Circular de Secretaría de la Corte N° 053 - 2024

Fecha del documento: 13 de Marzo del 2024
Fecha de Publicación: 04 de Abril del 2024

Documentos citados: Actas - Publicaciones

Publicada en SECRETARÍA GENERAL DE LA CORTE N°053 del 13 de marzo del 2024

CIRCULAR No. 53-2024.

Asunto: “Reglas Prácticas para la Adquisición Forense de Evidencia Digital”.

A TODOS LOS SERVIDORES, SERVIDORAS, DESPACHOS JUDICIALES DEL PAÍS,
INSTITUCIONES, ABOGADOS, ABOGADAS Y PÚBLICO EN GENERAL.

SE LES HACE SABER QUE:

La Corte Plena en sesión 08-2024 celebrada el 26 de febrero de 2024, artículo XXXI, aprobó las siguientes “Reglas Prácticas para la Adquisición Forense de Evidencia Digital”:

“REGLAS PRÁCTICAS PARA LA ADQUISICIÓN FORENSE DE EVIDENCIA DIGITAL

1.0 Objetivos:
El presente documento tiene como objetivo brindar una guía práctica en donde se establezcan los criterios y las reglas básicas a seguir por parte de los operadores del sistema de administración de justicia en materia penal y penal juvenil, ante las gestiones incoadas o sometidas a su conocimiento y que procuren la obtención de evidencia de índole digital. La diligencia de adquisición forense de la evidencia digital, podrá ser, en virtud de su tecnicismo, delegada en la oficina competente del Organismo de Investigación Judicial, lo anterior al amparo de lo estatuido en la ley.

2.0 Alcance:

El siguiente documento servirá de guía para todos los casos en los cuales el Ministerio Público ha gestionado una solicitud para la adquisición forense de evidencia digital contenida en dispositivos electrónicos.
Para tales fines, el personal técnico-pericial encargado de practicar la diligencia, utilizará los equipos (herramientas forenses de software y hardware), propiedad del Poder Judicial.

3.0 Normativa:

• Constitución Política de Costa Rica, art 24.
• Ley 7425, Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de
las Comunicaciones, art 2, 3, 4, 5, 6, 7, 26 y 27.
• Código Procesal Penal.

4.0 Responsabilidades:

a) Será responsabilidad del Ministerio Público establecer el mecanismo administrativo oportuno que complemente lo dispuesto en el presente instrumento. Asimismo, deberá velar porque las solicitudes presentadas ante el órgano jurisdiccional estén ajustadas a lo aquí dispuesto.

b) Es responsabilidad del Organismo de Investigación Judicial velar porque el personal técnico que ejecute la adquisición forense de la evidencia digital, realice sus acciones de conformidad con lo aquí dispuesto y según lo autorizado por el órgano jurisdiccional.

c) Es responsabilidad de cada persona juzgadora valorar la aplicación de las presentes reglas al resolver cualquier gestión planteada por el Ministerio Público y que verse sobre la adquisición forense de evidencia digital. Para tal fin, y en virtud del carácter técnico-pericial que caracteriza la adquisición forense de la evidencia digital, la autoridad jurisdiccional ponderará la conveniencia de delegar el acto en el Organismo de Investigación Judicial; lo anterior de conformidad con lo estatuido en la ley.

d) Es responsabilidad del Departamento de Prensa y Comunicación del Poder Judicial, crear las estrategias informativas de comunicación, así como futuras campañas de divulgación a nivel nacional, con el fin de que informe sobre la implementación de estas reglas prácticas.

e) La Comisión de la Jurisdicción Penal será la encargada de evacuar las dudas o consultas que pudiesen surgir a partir de la implementación de las presentes reglas.

Lo anterior, con el fin de que emita las recomendaciones que faciliten su mejora continua.

f) Será responsabilidad de la Escuela Judicial, así como de las Unidades de Capacitación
respectivas, gestionar la capacitación para todo el personal judicial de la materia penal, bajo la línea de las presentes reglas prácticas sobre aspectos relacionados con evidencia digital y ciberdelito.

5.0 Definiciones:

° Extracción forense o adquisición: Consiste en la recopilación segura de información digital relevante proveniente de un sistema informático o dispositivo electrónico.

° UFED (Universal Forensic Extraction Device): El UFED es un sistema operativo (software) y de herramientas (hardware) de la empresa Cellebrite empleado para la extracción de datos de dispositivos electrónicos por parte de las fuerzas del orden.

° IMEI (International Mobile System Equipment Identity): Alude a un código de quince dígitos pregrabado por el fabricante y que tiene como fin la identificación única e irrepetible de cada equipo o dispositivo móvil a nivel mundial.

° SIM (Subscriber Identify Module): Corresponde a una tarjeta que contiene un pequeño chip integrado para ser insertado en teléfonos móviles u otros dispositivos que permitan la transmisión de datos.

° HASH: Algoritmo matemático que, a partir de un archivo, genera un valor único e irrepetible que permite preservar su integridad e identidad.

6.0 Ventajas y seguridad del procedimiento:

• La diligencia tendiente a la adquisición forense de evidencia digital no dista de otras diligencias periciales y debe ejecutarse a partir de un fiel cumplimiento de estrictos controles que permiten determinar la integridad tanto de la información obtenida, como del acto realizado, todo ello sumado a los controles ya establecidos de cadena custodia en cuanto al manejo de los contenedores físicos de la evidencia digital.

• Mayor aprovechamiento del tiempo laboral de jueces, juezas, fiscalas, fiscales, defensoras y defensores, así como del personal de apoyo.

• Reducción de gastos administrativos en la Sección Especializada Contra el Cibercrimen del
Organismo de Investigación Judicial (SEC2).

• Aumento de la cantidad dispositivos procesados, por ende, mayor celeridad en la obtención de prueba para la resolución expedita de procesos penales.

• Mejor aprovechamiento del tiempo por parte del personal de la Sección Especializada Contra el Cibercrimen del Organismo de Investigación Judicial, lo que permite mayor asignación y atención de solicitudes.

• Se minimiza el riesgo de pérdida, robo o daño de los equipos forenses, puesto que los mismos no deben de ser trasladados y las diligencias se realizan en un ambiente controlado.

7.0 Solicitud del Ministerio Público:

a) El Ministerio Público requerirá ante el órgano jurisdiccional competente que ordene la
adquisición forense de la evidencia digital, para tales efectos en su solicitud indicará de manera clara los hechos que sustentan la investigación penal que es dirigida por su parte, la calificación legal provisional de los hechos, los elementos de prueba que serán procesados, o bien, los que posiblemente se obtendrán, así como la fundamentación jurídica y técnica de tal petición. El fiscal o fiscala a cargo de la investigación preparatoria solicitará a la autoridad jurisdiccional que, dado el carácter técnico-pericial de la adquisición forense de la evidencia digital, el acto sea delegado en la sección especializada del Organismo de Investigación Judicial; lo anterior de conformidad con lo estatuido en la ley.

7.1 Resolución:

La resolución de la persona juzgadora cumplirá con los requisitos procesales mínimos establecidos en la normativa correspondiente, tomando en consideración razones fundadas de hecho y de derecho. En caso de acceder a la petición fiscal, y dado el carácter técnico-pericial de la materia, la autoridad jurisdiccional ponderará la conveniencia de delegar la diligencia en la sección competente del Organismo de Investigación Judicial. Lo anterior, de conformidad con la facultad concedida por la Ley.

7.2 Diligencia técnica:

7.2.1 Proceso en dispositivo móviles:

Durante el proceso forense para extracción de evidencia digital contenida en dispositivos móviles (teléfonos, tabletas, entre otros), se utilizarán herramientas forenses especializadas. La herramienta utilizada actualmente se denomina UFED (Dispositivo Universal de Extracción Forense), la cual es producida por la empresa Cellebrite, pero se podrían utilizar otras según la necesidad.

Una vez que los indicios son puestos a disposición de la SEC2, se realizarán los siguientes pasos:

a. Se describirá el indicio, incluyendo el embalaje y la Boleta Única de Cadena de Custodia de Indicio (F-712).

b. Se hará apertura del embalaje por un costado y se describirá detalladamente su contenido, consignado marca, modelo, número de serie, serie electrónica (IMEI), color y estado del dispositivo, entre otros. Todos estos datos serán consignados en el acta de la diligencia y en el reporte técnico interno utilizado por la Sección.

c. A cada artículo se le asignará un identificador de nomenclatura, con el fin de identificarlo
durante toda la apertura.

d. Se verificará que el dispositivo se encuentre con carga en su batería, de no ser así se
procederá a cargar el mismo.

e. Si el dispositivo móvil logra ser encendido, se iniciará el proceso de extracción forense, el cual podrá ser realizado bajo las siguientes formas:

a. En primera instancia se conectará el dispositivo al UFED mediante los cables correspondientes y se intentará realizar la extracción de la información.

b. En caso positivo, la herramienta llevará a cabo de forma automática la adquisición de la
información sin la intervención del especialista de la Sección, quien solamente monitorea que el proceso culmine correctamente. De igual forma se procederá con relación a la tarjeta SIM y la memoria externa del dispositivo. Este proceso podría durar varias horas o inclusive días, situación que dependerá del modelo del dispositivo a procesar, tamaño de la memoria de almacenamiento y otros
factores técnicos.

c. Cuando no se logra tener acceso al dispositivo por razones técnicas (fallo o daño, factor de seguridad configurado), se descarta el realizar el procedimiento.

d. Una vez finalizada la adquisición del dispositivo, se procederá a generar un reporte con la
información extraída.

d. Se otorgarán los valores Hash correspondientes al reporte generado y quedará consignado en el acta de la diligencia.

e. Los indicios procesados serán nuevamente embalados debidamente y quedarán en poder del representante del Ministerio Público.

f. Todos los procesos anteriores, quedarán consignados en el acta de la diligencia.

h. En caso de que el dispositivo se encuentre en buen estado de funcionamiento y con capacidad de funcionamiento, no pueda ser procesado por la herramienta forense, en el tanto la autoridad jurisdiccional lo haya autorizado previamente, podrá respaldarse el contenido de la información mediante una grabación en vídeo.

g. El reporte o la información obtenida mediante el proceso de grabación será almacenada en un dispositivo USB u otro medio de almacenamiento, el cual quedará debidamente embalado, lacrado y con su respectiva Boleta Única de Control de Indicios (F-712). Se generará una copia en otro dispositivo USB u otro medio de almacenamiento sin embalar, que se utilizará como copia de trabajo para el Ministerio Público, y podrá ser facilitada a la defensa técnica y al cuerpo policial autorizado.

i.

7.2.2 Proceso en dispositivos de almacenamiento:

Durante este proceso se utilizarán medios tecnológicos, tanto de hardware, como de software para realizar la adquisición forense de evidencia digital contenida en dispositivos de almacenamiento. Este proceso realizará una copia íntegra del dispositivo.

Una vez que los indicios son puestos a disposición de la SEC2, se le realizarán los siguientes pasos:

a. Se describirá el indicio, incluyendo el embalaje y la Boleta Única de Cadena de Custodia de Indicio (F-712).

b. Se hará apertura del embalaje por un costado y se describirá detalladamente su contenido, consignando marca, modelo, número de serie, color, estado del mismo, entre otros. Todos estos datos serán consignados en el acta de la diligencia y en el reporte técnico interno utilizado por la Sección.

En caso de que sea una computadora, si es posible se procederá a extraer el o los disco(s) duros y se describirá la marca, número de serie y capacidad de almacenamiento.

a. A cada artículo se le asignará un identificador de acuerdo a una nomenclatura, con el fin de identificarlo durante toda la apertura.

b. Se procederá con el proceso de extracción forense utilizando las herramientas de hardware y software necesarias. Las herramientas llevarán a cabo de forma automática la adquisición de la información sin la intervención del especialista de la Sección, quien solamente monitoreará que el proceso culmine correctamente.

c. Una vez finalizado el proceso de adquisición forense, se registrará en el acta de la diligencia los valores hash generados por la herramienta utilizada.

f. El respaldo forense quedará conservado en un medio de almacenamiento, usualmente un
disco duro, el cual quedará debidamente embalado, lacrado y con su respectiva Boleta Única de Control de Indicios (F-712), cuyo análisis corresponderá, por cuestiones técnicas, a la SEC2.

g. Los indicios procesados se volverán a embalar debidamente y quedarán en poder del
representante del Ministerio Público.

f. Todos los procesos anteriores, quedarán consignados en el acta de la diligencia".

Publíquese una sola vez en el Boletín Judicial.

San José, 13 de marzo de 2024.

Licda. Silvia Navarro Romanini.
Secretaria General
Corte Suprema de Justicia

Refs: (422-2024 / 1226-2024)