

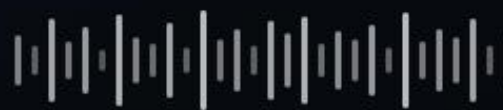
Sus Reuniones Confidenciales No Son Privadas

Riesgos de interceptación de conversaciones, grabación no autorizada y espionaje digital en Juntas Directivas, Comités y Entidades Gubernamentales.



● REC

00:12:05



Contenido

1. Resumen ejecutivo
2. ¿Cuál es el problema?
3. Grabación de conversaciones confidenciales en reuniones (Riesgos)
4. Controles para proteger conversaciones confidenciales

1. Resumen Ejecutivo

*La información más confidencial en sus reuniones **suele hablarse, no escribirse.***

Riesgo

Los dispositivos modernos han convertido cada sala de reuniones en una potencial plataforma de espionaje. Teléfonos inteligentes, relojes inteligentes, lentes inteligentes y laptop pueden capturar y transmitir conversaciones confidenciales, de forma intencional o accidental.

Impacto

- **Pérdida de ventaja estratégica:** Las filtraciones sobre decisiones o negociaciones en curso destruyen meses de preparación y eliminan la ventaja competitiva antes de ser ejecutadas.
- **Mayor exposición legal:** Las grabaciones crean registros permanentes de conversaciones exploratorias. Sacadas de contexto, pueden utilizarse como evidencia de mala conducta en litigios o daño reputacional.
- **Colapso de la confianza:** Las filtraciones inhiben la apertura en conversaciones. Cuando directores y asesores temen que puedan ser grabados, cesa la deliberación abierta y la calidad de las decisiones se deteriora de inmediato.

Alcance del documento

Este artículo aborda los riesgos derivados de dispositivos comunes presentes en reuniones como teléfonos inteligentes, dispositivos portátiles (wearables), computadoras portátiles e infraestructura de sala de reunión que pueden capturar o transmitir conversaciones de forma intencional o no intencional.

Este artículo ***no aborda software espía patrocinado por Gobiernos*** (como Pegasus u otras herramientas similares) que explota vulnerabilidades de los dispositivos para proporcionar acceso remoto a gobiernos o agencias de inteligencia. Esas amenazas requieren un marco de controles diferente, que incluye fortalecer los controles de los dispositivos, detección en “endpoints” y monitoreo forense, los cuales quedan fuera del alcance de las medidas de seguridad para salas de reuniones.

Los controles aquí descritos se enfocan en las fuentes más frecuentes de exposición de conversaciones en entornos reales de reuniones.

2. ¿Cuál es el problema?

Los riesgos reales no son hipotéticos.

Concejal renuncia a su escaño en el Ayuntamiento de Los Ángeles en medio del furor por una grabación de audio filtrada (*)

Crisis política cuando la primera ministra tailandesa corrió el riesgo de perder su escaño tras la filtración de una impactante grabación de audio con el presidente del Senado de Camboya (**)

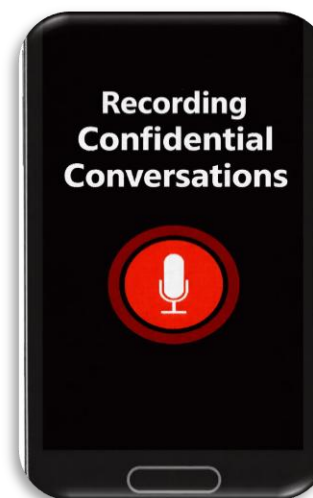
El audio filtrado de la famosa Compañía Campbell convirtió un producto básico de la despensa en una crisis de relaciones públicas (***)

Grabar conversaciones confidenciales sin autorización

Históricamente, las conversaciones en reuniones privadas estaban protegidas por límites físicos: una puerta cerrada, participantes limitados y documentos en papel. Hoy, la misma sala incluye múltiples laptops, teléfonos inteligentes, relojes inteligentes, audífonos inalámbricos, televisores inteligentes y, a veces, incluso asistentes de voz. Cada dispositivo adicional incrementa los posibles caminos de captura de audio y fuga de información.

La exposición de una reunión generalmente ocurre a través de grabaciones intencionales, sincronización no intencional de dispositivos, explotación de redes inalámbrica o dispositivos comprometidos.

En nuestra experiencia, los teléfonos inteligentes son el método preferido para grabar conversaciones confidenciales sin autorización.



* <https://deadline.com/2022/10/nury-martinez-resigns-from-los-angeles-city-council-seat-1235143013/>

** <https://moderndiplomacy.eu/2025/06/27/why-might-thai-prime-minister-lose-his-seat-after-leaked-recording-with-hun-sen/>

*** <https://fortune.com/article/campbell-leaked-audio-pr-crisis-comms-soup-meat/>

3. Grabación de conversaciones confidenciales en reuniones (Riesgos)

Los siguientes riesgos representan los vectores más comunes y observados en reuniones reales.

Explicación del Riesgo	Probabilidad de Ocurrencia
1. Filtración de audio en vivo vía llamada o una app. Un teléfono puede colocarse en modo silencioso y permanecer en una llamada activa, o una app de grabación puede quedar ejecutándose de forma anónima. Si el micrófono está activo, la sala se convierte en una transmisión en vivo. En algunos casos, el receptor solo escucha; en otros, el audio se graba y transcribe.	Alta
2. Grabación “offline” y filtración diferida. Incluso sin conectividad Wi-Fi, un dispositivo puede grabar conversaciones. La grabación puede filtrarse posteriormente cuando el dispositivo se reconecta a Internet.	Alta
3. Uso de accesorios inalámbricos (Bluetooth, relojes, audífonos). Un teléfono fuera de la sala de reunión puede permanecer emparejado con un reloj o auriculares dentro de la sala. Estos accesorios mantienen la señal de radio y pueden grabar de forma independiente.	Alta
4. Laptop/tablet con micrófono encendido. Una laptop/tablet dentro de la sala de reunión puede grabar la conversación y compartirla después.	Alta
5. Equipos-Dispositivos dentro de la sala con controles deficientes. Memorias USB, dongles HDMI desconocidos, Smart TVs, barras de conferencia, micrófonos de sala y asistentes de voz siempre activos pueden grabar conversaciones.	Medio

4. Controles para proteger conversaciones confidenciales

La consistencia importa más que la perfección. Tenga siempre en mente que un proceso simple y repetible supera a una política compleja que nadie cumple.

Los controles de la siguiente página están escritos para ser prácticos. Asumen que los directores mantendrán los teléfonos encendidos, y que las laptops/tablets son necesarias para materiales y apoyo a la toma de decisiones.

Los controles se enfocan en reducir tanto el riesgo de captura (grabación) como el riesgo de filtración (transmisión), manteniendo la reunión operable.

Ejemplos de controles físicos incluyen bolsas Faraday de alta calidad y cajas acústicas para teléfonos (lockboxes).



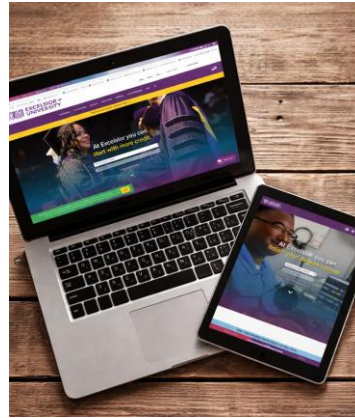
4. Controles para proteger conversaciones confidenciales



Teléfonos y dispositivos portátiles (wearables)

- Use una bolsa Faraday de alta calidad para teléfonos, relojes y audífonos.
- Introduzca los dispositivos en una bolsa Faraday y coloque esta dentro de una caja acústica durante conversaciones confidenciales para garantizar la seguridad.
- Implemente un “número de emergencia” fuera de la sala para los participantes de la reunión.

La bolsa reduce la transmisión de señales de radio. La caja acústica reduce la captura de audio utilizable y la línea de emergencia mantiene la usabilidad.



Laptops y tablets

- Cubiertas de webcam obligatorias.
- Wi-Fi y Bluetooth apagados salvo aprobación explícita.
- Prohibir hotspots personales; si se requiere Internet, use una red controlada.
- Sin almacenamiento externo; solo adaptadores/dongles provistos por el organizador de la reunión.
- Use un dispositivo dedicado para hacer presentaciones.

Los controles deben enfocarse en señales de radio, micrófono/cámara y periféricos.



Equipos o Dispositivos en la sala

- Retire o deshabilite asistentes inteligentes (software); evite micrófonos siempre activos.
- Use una pantalla y una barra de conferencia conocidas y administradas; mantenga el firmware actualizado.
- Ubique asientos y pantallas para reducir el shoulder surfing (miradas sobre el hombro).

Una reunión segura no depende solo de los participantes; los equipos y dispositivos de la sala también puede grabar y transmitir conversaciones confidenciales.



Personas y Procesos

- Defina niveles claros de reunión: estándar, sensible y de alto impacto.
- Checklist de ingreso en la puerta (2 minutos): embolsar teléfonos, cubrir cámaras, radios apagados.
- Asigne un responsable (gatekeeper) y un proceso de excepciones aprobado por la presidencia.
- Documente el protocolo y practíquelo como un simulacro.

La pregunta ya no es si las conversaciones confidenciales pueden ser grabadas sin autorización; la pregunta es si las instituciones gubernamentales y las organizaciones privadas cuentan con los controles para prevenirlo o detectarlo cuando ocurra.



En RISCCO, ayudamos a las juntas directivas e instituciones gubernamentales a traducir estos controles en salvaguardas prácticas y repetibles que protegen las conversaciones confidenciales y al mismo tiempo preservan la toma de decisiones efectiva.

Bibliografía

Imágenes

1. <https://openai.com/>

Fuentes

1. <https://marenius.com/noisebox/>
2. <https://mosequipment.com/collections/tablet-and-laptop-faraday-bags>
3. <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-espionage/>
4. <https://deadline.com/2022/10/nury-martinez-resigns-from-los-angeles-city-council-seat-1235143013/>
5. <https://moderndiplomacy.eu/2025/06/27/why-might-thai-prime-minister-lose-his-seat-after-leaked-recording-with-hun-sen>
6. <https://fortune.com/article/campbell-leaked-audio-pr-crisis-comms-soup-meat/>

CONTACTOS

Panamá, Centroamérica y El Caribe

Antonio Ayala I.
CEO
aayala@riscco.com

Rubén Fernández
Gerente de Consultoría
rfernandez@riscco.com

Marinelda Morales
Gerente Comercial
mmorales@riscco.com

República Dominicana y Puerto Rico

Eury Valdez
Asesor Comercial
efvaldez@riscco.com

El Salvador, Guatemala, Honduras, Costa Rica y Nicaragua

Gari Rojas
Asesor Comercial
grojas@riscco.com

Acerca de RISCCO

RISCCO es una firma de consultoría internacional e independiente, comprometida con transformar la forma en que las organizaciones gestionan el riesgo y adoptan la Inteligencia Artificial. Combinamos un enfoque riguroso en GRC (Gobernanza, Riesgo y Cumplimiento) con analítica de datos avanzada e Inteligencia Artificial para ayudar a nuestros clientes a anticipar riesgos, fortalecer la gobernanza y resolver desafíos complejos. Con sede en Panamá y presencia en seis países, en 2026 cumplimos 17 años sirviendo a más de 200 organizaciones líderes en Centroamérica y el Caribe.

Rigor internacional. Ejecución ágil. Impacto medible.

Pensamos como estrategas. Ejecutamos como especialistas.

riscco.com

© 2009–2026 RISCCO. Todos los derechos reservados.

