

CIRCULAR ADMINISTRATIVA

DE CONFORMIDAD CON LOS ARTICULOS 1, 13, 14 Y 25 DE LA LEY ORGÁNICA DEL MINISTERIO PÚBLICO, SE PONEN EN CONOCIMIENTO DE LAS FISCALAS Y LOS FISCALES LAS SIGUIENTES INSTRUCCIONES DE LA FISCALA GENERAL DE LA REPÚBLICA, LAS CUALES DEBEN SER ACATADAS DE INMEDIATO, A EFECTO DE CREAR Y MANTENER LA UNIDAD DE ACCIÓN E INTERPRETACIÓN DE LAS LEYES EN EL MINISTERIO PÚBLICO.

DE CONFORMIDAD CON LA LEY DE CONTROL INTERNO Y LA CIRCULAR FGR N° 10-2006, ES RESPONSABILIDAD DE LAS FISCALAS ADJUNTAS Y LOS FISCALES ADJUNTOS QUE LAS MISMAS SEAN CONOCIDAS Y APLICADAS POR LAS FISCALAS Y LOS FISCALES ADSCRITOS A SU FISCALÍA.

**TEMAS: REITERACIÓN DE LA
CIRCULAR FG-19-2000**

**LEVANTAMIENTO DE SECRETO
BANCARIO.**

Se reitera la circular de la Fiscalía General 19-2000, con respecto a la obligación de las fiscalas y los fiscales de solicitar la autorización del órgano jurisdiccional para suministro de información cubierta por el secreto bancario. En nuestro país los alcances del secreto bancario encuentran su sustento en el artículo 24 de la Constitución Política y en el artículo 615 del Código de Comercio, el cual señala que las cuentas corrientes bancarias son inviolables y los bancos sólo podrán suministrar información sobre ellas a solicitud o con autorización escrita del dueño

o por orden de autoridad jurisdiccional competente. De ello deriva la obligación de los bancos de no revelar a terceros la información y los datos referentes a sus clientes que lleguen a su conocimiento como consecuencia de esa relación comercial, a menos que exista la autorización expresa del propietario de la cuenta o un Juez o Jueza que ordene el levantamiento del secreto bancario.

De conformidad con el artículo 62 del Código Procesal Penal (en adelante cpp), el Ministerio Público ejercerá la acción penal, practicará las diligencias útiles para la investigación, pero cuando los actos que se requieran vulneren garantías constitucionales, gestionarán bajo control jurisdiccional, ejemplo de esos actos, son la solicitud de allanamiento, la solicitud de intervención telefónica, la intervención corporal o la solicitud de información protegida por el secreto bancario. Por su parte el artículo 198 del cpp dispone que la jueza o el juez, el Ministerio Público y la policía ordenarán el secuestro de información importante para la causa penal, siempre y cuando esa información no afecte derechos fundamentales. Por su parte, el artículo 277

del cpp, señala que le corresponderá realizar al órgano jurisdiccional otorgar autorizaciones y controlar el cumplimiento de las garantías establecidas en la Constitución, de manera que el órgano fiscal no puede realizar actos jurisdiccionales.

La ley 7425 sobre Registro, Secuestro y Examen de documentos privados e intervenciones de las comunicaciones, en sus artículos 1 y 2, dispone que los tribunales de Justicia podrán autorizar el registro, el secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento, así como que el órgano jurisdiccional 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 para la investigación penal.

De acuerdo a lo anterior, la fiscalía o el fiscal que tenga a su cargo una causa penal en la cual se deba solicitar el levantamiento de secreto bancario ante el órgano jurisdiccional, debe verificar que se cumplan los siguientes requisitos básicos:

1. Consignar en la solicitud el número de cuenta origen (afectada) y la cuenta destino (beneficiada), número de cédula de las personas dueñas de la

cuenta bancaria, así como el Banco al que pertenece.

En caso que el órgano fiscal no cuente con los números de cuenta bancarios del punto 1, que permita conocer con posterioridad la información bancaria, debe solicitar a la juez o jueza de la localidad que, mediante orden judicial, ordene a todas las entidades bancarias a nivel nacional, remita la información indicada.

2. Con la información antes brindada, ampliar la gestión ante el órgano jurisdiccional, la solicitud de información a diversas entidades bancarias sobre:

- 2.1 Periodo: Un mes antes y un mes después de las transacciones cuestionadas para determinar los movimientos habituales de la cuenta bancaria en casos de Estafa Informática y en los otros casos el plazo va a depender del caso en investigación.

- 2.2 Si la cuenta destino tiene alguna persona autorizada, que faciliten la información personal de la misma y si realizó algún retiro del dinero que se cuestiona.

- 2.3 Histórico de movimientos de la cuenta o las cuentas afectadas. Información que debe detallar la

hora, fecha, detalle, monto, número de transacción y lugar.

2.4 Detalle de los movimientos y eventos registrados en la bitácora del servicio Web en Internet del número de identificación (código de la persona usuaria) de la persona ofendida, en el mismo periodo de interés. Esta información debe ser aportada en formato electrónico, PDF.

2.5 . Cuáles personas funcionarias del banco efectuaron consultas, reimpresión de tarjetas o el número de identificación personal (PIN, u otra acción en torno a las cuentas afectadas).

2.6 Así como a la identificación de la persona titular de dicha cuenta y las personas autorizadas. Para ellos debe indicar, a saber: código de la persona usuaria, número de identificación, nombre de la persona funcionaria, fecha, hora, dirección IP, nombre del sistema involucrado, descripción del evento, en el periodo de interés.

2.7 Indicar si la persona titular de la cuenta o las personas autorizadas, previo a las fechas de los hechos arriba consignadas, tenían activo algún mecanismo adicional de

validación de su número de identificación (código de la persona usuaria) en el servicio web en internet, a saber: tarjeta dinámica token, acceso a banca telefónica, entre otros. Ante lo cual, debe suministrarse el detalle de la asignación y activación del dispositivo, así como el número de identificación de éste, la oficina y el nombre de la persona funcionaria que realizó el trámite.

2.8 En casos de estafa informática es importante Indicar la dirección IP, utilizada en las transacciones denunciadas.

2.9 Suministrar comprobante SINPE.

2.10 Movimientos de retiros mediante cajeros (automáticos o humanos) o débitos por medio de compras con las tarjetas ligadas a las cuentas destino, posteriores a las acreditaciones de los fondos, debe aportarse el comprobante original e indicar donde fue hecha la transacción. De igual forma, debe aportarse la secuencia fotográfica y los videos de seguridad en donde se hizo cada uno de los retiros, en caso de que alguno de los documentos o videos no sean ubicados indicarlo así en el respectivo oficio de respuesta.

Para los retiros en efectivo, mediante cajero automático y cajeros humanos, debe especificarse la ubicación exacta de los mismos para efectos de delimitar el primer evento realizado y si son varios de igual forma realizar la ubicación exacta donde se ubica la entidad bancaria ya sea en cajas o bien en cajero automático.

2.11 Detalle de los movimientos y eventos registrados en las bitácoras del servicio Web en Internet de los números de identificación (código de usuario) de los titulares de las cuentas destino identificadas. En los rangos de fechas ya indicadas.

2.12 Indicar el detalle de todos los reportes realizados por las personas titulares de las cuentas destino, sobre robo o extravío de las tarjetas asociadas a la cuenta o a las cuentas destino, en el periodo dicho después del hecho denunciado, especificar la fecha y motivo del reporte, número de tarjeta, tipo de tarjeta. En el caso de no existir ningún reporte de igual forma indicar el número de tarjeta asociada a la cuenta destino.

2.13 De existir transferencias de

fondos de las cuentas destinatarias hacia otras cuentas, que se presume son parte o la totalidad del dinero proveniente de las cuentas afectadas; debe suministrarse la información detallada en los apartados anteriores de esa otra cuenta bancaria y suministrar la misma información que es solicitada en las cuentas que aquí ya se conocen.

2.14 Comprobantes bancarios del evento delictivo siempre y cuando no sea aportado por la persona víctima.

2.15 Se requiere que la entidad bancaria aporte la copia certificada del informe de la investigación administrativa, realizado en el Departamento de Seguridad. Además, indicar de manera clara si se determina que la persona que considera cuenta destino se presentó a la entidad bancaria a realizar algún trámite conforme a lo indicado en la denuncia.

2.16 Copia escaneada del expediente original de apertura de cada una de las cuentas de destino, de no contar con el expediente original, informar el por qué (ya sea por decomiso previo, extravío, destrucción, entre otros). Aportar

en formato PDF.

2.17 Si posee cajas de seguridad.

Finalmente es importante recordar que cualquier información de cuentas corrientes, cuentas de ahorros, depósitos a plazo, créditos, caja de seguridad, fondos de inversión, debe ser solicitada la información por medio de la solicitud de levantamiento de Secreto Bancario.

Es importante consignar en la solicitud de levantamiento de Secreto Bancario ante el órgano jurisdicción, que la información requerida a la entidad Bancaria se requiere a más tardar dos meses posteriores a la notificación realizada por parte del Organismo de Investigación Judicial.

Las presentes disposiciones rigen a partir de su comunicación.

EMILIA NAVAS APARICIO
FISCALA GENERAL DE LA REPÚBLICA
JUNIO, 2019
[ORIGINAL FIRMADO]