Guía de Seguridad

Fecha de publicación: 21/05/2020

Tema: Recomendaciones de seguridad para aplicaciones de teleconferencias.

Existe una gran variedad de herramientas de teleconferencias, y su uso se ha incrementado con la situación generada por la emergencia sanitaria **COVID-19**, que ha obligado a muchos organismos y ciudadanos a utilizar estas plataformas en sus actividades. Es por ello que debemos tomar algunas consideraciones de seguridad para minimizar los riesgos.
Estas recomendaciones aplican para clases virtuales, reuniones laborales, llamadas con familiares o amigos, videollamadas o teleconferencias grupales en general. Algunas de estas plataformas son: Zoom, Google Meets, Microsoft Teams, Jitsi, etc.

Recomendaciones de seguridad generales para usuarios (anfitriones e invitados):

- Utilizar aplicaciones de teleconferencias reconocidas, y descargarlas desde los sitios web oficiales en sus versiones para PC (sitios web oficiales de los proveedores) y/o móviles (Google Play o App Store).
- Mantener las aplicaciones de teleconferencias seleccionadas actualizadas a sus últimas versiones disponibles en los sitios web oficiales de los fabricantes. Igualmente, mantener actualizado el sistema operativo y el software antivirus del equipo donde hace uso de las aplicaciones de teleconferencias, con los últimos parches de seguridad publicados por los fabricantes en sus sitios web oficiales.
- Tener cuidado con las invitaciones recibidas o recordatorios por correo electrónico, solo ingresar a enlaces enviados por personas de confianza y/o instituciones oficiales. No aceptar llamadas o chats de usuarios desconocidos.
- En caso de ser anfitrión o moderador de una reunión privada:
    - Tomarse el tiempo de revisar todas las opciones de configuración que posee la plataforma seleccionada, y ponga foco en aquellas que sean de seguridad.
    - Utilizar formas seguras de invitación, compartiendo las URL de las reuniones solamente a las personas invitadas, y si se remite a un grupo asegurar de que

solo estén las personas autorizadas. Evitar configurar la reunión como pública si no lo es.

- No compartir el enlace de reuniones privadas en redes sociales.
- Establecer una contraseña segura para la reunión y no publicarla en las redes sociales (Facebook, Instagram, etc). En caso de que la contraseña deba ser compartida con un grupo, ya sea a través de aplicaciones de mensajería (Whatsapp u otros), indicar a las personas que no la compartan fuera de dicho grupo.
- Controlar el acceso de los participantes. Siempre que sea posible, mantener a los participantes en una **"sala de espera"** y aprobar la conexión de cada uno.
- Bloquear la reunión una vez que todos los participantes se hayan unido a la llamada.
- Deshabilitar la opción de video por defecto. Habilitarla solo cuando sea necesario, y en ese caso tener cuidado de no mostrar información no deseada a través de la Webcam y utilizar funciones como fondo virtual. Apagar o silenciar los micrófonos de los participantes cuando el sistema no está en uso.
- Deshabilitar la opción de grabación de las reuniones a menos que se necesite y que esté autorizado.
- Deshabilitar la opción de compartir de escritorio por defecto. Habilite solo cuando esta sea necesaria. En caso de compartir pantalla tener cuidado de no compartir información sensible.
- En caso de compartir archivos, o permitir que los invitados compartan archivos, considerar limitar los tipos de archivos que se pueden enviar; por ejemplo, no permitir archivos ejecutables (como archivos .exe)

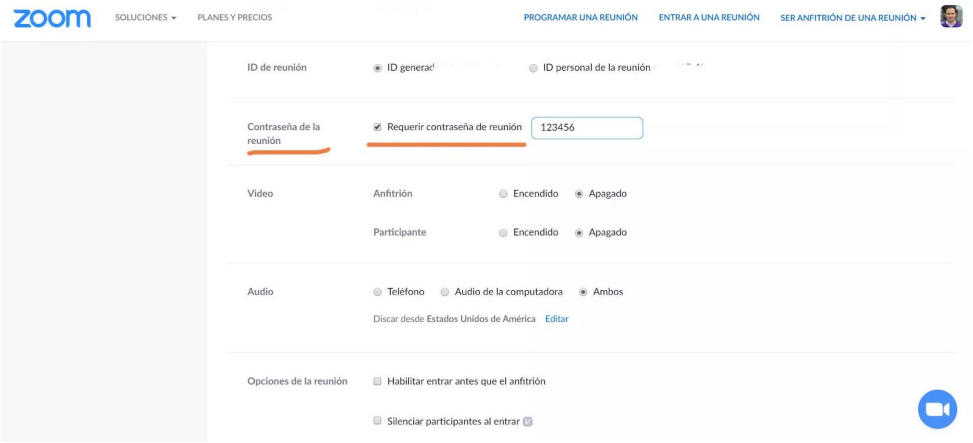
A continuación algunas recomendaciones específicas para las aplicaciones de teleconferencias más utilizadas:

Zoom:

1. **Establecer contraseñas para el ingreso a las reuniones:**.

   Para establecer una contraseña, debe seguir los siguientes pasos:

a. Ingresar a la página web o aplicación de Zoom,
b. Seleccionar **Mi cuenta** o **My Account**,
c. En el menú izquierdo seleccionar **Reuniones**,
d. Seleccionar **Programar una reunión nueva**,
e. Luego de tener los **datos generales** de la reunión a crear, bajar hasta encontrar la sección de **Contraseña de la reunión**, activar la opción **Requerir contraseña** y
f. Finalmente establecer una contraseña y seleccionar **Guardar.**



2. **<u>Utilizar formas seguras de invitación</u>:**

Se recomienda siempre enviar el identificador de la reunión y la contraseña individualmente a los invitados (correo electrónico o mensaje privado), es importante evitar compartir la URL con cualquier contacto o vía redes sociales.

3. **<u>Gestionar el acceso de los participantes</u>:**

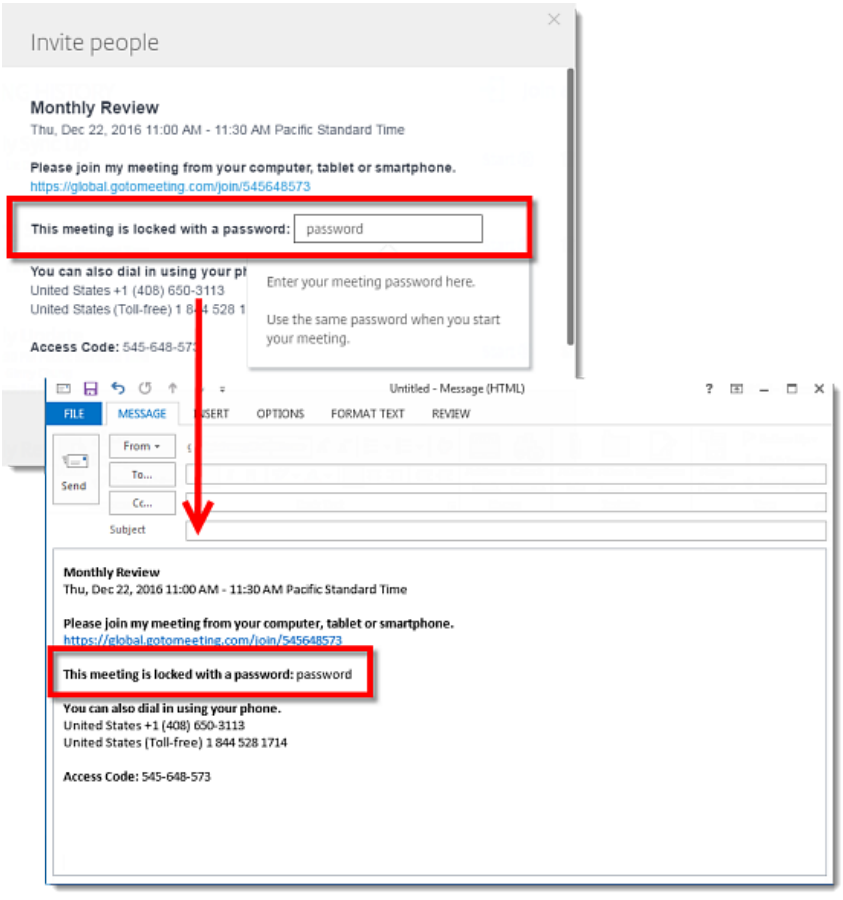
Se recomienda usar la opción de "**Sala de Espera**" en donde el anfitrión se encarga de confirmar el ingreso de cada participante individualmente Para habilitar esta opción, siga los siguientes pasos:

a. Antes de crear una nueva reunión, dirigirse al apartado de **Opciones de la Reunión** y
b. Seguidamente marcar la opción **Habilitar sala de espera**.

4. Se recomienda que el anfitrión de la reunión decida a través de la opción "**Allow Record**" quienes pueden grabar la llamada.

GotoMeeting:

1. **<u>Proteger la reunión mediante una contraseña</u>**
   a. **Desde la web:**
      i. Crear una nueva reunión o editar alguna ya existente,
      ii. En la sección Contraseña, marcar la casilla "**Contraseña de Reunión obligatoria**" y
      iii. Por último establecer la contraseña.

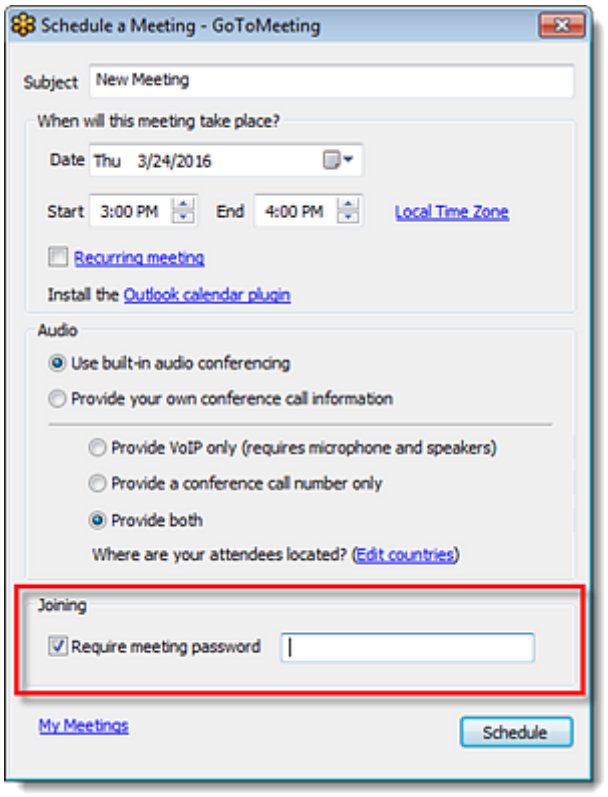


   b. **Desde la aplicación de escritorio:**
      i. Primeramente iniciar o editar una reunión,

ii. En la parte inferior de la ventana, activar la casilla "**Contraseña de reunión obligatoria**",

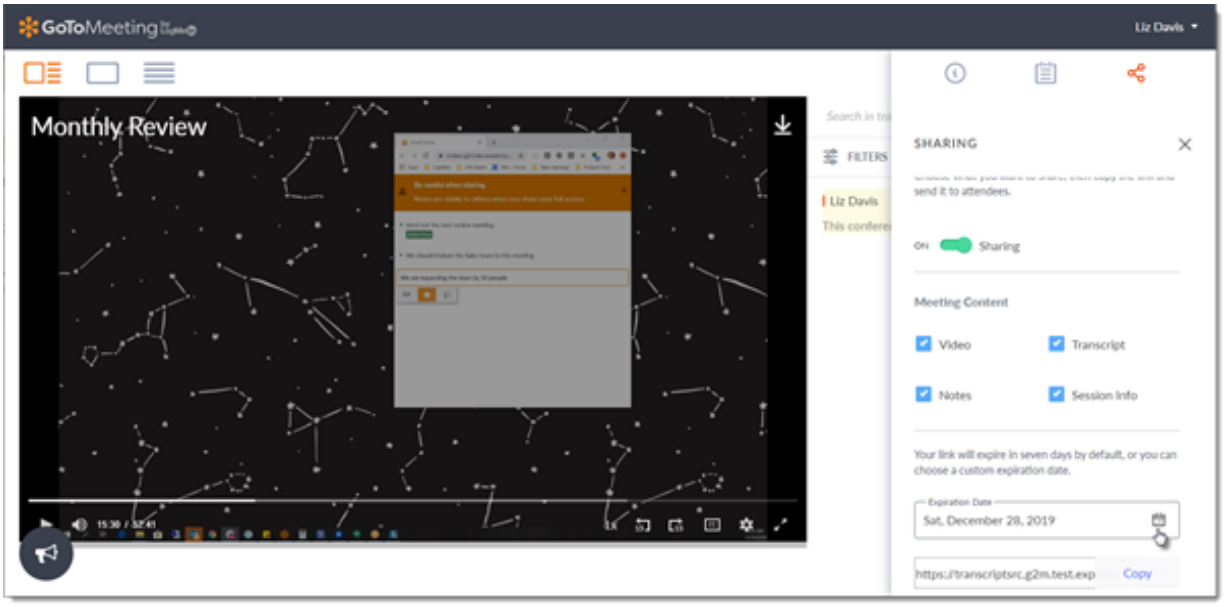
iii. Especificar la contraseña deseada y

iv. Por último hacer clic en **Programar** una vez finalizada la configuración.



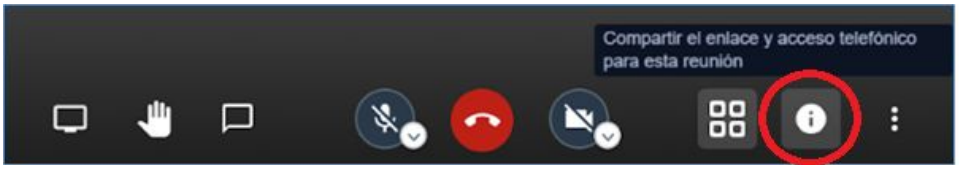
2. **<u>Bloquear la reunión</u>**, para impedir que personas no invitadas se unan a la sesión actual:
   a. En el panel de control, hacer clic en **Personas** y modificar la opción de **"Reunión bloqueada"** en la parte inferior.
   b. El icono de Bloqueo se cerrará y se podrá ver el mensaje **"Esta reunión está bloqueada".**
   c. Se notificará cuando una persona intente unirse a la sesión bloqueada.
   d. Para **desbloquear** y conectar a todas las personas en espera a la reunión, hacer clic de nuevo en el interruptor. El icono de Bloqueo cambiará a un candado abierto.

3. **<u>Establecer una fecha de caducidad en la grabación realizada</u>**, de forma predeterminada la grabación una reunión caduca a los 7 días. Para establecer una fecha de caducidad, debe seguir los siguientes pasos:
    a. Hacer clic en la pestaña **Historial** y marcar la casilla **Grabado** para filtrar las sesiones grabadas.
    b. Buscar la reunión deseada y hacer clic en **Abrir grabación**.
    c. Hacer clic en el icono Compartir y establecer la fecha de caducidad.
    d. Copiar el enlace de la grabación de la reunión y compartir con quien desee.



Jitsi:

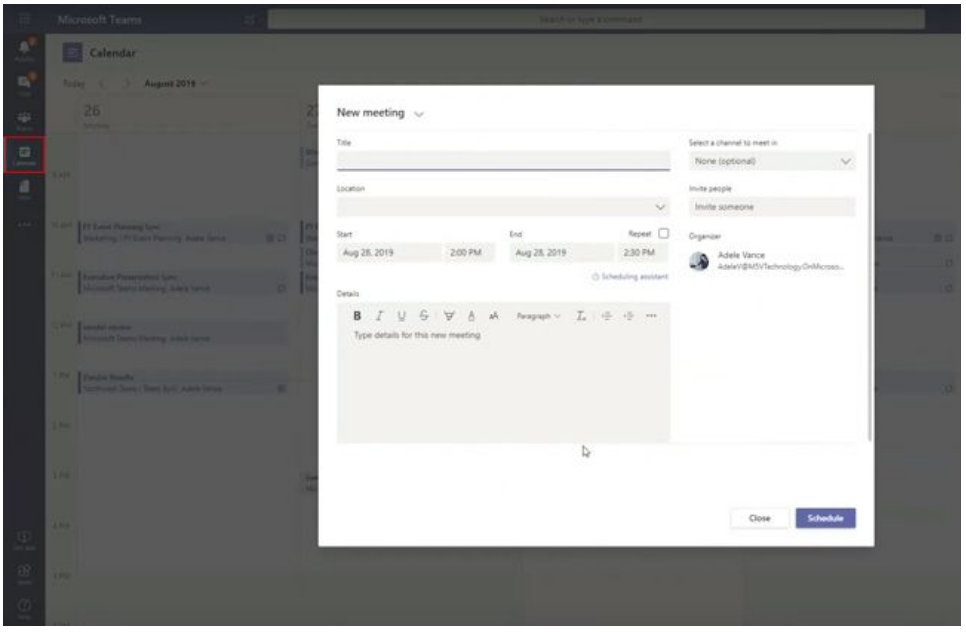
1. **<u>Establecer una contraseña para ingresar a las reuniones</u>**: Primeramente ingresar a la página web de Jitsi y seleccionar **Empezar una reunión**,
    a. Elegir un nombre para la reunión y seleccionar **Ir**,
    b. Seleccionar el icono de **"Compartir el enlace y acceso telefónico para esta reunión"** y



c. En la ventana abierta con la información general de la reunión seleccionar **Agregar contraseña**.

Microsoft Teams:

1. **<u>Controlar el acceso de personas a las reuniones</u>**, Realice las configuraciones desde **Calendario > Seleccionar una reunión > Opciones de Reunión.**



2. **<u>Limitar el acceso a las grabaciones de las reuniones realizadas por medio de directivas,</u>** de la siguiente manera:
   a. En el panel de navegación izquierdo del **Centro de administración de Microsoft Teams**, dirigirse a **Usuarios** y, después, haga clic en el usuario.
   b. Para seleccionar el usuario, hacer clic a la izquierda del nombre de usuario y, después, en **Editar configuración**.

c. En **Directiva de reunión**, seleccionar la directiva que quiera asignar y clic en **Aplicar**.
   i. Para crear una directiva personalizada, dirigirse a **Centro de administración de Microsoft Teams > Reuniones > Directivas de reunión > Agregar**
   ii. Deshabilitar la opción "**Permitir la grabación en la nube**"

Referencias

- https://support.zoom.us/hc/es/categories/201146643
- https://www.gotomeeting.com/es-co/webinar/online-webinar-support?sc_lang=es-co
- https://jitsi.org/user-faq/
- https://support.office.com/es-es/teams
- https://www.welivesecurity.com/la-es/2020/04/03/teletrabajo-consideraciones-seguridad-realizar-videoconferencias/
- https://www.computerworld.es/tecnologia/medidas-para-hacer-videoconferencias-seguras
- https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9941-como-teletrabajar-de-forma-segura-sin-poner-en-riesgo-a-usuarios-y-organizacione