FISCALÍA GENERAL DE LA REPÚBLICA

MINISTERIO PÚBLICO DE COSTA RICA
PODER JUDICIAL

02-ADM-2021

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.

DISPOSICIONES GENERALES SOBRE EL ABORDAJE INICIAL EN CAUSAS POR ESTAFA INFORMATICA.

Abordaje inicial en las investigaciones por Estafas Informáticas.

Artículo 1. Introducción.

ESTAFAS INFORMÁTICAS

La estafa informática supone un fenómeno criminal de una naturaleza altamente dinámica, cuyos mecanismos de ejecución varían al ritmo de las nuevas tecnologías lo que requiere ser necesarias para una adecuación continua de las líneas de investigación por parte del Ministerio Público, por esta razón se establecen una serie de diligencias básicas a fin de proveer un rango de acción amplia en la dirección de las investigaciones de este delito, por lo que, se define a continuación aspectos relacionados al abordaje inicial de las causas según su categorización.

Artículo 2. Estafa Informática mediante la utilización de técnicas de ingeniería social.

Este supuesto de hecho incluye aquellos casos en que una persona integrante de un grupo delictivo contacta a la persona víctima y le hace creer que es una persona funcionaria de una entidad pública o privada, (Bancos, Ministerio de Hacienda, u otras) y

mediante engaño logra que ésta le facilite información referente a los dispositivos de seguridad necesarios para el acceso de sus cuentas bancarias.

Otra de las modalidades relacionadas, es cuando la persona víctima es guiada mediante engaño hasta un sitio web o plataforma informática, que simula ser un sitio oficial y que es controlado por una persona del grupo criminal, en el cual la persona victima ingresa sus claves o dispositivos de seguridad.

Una vez que se ha obtenido los datos sensibles de la persona víctima, proceden principalmente de la siguiente manera:

1. Trasladan el dinero de la persona víctima mediante transferencia electrónica hacia una o varias cuentas destinos, a cuyos titulares se les considera en primer momento como personas imputadas.

2. Utilizan el dinero de la cuenta bancaria de la persona víctima para cancelar recibos por servicios públicos locales, multas o impuestos, entre otros.

3. Trasladan el dinero de la persona víctima mediante transferencia electrónica a una cuenta puente y luego de forma inmediata, lo transfieren a otras cuentas destino o bien se cancelan diversos tipos de servicios.

Artículo 3. Abordaje inicial en la investigación relacionada a las técnicas de ingeniería social.

1. La denuncia se recibirá por parte del Organismo de Investigación Judicial, el cual procederá a realizar las diligencias de investigación necesarias para la verificación del hecho denunciado, incluida la solicitud de rastreo telefónico si fuese procedente y coordinará lo necesario para la conservación de elementos de prueba. Posteriormente, realizará el informe policial en el cual se incluye la especificación del hecho delictivo, la identificación de la o las personas imputadas, la existencia de elementos de prueba que requieran autorización jurisdiccional para su debida incorporación. Una vez recibido el informe policial en la fiscalía correspondiente, se deberá proceder como mínimo con las

siguientes diligencias de investigación:

1.1. Si la acción se subsume preliminarmente en el tipo penal de Estafa Informática, (artículo 217 bis, segundo párrafo) y el hecho concreto refiere que el dinero fue trasladado a una o varias cuentas destino, se deberá solicitar al órgano jurisdiccional de la etapa preparatoria autorización para el acceso a la información privada bancaria (Orden de Levantamiento de Secreto Bancario), respecto a las cuentas bancarias a las cuales se trasladó el dinero de la persona víctima; asimismo deberá citarse a cada persona imputada en la fiscalía para identificarlo desde el inicio de la investigación(Datos previos).

1.2. Una vez obtenida la información bancaria, las personas encargadas de la investigación en el Organismo de Investigación Judicial deberán realizar Dirección Funcional con la fiscalía de su circunscripción territorial, con el fin de analizar las circunstancias del caso y las condiciones particulares de las partes involucradas en el fenómeno criminal investigado, y será responsabilidad de la persona fiscal encargada o asignada para valorar la pertinencia o no de solicitar la ampliación del informe policial.

2. Cuando el Organismo de Investigación Judicial presente el informe con los resultados de la información bancaria obtenida mediante la autorización jurisdiccional, se deberá realizar la apertura de la evidencia. En caso de que resultar necesario certificar una copia, la misma será agregada al expediente principal y el original se mantendrá en la Bodega. La evidencia deberá custodiarse con clara indicación de la persona imputada a la que está relacionada, por lo que, deberá contar con un número de objeto independiente. En el caso de que, se identifique del informe policial la existencia de dinero retenido en la o las cuentas destino, con ocasión de las transferencias fraudulentas, se deberá dirigir de forma inmediata a la entidad bancaria

que corresponda una solicitud de reversión de fondos congelados hacia la cuenta bancaria de origen (cuenta bancaria de la persona víctima).

Artículo 4. Estafa Informática mediante materialización de compras en línea o pago de servicios a proveedores de servicio que operan en internet.

Está modalidad criminal se caracteriza porque la persona víctima no ha tenido una comunicación con las personas responsables del hecho delictivo, sino que, por algún medio, se han impuesto de los datos de la tarjeta o cuenta bancaria de las víctimas para incidir en el procesamiento de datos del sistema automatizado de la entidad bancaria, garantizando su acceso, para con ello, realizar compras de productos o servicios a empresas que operan en internet. Para tales casos, deberá realizar las siguientes diligencias:

Artículo 5. Abordaje inicial en causas relacionadas a la modalidad de pagos o compras a proveedores de servicio que operan en internet.

1. Determinarse la identidad del objeto de la transacción a fin de definir si obedece a un producto o un servicio.

2. Consultar al comercio por cualquier medio idóneo, los datos de la facturación de la transacción, los datos de registro del usuario, relacionados con la operación fraudulenta.

3. En aquellos casos en que se ha logrado determinar que el objeto de la transacción es un producto, deberá identificarse: el medio de entrega, persona que realizo la entrega del producto (mensajero) y lugar de entrega, como mínimo, entre otros.

4. Cuando el objeto de la transacción sea el pago o compra de un servicio, deberá consultarse al proveedor de servicios lo siguiente: datos de registro referidos al abonado, tales como: nombre, usuario, dirección IP, correo electrónico, número de teléfono, así como cualquier otro dato que permita identificar a la persona usuaria registrada para el servicio de interés.

Artículo 6. Sobre la Competencia.

Anteriormente la competencia administrativa, se determinaba por el lugar en donde la persona ofendida recibía la llamada telefónica (circular 18-

ADM-2019), por considerarse este evento como el primer acto preparatorio del fenómeno criminal, no obstante, el dinamismo de este fenómeno y su constante actualización en métodos ejecutivos ha obligado a generar una reestructuración en su abordaje, considerando que en la actualidad, los accesos a internet se realizan desde unidades móviles, las cuales se caracterizan por un desplazamiento continuo, lo cual amplía el espectro de las posibilidades del lugar del hecho en que se realizó la acción típica, por lo que, atendiendo a esta realidad, se deberán seguir las siguientes reglas de competencia, establecidas en el Código Procesal Penal artículo 47 inciso d) en relación con el 20 del Código Penal, con las siguientes determinaciones:

1. El primer aspecto para establecer la competencia será el lugar de la comisión del hecho punible. El hecho se considerará cometido:

a) En el lugar en que se desarrolló, en todo o en parte la actividad delictiva de autores o participes. Es decir, donde se perfeccionó uno de los elementos objetivos del tipo penal, sea el uso indebido de datos, la manipulación o la incidencia en un sistema automatizado de datos.

2. Si se desconoce el lugar del hecho punible, la competencia la tendrá la fiscalía más cercana al domicilio de la persona imputada. En los casos en los cuales en la investigación figure más de una persona imputada se deberá de analizar a cuál de ellas se le realizó la primera transferencia ilícita, por lo cual la competencia la tendrá la fiscalía más cercana al domicilio de dicha persona imputada.

3. Si se desconoce el lugar en que se desarrolló, en todo o en parte la actividad delictiva de autores o participes y se desconoce el domicilio de la persona imputada, la competencia la tendrá la fiscalía más cercana al lugar donde se dio la primera disposición patrimonial *(cajero automático, ventanilla de la entidad bancaria, comercio).*

4. Si se desconoce el lugar donde se ejecutó la primera disposición patrimonial, la competencia la tendrá el despacho más cercano al domicilio de la parte ofendida.

5. Si se desconoce el domicilio de la persona víctima, la competencia se determinará por la ubicación de la entidad bancaria donde la persona ofendida aperturó la cuenta bancaria afectada o donde se emitió la tarjeta, en caso de que sean varias las cuentas bancarias afectadas, deberá tomarse para efectos de competencia, la cuenta bancaria en la cual se realizó la primera acción delictiva.

6. En los casos en que, una Fiscalía ordenó el Archivo Fiscal de la causa, y posteriormente resultó necesario continuar con la investigación, la Fiscalía competente es quien emitió la resolución de Archivo Fiscal, y deberá continuar con la causa hasta la conclusión de la etapa preparatoria.

7. En el caso de la Fiscalía que asumió la investigación siguiendo las anteriores reglas de competencia, deberá continuar con la instrucción de la causa hasta concluir la fase preparatoria y en caso de no ser finalmente el competente, deberá dirigir el requerimiento conclusivo al órgano jurisdiccional que corresponda, con la indicación de que, será la fiscalía de dicho lugar, quien deberá asumir las etapas posteriores del proceso.

Artículo 7. Acumulación de causas.

La Fiscala o el Fiscal debe solicitar al Organismo de Investigación Judicial, que indique en el informe policial si la o las personas imputadas cuenta con otras causas por delitos de la misma naturaleza, si ello ocurre, deberán informarlo con indicación del despacho en el cual se tramita, con el fin de valorar si es procedente la acumulación de las causas. Acumulándose la causa nueva a la más antigua.

Artículo 8. Sobre la aplicación de criterios de oportunidad.

La autorización de criterios de oportunidad estará a cargo del Fiscal Adjunto de la Fiscalía Adjunta de Fraudes y Cibercrimen, así como del Fiscal Coordinador de la Unidad de Cibercrimen, despacho que ejerciendo su función de rectoría deberá diseñar un protocolo para la tramitación de estas autorizaciones y comunicarlo al resto de fiscalías del país.

Artículo 9. Sobre la Rectoría.

La Fiscalía Adjunta de Fraudes y Cibercrimen será la fiscalía Rectora a nivel nacional en los asuntos relacionados a cibercrimen. Y podrá realizar gestiones de supervisión y recomendaciones a fiscalías territoriales en la materia de su especialización.

Artículo 10. Remisión de causas a la Fiscalía Adjunta de Fraudes y Cibercrimen.

La Fiscala o Fiscal encargado de la investigación deberá comunicarlo a la Fiscala Adjunta o Fiscal Adjunto, la Fiscala Coordinadora o el Fiscal Coordinador de Fraudes y Cibercrimen, para su análisis y valoración previo a su remisión.

Cuando se investiguen grupos de criminalidad organizada y la causa no ha sido asumida por la Fiscalía Adjunta de Fraudes y Cibercrimen, previa valoración, está ultima podrá brindar el acompañamiento que resulte necesario para asegurar un resultado positivo en la investigación.

Artículo 11. Transitorio.

Los expedientes en los cuales los despachos iniciaron la investigación siguiendo lo establecido en la circular 18-ADM-2019, deberán de concluir la misma, hasta su finalización con el requerimiento conclusivo, esto con el fin de evitar atrasos en la tramitación; se señalará para notificaciones el despacho correspondiente según los parámetros indicados, por cuanto con respecto a la competencia se debe recordar que el Ministerio Público tiene por imperativo legal el ejercicio de la acción penal en todo el territorio nacional. Por lo que, a partir de la comunicación de la presente circular se deja sin efecto la circular administrativa 18-ADM-2019.

Las presentes disposiciones rigen a partir de su comunicación oficial.

EMILIA MARIA NAVAS APARICIO (FIRMA)

Firmado digitalmente por EMILIA MARIA NAVAS APARICIO (FIRMA)
Fecha: 2021.01.08 15:13:27 -06'00'

EMILIA NAVAS APARICIO
FISCALA GENERAL DE LA REPÚBLICA
ENERO, 2021
[ORIGINAL FIRMADO]