GUÍA

PARA EL BLOQUEO PREVENTIVO DE FONDOS PROVENIENTES DE TRANSFERENCIAS SOSPECHOSAS DE UNA ESTAFA INFORMÁTICA

CONSIDERANDO:

a) Que las formas de delinquir contra los sistemas financieros se han ampliado, siendo la estafa informática una de las preocupaciones que ha afectado más a la banca costarricense y a sus clientes.

b) Que de acuerdo con datos del Organismo de Investigación Judicial, hay una importante cantidad de denuncias por fraudes en medios informáticos.

c) Que se ha comprobado por medio de las experiencias acontecidas, que la recuperación del dinero sustraído por el delito de estafas informáticas se ha tornado difícil para los clientes.

d) En virtud de lo anterior, con el propósito de procurar una mayor eficiencia en el apoyo a las autoridades y a los clientes, se emite la presente Guía a la cual pueden adherirse voluntariamente las entidades o intermediarios financieros, la cual tiene como objetivo promover un procedimiento estandarizado a nivel del Sistema Financiero Nacional, para el bloqueo preventivo de fondos provenientes de transferencias sospechosas de una aparente estafa mediante el uso de medios informáticos.

PRIMERO: DE LAS DEFINICIONES. - Para efectos de implementar, aplicar e interpretar la presente Guía , se utilizarán las siguientes definiciones:

a) ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR: será toda entidad financiera adherente que reciba una transferencia de fondos producto de un aparente delito de estafa informática.

b) CLIENTE: aquella persona física o jurídica que contrata un producto o un servicio con una entidad bancaria o financiera debidamente regulada por la SUGEF para realizar actividades de intermediación financiera.

c) CUENTA ORIGEN: se trata de la cuenta de ahorro, corriente o IBAN que fue objeto del débito o transferencia constitutivo del posible delito de estafa mediante el uso de medios informáticos.

d) CUENTA DESTINO: es aquella cuenta de ahorro, corriente o IBAN a la que fueron transferidos los fondos provenientes de la "cuenta origen".

El alcance de la "cuenta destino" comprende únicamente la primera cuenta en la que se reciben los fondos procedentes de la cuenta origen. Si se presentan transferencias de

fondos a otras cuentas no aplica el presente instrumento, sin perjuicio de otras medidas que de conformidad con las políticas o procedimientos internos puedan adoptar las entidades financieras, mediante las cuales dispongan extender el bloqueo preventivo a otras cuentas que se sospeche son parte de la estructura ideada para cometer la estafa.

e) **ENTIDAD O INTERMEDIARIO FINANCIERO:** Todos los Bancos e instituciones financieras reguladas por SUGEF que se adhieran a este instrumento.

f) **ESTAFA INFORMÁTICA:** es la acción de un tercero no autorizado de manipular el ingreso, procesamiento o resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos obtenidos fraudulentamente o mediante cualquier herramienta de ingeniería social, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual se procure un beneficio patrimonial o indebido para sí o para terceros. Dichas conductas pueden ser cometidas también contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cometidas por un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que el autor en razón de sus funciones tenga acceso a dicho sistema.

g) **INFORMACIÓN CONFIDENCIAL**: para los efectos de la presente Guía y sin perjuicio de las obligaciones legales que se deriven de la legislación aplicable, se refiere a toda aquella información escrita, compartida oral, visual y electrónicamente o bajo cualquier otro medio o circunstancia, que esté relacionada con la transferencia de fondos sospechosa de fraude electrónico y las cuentas involucradas.

h) **RIESGO:** Posibilidad de afectación en este caso al cliente bancario y/o a la entidad o intermediario financiero.

q) **SEGURIDAD:** Medidas dirigidas a la prevención de riesgos, protección de personas y sus bienes patrimoniales a fin de reducir los efectos provocados por una conducta ilícita.

j) **TERCEROS:** toda persona ajena a la relación comercial o jurídica existente entre las entidades adherentes y sus clientes.

k) **BLOQUEO PREVENTIVO DE FONDOS:** es el bloqueo preventivo de dinero que hace la entidad o intermediario financiero receptor del depósito proveniente de una transferencia en que la entidad o intermediario financiero de la cuenta origen reporta que el mismo podría ser producto de una aparente estafa informática en cualquiera de sus diferentes modalidades, a efecto de verificar el origen de los fondos.

SEGUNDO: DEL OBJETO. La presente Guía tiene como fin principal proponer un procedimiento estandarizado de libre adhesión que facilite poner en práctica una colaboración entre las entidades e intermediarios financieros, para el bloqueo preventivo de fondos en cuenta en protección de los clientes, que permita enfrentar las diversas formas de delincuencia informática y/o tecnológica.

TERCERO: **DE LAS CAPACITACIONES Y OTROS**. Dentro de las prácticas que incluyen dichas mejoras, es necesario incluir la promoción de capacitaciones periódicas encaminadas a prevenir y filtrar los accesos que facilitan la comisión del delito de estafa informática que afecta a clientes y entidades del sistema financiero nacional.

CUARTO: **DE LA COMISION DE SEGUIMIENTO Y ACTUALIZACIÓN**. Para actualizar la presente Guía e incorporar las mejores prácticas en la prevención de los fraudes informáticos, el Foro Interbancario Legal de la Cámara de Bancos e Instituciones Financieras de Costa Rica (en adelante el "Foro") dará seguimiento a la planeación, desarrollo y evaluación de las actividades propias de la ejecución de este instrumento a fin de cumplir con los objetivos de este. El Foro podrá además invitar los asesores en las materias que consideren necesarias para desarrollar en forma más eficiente su labor.

QUINTO: **DE LA COOPERACIÓN INTERINSTITUCIONAL**. Para una mejor eficiencia en la consecución de los objetivos del presente instrumento, los miembros de la Cámara de Bancos e Instituciones Financieras se intercambiarán experiencias que hayan tenido sobre tendencias o modalidades utilizadas por estafadores para realizar fraudes mediante canales electrónicos, así como compartir conocimientos de mejores prácticas para mitigar su ocurrencia de este tipo de ilícitos. Se procurará poner en funcionamiento el equipo y procedimientos idóneos para facilitar la comunicación segura, confiable y oportuna entre todas las entidades e intermediarios financieros que permita alcanzar los objetivos de esta Guía.

SEXTO: **SOBRE EL BLOQUEO PREVENTIVO** Cuando a la entidad o intermediario financiero le corresponda el rol de **"ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR"**, se procederá a realizar un "bloqueo preventivo" de fondos, considerando las siguientes etapas:

a) Para adoptar la medida del "bloqueo preventivo", será necesario haber recibido una comunicación -mediante canales digitales o aquél que definan los adherentes- de parte de la entidad o intermediario financiero de la cuenta origen, de parte de la persona que cada entidad o intermediario financiero designe para ese tipo de situaciones en la que se informa del potencial hecho delictivo. Para esta comunicación se procurará la mayor agilidad posible debido a las características que tienen estas prácticas delictivas.

b) LA ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR procederá al bloqueo preventivo de los fondos provenientes de la transferencia sospechosa de fraude informático una vez que se emita la recomendación del área de seguridad respectiva. Por la celeridad con que se cometen estos delitos, se recomienda que el bloqueo preventivo se disponga en el menor plazo posible una vez recibida la comunicación. Para estos efectos, LA ENTIDAD O INTERMEDIARIO FINANCIERO DE LA CUENTA ORIGEN debe proveer la información detallada de manera que sirva de respaldo al bloqueo de los fondos provenientes de la transferencia que se presume puede ser producto de una estafa.

c) Este bloqueo se mantendrá por el plazo que determine la política interna de cada entidad, a efecto de que el titular de la cuenta objeto de la presunta estafa presente dentro de ese

plazo una resolución de autoridad judicial competente o se presenten circunstancias que conforme con dicha política interna justifiquen mantener el bloqueo preventivo.

d) Para estos efectos, la ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR, ejercerá una debida diligencia reforzada para determinar adecuadamente el origen y naturaleza de los fondos recibidos y originados en un supuesto fraude informático.

SÉTIMO: DEL ALCANCE DE LOS COMPROMISOS.

a) Es entendido que la ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR procederá a realizar el bloqueo preventivo, siempre y cuando el cliente no haya dispuesto de los fondos.

b) La ENTIDAD O INTERMEDIARIO FINANCIERO RECEPTOR y la ENTIDAD O INTERMEDIARIO FINANCIERO DE LA CUENTA ORIGEN, se comprometen expresamente a brindar la colaboración a su alcance y de acuerdo con el ordenamiento jurídico, a las autoridades policiales y judiciales a cargo de la investigación, persecución y represión de los que originaron las transferencias de fondos que presumiblemente se originan en una estafa informática.

OCTAVO: **INFORMACION CONFIDENCIAL**. Para el cumplimiento de lo anterior, se debe respetar la información calificada como confidencial de acuerdo con los términos indicados en el literal g) de la Cláusula Primera. La misma será usada únicamente:

a) Con el exclusivo propósito de la ejecución de las cláusulas numeradas como **SEXTO** y **SÉTIMO** de esta Guía, se abstendrán de utilizarla para cualquier otro propósito distinto del señalado en estos puntos.

b) Permitirán el acceso a la información sólo a directores, encargados responsables del área de seguridad, representantes y asesores externos (legales, auditores y otros semejantes) que deban conocerla, en atención al fin para el cual fue brindada, debiendo advertir a estas personas el carácter confidencial de la información e instruirlos para que sea tratada como tal, dentro de los términos de la presente Guía y lograr que éstos la reciban con tal carácter y con ese compromiso. Sin perjuicio de lo anterior, el deber de confidencialidad que asumen las entidades o intermediarios financieros adherentes se hace extensivo al hecho de que sus directores, empleados y asesores que hayan tenido o puedan tener conocimiento de todo o parte de la información, mantendrán la misma confidencialidad a la cual estas entidades o intermediarios financieros se encuentran obligados.

c) No se hará ninguna reproducción electrónica ni física de la información confidencial de las cuentas del cliente.

d) No obstante lo anterior, mediante el presente instrumento los adherentes acuerdan que con la información de las denuncias por estafa informática que se realicen formalmente ante el Organismo de Investigación Judicial o el Ministerio Público por los clientes afectados, se podrá crear una base de datos -para uso confidencial- ya sea en alguna de estas instituciones con el apoyo logístico que puedan brindar los miembros de la Cámara de Bancos e Instituciones Financieras de Costa Rica la cual podrá ser de acceso por parte de las entidades o intermediarios financieros al igual que las listas de OFAC, FINCEN u otros, con el propósito de ser considerada de previo a la apertura de servicios y para el monitoreo requerido para la prevención de fraudes.

NOVENO: **DEL LIMITE DE RESPONSABILIDAD.** La adhesión a la presente Guía no implica la asunción de una obligación de resultados, por lo que se entiende que cada entidad o intermediario financiero asume el compromiso de realizar el mejor esfuerzo posible para alcanzar los objetivos propuestos, sin que el eventual incumplimiento acarree responsabilidades de ningún tipo.

La entidad o intermediario financiero de la cuenta origen deberá mantener indemne a la entidad o intermediario financiero receptor de toda responsabilidad civil que se derive como consecuencia de la solicitud de bloqueo de fondos que formule con fundamento en esta Guía, lo que incluye costos o gastos en que esta incurra por lo que en caso de que surja alguna situación de responsabilidad como consecuencia del bloqueo realizado, deberá ser plenamente asumida por la entidad o intermediario financiero de la cuenta origen.

DÉCIMO: **DE LA TERMINACIÓN.** Las partes que se adhieran a la presente Guía podrán separarse de manera unilateral.