



CONSEJOS DE CSIRT

SEGURIDAD PARA VIDEOCONFERENCIAS



El trabajo a distancia ofrece muchas ventajas, pero no está libre de riesgos de seguridad, especialmente si se trata de compartir información entre los miembros de un grupo de trabajo o de asegurar la privacidad de la reunión. Dado que no existe un medio tecnológico libre de estas amenazas y riesgos, el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT, entrega algunas recomendaciones para que la información que se transmite, al realizar una teleconferencia, pueda desarrollarse de la manera más segura posible.

1



ACTUALIZA el software que utilizas para mantener los más **altos niveles de seguridad**.

2



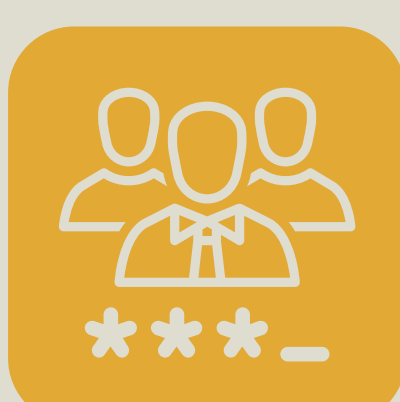
UTILIZA nombre de usuario y contraseña **al configurar una reunión**.

3



ASEGURATE de conectarte a una red WiFi segura y confiable. **Evita las redes públicas**.

4



GESTIONA el acceso de los participantes. **Permite sólo participantes registrados**.

5



RECUERDA actualizar el **computador y antivirus**.

6



CUIDADO con quien te envía una invitación. Nunca ingreses a una reunión **si no conoces al organizador**.

7



NUNCA entregues el control de la pantalla compartida para evitar que se **compartan contenidos no deseados**.

8



UTILIZA versiones que garanticen soporte y **responsabilidad de la empresa**.

9



TRATA de no grabar las reuniones, se pierde la **encriptación de la comunicación de extremo a extremo**.

10



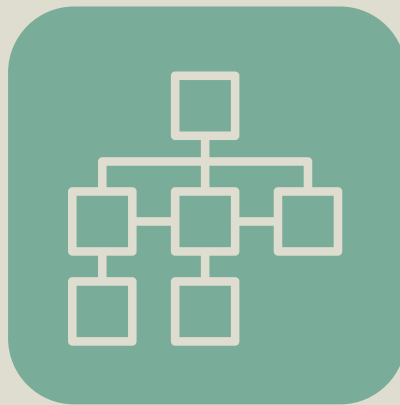
BLOQUEA la opción que permita transmitir **archivos durante el evento**.

11



EVITA realizar reuniones públicas y **entrega siempre a los participantes un ID**.

12



IDENTIFICA el canal de comunicación oficial con el área de soporte para la **resolución de problemas técnicos que pudieras tener**.