Junta de Andalucía

Agencia Digital de Andalucía

Consejería de Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Agencia Digital de Andalucía

REUNIONES EN ZOOM

Recomendaciones de uso y seguridad

Mitel + ZOOM

TABLA DE CONTENIDO

1. Introducción 3
2. Recomendaciones de seguridad para la creación de reuniones 4
2.1. Activar mecanismos de control de acceso 4
2.2. Elegir el tipo adecuado de reunión según el objetivo 5
3. Buenas Prácticas al Compartir Enlaces de Reuniones 6
3.1. Compartir en canales controlados 6
3.2. Evitar compartir enlaces en redes sociales públicas 6
4. Consecuencias de Publicar Enlaces sin Restricciones de Acceso 7
4.1. Zoombombing 7
4.2. Riesgo reputacional 7
4.3. Sobrecarga o limitación del servicio 7
4.4. Consecuencias para la cuenta de Zoom 7
4.5. Filtración de información 7
5. Resumen de Reglas Clave 8

1. Introducción

En los últimos años, plataformas como Zoom se han convertido en una pieza clave para trabajar, colaborar y comunicarnos con clientes, equipos y colaboradores. Sin embargo, a medida que aumenta su uso, también lo hacen los riesgos que pueden surgir cuando los enlaces de acceso a reuniones se comparten sin la protección adecuada.
De hecho, gran parte de las interrupciones o accesos no deseados en videollamadas se deben simplemente a que el enlace se hizo público sin ningún filtro.

El objetivo de esta guía es ofrecer recomendaciones claras y fáciles de aplicar para minimizar estos riesgos. Siguiendo estas pautas, podremos asegurar reuniones más seguras, fluidas y profesionales, garantizando una mejor experiencia tanto para la organización como para los asistentes.

2. RECOMENDACIONES DE SEGURIDAD PARA LA CREACIÓN DE REUNIONES

2.1. Activar mecanismos de control de acceso

Una de las formas más efectivas de evitar problemas en las reuniones es asegurarse de que solo entren las personas que realmente tienen que estar allí. Para ello, Zoom ofrece varias opciones que conviene activar:

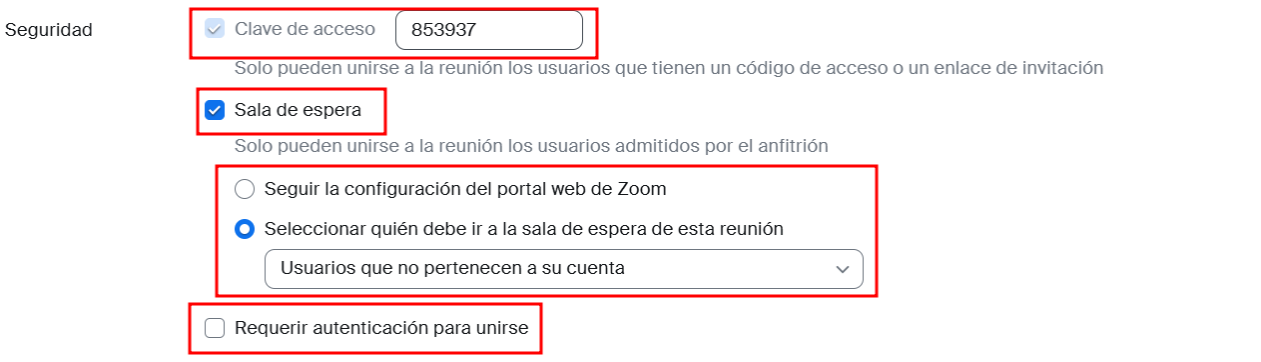
• **Sala de espera:** Funciona como una recepción virtual. Permite revisar quién está intentando entrar antes de admitirlo. Es especialmente útil cuando no conocemos de antemano a todos los asistentes o cuando la reunión está dirigida a un público amplio.

• **Código de acceso:** Añade una capa de seguridad muy sencilla pero efectiva. Zoom permite incluir el código directamente dentro del enlace, por lo que los asistentes no tienen que escribir nada, pero el acceso no queda completamente abierto.

• **Acceso restringido a usuarios autenticados:** En este caso, la reunión solo permite la entrada a usuarios que hayan iniciado sesión con una cuenta de Zoom. Es la opción más recomendable para sesiones internas o de carácter privado, ya que garantiza que solo acceda personal identificado.

Aplicando una o varias de estas medidas, reducimos considerablemente la posibilidad de accesos no autorizados y protegemos tanto la dinámica de la reunión como la información compartida en ella.

En esta captura de creación de una reunión se puede observar en **Seguridad** las distintas opciones comentadas.



2.2. Elegir el tipo adecuado de reunión según el objetivo

• Eventos abiertos al público: Se recomienda utilizar Zoom Webinars o Zoom Events, ya que ofrecen mayor seguridad, opciones de registro y control sobre la audiencia.

Ventajas de Zoom Webinars para eventos públicos

- **Mayor control sobre la audiencia:** Solo los ponentes pueden usar audio y vídeo, lo que evita interrupciones y mantiene la sesión ordenada.
- **Acceso más seguro:** Permiten activar el registro previo y gestionar quién entra, algo clave cuando el evento es público.
- **Experiencia más fluida para grandes grupos:** Están diseñados para audiencias amplias, sin los problemas habituales de una reunión llena de participantes.
- **Herramientas específicas para eventos:** Ofrecen funciones como panel de preguntas, encuestas y métricas detalladas que ayudan a mejorar la sesión.
- **Presentaciones más profesionales:** La interfaz centra la atención en los ponentes y el contenido, transmitiendo una imagen más pulida.

• Reuniones internas o privadas: Pueden realizarse mediante reuniones estándar, siempre que se activen la sala de espera, el código de acceso y se desactive la opción de entrar antes que el anfitrión.

Ventajas de Zoom Meetings para reuniones privadas

- **Interacción más directa:** Todos los participantes pueden activar cámara y micrófono, lo que facilita conversaciones reales, trabajo en equipo y dinámicas colaborativas.
- **Funciones colaborativas completas:** Salas para grupos pequeños, compartir pantalla de varios usuarios, pizarra colaborativa… todo orientado a trabajar juntos.
- **Configuración más sencilla:** Crear una reunión es rápido y no requiere definir roles de ponente o asistente.
- **Mejor para grupos pequeños o medianos:** Cuando el objetivo es hablar, debatir o tomar decisiones, las reuniones son el formato más eficiente.

3. Buenas Prácticas al Compartir Enlaces de Reuniones

3.1. Compartir en canales controlados

Se recomienda compartir los enlaces de forma privada a través de:

- **Correo electrónico**
- **Grupos cerrados**
- **Intranet corporativa**
- **Formularios de registro**

3.2. Evitar compartir enlaces en redes sociales públicas

No se deben publicar enlaces directamente en:

- **Facebook, Instagram, X/Twitter**
- **Historias o publicaciones públicas**
- **Comentarios accesibles a desconocidos**
- **Foros o espacios abiertos al público**

En caso de requerir difusión pública, se recomienda utilizar formularios de inscripción en los que, al completar el registro, el participante recibe el enlace en su correo electrónico.

4. Consecuencias de Publicar Enlaces sin Restricciones de Acceso

4.1. Zoombombing

Personas ajenas pueden entrar sin permiso e interrumpir con ruido, mensajes, o en el peor de los casos, contenido inapropiado. Esto puede arruinar una sesión en cuestión de segundos.

4.2. Riesgo reputacional

Un comportamiento inapropiado por parte de alguien externo puede dar una imagen negativa ante clientes, asistentes o colaboradores, afectando la percepción de profesionalidad.

4.3. Sobrecarga o limitación del servicio

Si el enlace se vuelve público, pueden entrar bots o más usuarios de los previstos, impidiendo el acceso a quienes realmente deben participar o saturando la reunión.

4.4. Consecuencias para la cuenta de Zoom

Un uso que Zoom considere sospechoso podría desencadenar advertencias o limitaciones temporales en la cuenta.

4.5. Filtración de información

Cualquier persona que entre sin control puede escuchar, grabar o difundir contenidos compartidos durante la reunión, incluso si eran internos o confidenciales.

5. Resumen de Reglas Clave

Para garantizar reuniones seguras, profesionales y sin interrupciones, es importante seguir unas pautas básicas:

• No publicar nunca un enlace sin sala de espera o sin código de acceso.

• Utilizar plataformas adecuadas como Zoom Webinars o Zoom Events para eventos públicos o de alta difusión.

• En reuniones internas, limitar el acceso a usuarios autenticados.

• Compartir enlaces únicamente a través de canales privados o tras un proceso de registro.

• Revisar siempre la configuración antes de crear y compartir la reunión.

Siguiendo estas recomendaciones, podremos ofrecer una experiencia más segura y controlada, protegiendo tanto la operación del servicio como la imagen de la organización.