INFORMES TÉCNICOS

Experiencias internacionales en almacenamiento y acceso de Entrevistas Investigativas Videograbadas y/o declaraciones judiciales

Octubre, 2019

FUNDACIÓN
AMPARO Y JUSTICIA

FUNDACIÓN
AMPARO Y JUSTICIA

EXPERIENCIAS INTERNACIONALES EN ALMACENAMIENTO Y ACCESO DE ENTREVISTAS INVESTIGATIVAS VIDEOGRABADAS Y/O DECLARACIONES JUDICIALES[1]

Uno de los desafíos de países que han implementado la Entrevista Investigativa y/o la Declaración Judicial Videograbada con niños, niñas y adolescentes ha sido la instalación de un sistema de almacenamiento y acceso a los registros videograbados que permita evitar que personas no autorizadas accedan a su contenido y que éste sea manipulado, publicado o difundido, conllevando consecuencias perjudiciales, tanto para el proceso penal, como para las víctimas y/o testigos involucrados.

A nivel internacional, en general, existen **dos vías de almacenamiento y acceso** a los registros videograbados de la entrevista y/o declaración: el físico (CD, DVD o USB) y el virtual o en red[2]. Una práctica internacional habitual es el **almacenamiento físico** de los registros en DVDs. Si bien la custodia y traslado de archivos de video mediante CDs o DVDs está libre de amenazas cibernéticas, la inminente obsolescencia de los discos en el comercio, las complejidades de la logística del almacenamiento (espacio físico, sobres, etiquetado), traslado (correo, encriptación) y destrucción de estos, sumado a los riesgos de pérdida, daño o deterioro con el tiempo, apremian buscar soluciones tecnológicas más avanzadas que permitan, por un lado, almacenar y compartir información de forma segura ante amenazas virtuales y, por el otro, que hagan frente a posibles peligros que conlleva el almacenamiento y acceso físico a los registros videograbados.

Ante estos riesgos, algunos países han optado por el **almacenamiento en red o virtual** de sus registros videograbados, o se encuentran en transición hacia esta modalidad, utilizando la modalidad física, complementada con el almacenamiento en red. Algunos de estos ejemplos son Inglaterra, países nórdicos con centros Barnahus[3] y estados de Canadá y Estados Unidos.

El presente documento tiene como fin dar cuenta de prácticas internacionales y opciones tecnológicas disponibles para facilitar el **almacenamiento y acceso seguro** a los registros videograbados de entrevistas investigativas y declaraciones en juicio oral de víctimas y/o testigos niños, niñas y adolescentes.

---

[1] Documento elaborado por Valentina Ulloa en octubre de 2019.

[2] Esta información fue obtenida a través de la revisión de leyes y protocolos nacionales, locales o institucionales; entrevistas con operadores de dichos sistemas de justicia, académicos y expertos de Inglaterra, Escocia, Noruega, Estados Unidos, Canadá, Australia, Nueva Zelanda, República Dominicana, Argentina e Israel.

[3] "Casas de Niños" en Europa, o centros multidisciplinarios para niños víctimas de abuso sexual y/o maltrato.

Almacenamiento y acceso físico

En algunos países, los videos de las entrevistas suelen ser almacenados en **discos o en dispositivos USB**. En caso de uso de DVD, los reglamentos o protocolos establecen la realización de dos o más copias inmediatamente después de grabada la entrevista: una copia maestra, almacenada en el centro donde se realizó la entrevista, y una o más copias de trabajo, que se suelen enviar a Fiscalía, al Juzgado, a los investigadores del caso, entrevistadores o supervisores, y que es la que se utiliza para realizar copias extras o editadas. Los discos **quedan custodiados o son compartidos bajo estrictas medidas de seguridad**, entre las que se incluyen:

- Almacenamiento y traslado seguro: Los discos o dispositivos suelen ser almacenados y trasladados en sobres lacrados o sellados, correctamente etiquetados, y luego guardados dentro de cajas fuertes o en lugares con acceso restringido. En caso traslado, éste se realiza bajo una serie de medidas de seguridad, entre ellas, traslado por parte del entrevistador que tomó la declaración, sobre sellado, correo interno o certificado, entre otras.

- Encriptación: Los DVDs o USBs en algunos países son grabados con encriptación, lo que incluye diversas medidas de resguardo como:
  - ✓ Acceso mediante contraseña. Pueden agregarse contraseñas por grupo.
  - ✓ Prohibición de hacer copia del DVD, editar la información o agregar nuevos datos.
  - ✓ Visualización restringida a ciertos computadores (IP) o lugares con permiso para reproducir el disco.

- Marca digital del registro*:* Se suele agregar una marca de agua al DVD, indicando el nombre de la persona que accedió a la copia, la fecha, entre otros datos.

- Formulario y etiquetado: Los discos deben ser correctamente etiquetados y almacenados junto a un formulario o acta que indique la información básica sobre la entrevista (participantes, número de caso, fecha, número de referencia, etc.). Cabe destacar que, en Reino Unido, uno de los problemas que tuvieron con la implementación de la entrevista videograbada fue el mal etiquetado de DVDs, lo cual conllevó dificultades para la identificación y búsqueda del contenido de los discos.

- Registro o historial: Siempre se lleva un registro electrónico donde se documenta, además de los datos de la entrevista como fecha y participantes, la reproducción de copias adicionales, las personas que han observado o se les ha hecho entrega de una copia, fechas de devolución y/o de destrucción, número de referencia de cada copia o número de causa.

- Devolución o destrucción de la copia: Las copias entregadas, ya sea por medio de discos o de dispositivos USB, en general, deben ser devueltas a la institución donde se almacena la copia, luego del evento de formación o supervisión, o eliminadas del disco o dispositivo. Algunos países especifican un rango de meses para la destrucción de las copias de trabajo o las adicionales finalizado del proceso de investigación. La devolución de un disco encriptado (e.g. con prohibición de copia), asegura en mayor medida que la evidencia no sea difundida o extraviada, al hacer responsable a la institución encargada del almacenamiento de los registros de su destrucción, en vez de la persona que lo solicitó. En Israel, por ejemplo, los DVDs son destruidos, enviándolos a una compañía especializada en este tipo de trabajo.

Almacenamiento y acceso virtual

Algunos países como Inglaterra, Estados Unidos, Canadá, Noruega y otros países nórdicos, almacenan los registros utilizando **softwares o sistemas basados en servidores internos o en nubes virtuales**[4], que cuentan con una serie de funciones que permiten respaldar y compartir las videograbaciones de forma segura. Algunas de las funciones o herramientas con las que cuentan estas aplicaciones son:

- Registro/historial: Permiten organizar y etiquetar la información, así como visualizar y compartir archivos por nombre del funcionario, fecha, localización o ID del caso. Mantienen un historial con la cadena de custodia de la evidencia y las acciones o movimientos realizados por los usuarios.

- Contraseña: Permiten acceder y compartir los datos con contraseñas. Los softwares ofrecen la posibilidad de otorgar permisos diferenciados por grupos y funciones

- Acceso dentro de premisas o remoto: Es posible acceder a los videos, ya sea en oficinas de las instituciones, como remotamente, mediante intranet o sitios web. También permiten compartir videos mediante un link que puede ser temporal (expirar después de un tiempo) y con contraseña. Algunos permiten el acceso desde celulares o tablets.

- Restricción y selectividad del acceso: Permiten restringir el acceso o realización de copias de los videos, incluyendo, cantidad y frecuencia de visualizaciones, periodo de vigencia, rango de horario, lugar (e.g. asociación a un IP), visualización diferenciada de distintas versiones de la entrevista (e.g. distorsionada y original). También permiten anular claves.

- Edición: Incluyen la posibilidad de editar videos, incluyendo distorsión de voz y/o de imagen, difuminación masiva, marcas de seguridad de quien accede, selección de extracto de video, y/o agregar clips o marcadores.

- Herramientas de transcripción: Facilitan la transcripción de los videos.

- Análisis: Permiten realizar análisis estadísticos de metadatos como total de videos, accesos, participantes, interacciones, eliminaciones. Además, generan planillas con la información.

- Notas: Permiten agregar comentarios o completar viñetas con información del caso o de la calidad de entrevista, desempeño del entrevistador, retroalimentación al entrevistador e incluso información para planificar la entrevista.

- Evidencia complementaria: Hacen posible agregar información, documentos, fotografías, que complementen la información del caso, pre o post carga de la entrevista.

[4] Los softwares basados en servidores internos (VPN) constituyen una opción segura ante amenazas cibernéticas y no necesariamente requieren de acceso a internet. Los basados en nubes, requieren de acceso a internet, pero constituyen una opción que puede ser más económica y permite acceso remoto desde PC, celular o Tablet.

A continuación, se presentan algunas opciones de software utilizadas a nivel nacional e internacional:

VSN Innovation and media solutions[5]

Es una empresa con más de 20 de años de experiencia en el rubro y presencia en prácticamente todos los países del mundo. Cuenta con los recursos y proveedores para habilitar una sala de entrevista investigativa videograbada, contemplando: a) el equipamiento tecnológico, insumos adquiridos con sus socios, b) el servicio de grabación y encriptación, y/o c) el software de almacenamiento y gestor de contenidos. En relación al software, ofrecen una plataforma que puede estar, ya sea basada en un servidor físico, el cual requiere contar un servidor institucional interno, que puede prescindir de internet o en la nube.

En Chile han asesorado a Centros de Atención a Víctimas (CAVAS) de la PDI, Canal 13, Congreso de Chile, Intesis Chile, entre otros. CAVAS adquirió un servicio por cinco años de 100 licencias (acceso simultáneo de 100 funcionarios), utilizando un servidor físico. Si bien el servicio expiró el 2019, la empresa ofrece la opción de actualizar el servicio, en vez de adquirir uno nuevo para reducir costos.

Contacto: Roi Neira Mail: rneira@vsn-tv.com Teléfono: +56972018105

Axon Evidence[6]

Es una compañía que ofrece tecnologías de última generación para la seguridad pública, y es utilizada por agencias de seguridad pública tales como la Policía de Londres en Inglaterra; de Miami y Los Ángeles, en EE. UU; la Policía Federal de Australia y la Policía Municipal de Madrid en España. Para el caso de la gestión de entrevistas videograbadas, Axon Evidence es una plataforma de gestión de evidencia digital (videos, fotografías, documentos). Provee un servicio de sistema o aplicación basada en la nube que consolida todos los archivos digitales, permitiendo manejar y compartir datos, manteniendo la seguridad y cadena de custodia.

En Chile, este año, Carabineros de Chile implementó un plan piloto de sistema de televigilancia en Santiago (San Joaquín), adquiriendo los servicios de cámaras corporales, para vehículos y de vigilancia, almacenamiento de la evidencia en la nube y un centro de monitoreo.

Contacto: Arthur Bernardes Mail: abernardes@axon.com Whatsapp: +52 (55) 4117 9128 (WhatsApp) y Francisco del Campo (distribuidor en Chile) Mail: fndelcampo@smartpartners.cl Teléfono: +56994990934

Indico[7]

Es una empresa proveedora del servicio de grabación (Indico Recorder) y gestión de archivos (Indico Server), utilizado por las Policías y Barnahus en Reino Unido y otros países estos centros, como Noruega. Cuentan con amplia experiencia en videograbaciones de entrevistas investigativas para órganos de Justicia Penal (Policía y Tribunales) y son los auspiciadores del International Investigative Interviewing Research Group (iIIRG). Ofrecen un software de almacenamiento de información basado en un servidor interno, diferente de una nube, que permite guardar las videograbaciones en una red interna, en donde sólo tienen acceso algunas personas con los permisos acordes.

[5] https://www.vsn-tv.com/en/
[6] https://la.axon.com/products/evidence
[7] http://www.indicosys.com

Si bien, la compañía no cuenta actualmente con un business partner en Chile, según ejecutivos de Indico, se encuentran en búsqueda de una alianza con un proveedor chileno, posiblemente para el tercer trimestre de 2019.

Contacto: Emil Flam Mail: emil@indicosys.com Teléfono:+4795898445 y Henrik-Andre Kalleberg Mail: henrik@indicosys.com Teléfono: +4790075557

IMS The Tiles Solution[8]

Es una herramienta, basada en la nube, de planificación y manejo de entrevistas investigativas, que permite almacenar de manera segura, planificar, conducir y evaluar o supervisar entrevistas en un ambiente digital. Ayuda a generar un flujo de los casos a partir de distintas piezas de evidencia, incluyendo funciones de mapeo, línea del tiempo, entre otros, reduciendo el tiempo de preparación y planificación de una entrevista. La compañía ha sido también uno de los auspiciadores del congreso de International Investigative Interviewing Research Group (iIIRG) en varias versiones.

Contacto: Daren Jay djay@interviewmanagementsolutions.com

Forensic Interview Trace[9]

The Forensic Interview Trace (FIT™) es una aplicación/software basada en la nube, segura y de fácil uso, diseñada para registrar la estructura, el contenido y las características de las entrevistas forenses con víctimas, testigos y sospechosos de delitos, tanto en **v**ideos como en audios. Fue lanzada en la Conferencia iIIRG 2016 en Londres y muchos delegados expresaron un gran interés en probar la versión inicial de FIT™ en sus organizaciones como piloto.

Contacto: info@forensicinterviewtrace.com y laura@forensicinterviewtrace.com

Plataformas de almacenamiento en nube

Además de los softwares de gestión de evidencia, como los recientemente mencionados, existen empresas que proporcionan plataformas en la nube que permiten principalmente almacenar, de forma segura, todo tipo de datos o archivos, los cuales son administrados por el proveedor del servicio. Existen plataformas basadas en nubes públicas, en las cuales se comparten recursos con otras organizaciones, en nubes privadas, en las cuales los servicios se mantienen en una red privada y se dedican solamente a una organización, y las híbridas. Entel Secure Cloud, entre otras compañías, constituye un ejemplo de estas última, combinando la flexibilidad de la nube pública y la seguridad de la nube privada.

Contacto: Pablo Palomé Mail: ppalome@entel.cl Teléfono: +56 9 6587 7643

[8] https://interviewmanagementsolutions.com/
[9] http://www.forensicinterviewtrace.com/

Medidas de seguridad adicionales

Por último, algunas medidas adicionales que los países revisados contemplan para regular el acceso a las copias de los videos y/o cumplir con estándares de protección de los datos[10] son:

- Consentimiento informado de víctima/representante: Antes de realizar la entrevista se suele solicitar la firma de un consentimiento informado a la víctima, y si ésta no está en condiciones, se recurre a su representante legal. Esto no significa que cualquiera que desee ver la grabación pueda hacerlo. El consentimiento especifica los fines para los cuales será usado el registro.

- Formulario de solicitud/ retiro de registro: En general, quien toma una copia debe firmar un formulario o acta para acceder a ésta.

- Confidencialidad y carta de compromiso: En todos los países estudiados existen, en distintos grados o formas, condiciones de confidencialidad para la observación o acceso a una copia de las entrevistas, entre las cuales se encuentran: la prohibición de filmar, fotografiar, difundir, transmitir o realizar copias adicionales de la videograbación. En algunos países la ley considera una sanción monetaria o penal por el no cumplimiento de ellas. Asimismo, se exige a quien retira una copia que firme una carta, acta de confidencialidad o compromiso a preservar el material (e.g. solicitud de guardar copia en lugar seguro) y garantizar la cadena de custodia).

- Destrucción de registro original: Las normativas de los países también establecen, en general, directrices para la destrucción de los registros audiovisuales originales, aunque con diferentes plazos. Éstos van entre uno, tres, seis, siete o diez años después de la sentencia definitiva o cierta cantidad de años cuando los casos no prosperan (siete, cincuenta).

Octubre, 2019

[10] En Chile, la ley 19.628 regula el tratamiento de datos personales en registros de organismos públicos o particulares.