DISCURSO DE INSTALACIÓN
VII CONGRESO DE PREVENCIÓN DE FRAUDE Y SEGURIDAD
MARÍA MERCEDES CUÉLLAR, PRESIDENTE
BOGOTÁ D.C., 7 DE NOVIEMBRE DE 2013

En nombre de la Asociación Bancaria y de Entidades Financieras de Colombia, quiero dar la más cordial bienvenida a todos los participantes, a los conferencistas nacionales e internacionales y a los invitados especiales a este séptimo *Congreso sobre Prevención de Fraude y Seguridad.*

Mi reconocimiento a la labor del Comité de Seguridad de ASOBANCARIA y de los grupos de trabajo conformados, por sus esfuerzos para promover e implementar acciones y estrategias gremiales que ayuden a la mitigación de los riesgos asociados con estos temas.

En múltiples ocasiones hemos hecho referencia a la caracterización de los fraudes asociados con los servicios que presta el sistema financiero. Las investigaciones demuestran que, detrás del actuar delincuencial, existen complejas y organizadas estructuras. Además, es evidente que la mayor motivación de esas organizaciones es económica y su fin último es el apoderamiento de recursos de la víctima, que puede ser el banco o el cliente de las entidades financieras.

Por su parte, es una realidad que la delincuencia informática está a la vanguardia, lo que trae consigo importantes ventajas para el actuar ilícito frente a otras modalidades de criminalidad. En primer lugar, los avances tecnológicos le facilitan al defraudador adquirir herramientas y establecer contacto con organizaciones ilegales de otros territorios. Es decir, los grupos criminales no solo están debidamente estructurados sino que, además, son transnacionales. En segundo lugar, la *Internet* favorece el anonimato y hace que el delincuente se sienta menos expuesto ante la víctima y ante las autoridades. Y en tercer lugar, estas tipologías delictivas generan economías de escala, en razón de la disposición de redes globales que posibilitan el acceso y ataque a múltiples usuarios mediante una única acción.

Los informes de las instituciones que se dedican a estudiar el comportamiento de la seguridad informática presentan cifras preocupantes. Según el último estudio de la empresa Symantec, las amenazas informáticas crecieron en 2012 en un 42% en relación con 2011 y se encontraron 5.291 nuevas vulnerabilidades el año pasado. Además, siete de cada 10 correos electrónicos enviados fueron los denominados *spam*.

De todos los análisis sobre estos asuntos surgen tres conclusiones principales. Primero, las amenazas avanzan rápido y son tan cambiantes como la propia tecnología. Segundo, debido a la penetración exponencial de los móviles en la población mundial, la mayor amenaza se concentra cada vez más en el *software* malicioso diseñado para atacar esos dispositivos. Según el mismo informe de Symantec, el incremento de *malware* para móviles fue de 58% entre 2011 y 2012. Y tercero, la mayor parte de los ataques informáticos tiene como objetivo la malversación, el robo de datos de tarjetas de pago, de usuarios y claves financieras o fraudes similares. Es decir, el objetivo es económico y las víctimas se concentran en los usuarios o clientes bancarios.

Para enfrentar esos desafíos se requiere **romper los paradigmas** sobre los cuales se han abordado estos asuntos. A continuación haré referencia a algunos de ellos.

El primero está relacionado con que los **asuntos de seguridad informática son un problema de los ingenieros**. Si bien existe un conjunto de amenazas sofisticadas desde el punto de vista tecnológico, en la mayoría de casos, la dificultad en los ataques es baja o moderada y se utilizan métodos básicos sin requerimientos de cuantiosos recursos. En muchas ocasiones más que el desarrollo técnico, la delincuencia se

centra en engañar a la víctima o robarle información a través de métodos de ingeniería social. Inclusive, algunos casos que parecieran producto de delitos informáticos terminan siendo situaciones de infidelidad, corrupción o fraude interno.

A manera de ejemplo, en un caso, que se encuentra en investigación judicial, sucedido en una entidad pública, la búsqueda inicial de responsabilidades se concentró en el uso de *software* a través del cual se robaron datos de autenticación para acceder a canales bancarios y realizar pagos fraudulentos. Durante el rumbo de la indagación, los investigadores encontraron que se trataba de un empleado corrupto que utilizaba falsos contratistas, a quienes les pagaba por servicios no prestados y se escudaba aduciendo fraude informático.

Es por lo anterior, que las labores de prevención, detección e investigación, y en general, el diseño e implementación de estrategias relacionadas con los riesgos de fraude, deben contar con equipos interdisciplinarios que permitan abordar una visión integral de la seguridad. Esto es aplicable no solo para las entidades bancarias sino también para instituciones de otros sectores.

Precisamente el segundo paradigma al que quiero referirme es que **las amenazas de fraude están en particular dirigidas a las entidades financieras**. Las cifras del estudio de Symantec para 2012 muestran lo contrario: solo el 19% de los ataques informáticos se dirigieron a entidades financieras o aseguradoras, mientras que el resto, es decir el 81%, se efectuaron en otros sectores, como el industrial, gubernamental y empresas de servicios.

Como bien lo anotamos, los delincuentes tienen como objetivo apoderarse de recursos económicos. Para tal fin, y tal como lo señalan los expertos en estas materias, para estos propósitos buscan atacar el eslabón más débil de la cadena. Significa que, aun cuando existen diversos tipos de ataques a los bancos, los bandidos han entendido que es más difícil materializar un fraude "asaltando" a la entidad financiera que atacando directamente al cliente.

Es por esto que, aun cuando una víctima de delitos bancarios tiene la percepción de que la obtención de su información financiera o de sus credenciales de autenticación fue provocada por una fuga de datos del banco, la verdad es que, en la gran mayoría de los casos, el origen de la pérdida se origina en el cliente mismo. De acuerdo con Symantec, en el ámbito empresarial, sectores como salud, educación y gobierno

representaron casi las dos terceras partes del total de casos de violación de datos personales a través de medios informáticos.

El tercer paradigma se refiere a que **la responsabilidad frente a la prevención de los fraudes bancarios es exclusiva de las entidades financieras**. No se debe desconocer que en una transacción financiera se ven involucrados muchos actores, no solo a partir de la operación propiamente dicha, sino inclusive desde el mismo ámbito normativo. Un pago o una compra a través del sistema financiero involucran, más allá del banco y de su cliente, a las redes de procesamiento, empresas de telecomunicaciones y establecimientos de comercio, entre otros. Además, las operaciones financieras se desarrollan dentro del marco de reglas de juego definidas por el Estado con anterioridad. Por lo tanto, las acciones de mitigación de los riesgos asociadas con esas operaciones no pueden ni deben estar asociados exclusivamente con la entidad financiera. Desconocer lo anterior significa desconocer la realidad en la que se desarrolla la operación bancaria. Cada agente debe comprender su papel y asumir las acciones que le corresponden para contribuir a blindar las operaciones ante los ataques criminales.

Así las cosas, los **bancos** invierten cada año cientos de millones de dólares en la implementación y ejecución de herramientas que ayudan a

asegurar sus propios sistemas, así como en los canales que ponen a disposición de sus clientes. La lista es innumerable. Se resaltan medidas como la migración a la tecnología EMV en todo el sistema de tarjetas débito y crédito que, de acuerdo con las metas establecidas por el regulador, debe haber quedado incorporada en su totalidad en los establecimientos de crédito a finales del próximo año. Hoy en día, el 60% de los plásticos ya cuentan con *chip* y el cien por ciento de los datafonos están listos para procesar transacciones a través del estándar EMV. Por su parte, los cajeros automáticos tienen adecuados el *hardware* y el *software* para recibir transacciones con esta tecnología, aunque inicialmente solo tienen habilitado el procesamiento de operaciones con tarjetas propias.

También sobresalen estrategias como el fortalecimiento de los mecanismos de autenticación en canales virtuales, en particular a través de claves dinámicas; la entrega de información en línea por medio de mensajes de texto o correos electrónicos relativos a las operaciones realizadas; y el análisis constante de posibles ataques a los sistemas informáticos del banco, entre otras.

La cambiante criminalidad hace que los bancos deban estar preparados para seguir evaluando y efectuando diversas acciones que contribuyan a

contrarrestar su dinámica. Sin embargo, más allá de un listado estándar de herramientas, estrategias o tecnologías a implementar, la orientación debe dirigirse hacia una *gestión integral del riesgo de fraude*, acorde con las características de cada entidad, de sus clientes, de su mercado objetivo y de sus canales.

Por parte de los **clientes**, su papel en la prevención del fraude es fundamental. Como se anotó, cada agente tiene un rol particular y, por lo tanto, los usuarios también deben realizar acciones o tener comportamientos adecuados en el ámbito que les corresponde.

No nos cansaremos de insistir en que los usuarios deben adoptar *prácticas seguras* al realizar sus operaciones financieras y en el manejo de su información y de sus medios transaccionales. Es una triste realidad enfrentarnos al hecho de que el ciudadano cuida más la billetera que guarda en el bolso o en el bolsillo, que los datos de las tarjetas de crédito o los usuarios y claves para acceder a los canales transaccionales. No existe conciencia de que la disponibilidad de esa información permite acceder a su dinero o a sus cupos de crédito, es decir, a los recursos que tiene en el sistema financiero.

Desde hace varios años hemos insistido, a través de diferentes entidades del gobierno, en la necesidad de trabajar con mayor firmeza en ese sentido. Por fortuna, a finales del año pasado encontramos *eco en el Ministerio de las Tecnologías de la Información y las Telecomunicaciones*, y en particular en el Viceministerio de Tecnologías y Sistemas de la Información, que abrió la posibilidad de generar una *alianza estratégica*, inicialmente centrada en dos frentes de trabajo: el uso responsable de las TIC y la seguridad en las transacciones de comercio electrónico.

En el primero de ellos –esto es en el *uso responsable de las TIC*– esperamos ver pronto publicado el documento que contiene los lineamientos de seguridad que deben tener los equipos y/o terminales desde donde se realizan transacciones financieras con recursos públicos, en el cual trabajamos en conjunto con el Ministerio. El objetivo es que los dispositivos desde los cuales las entidades públicas realizan operaciones bancarias cuenten con unos requisitos mínimos de seguridad, tanto física como lógica. Estamos seguros de que esta medida ayudará a mitigar los riesgos de que esas instituciones sean víctimas de delitos bancarios a través de medios electrónicos.

En el segundo –la *seguridad en las transacciones de comercio electrónico*– el trabajo debe centrarse en la promoción de los mecanismos de pago electrónicos y el uso de las TIC para la realización de operaciones financieras, complementado con elementos educativos de los ciudadanos relativos al uso debido de esos canales, los riesgos y las recomendaciones para su utilización de manera segura.

En cuanto a los **demás actores** que participan en la realización de transacciones financieras, la apuesta es a continuar *trabajando en actividades conjuntas que generen valor a la cadena de mitigación de riesgo*, en el ámbito que corresponda a cada uno de ellos. Así las cosas, a manera de ejemplo, ASOBANCARIA viene trabajando con la Cámara Colombiana de Comercio Electrónico, las pasarelas de pago, INCOCRÉDITO, los bancos emisores y adquirentes y los establecimientos de comercio en la revisión de los esquemas de operación de compras o pagos a través de *Internet*, y en el diseño y ejecución de estrategias conjuntas que permitan hacer frente a la delincuencia.

En este punto es relevante resaltar que tal vez uno de los grandes errores que comete la sociedad, y en particular los actores que hacen parte o tienen relación con la realización de una transacción financiera, es buscar sin cesar al culpable de un fraude o ilícito entre ellos mismos.

Es pertinente recordar que el culpable de un fraude es el delincuente, y que asignarse responsabilidades entre unos y otros favorece el actuar de la criminalidad que, por el contrario, trabaja de forma estructurada y organizada. Si se cambiara esta mentalidad, con seguridad se podrían ejecutar acciones que desestimulen el actuar de los delincuentes o establecer procedimientos para recuperar los dineros producto de ilícitos que hoy no se aplican por la desarticulación institucional.

A manera de ejemplo, cada vez con mayor frecuencia se evidencia que las bandas criminales pagan servicios públicos o privados a través de *Internet* utilizando usuarios, claves y otros mecanismos de autenticación que de manera previa fueron robados a los clientes bancarios.

Las investigaciones de las autoridades judiciales muestran que el usuario del servicio o tercero que está obligado al pago, en la mayoría de situaciones, ha aceptado entregar el dinero de la factura, orden o recibo de pago bajo el incentivo de sufragar la deuda por un menor valor. La pregunta que surge es: ¿el beneficiario es un ciudadano incauto y de buena fe, o es, entre comillas, un "cómplice" por el hecho de pagar por menor valor una obligación? En realidad las dos situaciones son posibles. Frente a esta situación, medidas como la *reversión de la operación,* sin lugar a dudas, ayudarían a desestimular el actuar de este

tipo de delincuentes. Esta herramienta limitaría las posibilidades de que el criminal pueda recuperar el efectivo al realizar un pago, o una compra, con usuarios y claves usurpados.

Por lo tanto, es imperioso tramitar una ley que autorice la realización de *reversiones de transacciones financieras* cuando el cliente originador afirme no haber efectuado o autorizado dicha operación. Hoy en día, el Estatuto de Protección al Consumidor contempla la reversión de pagos, pero solo para las ventas de bienes realizadas a través de comercio electrónico. No obstante, aun en este caso no se ha expedido la reglamentación a que hace alusión la norma. Por esto, es necesaria una reforma legal que contemple la posibilidad de realizar reversiones considerando cualquier tipo de pago o transacción, inclusive las de servicios públicos, impuestos o seguridad social.

No quiero terminar sin reiterar el llamado a la necesidad de avanzar en el *fortalecimiento de las acciones judiciales* en contra de las bandas criminales. Estamos seguros de que, mientras no existan castigos ejemplares, el potencial delincuente no va a percibir suficientes riesgos como para desistir de la acción ilegal.

En múltiples ocasiones hemos anotado la complejidad de las labores de investigación y en especial de la judicialización en los delitos cometidos en contra de los bancos y sus clientes. Por esto, desde ASOBANCARIA se han venido apoyando las labores de investigación criminal de la Policía Nacional y de la Fiscalía General de la Nación, en particular en el mejoramiento de sus herramientas tecnológicas. También hemos financiado programas de educación en estas materias, dirigidos a las autoridades de investigación y judicialización.

Sin embargo, estos esfuerzos son parciales, porque la competencia para la investigación de los delitos informáticos está en manos de 1.300 fiscales locales, quienes, además, tienen a su cargo procesos de la más diversa índole. Lo mismo sucede con los jueces penales municipales, a quienes la Ley 1273 consideró responsables de conocer este tipo de conductas.

Desde la administración del doctor Iguarán en la Fiscalía General de la Nación hemos insistido en la necesidad de que las autoridades asignen la competencia de la investigación y judicialización de los delitos informáticos a grupos especializados. Según entendemos, desde ese momento y hasta ahora, la decisión ha estado suspendida por la atención que se estaba prestando a la reestructuración de la institución.

En la actualidad, con la aprobación de la Ley 1654 de 2013, que otorga facultades extraordinarias al Presidente de la República para modificar la estructura y la planta de personal de la Fiscalía General de la Nación, esperamos que esa necesidad se convierta en una realidad.

De acuerdo con reuniones sostenidas con el señor Vicefiscal y sus delegados, la criminalidad informática es una prioridad en los procesos de investigación judicial en el país. Incluso, se está evaluando la posibilidad de crear una Dirección Nacional de Delitos Financieros que involucre no solo las tipologías informáticas sino todas aquellas que tengan que ver con el sector. El objetivo es desarticular las grandes estructuras criminales a través de la concentración de investigaciones; el análisis de conexidad de casos y la especialización de los investigadores y de la policía judicial en las tipologías de las que son víctimas las entidades financieras y sus clientes. Desde ASOBANCARIA apoyamos esa iniciativa y esperamos que se encuentre materializada en el corto plazo. Estamos seguros de que ello ayudará a concentrar los esfuerzos de las diferentes autoridades en las investigaciones y dará mejores resultados en la judicialización de las estructuras criminales.

Para terminar, espero que este Congreso sirva para proveernos de mayores conocimientos y que éstos, a su vez, contribuyan a prevenir

diferentes tipos de fraude y a fortalecer las condiciones de seguridad de los ámbitos en los que cada uno de nosotros nos encontremos.

Muchas gracias.