver si corresponde el nombre proporcionado con la persona en imagen. Se debe evitar en la medida de lo posible conexiones solo de audio por lo anteriormente expuesto.

4.7 Recomendaciones generales para una mejor experiencia

Absténgase de hacer otras tareas en su ordenador/teléfono durante la llamada. Cierre otras aplicaciones para conservar los recursos del ordenador/teléfono y el ancho de banda. Se recomienda que el presentador sólo abra las aplicaciones relevantes para su reunión o presentación. Si realmente necesita trabajar en otros asuntos durante la llamada, se debe considerar la posibilidad de utilizar un dispositivo diferente.

Utilice un micrófono con cable en lugar de un micrófono bluetooth y silencie el micrófono cuando no esté hablando. El micrófono capta el sonido de fondo, que se transmite y consume ancho de banda.

RECUERDE: Es importante usar Jitsi Meet sólo en servidores de confianza. El uso de Jitsi Meet en servidores no confiables puede comprometer la seguridad de la llamada.

5. CONCLUSIONES

Se debe diferenciar el **servicio meet.jit.si** al cual todo el mundo se refiere como Jitsi, de la tecnología de Jitsi.org y sus implementaciones particulares on-premise. Si bien ambas

comparten funcionalidades y características a nivel de experiencia de usuario, a nivel de privacidad y seguridad son entornos claramente diferentes.

Meet.jit.si se considera adecuado siguiendo las recomendaciones anteriormente indicadas para un intercambio de información no sensible u oficial, siendo transparente (como ya se ha analizado anteriormente) en los datos que analiza y recoge de los participantes y las sesiones que concurren.

No se recomienda el uso de la plataforma meet.jit.si para organizaciones que deban asegurar la confidencialidad del dato y contenido de las sesiones. **Se recomienda la implementación de servidores** (instancias) de Jitsi Videobridge on-premise para este tipo de entidades.

6. BIBLIOGRAFÍA Y ENLACES

- https://www.8x8.com
- https://github.com/jitsi
- https://jitsi.org/security/