

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

**NOTA DE ORIENTACIÓN N° 2: ANÁLISIS DE LA OBTENCIÓN DE
EVIDENCIA DIGITAL CONTENIDA EN DISPOSITIVOS ELECTRÓNICOS**

La presente nota tiene como finalidad brindar orientación en cuanto al procedimiento legal y alcances procesales, que posee la práctica judicial de investigación, para la obtención de evidencia digital que se encuentra contenida en dispositivos electrónicos, lo cual en muchas ocasiones es utilizada como prueba en diferentes procesos penales, sin importar el tipo de delito investigado. Tal posición emana de lo dispuesto en la resolución 04-2023 de la Fiscalía General de la República, mediante la cual la rectoría en evidencia digital le corresponde a la Unidad de Cibercrimen del Ministerio Público, así mismo mediante este criterio, se pretender generar unificación de posiciones entre los diferentes miembros del ente fiscal, de conformidad a lo dispuesto en el artículo 1 de la Ley Orgánica del Ministerio Público, a saber el principio de unidad de actuación.

JURISPRUDENCIA:

Voto 2022-01076 de las once horas cincuenta y tres minutos del catorce de octubre de dos mil veintidós de la Sala de Casación Penal, en tanto indicó:

“En cuanto al primero, es necesario tener a la vista que la queja del defensor público proviene de que, a su parecer, la

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

apertura de un aparato celular y la copia o respaldo a espejo de la información allí almacenada, es un acto definitivo e irreproducible. En tanto es así, según el artículo 293 del Código Procesal Penal, debió haber sido efectuado por un juez. Asimismo, señala que, de consuno con el numeral 294 de ese mismo código, por no saberse en ese momento la identidad de los posibles endilgados en la causa, debió haberse convocado a un defensor público, para que presenciara la regularidad de

dicho acto. Este es un alegato equivocado. La apertura de un dispositivo electrónico y el respaldo o copia a espejo de la información que contiene, no es un acto definitivo e irreproducible. Una vez que se procede a la apertura del dispositivo, lo que se hace es copiar la información que aquél contiene, para respaldarla, pero ello no hace que sea una diligencia que se pueda realizar una única vez (no es definitiva) ni que implique la modificación del contenido probatorio original, sino que ese contenido se puede volver a obtener las veces que sea necesario (es reproducible). La información original quedará contenida en ese dispositivo, pudiendo las partes solicitar la repetición del acto, si es que hay motivos para inferir alguna irregularidad en la maniobra. En este asunto, no existían motivos para que así se estimara; ni mucho menos para presumir que en la misma se hubiera alterado la calidad de la prueba obtenida o su calidad convincente.

Haciéndose eco de lo que al respecto se

había señalado en la sentencia de juicio, de folio 1258 en

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

adelante, el fallo de apelación explicó puntualmente las razones de por qué una diligencia probatoria como esa no es un acto definitivo e irreproducible. "... ' debe indicarse, que la apertura y extracción de la información contenida en el aparato celular, no ostenta la naturaleza de un acto definitivo e irreproducible, a contrario sensu a lo referido por el señor defensor Gutiérrez Carro, pues es definitivo el acto que se pueda incorporar al debate sin necesidad de repetirlo e irreproducible el acto que no puede ser llevado a cabo en idénticas condiciones en diferentes oportunidades, lo cual no es el supuesto del acto de apertura y extracción de la información contenida en el teléfono marca SAMSUNG, lo cual se verifica cuando en fecha posterior era factible replicar la audiencia de apertura, pues nuevamente podía extraerse del teléfono celular secuestrado el contenido de los datos o información almacenada en el mismo, e inclusive pese a que no fue requerido por las partes, podía reproducirse en debate.

En el caso de secuestro de teléfonos móviles la evidencia física es el teléfono y la evidencia digital es la información allí contenida que debe extraerse para peritarse. En la práctica, por lo general, se extrae la totalidad de la información allí almacenada y se preserva en un dispositivo portátil de almacenamiento de datos (p. ej., discos rígidos extraíbles, discos de memoria USB). La obtención de la prueba electrónica se realiza mediante la utilización de herramientas forenses adecuadas que preservan la autenticidad y la integridad de la prueba almacenada en un

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

dispositivo electrónico. En el caso que se comenta, se utilizó el programa UFED para realizar el clonado de la información digital almacenada en el teléfono celular secuestrado. UFED es una herramienta informática para la extracción segura de información almacenada en dispositivos móviles o teléfonos celulares y no solamente un software. Sencillamente explicado, se trata de una herramienta forense que se coloca entre el puerto del dispositivo secuestrado y el puerto del ordenador que, a través de un software, se encargará de extraer la prueba sin alterarla y permitirá almacenarla en el soporte en el que se copiará. A través de ese tipo de herramientas forenses se realiza el clonado de la prueba. Clonar un dispositivo electrónico implica efectuar una imagen en espejo o “mirror image”, es decir, realizar una copia que duplica la información bit a bit. El clonado es, entonces, la reproducción o copia de la totalidad de la información original almacenada en el dispositivo electrónico. Tal clonación o “mirror image” del dispositivo electrónico puede ser reproducida en caso de así requerirse en infinidad de ocasiones.’ [...] Cabe agregar, que el recurrente no acredita que en la especie el dispositivo electrónico Universal Forensic Extraction Device (UFED), haya tenido algún problema para desbloquear el teléfono celular antes descrito, o que las condiciones de seguridad del mismo hayan influido en la clonación de la información que se encuentra en el mismo, o que ello implique que tal ejercicio informático no se pueda repetir en la mismas condiciones originales, lo que revela el

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

tinte especulativo e improcedencia de su argumentación, en cuanto a que en el sub judice se está en presencia de un acto irreproducible. Al respecto, debe tenerse presente que el abogado defensor pudo gestionar a lo largo de todo este proceso, prueba tendiente a acreditar que la apertura del teléfono celular no se podía reproducir en idénticas circunstancias a las originarias.

Lo anterior, hubiese permitido contar con elementos de convicción objetivos para establecer que en el presente caso el argumento que se dilucida es valedero y esencial, en cuanto a la aplicación de los artículos 293 y 294 del Código Procesal Penal. Por ejemplo, ofreciendo el testimonio de los agentes de la Sección de Delitos Informáticos del Organismo de Investigación Judicial que realizaron la extracción de la información de marras y el manejo de la evidencia recolectada hasta que se incorporó al sumario de investigación, para que explicaran bajo qué condiciones se dio todo ello, así como para acreditar, según su reclamo, que no es posible llevar a cabo la apertura de la evidencia de marras, en situaciones idénticas a la que se hizo en un primer momento de la pesquisa. Al respecto, se considera que la defensa técnica no tuvo limitaciones infranqueables para sustentar el reparo, con base en el que pretende la nulidad del acto procesal que se analiza y de la prueba que del mismo se derivó, lo cual revela la superficialidad e insubsistencia de su alegato.” En resumen, no se está ante un acto definitivo o irreproducible, toda vez que la copia de la información que aparecía en el dispositivo electrónico en

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

mención podía hacerse en un sinnúmero de ocasiones, sin que ello la afectara, alterándola o haciéndola venir a menos. Por otra parte, si es que, como se indica en el fallo de apelación, el recurrente estimaba que ello no era posible, porque esa información desapareciera o se alterara, lo cual entonces hacía que el acto fuera definitivo o irreproducible, debió haberlo fundamentado. Pero eso no lo hizo en apelación ni lo hace ahora en casación. El defensor cuestiona la conclusión refrendada por el tribunal de alzada, pero no entra a cuestionar o a analizar las razones que éste proporcionó. Es decir, se trata de una inconformidad con lo que se le resuelve y con las consecuencias generales que dice que podrían derivar de una decisión como esa, mas no entra a concretar por qué esas razones de los jueces están equivocadas o son ilegales. Nótese que no solo se omite fundamentar ese aspecto central, sino que tampoco se explica en qué sentido la información recuperada pudo haberse visto afectada. Eso nos lleva al segundo gran argumento, relativo a que no logra demostrarse una lesión procesal concreta a los intereses de la defensa. O sea, no se demuestra un agravio. Como se dijo antes, el defensor muestra sanas preocupaciones teóricas y prelegislativas sobre el alcance o repercusiones forenses que pueda tener una conclusión como la que critica. Sin embargo, no intenta siquiera argüir un menoscabo para la estrategia de defensa ni para el ejercicio de la misma. De manera que, aunque en el plano de política prelegislativa, el tema que cuestiona el

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

petente puede ser un tópico de mucha relevancia, en lo tocante al procedimiento penal que efectivamente rige la Administración de Justicia, no se logra demostrar una irregularidad ni que se perjudicara la defensa desplegada por el quejoso....” *La negrita, subrayado y marcado no corresponden al original.*

**ANÁLISIS DEL TEMA DE LA EXTRACCIÓN DE
EVIDENCIA DIGITAL (APERTURA DE EVIDENCIA)**

Actualmente el uso de tecnologías de la información y la comunicación (TIC's) es una realidad innegable en la mayoría de sociedades, siendo que nuestro país no escapa a dicha situación, toda vez que el fin de éstas es facilitar el diario vivir y muchas de nuestras tareas ordinarias, laborales, educativas y de ocio, de igual manera ello ocurre con los delincuentes, quienes valoran dichas tecnologías como una plataforma criminal para facilitar la comisión en todo o en parte de sus actividades ilícitas. Ejemplo claro de ello es el uso de la tecnología telefónica, en donde al igual que el resto de la sociedad, los delincuentes utilizan aparatos telefónicos o computadoras para comunicarse entre sí, ya sea mediante llamadas telefónicas habituales, mensajería de texto SMS o en su mayoría mediante aplicaciones tecnológicas para la comunicación como lo son WhatsApp, Telegram, Messenger, etc, así como con el fin de almacenar información relacionada a actividades criminales, en dispositivos de almacenamiento digital como lo son USB o discos duros, lo que denota suma importancia para las

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

diversas investigaciones que realiza el Ministerio Público, puesto que el hecho de lograr obtener dicha prueba resulta de sumo interés para poder acreditar situaciones tan relevantes tales como actos preparativos, la misma comisión del hecho o bien actos de agotamiento. De ahí entonces la relevancia de poder acceder a dichos aparatos electrónicos, **los cuales en todo caso se tratan de meros contenedores de información, siendo precisamente la quid del asunto la información ahí contenida, la cual se trata claramente de evidencia digital.**

Es de alta relevancia el destacar el hecho de que el procurar obtener evidencia electrónica es una tarea que ocupa a las diferentes oficinas de la Fiscalía a lo largo y ancho del territorio nacional, sin importar condiciones como especialidad, provincia o tamaño del despacho, de ahí pues lo necesario de contar con un documento como el que aquí se expone, con el fin de dar claridad y uniformidad en cuanto al proceso técnico-forense de adquisición de evidencia digital para los procesos penales.

En nuestro país debe de aclararse como más adelante se demostrará que no existe ninguna norma taxativa que describa de manera puntual el concepto evidencia digital y cuál además es el procedimiento para su obtención, manejo y custodia, por lo que se realizan una equiparación a la información privada de índole documental.

Tal circunstancia propia de un vacío normativo, ha ocasionado una serie de prácticas judiciales infundadas, que al final de cuentas inciden negativamente en la tarea de ejercitar la acción penal que le ha sido encomendada por parte del

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

legislador al Ministerio Público.

NORMATIVA NACIONAL:

En nuestro país como se ha indicado, no existe formalmente norma alguna que regule el concepto claro y expreso del significado y alcances de la evidencia digital en el marco penal, de igual forma Costa Rica no presenta un procedimiento fundado en cuerpo legal alguno, que establezca de manera técnica el rito adecuado tanto para el manejo de la evidencia digital y su posterior obtención.

Debido a esto sin tener conocimiento de cuál fue el momento o motivo que originó la práctica que hoy en día se sigue de manera consuetudinaria en las diferentes jurisdicciones, se estableció una máxima en la cual el ente fiscal requerirá antes el órgano jurisdiccional de etapa preparatoria la autorización para acceder a la información contenida en dispositivos electrónicos, bajo la perspectiva de que tal diligencia violenta el derecho a la intimidad, cuestión que se comparte, no obstante la problemática radica en el hecho de que los jueces, quizás por desconocimiento, realizan valoraciones sin brindar una justificación fundada que motive tal apreciación, el hecho de que la diligencia técnica que ejerce el personal informático de la Sección Especializada Contra el Cibercrimen, se trata de una prueba única e irreproducible, motivo por el cual imponen que el acto pericial se realice en presencia de las partes, de nuevo sin realizar una fundamentación clara del motivo de tal decisión.

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

Reflejo de esta realidad lo es el estudio realizado por el programa internacional EL PAcCTO, el cual se denomina: "La prueba electrónica en el marco nacional y en el internacional en latinoamérica" (<https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf>) en donde al analizar la existencia de normativa doméstica en nuestro país, se establece que el manejo de evidencia digital y su equiparación se realiza hacia lo regulado en la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, norma la cual data del año 1994, la cual además al día de hoy a casi 30 años después no ha sufrido modificación o actualización alguna, aunado a ello se hace ver en dicho estudio que pese al hecho de que nuestro país tuvo como avance el hecho de suscribir el Convenio de Budapest o Convenio Sobre la Ciberdelincuencia, la cual fue promulgada como Ley de la República bajo el número 9452, se hace ver que bajo el programa Glacy+ del Consejo de Europa, se elaboró un Proyecto de Ley que incluía recomendaciones técnicas jurídicas en pro de la aplicación y armonización de la ley nativa con la de dicho marco internacional y la misma no fue tramitada (<http://www.aselex.cr/boletines/Proyecto-21187.pdf>).

Debe de indicarse además que tal y como se evidencia en el estudio señalado, y que además ha podido así ser verificado debido a capacitaciones internacionales, nuestro país es el único de la región que no solo posee muy poca legislación específica, sino además el que pese a la inexistencia de legislación concreta, labora con un modelo de trabajo de extracción de evidencia digital mediante audiencia con convocatoria a las partes, en la gran mayoría de países

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

no solo de América sino del mundo, tal diligencia se ejecuta en laboratorios forenses de los cuerpos de policía, en donde la extracción de evidencia o "volcado" no se ejecuta en presencia de las partes.

Así las cosas la norma existente y que se entiende relacionada a la obtención de la evidencia digital es la siguiente:

24 Constitución Política (Derecho a la Intimidad)

ARTÍCULO 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.

Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.

Ley 7425 Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones.

ARTÍCULO 2.- Atribuciones del Juez.

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

Cuando resulte indispensable para averiguar la verdad, el Juez podrá ordenar, de oficio, a petición de la autoridad policial a cargo de la investigación, del Ministerio Público o de alguna de las partes del proceso, el registro, el secuestro y el examen de cualquier documento privado, siempre que pueda servir como prueba indispensable de la comisión de alguna conducta delictiva. El Juez realizará personalmente la diligencia, salvo en casos de excepción, en los que, según su criterio, pueda ser delegada en miembros del Organismo de Investigación Judicial o del Ministerio Público, quienes deberán informarle sobre el resultado de la diligencia.

ARTÍCULO 3.- Requisitos de la orden de secuestro, registro o examen.

La orden de secuestro, registro o examen deberá efectuarse, so pena de nulidad, mediante auto fundado en el que se individualicen, de ser posible, los documentos sobre los que se ejecutará la medida de registro, secuestro o examen, el nombre de la persona que los tenga en su poder y el lugar donde se encuentran.

De ser secuestrados otros documentos que no se incluyan en la orden, deberán restituirse inmediatamente a quien se le secuestraron, salvo que el Juez los estime trascendentales para esa u otra investigación; si así fuera, el Juez deberá ampliar la orden para incluirlos y justificar el motivo por el cual se incluyeron.

ARTÍCULO 4.- Derechos del intervenido.

Al ejecutar el registro, el secuestro o el examen, el Juez o el funcionario designado notificará y entregará copia de la orden judicial que lo autoriza, a quien le sean registrados, secuestrados o examinados los documentos. De esto se levantará un acta de la cual también se le entregará una copia, al finalizar la

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

diligencia.

El interesado, dentro de los tres días posteriores a la ejecución de la medida, podrá solicitar su reconsideración y que se le restituyan los documentos secuestrados. La resolución de la anterior solicitud se sustanciará dando audiencia, por tres días a las partes. Contra lo resuelto por el Juez cabrá recurso de apelación.

ARTÍCULO 5.- Inventario, custodia y reproducción de documentos.

Se efectuará un inventario de los documentos secuestrados y se mantendrán en segura custodia, a disposición del Tribunal, el cual entregará al interesado un recibo detallado de los documentos que permanezcan en su poder.

Únicamente en casos de sentencia condenatoria, en los que sea aplicable el comiso, los documentos secuestrados quedarán en poder del Juez.

Cuando los documentos secuestrados corran riesgo de desaparecer, alterarse, sean de difícil custodia o así convenga al proceso, podrá disponerse la obtención de copias o reproducciones de ellos. Los documentos deben asegurarse con el sello del Tribunal, con la firma del Juez y la del Secretario; además, las copias deberán firmarse en cada una de sus hojas. Igual procedimiento ha de seguirse si se entrega copia de los originales a quien le fueron secuestrados. Cuando su depósito le cause algún perjuicio al interesado, y sea posible a juicio del Juez, le serán devueltos los documentos originales. En ese caso, quedarán en custodia del Tribunal copias auténticas de ellos.

ARTÍCULO 7.- Condiciones para examen técnico de documentos.

Cuando los documentos secuestrados deban ser sometidos a exámenes técnicos

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

de cualquier tipo, la remisión deberá efectuarla la autoridad judicial y asegurarse de que, en el despacho, siempre permanezca agregada al expediente de la causa, una copia certificada de esos documentos.

ARTÍCULO 8.- Copia certificada para proteger documentos.

Cuando los documentos puedan alterarse por cualquier motivo o cuando, por su naturaleza o contenido, sean de difícil reposición en caso de extravío, se procederá en la forma estipulada en el artículo anterior.

ARTÍCULO 22.- Prohibiciones a los encargados de intervenir.

A los funcionarios y empleados participantes en la intervención de las comunicaciones, el registro, el secuestro o el examen de documentos o a quienes tengan la potestad de solicitar estas medidas, se les prohíbe lo siguiente:

- 1.- Utilizar los resultados de la intervención para propósitos distintos de los que la motivaron.
- 2.- Ayudar, directa o indirectamente, a alguien para que eluda las investigaciones de la autoridad o se sustraiga de su acción.
- 3.- Violar la confidencialidad y el secreto de todas las medidas e informaciones autorizadas en esta Ley, salvo para los efectos que originaron el acto.
- 4.- Inducir al Juez a disponer una intervención de comunicaciones, el registro, el secuestro o el examen de documentos privados, por medio de la simulación, la alteración, el ocultamiento, la suposición de hechos o documentos falsos o la deformación de los verdaderos.

ALCANCES DE LA NORMA UTILIZADA, LEY SOBRE REGISTRO,

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

**SECUESTRO Y EXAMEN DE DOCUMENTOS PRIVADOS E INTERVENCIÓN DE
LAS COMUNICACIONES:**

De inicio debe distinguirse que lo dispuesto en esta norma, aplica para cualquier situación en la cual como parte de las diligencias de investigación, se requiera el registro, secuestro y examen de un documento privado, no obstante, sin poder aún saber el origen, se ha realizado siempre una distinción respecto al respaldo de evidencia privada contenida en dispositivos electrónicos (evidencia digital) y evidencia física. En dicha norma en su artículo 2, el legislador estableció que será el juez el encargado de realizar la diligencia que contenga los verbos: registrar, secuestrar y examinar, con el fin de obtener prueba para un proceso de índole penal. No obstante permite una excepción para que en casos, en los que según **el criterio del juez**, en su condición de autoridad jurisdiccional, podrá determinar que la diligencia sea realizada por parte del Ministerio Público y/o la policía judicial, es decir delegar la práctica de lo dispuesto en la norma.

Esta posibilidad como se puede desprender de lo señalado por el artículo 2, **si bien es excepcional, otorga un peso fundamental al criterio del juez, es decir a sus consideraciones, del porque el registro, secuestro y examen pueden recaer en el ente fiscal o la policía.** Tal excepcionalidad, que además se acompaña de las consideraciones del juez, así como en relación a la naturaleza propia de la diligencia, la cual es totalmente técnica, con operación de equipos forenses de hardware y software se trata entonces de una condición de excepcionalidad por el tecnicismo.

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

Lo mismo ocurriría con el examen (análisis de la información obtenida), lo cual también de acuerdo a la norma indicada, su práctica puede ser delegada, por cuanto este examen también reviste tecnicismo, en uso de herramientas de búsqueda a la hora de revisar la evidencia digital respaldada, o por razón de la propia investigación, pensemos en el léxico criminal que utiliza la estructura, la búsqueda de elementos de investigación que solamente son del conocimiento de la policía, la identificación de otras personas que aún no figuraban en la investigación, etc.

Por otra parte en cuanto a la información del resultado, que debe de realizarse al juez que delegó la diligencia, la norma no es clara en cuanto al momento del informe del resultado, de tal suerte ello bien podría incluso ocurrir una vez que es finalizada la investigación, en donde de acuerdo al principio de objetividad, una vez analizado el caso y todo el elenco probatorio, bien podría solicitarse por el ente fiscal un sobreseimiento definitivo, el cual evidentemente debe de ir fundamentado y ahí se haría mención a los hallazgos de esta diligencia y su examen, o bien cuando se realiza una pieza acusatoria y esta prueba es ofrecida para el contradictorio, siendo que de igual forma en la eventual audiencia preliminar se le estaría informando el resultado de la diligencia en cuestión al juez.

Y tal y como ha quedado evidenciado de la jurisprudencia aportada, esta diligencia no se trata de una con condición de "única e irreproducible", por lo contrario en virtud de la forma en la que se desarrolla la misma, partiendo de criterios técnicos en cuanto al manejo de hardware y software adecuado por parte

Tel: 2295-3279 Fax: 2295-3858

Correo electrónico: ue_estafas@poder-judicial.go.cr

COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN

San José, Costa Rica

de la Sección Especializada Contra el Cibercrimen del Organismo de Investigación Judicial, se trata de una diligencia reproducible y constatable las veces que se requiera, en el tanto exista alguna duda o bien un alegato en contra. **Siendo así debe de velarse por el hecho de que los dispositivos electrónicos originales que fueron respaldados inicialmente, sean siempre custodiados y también ofrecidos al respectivo contradictorio.** Esto permitiría verificar el resultado del respaldo realizado en caso de cuestionamiento y comparar la información inicial en caso de requerirse.

**EN CUANTO A OTROS ACTOS PROCESALES, QUE BLINDAN EL
PROCEDIMIENTO DE APERTURA DE EVIDENCIA SE TIENEN:**

Durante el abordaje investigación de la fase preparatoria del proceso penal, existen múltiples actos, que blindan de manera absoluta la práctica propuesta en el documento en estudio, y que se acoplan en un todo a la misma, con el fin de proteger el debido proceso, algunas de ellas serían:

1.- Confección de acta, embalaje del dispositivo decomisado, asignación de boleta física de cadena de custodia, inclusión de esta información en el respectivo informe policial, la cual evidentemente debe de coincidir entre sí. Todas ellas permiten determinar la integridad del elemento de prueba física. Y por ende es posible reconstruir su primera ubicación, su identidad y su adecuada custodia.

2.- Solicitud a control jurisdiccional para la "adquisición forense de
Tel: 2295-3279 Fax: 2295-3858
Correo electrónico: ue_estafas@poder-judicial.go.cr

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

evidencia digital" y resolución de autorización judicial. En donde evidentemente lo gestionado y lo ordenado, debe de corresponder en un todo con el dispositivo o contenedor en cuestión, además de que se fundamentan las razones de facto y de derecho para proceder con tal diligencia.

3.- Diligencia de "generación de copia forense", en ella se seguirá manejando la cadena de custodia, se revisará el embalaje, y todo ello es consignado en un acta por quien realiza la diligencia. Posteriormente se explicará el procedimiento técnico a seguir, mediante el cual utilizando herramientas de hardware y software, se gestiona la adquisición y respaldo de la información digital. De ello se emitirá un reporte que otorga la herramienta forense, además de que al resultado obtenido se le aplicará función de hash, que como se ha señalado esta técnica matemática-informática de criptografía, permite brindar total certeza e identidad en cuanto a lo obtenido y que puede de hecho ser replicado y comparado en cualquier momento del proceso. Como se puede ver ahí se suman al menos otras 4 posibilidades adicionales para la reconstrucción de la diligencia.

4.- Una vez concluida se generará un respaldo original y uno de trabajo. Siendo que a éstos bien puede tener acceso cualquiera de las partes, y por ende se termina de blindar la diligencia en cuanto a su posibilidad de reconstrucción.

**COSTA RICA
PODER JUDICIAL - MINISTERIO PÚBLICO
UNIDAD DE CIBERCRIMEN**

San José, Costa Rica

**Esteban Aguilar Vargas
Fiscal Coordinador
Unidad de Cibercrimen**