APRUEBA PROTOCOLO DE RESGUARDO REMOTO DE EVIDENCIA DIGITAL

RESOLUCIÓN Nº 295/22/PG

Viedma, 30 de noviembre de 2022.-

VISTOS:

Los principios, derechos y garantías que rigen el procedimiento penal de nuestra provincia desde la entrada en vigencia de la Ley 5020, lo dispuesto en el art. 46 de la Ley 4199, la Resolución 68/15/PG por la cual se establecieron las misiones y funciones de la OITEL, la Instrucción General 9/18/PG que creó el Protocolo General de Actuación del MPF en casos de Ciberdelitos, teniendo presente lo normado por el Superior Tribunal de Justicia mediante Ac. 8/2019; y

CONSIDERANDO:

Que transcurrido un tiempo prudencial desde la entrada en vigencia del nuevo Código de Procedimientos Penal, la experiencia adquirida revela la necesidad de normar los procedimientos de resguardo de evidencia digital que llevan a cabo los profesionales que integran la OITEL;

Que dicho organismo entre el año 2017 y el año 2021 vio incrementado en un 91% los requerimientos de extracción de evidencia digital de dispositivos móviles recibidos por parte de organismos del Ministerio Público (Fiscalías y Defensorías Oficiales), lo que demuestra que la evidencia digital resulta vital en la investigación penal;

Que dicha afirmación se encuentra robustecida por el uso generalizado de dispositivos electrónicos y aplicaciones Web por gran parte de la sociedad no solo como herramienta de comunicación, sino también para desarrollar actividades laborales, de capacitación, recreativas y el resguardo de información de todo tipo;

Que del mismo modo que las situaciones de la vida cotidiana fueron transformadas por la irrupción de estas tecnologías, también migró hacia esos entornos el fenómeno delictivo y por ende, la investigación penal;

Que en razón de ello y en el marco de la Ac. 8/2019, profesionales de la OITEL comenzaron a analizar las posibilidades de realizar resguardos remotos de evidencia digital

utilizando diversas herramientas forenses, como así también explorando las utilidades de las aplicaciones y proveedores de servicios más utilizados por los usuarios, tales como Google, WhatsApp, Telegram, entre otros.

Que luego de ello, comenzaron a aplicar tales procedimientos de resguardo remoto de evidencia digital primero en legajos donde la urgencia y el peligro en la demora indicaban la necesidad de poner a disposición del Fiscal alternativas que agilizaran el resguardo de la evidencia y, en virtud de sus beneficios y eficacia, lo extendieron a mayor cantidad de casos, realizando 6 procedimientos de resguardo remoto en 2020, 15 en 2021 y 77 en 2022.

Que evidencias digitales obtenidas a través de estos procedimientos ya han sido incorporadas en diversos procesos e incluso en el Legajo MPF-RO-03897-2020, se ha adquirido la experiencia de aplicarlo durante el juicio en los términos de la última parte del art. 177 del CPP y dando como resultado una sentencia condenatoria, que ya fue revisada por el Tribunal de Impugnación y confirmada por el Superior Tribunal de Justicia mediante Se. 107/22.

Que, en este camino, las formas de obtención de estos medios probatorios hacen a la legalidad del procedimiento y resultan vitales al momento ofrecerlos e incorporarlos en los debates orales, tornándose necesario reglar los procedimientos y técnicas de adquisición y preservación de la evidencia digital existentes a los fines de evitar planteos de nulidad que interrumpan el desarrollo de los procesos;

Que, en relación con lo anterior, se prevé que los Procedimientos de Resguardo Remoto independientemente de quien los solicite y a su criterio, sean controlados por la contraparte pudiendo participar del procedimiento y si decidiera no hacerlo, se incorpora en el Informe Técnico con sus resultados, el registro audiovisual de todas las tareas llevadas a cabo durante el procedimiento para que pueda ser analizado por peritos de parte si la estrategia procesal lo hiciera necesario y, además, para que pueda visualizarse durante el debate;

Que estos Procedimientos de Resguardo Remoto de Evidencia Digital tienen dentro de sus principales objetivos resguardar la evidencia digital de forma rápida y ágil, simplificando los procedimientos, aprovechando las utilidades disponibles en las distintas aplicaciones utilizadas por los usuarios, permitiendo disminuir las gestiones administrativas y costos económicos que implica el traslado de dispositivos en el vasto territorio provincial, logrando un uso más eficiente de los recursos del Ministerio Público;

APRUEBA PROTOCOLO DE RESGUARDO REMOTO DE EVIDENCIA DIGITAL

RESOLUCIÓN Nº 295/22/PG

Que, por otro lado, resulta de sustancial importancia disminuir el máximo posible las molestias y el estado de vulnerabilidad que genera a las víctimas del delito las ser despojadas de sus dispositivos electrónicos para ser peritados, sobre todo en aquellos casos que suceden en contextos de violencia de género, donde esos dispositivos se tornan imprescindibles para su cuidado personal.

Que la Secretaría de Superintendencia y Técnica Nro. 1 intervino como reglamentariamente le compete.

Que la Dirección de Asesoramiento Legal de esta Procuración ha tomado intervención en los términos del art. 12 de la Ley A 2938.

Por ello y en orden a las facultades provenientes del art. 215 de la Constitución Provincial, arts. 10,11 y cctes. de la Ley K 4199,

El Sr. PROCURADOR GENERAL

R E S U E L V E:

Art. 1) Aprobar en el ámbito de la Provincia de Río Negro, el Protocolo de Resguardo Remoto de Evidencia Digital que se adjunta como Anexo I de la presente.

Art. 2) Disponer que el organismo responsable de su aplicación será la OITEL, el cual además deberá llevar un registro estadístico sobre su aplicación y resultados y velará por la revisión periódica y actualización constante de dichos procedimientos.

Art. 3) Encomendar al Ing. Baffoni, responsable de la OITEL, capacitar a Fiscales, Defensores y Adjuntos respecto de la aplicación, requisitos y objetivos del Protocolo de Resguardo Remoto de Evidencia Digital.

Art. 4) Regístrese, notifíquese y publíquese en el sitio web de este Ministerio Público.-

Jorge Oscar Crespo
Procurador General
Poder Judicial
Provincia de Río Negro

CRESPO Jorge Oscar
Firmado digitalmente por CRESPO Jorge Oscar
Fecha: 2022.11.30 09:54:31 -03'00'

ANEXO I

PROTOCOLO DE RESGUARDO REMOTO DE EVIDENCIA DIGITAL

1. REGLAS GENERALES, DEFINICIONES Y PRINCIPIOS

El siguiente Protocolo de Resguardo Remoto de la Evidencia Digital tiene como objetivo establecer las pautas y los procedimientos que deben seguir los cuerpos técnicos forenses al momento de realizar el resguardo de evidencia digital de manera remota, sea que estén almacenados en la memoria de dispositivos (celulares, tablets, etc.) o en la “nube” (base de datos de sitios web).

El objetivo de estos procedimientos de Resguardo Remoto de Evidencia Digital es acceder, descargar, resguardar y preservar de forma ágil y confiable la evidencia digital de interés para una investigación penal, sin tener la necesidad de contar físicamente con el dispositivo que contiene la información o las credenciales de acceso al lugar donde está almacenada la misma (credenciales de acceso a la “nube”).

Un aspecto importante de este protocolo es permitir a las partes controlar y auditar los procedimientos realizados, debido a que por las características dinámicas de la evidencia digital los mismos pueden tornarse irreproducibles.

La aplicación de lo aquí dispuesto dependerá de las particularidades de cada caso, pero debe tenerse presente que sus principales objetivos son resguardar la evidencia digital de forma rápida, simplificando los procedimientos, aprovechando las utilidades que las distintas aplicaciones ponen al servicio de los usuarios, disminuyendo las gestiones administrativas y costos económicos que implica el traslado de dispositivos en el vasto territorio provincial y sobre todo, aminorando las molestias que genera a las víctimas del delito despojarse de sus dispositivos electrónicos.

2. CONCEPTOS IMPORTANTES

a. EVIDENCIA DIGITAL EN DISPOSITIVO MÓVIL: es toda aquella información digital de interés para un proceso penal que se encuentre almacenada en la memoria de un dispositivo móvil. (Ej. WhatsApp, Telegram, etc.)
b. EVIDENCIA DIGITAL EN LA NUBE: es toda aquella información digital de interés para un proceso penal que se encuentra almacenada en una plataforma o sitio web, pudiendo o no existir una copia de esta información en la memoria de un dispositivo móvil/computadora (Ej. Facebook, Instagram, Twitter, etc).

c. EVIDENCIA DIGITAL EN LA NUBE DE ACCESO PÚBLICO: es toda aquella información digital de interés para un proceso penal que se encuentra almacenada en una plataforma o sitio web que es visible públicamente, es decir, sin la necesidad de contar con las credenciales específicas de un determinado usuario.

d. EVIDENCIA DIGITAL EN LA NUBE DE ACCESO RESTRINGIDO: es toda aquella información digital de interés para un proceso penal que se encuentra almacenada en una plataforma o sitio web que solo es visible si se ingresa con las credenciales de acceso (usuario/contraseña) de un determinado usuario o grupo de usuarios.

e. HASH: Algoritmo matemático encargado de transformar cualquier bloque arbitrario contenedor de datos en una serie de carácteres o dígitos de longitud fija. Se utiliza para la identificación de elementos, es decir, garantizar la inalterabilidad de un documento o archivo, ya que si se modifica el archivo, se modifica el valor hash del mismo.

f. SIM CARD: La tarjeta SIM o módulo de identificación del suscriptor consiste en una pequeña tarjeta de plástico con un chip integrado que se coloca dentro de un teléfono móvil para permitir que este pueda operar con la red de telefonía móvil. Estas almacenan la identidad del usuario, los algoritmos de autenticación que garantizan dicha identidad y los algoritmos de cifrado que garantizan la confidencialidad de las comunicaciones. Cada tarjeta SIM posee un número de identificación único de 19 dígitos - ICC o International Circuit Card - el cual el operador de telefonía móvil asocia a un número de abonado determinado.

3. PROCEDIMIENTOS

a) RESGUARDO REMOTO EVIDENCIA DIGITAL ALMACENADA EN DISPOSITIVO MÓVIL

i. Objetivo: Resguardar de manera remota Información Digital que se encuentra almacenada en la memoria de un dispositivo, sin que su propietario haga entrega del mismo.

ii. Requerimientos: para acceder a la información digital almacenada en la memoria del dispositivo, la aplicación instalada en el mismo debe poseer un servicio de acceso de forma remota mediante internet que permita su vinculación con el dispositivo (por ej. Web.WhatsApp, Web Telegram, entre otras)

iii. Procedimiento:

iii.a. El Fiscal/Defensor requirente deberá enviar mediante correo electrónico la solicitud de turno de “Resguardo Remoto de Evidencia Digital” a la OITEL (oitel@jusrionegro.gov.ar) indicando detallada y concretamente qué tipo de información se desea resguardar, nombre de la aplicación en la que se encuentra, rango temporal en la cual se produjo tal evidencia, etc.

iii.b. La OITEL comunicará mediante correo electrónico el día y hora fijados para la realización del procedimiento, para que, en el caso que corresponda, el Fiscal/Defensor requirente pueda notificar a la contraparte del turno asignado, por si ésta desea presenciar y controlar el procedimiento.

iii.c. El día asignado para el procedimiento, la OITEL realizará una videoconferencia con el organismo solicitante, la que será grabada para contar con el registro audiovisual de las actividades realizadas. El organismo solicitante deberá conectarse a la videoconferencia junto a la persona que aporta el dispositivo que contiene la evidencia a resguardar, asegurando que el dispositivo cuente con acceso a internet, sea por Wifi o Datos móviles.

iii.d. El Profesional designado por la OITEL para la realización del procedimiento compartirá pantalla en la videoconferencia y mostrará en todo momento cada uno de los pasos que realiza para acceder a la evidencia digital que se encuentra almacenada en el dispositivo, tales como el acceso a la plataforma WEB que permite la vinculación al dispositivo, el proceso de autorización (ej. escanear código QR), el acceso a la información de interés, la visualización y/o descarga de archivos, etc.

iii.e. Una vez culminado el procedimiento, el profesional interviniente confeccionará un Informe Técnico en el que detallará todos los pasos realizados. Tal informe será acompañado de un Anexo en el cual se adjuntará la evidencia digital resguardada y el video completo del procedimiento. Para garantizar la integridad de la evidencia digital, se generarán valores HASH, de los que se dejará constancia en el mismo informe. En todos los casos y sin excepción los Informes Técnicos

deberán ser firmados digitalmente por los profesionales de la OITEL que intervinieron en el procedimiento.

b) RESGUARDO REMOTO EVIDENCIA DIGITAL ALMACENADA EN LA NUBE - ACCESO PÚBLICO

i. Objetivo: Resguardar de manera remota Información Digital que se encuentra almacenada en la nube y que es visible de forma pública.

ii. Requerimientos: se debe poseer un enlace o link al sitio web donde se encuentra visible la información de interés (texto, audio, imagen, video). Los técnicos de la OITEL que realizan el procedimiento deberán contar, en caso que sea necesario, con un usuario de acceso a la red social/sitio web donde se encuentra alojada la evidencia a resguardar (por ej. Facebook, Instagram,Twitter, entre otras).

iii. Procedimiento:

iii.a. El Fiscal/Defensor requirente deberá enviar mediante correo electrónico la solicitud de turno de “Resguardo Remoto de Evidencia Digital Almacenada en la Nube” a la OITEL (oitel@jusrionegro.gov.ar) suministrando el enlace o link que permite acceder al contenido de interés. Además, deberá indicar detallada y concretamente qué tipo de información se desea resguardar, nombre de la red social/sitio web donde se encuentra la información a resguardar, rango temporal de en la cual se produjo tal evidencia, etc.

iii.b. Recepcionado el correo electrónico del organismo requirente, un profesional de la OITEL ingresará al enlace proporcionado a través de un navegador web, accediendo y descargando, cuando sea posible, la información que se desea resguardar. Todo este procedimiento será videograbado para que luego pueda ser controlado por quien lo requiera.

iii.c. Una vez culminado el procedimiento, el profesional interviniente confeccionará un Informe Técnico en el que detallará todos los pasos realizados. Tal informe será acompañado de un Anexo en el cual se adjuntará la evidencia digital resguardada y el video completo del procedimiento. Para garantizar la integridad de la evidencia digital, se generarán valores HASH, de los que se dejará constancia en el mismo informe. En todos los casos y sin excepción los Informes Técnicos

deberán ser firmados digitalmente por los profesionales de la OITEL que intervinieron en el procedimiento.

c) RESGUARDO REMOTO EVIDENCIA DIGITAL ALMACENADA EN LA NUBE - EVIDENCIA DIGITAL DE ACCESO RESTRINGIDO

i. Objetivo: Resguardar de manera remota Información Digital que se encuentra almacenada en la nube, pero que solo resulta visible desde un usuario o cuenta en particular (no es de acceso público), sin que su titular haga entrega del dispositivo para acceder a la cuenta desde donde es visible la información de interés.

ii. Requerimientos: para acceder a la información digital almacenada en la nube de forma restringida (sólo visible desde el perfil de un usuario o grupo de usuarios) el requirente debe aportar las credenciales de acceso al sitio (por ej. usuario y contraseña de Facebook, Instagram, cuenta de Google, entre otras) y tener a disposición los medios de autenticación de dos pasos, en caso de estar configurados (celular/correo electrónico/aplicación de autenticación vinculado a la cuenta).

iii. Procedimiento:

iii.a. El Fiscal/Defensor requirente deberá enviar mediante correo electrónico la solicitud de turno de “Resguardo Remoto de Evidencia Digital Almacenada en la Nube” a la OITEL (oitel@jusrionegro.gov.ar) indicando detallada y concretamente qué tipo de información se desea resguardar, nombre de la aplicación en la que se encuentra, rango temporal en la cual se produjo tal evidencia, etc.

iii.b. La OITEL comunicará mediante correo electrónico el día y hora fijados para la realización del procedimiento, para que, en el caso que corresponda, el Fiscal/Defensor requirente pueda notificar a la contraparte del turno asignado, por si ésta desea presenciar y controlar el procedimiento.

iii.c. El día asignado para el procedimiento, la OITEL realizará una videoconferencia con el organismo solicitante, la que será grabada para contar con el registro audiovisual de las actividades realizadas. El organismo solicitante deberá conectarse a la videoconferencia junto a la persona que aporta las credenciales de acceso a la plataforma donde se encuentra la evidencia a resguardar, teniendo a disposición el celular que

posee la línea/correo electrónico/aplicación de autenticación asociado a la cuenta para obtener el código de doble autenticación, en caso de que esté activado este mecanismo.

iii.d. El Profesional designado por la OITEL para la realización del procedimiento compartirá pantalla en la videoconferencia y mostrará en todo momento cada uno de los pasos que realiza para acceder a la evidencia digital almacenada en la nube, tales como el acceso a la plataforma WEB, el proceso de autorización ingresando usuario y clave, el acceso a la información de interés, la visualización y/o descarga de archivos, etc.

iii.e. Una vez culminado el procedimiento, el profesional interviniente confeccionará un Informe Técnico en el que detallará todos los pasos realizados. Tal informe será acompañado de un Anexo en el cual se adjuntará la evidencia digital resguardada y el video completo del procedimiento. Para garantizar la integridad de la evidencia digital, se generarán valores HASH, de los que se dejará constancia en el mismo informe. En todos los casos y sin excepción los Informes Técnicos deberán ser firmados digitalmente por los profesionales de la OITEL que intervinieron en el procedimiento.

d) RECUPERACIÓN DE CREDENCIALES DE ACCESO A CUENTAS EN LA NUBE MEDIANTE LÍNEA DE CELULAR ASOCIADA.

i. Objetivo: Recuperar las credenciales de acceso (usuario/contraseña) a una cuenta en la nube, a través de la línea de celular asociada a dicha cuenta, con la finalidad de acceder a la evidencia digital que allí hubiera.

ii. Requerimientos: para intentar recuperar las credenciales de acceso a una cuenta en la nube, es necesario conocer el número de línea a la cual está asociada la cuenta. Además es importante contar con el nombre de usuario, o en su defecto, con los datos de la persona que usa la cuenta (Nombre, Apellido, DNI, etc.) El éxito de este procedimiento dependerá de varios factores, entre ellos: que la cuenta tenga configurado como medio de recuperación SMS/Llamada a la línea asociada, se conozca el nombre de usuario de la cuenta o que los nombres/apellidos configurados coincidan con los aportados por el requirente, etc.

iii. Procedimiento:

iii.a. El Fiscal/Defensor requirente deberá enviar mediante correo electrónico la solicitud de turno para “Recuperar credenciales de acceso (usuario/contraseña) a una cuenta en la nube” a la OITEL (oitel@jusrionegro.gov.ar) indicando detallada y concretamente la información que tiene de la cuenta: nro de línea, Nro. de SIM CARD, plataforma de la cuenta (Google, Facebook, Instagram, etc.), nombre de usuario, Nombre, Apellido y DNI de la persona que utiliza dicho usuario, etc.

iii.b. La OITEL comunicará mediante correo electrónico el día y hora fijados para la realización del procedimiento para que, en el caso que corresponda, el Fiscal/Defensor requirente pueda notificar a la contraparte del turno asignado, por si ésta desea presenciar y controlar el procedimiento.

iii.c. Previo al día asignado, la OITEL deberá contar en sus oficinas con una SIM CARD donde esté operativa la línea asociada a la cuenta que se desea recuperar.

iii.d. El día asignado para el procedimiento, desde la OITEL realizará una videoconferencia con el organismo solicitante, la que será grabada para contar con el registro audiovisual de las actividades realizadas. Luego, un profesional de la OITEL colocará la SIM CARD remitida en un celular acondicionado para esta tarea (celular vacío, restaurado con datos de fábrica) y realizará el proceso de recuperación de contraseña de la cuenta de interés que deberá culminar con el envío de un SMS con la nueva contraseña temporal (siempre y cuando se dan los supuestos mencionado en el inciso d) punto ii).

iii.e. Si el proceso de recupero es exitoso, el profesional de la OITEL procederá a establecer una nueva contraseña permanente para ser utilizada a posterior según lo requiera el organismo requirente (Ej. solicitar un Resguardo Remoto de Evidencia Digital).

iii.d. Una vez culminado el procedimiento, desde la OITEL se confeccionará un Informe Técnico en el que se detallarán todos los pasos realizados, adjuntando como ANEXO el video completo del procedimiento. Para garantizar la integridad del ANEXO, se generará valor HASH del mismo dejando constancia de este en el informe. En

todos los casos y sin excepción los Informes Técnicos deberán ser firmados digitalmente por los profesionales de la OITEL que intervinieron en el procedimiento.

CRESPO
Jorge Oscar

Firmado
digitalmente por
CRESPO Jorge Oscar
Fecha: 2022.11.30
09:55:15 -03'00'