Recomendaciones para reuniones llevadas a cabo en formato presencial

Abstract: en este documento se recogen una serie de recomendaciones y buenas prácticas atendiendo a diferentes circunstancias tomando como premisa su validez exclusivamente para aquellas reuniones mantenidas en un formato presencial. La aplicación de las siguientes medidas contribuye a la reducción de la superficie de exposición para la protección e intimidad de las conversaciones.

Contenido:

1. INTRODUCCIÓN

Las filtraciones de conversaciones que se mantienen en un contexto determinado persiguen en muchas circunstancias causar un perjuicio significativo que atiende a intereses dispares. Es por ello, por lo que en algunas ocasiones es necesario poner en práctica determinadas medidas que permitan minimizar la posibilidad de grabación o si fuera factible su total anulación.

En este sentido se puede determinar dos (2) posibles orígenes para las grabaciones:

- **Voluntaria**. Aquella que realiza el interviniente en una conversación de forma consciente. Por ejemplo, a través de un grabador o con las funciones propias de un dispositivo móvil.
- **Involuntaria**. Aquella que realiza el interviniente en una conversación, no siendo consciente de ese hecho. Por ejemplo, cuando su dispositivo móvil tiene instalada una aplicación no autorizada que permite un control y una escucha remota.

Dentro de las recomendaciones posibles para limitar estas acciones, sean o no voluntarias, se establecen tres (3) mecanismos fundamentales que podrían ser aplicados de manera independiente o concurrentemente:

- Procedimiento y operativa manual para el mantenimiento de dispositivos móviles y equipos de grabación fuera del contexto de la reunión.
- Empleo de tecnologías para limitar los procesos de grabación.
- Medidas mínimas de salvaguardas para la protección de dispositivos móviles y prevenir la instalación de aplicaciones no deseadas en los mismos.

2. PROCEDIMIENTO PARA LA SALVAGUARDA DE DISPOSITIVOS MÓVILES O DE GRABACIÓN

Con objeto de limitar el uso de dispositivos móviles o de grabación en una reunión, se puede proceder de acuerdo a las siguientes pautas:

- Se colocarán unos casilleros con compartimentos individuales, y con llave por cada uno de ellos, bien dentro o fuera de la sala donde se lleven a cabo las reuniones.
- Dichos casilleros, si se ubican externamente a la sala de reuniones, no deberán tener ninguna consideración especial, salvo los propios mecanismos de seguridad que impidan a terceros acceder al contenido mientras se encuentren cerrados.
- En el caso de que se ubicasen dentro de la sala, sería recomendable que tuvieran apantallamiento acústico y protección frente a emanaciones para evitar que en caso dejar los dispositivos en un modo activo, puedan grabar o servir de escucha de lo que sucede en la sala.
- Los dispositivos una vez apagados se depositarán en los compartimentos. En el caso de dispositivos tipo *smartphone* se pondrán al menos en modo avión.
- Cada persona custodiará la llave correspondiente al compartimento donde habrá depositado sus dispositivos.
- Por último, se puede recurrir a fundas apantalladas que bloquean las señales y que, en apariencia, no difieren de cualquier funda de plástico. El objetivo es impedir cualquier conexión desde o hacia el móvil anulando la posibilidad de que se interactúe con un dispositivo, más aún con software malicioso instalado.

3. USO DE TECNOLOGÍAS PARA LIMITAR GRABACIONES.

En el caso de que fuera necesario disponer de dispositivos móviles en las reuniones, existen elementos tecnológicos capaces de limitar la capacidad de grabar una conversación, como los anuladores de grabadoras y micrófonos.

Estos componentes no son inhibidores de señales en sí, ni van a impedir el funcionamiento de los dispositivos de grabación. Básicamente hacen ininteligible las conversaciones grabadas a través de grabadoras convencionales o de dispositivos móviles.

Este tipo de dispositivos operan mediante el uso de múltiples emisores ultrasónicos, imperceptibles para el oído humano. Emiten multidireccionalmente y con distancias desde el lugar donde se ubica el aparato de hasta 10 o 12 metros en los modelos más eficientes.

Aunque existen dispositivos más económicos basados en la generación de ruido blanco, nos son totalmente efectivos contra determinados tipos de escuchas incluyendo las que se producen a través de dispositivos móviles.

En este sentido, aunque no son tan económicos, es preferible la adquisición de aparatos basados en distorsión de ruido y reverberación en secuencia aleatoria.

4. MEDIDAS PARA LA PROTECCIÓN DE DISPOSITIVOS MÓVILES FRENTE A INSTALACIÓN DE APLICACIONES ILÍCITAS.

Al igual que sucede con otras tecnologías, como los puestos de trabajo, las funcionalidades de los dispositivos móviles los hacen proclive a software malicioso o aplicaciones no autorizadas que permiten a un tercero tener un control absoluto del mismo.

Con objeto de limitar esa posibilidad, se aconseja aplicar medidas mínimas de protección y uso seguro de este tipo de dispositivos:

- En los ajustes del dispositivo, se han de comprobar las aplicaciones que han solicitado acceso al micrófono y a la cámara del dispositivo, y revisar aquellas a las que se les ha otorgado este permiso. En este sentido, se aconseja no otorgar permisos innecesarios o excesivos a las *App*, limitando así los datos y la funcionalidad a la que éstas tendrán acceso.
- Todo dispositivo deberá disponer de una clave de al menos ocho (8) caracteres o de tecnología basada en biometría para acceder al mismo. Dicha medida será de aplicación también cuando sea necesario el desbloqueo del móvil.
- Como cualquier otro dispositivo, se mantendrán siempre actualizados al máximo posible, atendiendo para ello a las especificaciones que establece el fabricante.
- No se deberá emplear ninguna metodología para romper la seguridad o suprimir las limitaciones que ha definido el fabricante. No se deberían aplicar métodos tales como *Jailbreak* (para dispositivos *iOS*) o *Rootear* (para dispositivos *Android*).
- Solo se deberán instalar aplicaciones de orígenes de confianza como las tiendas del fabricante del dispositivo. Por ejemplo, *App Store* o *Google Play Store*.
- Se recomienda desinstalar aquellas aplicaciones que el usuario ha dejado de utilizar en su dispositivo móvil.
- Si se dispone de correo electrónico en el dispositivo móvil, no se deberían abrir correos o adjuntos de fuentes no conocidas o de dudosa procedencia.
- Se debería evitar dar respuesta a través de SMS o aplicaciones de mensajería instantánea a peticiones de terceros que impliquen dar datos propios del dispositivo móvil o de códigos que se emplean para procesos de autorización.

- Las aplicaciones o cuentas de correo electrónicos vinculados al dispositivo móvil, tales como cuentas de *iCloud* o *Google*, deberían tener contraseñas diferenciadas de otras cuentas personales que se emplean para acceder a portales u otras aplicaciones.
- Preferiblemente y si es factible, se deberán emplear mecanismos de doble factor de autenticación para el acceso a las aplicaciones.
- Por último y en la medida de lo posible, las organizaciones deberían emplear tecnologías MDM (*Mobile Device Management*). Esto permitirá tener un control de los dispositivos móviles y aplicar medidas de seguridad de forma centralizada.