LA NECESIDAD DEL ANEXO POR FRAUDES POR SISTEMAS COMPUTARIZADOS FRENTE AL FRAUDE ELECTRÓNICO EN CUENTAS MAESTRAS EN COLOMBIA.

EDUARD JAVIER MORA TÉLLEZ

Tutor: LUZ ELVIRA MORENO DUEÑAS

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS JURIDICAS

MAESTRIA EN DERECHO DE SEGUROS

BOGOTÁ D.C.

2022

Tabla de contenido

Pág.

Introducción

Cuando decidí emprender esta tesis, eran múltiples las inquietudes que me surgían frente a la seguridad que tienen aquellas cuentas en las que el Gobierno deposita los dineros que recauda o con los que afronta los diferentes gastos públicos o de inversión social acorde al Presupuesto de la Nación, ello porque desde mi experiencia profesional encontraba que si bien las entidades financieras y públicas tomaban pólizas para cubrir distintos riesgos, a la hora de la ocurrencia de un siniestro por un fraude electrónico y establecer con qué amparo se contaba, se podía constatar que respecto de dicha situación no se tomaba un anexo específico para esos eventos ni en los que se tomaban, se cubrían las nuevas realidades cibernéticas con que se podían afectarse los recursos públicos.

Es por ello que en este breve escrito, expongo desde el panorama de la definición de cuenta maestra, su regulación e importancia, así como el panorama de fraudes electrónicos y los riesgos cibernéticos, la realidad de la contratación de pólizas que circulan en el mercado que son adquiridas tanto por entidades financieras como no financieras, así como la regulación fiscal que rodea el punto, para evidenciar que aunque sí existe un mercado asegurador para este tipo de riesgos y contratación de pólizas por las entidades públicas que manejan recursos públicos a través de cuentas maestras, el mismo no está ajustado a la realidad y necesidad de proteger debidamente esos dineros que no son cualquier tipo de recursos, sino destinados a la población colombiana en la atención prioritaria de servicios de salud, educación, apoyo a la niñez, población indígena y vulnerable, pago de pensiones nómina, entre otros.

Lo anterior, de reparar en que los clausulados que rigen las pólizas, en primer lugar, obedecen a un mercado internacional con algunas adaptaciones para el marco local; segundo, carecen de una debida y permanente actualización; y, tercero, deberían tener una real perspectiva de necesidad y no un mero formalismo fiscal, cuyo impacto se vería tan solo en el momento en que se da la defraudación, más no de cara a su prevención.

Así las cosas, este análisis pretende ser un referente de la necesidad de que tanto las entidades financieras como las entidades públicas que administran o manejan cuentas maestras, adquieran un anexo por fraudes por sistemas computarizados frente al fraude electrónico que aquellas puedan sufrir, que realmente garantice que de verse afectadas por un ataque cibernético los dineros depositados en las mismas puedan ser respaldados. Además, sin dejar de relievar que lo que aquí se propone se puede extender a la protección de los recursos públicos que se manejan a través de otro tipo de productos financieros.

Capítulo I. Origen y Definición de las Cuentas maestras para las entidades territoriales en el Sistema Financiero Colombiano.

Las cuentas maestras son productos financieros cuyas características más relevantes consisten en que sus recursos se deben administrar de forma exclusiva, la realización de pagos con cargo a los depósitos de estas se hace únicamente a través de transferencias electrónicas a los beneficiarios, que deben estar previamente inscritos ante una entidad bancaria y, de cuyos movimientos, se debe rendir reportes específicos y periódicos al Gobierno Nacional.

En Colombia, este tipo de cuentas, que son de ahorros, se empiezan a implementar desde el año 2006 inicialmente en el sector salud, en vista de la necesidad de manejar controladamente los recursos del sistema, tomando en cuenta que este producto financiero, por sus características, fortalecía la recopilación de información del Gobierno Nacional respecto de la administración de los dineros destinados a ese sector, permitiendo mayor control de los movimientos, la transparencia de las operaciones económicas y facilitando la implementación de herramientas de fiscalización de aquellos.

Su regulación se ve reflejada en las Circulares número 007 de marzo 5 de 2012 y 0041 de julio 24 de 2012 del Departamento Nacional de Planeación, las disposiciones del Ministerio de Hacienda y Crédito Público y la Ley 1753 de 2015, Plan Nacional de Desarrollo, que se establece que será a través de este tipo de cuentas que se manejen los recursos del Sistema General de Participaciones. Constituyen el marco de la implementación y desarrollo de este tipo especial producto bancario, entre otras, la Resolución 4835 de 2015, por la cual se reglamentan las Cuentas Maestras de las

entidades territoriales y sus entidades descentralizadas para la administración de los recursos del Sistema General de Participaciones de Propósito General, las Asignaciones Especiales y la Asignación para la Atención Integral a la Primera Infancia, modificada mediante Resolución 1019 del 17 de abril de 2020, en sus artículos 11 y 13; la Resolución 12829 de 2017, por la cual se reglamentan las Cuentas Maestras de las entidades territoriales para la administración de los recursos del Sistema General de Participaciones en Educación en sus componentes de prestación del servicio, cancelaciones, calidad matrícula y calidad gratuidad; la Resolución 660 de 2018 Por la cual se reglamentan las Cuentas Maestras Pagadoras y las Cuentas de Manejo de Garantías de las Participaciones de Agua Potable y Saneamiento Básico, Educación, Propósito General, las Asignaciones Especiales y la Asignación para la Atención Integral a la Primera Infancia del Sistema General de Participaciones; la Resolución 2248 de 2018 por medio de la cual se reglamenta las cuentas maestras del Programa de Alimentación Escolar.

Se abre así un escenario de digitalización de pagos, con lo cual el Gobierno Nacional promueve la bancarización de los recursos públicos, con parámetros de eficiencia y modernidad en la administración pública, a partir de toda una reglamentación con que regula su uso y aplicación por cada sector, siendo varios los actores que participan en la creación y desarrollo de las cuentas maestras:

- El ejecutor: Entidad territorial, fondo o quien está encargado legalmente de la administración y ejecución del recurso y también de la cuenta maestra.
- El Banco: Entidad financiera en la cual el ejecutor de los recursos apertura la cuenta maestra y ante quien se registran los beneficiarios de los pagos o trasferencias electrónicas

en la periodicidad y monto definida. Igualmente es la que rinde informe al ejecutor y órgano rector de los movimientos del producto.

- Organismo rector: Es el Ministerio o Departamento del Gobierno Nacional ante quien se registran las cuentas abiertas en entidades financieras que tiene a su cargo la administración, control o manejo de los recursos que se ejecutan a través de las cuentas maestras.
- El beneficiario: Es la persona natural o jurídica a quienes el ejecutor a través de la cuenta le realiza los pagos o transferencias electrónicas.

Se ha dicho entonces que este tipo de cuentas ha traído múltiples beneficios, no sólo para el Estado en el manejo de los recursos pues permite, como se anotó, que pagos del erario público se realicen de manera digital con plena trazabilidad entre la fuente y el receptor, con un control frente a los mismos y optimización de costos; sino también ha fomentado la inclusión financiera, llevando al sector bancario a estructurar un producto que cumpla con ese fin acorde a la reglamentación vigente, haciendo uso de las tecnologías y sus portales electrónicos, escenario este que si bien ofrece ventajas tecnológicas y operativas también conlleva los riesgos propios del uso de esas herramientas.

1.1. Condiciones para la apertura, registro y operación de las cuentas maestras de las Entidades Territoriales y sus entidades descentralizadas

La ley 1753 de 2015, Plan Nacional de Desarrollo 2014-2018, cuya vigencia no decayó con la Ley 1955 de 2019 (PND 2018-2022), contempla que los recursos del Sistema General de Participaciones deben manejarse a través de cuentas bancarias debidamente registradas.

Como estas cuentas solo pueden aceptar operaciones de débitos por transferencia electrónica a aquellas cuentas bancarias que pertenecen a beneficiarios naturales o jurídicos identificados formalmente como receptores de estos recursos, la apertura de estas por parte de las entidades territoriales se efectuará conforme la metodología que determine el ministerio que gira los recursos.

Es decir, conforme a las reglas que fije el Ministerio de Salud y Protección Social para participación en salud, el Ministerio de Educación Nacional para participación en educación, el Ministerio de Vivienda, Ciudad y Territorio para participación en agua potable y saneamiento básico y, el Ministerio de Hacienda y Crédito Público para la administración de los recursos del Sistema General de Participaciones del Propósito General, las asignaciones especiales y la asignación integral para la primera infancia.

En este sentido, con la uniformidad que tiene el manejo de los recursos a través de este tipo de cuentas, el Ministerio de Hacienda y Crédito Público reglamentó la apertura, registro, sustitución y operación de las cuentas maestras para lo que al Sistema General de Participaciones respecta.

Esta cartera ministerial, a partir de definir por cuenta maestra aquella *"que ha sido aperturada en una entidad bancaria vigilada por la Superintendencia Financiera de Colombia, en condiciones de mercado, la cual solo acepte como operaciones débito las transferencias electrónicas que se realicen a través de la plataforma de servicios de cada entidad bancaria a beneficiarios*

previamente registrados", estableció que, la apertura, debe gestionarse una para cada recurso, mediante la suscripción de un convenio que como mínimo contemple:

i. El reconocimiento de la entidad bancaria de los rendimientos financieros producto del manejo de los recursos en la Cuenta Maestra.
ii. El registro de la entidad bancaria de los ingresos y egresos de la totalidad de los recursos, identificando el origen y destino de los mismos.
iii. La remisión del Banco de los reportes que solicite el Ministerio de Hacienda y Crédito Público y los demás organismos de control.
iv. El registro de los beneficiarios reportados por la entidad territorial o la entidad descentralizada, acorde a la Resolución 4835 de 2015, por parte de la entidad bancaria.
v. La exención del gravamen a los movimientos financieros para los recursos del Sistema General de Participaciones administrados en dichas cuentas.

De la cuenta constituida, se debe a proceder a su registro en la sede electrónica del Ministerio de Hacienda por parte del Representante legal de la Entidad Territorial, el cual se entiende perfeccionado con el primer giro o trasferencia de recursos y debe acompañarse de los documentos correspondientes, como lo son a) el oficio de solicitud de registro de la cuenta debidamente firmado por el Representante Legal de la entidad territorial, b) el formato para el Registro de Cuentas Maestras; c) Registro Único Tributario actualizado y completo; d) Certificación expedida por la entidad bancaria de la Cuenta Maestra; e) Copia del convenio de cuenta maestra; f) Copia de la comunicación mediante la cual se le socializó a la autoridad indígena la información

correspondiente a la Cuenta Maestra, si se trata de las entidades territoriales que administren recursos de la Asignación Especial para Resguardos Indígenas.

Para la sustitución o cambio de cuenta maestra, debe mediar previamente una autorización del ente ministerial que debe ser registrada igualmente ante la sede electrónica del Ministerio de Hacienda, lo cual no procede por casos de medidas cautelares. Del mismo modo, las cuentas maestras receptoras de los recursos del Sistema General de Participaciones no pueden ser canceladas o pasar a estado inactivo ante el banco respectivo, sin previo aviso por parte de esta cartera ministerial.

Los beneficiarios de las cuentas maestras necesariamente lo serán las personas naturales o jurídicas de derecho público o privado que presten o suministren bienes y/o servicios a las Entidades Públicas. En el caso de las aperturadas por entidades territoriales y de sus entidades descentralizadas, los beneficiarios lo serán los titulares de tributos nacionales, departamentales y municipales asociados a la ejecución de los recursos del Sistema General de Participación de propósito general, las asignaciones especiales para alimentación escolar, municipios ribereños del Río Grande de la Magdalena y resguardos indígenas y la asignación para la atención integral a la primera infancia.

En cuanto a su cancelación, ello también debe darse previa autorización y acreditación de la entidad bancaria de que la cuenta fue cerrada sin saldo o con este debidamente trasferido a la que haya sido registrada conforme a lo previsto como aquella que fue aperturada para el manejo de los recursos a partir del momento.

Finalmente, en la Resolución 0660 de 9 de marzo de 2018 el Ministerio de Hacienda y Crédito Público definió que existirá una cuenta maestra pagadora, como aquella cuenta, que debe ser de ahorros, complementaria a la cuenta maestra registrada, la cual acepta exclusivamente trasferencias electrónicas de crédito para el pago inmediato de obligaciones registradas en el convenio y únicamente débitos por botón de pago electrónico seguro en línea – PSE con cargo a los recursos de las Participaciones de Agua Potable y Saneamiento Básico, Educación, Propósito General, las Asignaciones Especiales y la Asignación para la Atención Integral a la primera infancia de los recursos del Sistema General de Participaciones, tales como: el Pago de contribuciones inherentes a la nómina mediante los operadores de la Planilla Integrada de Liquidación de Aportes; el pago por concepto de ahorros voluntarios (cuentas AFC y pensiones voluntarias), la constitución de títulos judiciales a favor de terceros mediante el comercio autorizado para tal fin; el pago de servicios públicos habilitados mediante botón de pago electrónico seguro en línea – PSE; el pago de impuestos nacionales - DIAN que se generen en la ejecución de los recursos de las participaciones y asignaciones del Sistema General de Participaciones.

En estas cuentas no proceden las consignaciones en efectivo por ventanilla, corresponsal bancario o depósito de cheques y son operaciones débito NO autorizadas las trasferencias electrónicas hacia otras cuentas, la expedición de cheques de gerencia, retiros por ventanilla, operaciones por corresponsal bancario, retiros por cajero electrónico, los débitos automáticos y todos aquellos pagos no indicados en la Resolución en mención.

También se prevé la creación de unas cuentas de manejo, que son las utilizadas para honrar el servicio a la deuda con recursos de las Participaciones de Agua Potable y Saneamiento Básico, y Propósito General de los recursos del Sistema General de Participaciones, cuya estructura en general en cuanto a creación guarda identidad, pero debe existir una por cada crédito existente y se registra como beneficiaria de la cuenta maestra para recibir los recursos para el pago de la obligación. Solo operan para este fin y está prohibida la realización de cualquier otro tipo de movimiento.

Cumple destacar que, en la citada normativa, se contempla expresamente que las entidades financieras donde se aperturen dichas cuentas reportarán la información con corte mensual dentro de los veinte (20) primeros días de cada mes, a través de la Plataforma de Integración de Información – PISIS del Sistema Integral de Información de la Protección Social - SISPRO del Ministerio de Salud y Protección Social

Y su manejo está bajo la responsabilidad del representante legal de la entidad territorial, entidad descentralizada, territorio indígena certificado, resguardo indígena certificado o la asociación de resguardos según sea el caso, o del ordenador del gasto del fondo de servicios educativos, atendiendo criterios de seguridad, economía y eficiencia en el manejo del recurso público.

1.2. Importancia del buen manejo de los recursos públicos.

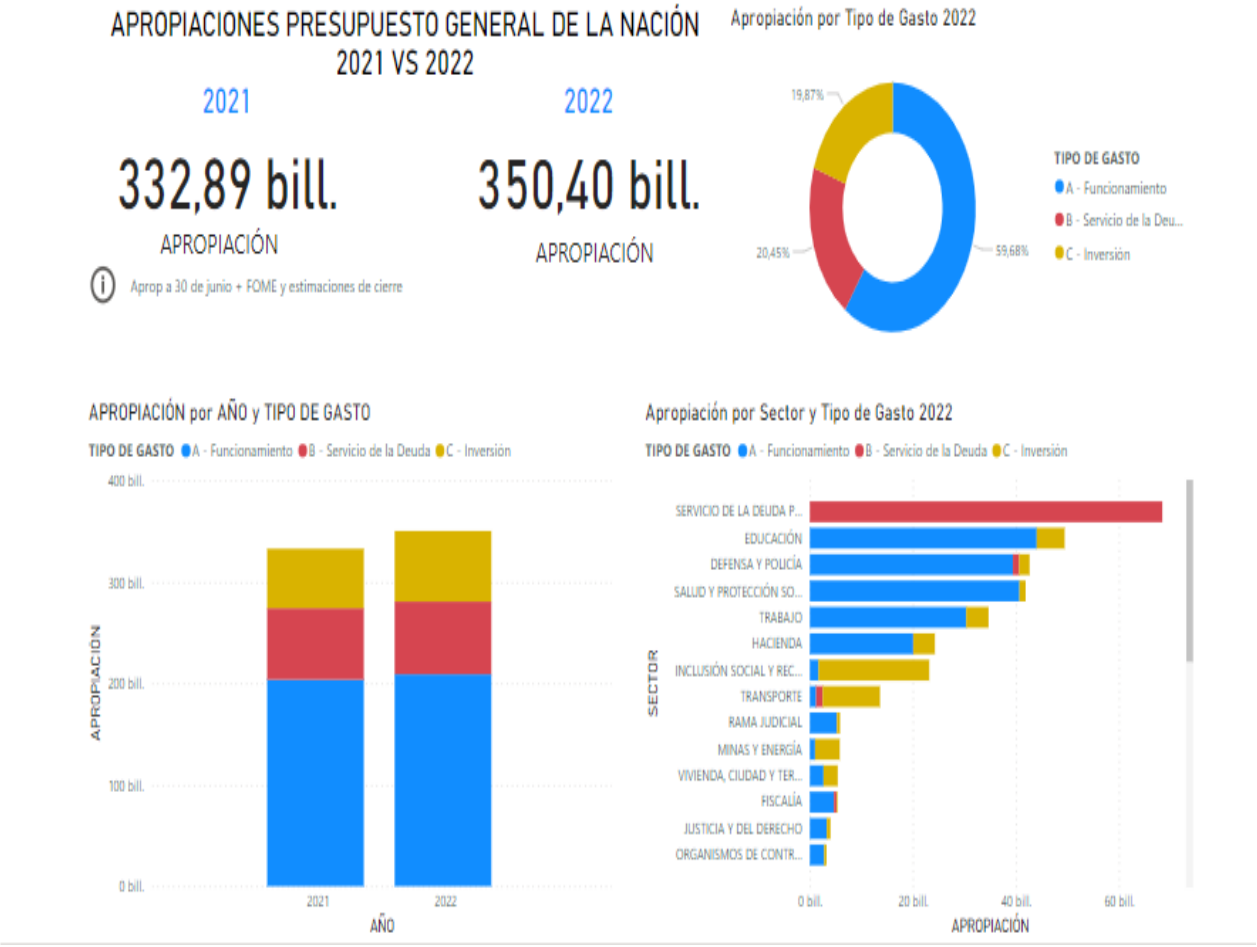
Como ya tuvimos oportunidad de exponer al inicio de este capítulo, las cuentas maestras surgen como una necesidad de controlar los recursos del erario público destinados a cubrir obligaciones

del Estado en diferentes ámbitos, pues ciertamente el uso de dinero en efectivo y otro tipo de canales transaccionales no resultan suficientes para generar el seguimiento y proyectar trasparencia en el manejo de las operaciones que involucran tales rubros.

Y es que teniendo en cuenta que el grueso de las trasferencias que se movilizan a través de dichas cuentas lo son recursos que dispersa el Gobierno Nacional a nivel Central a las entidades territoriales (Departamentos, Distritos o Municipios), con un destino previamente establecido, es más que imperativo contar con un mecanismo de control, que de manera eficaz permita tener información del uso dado a aquellos.

Entonces es precisamente ese contexto, el que determina, por la obligatoriedad de registrar previamente a quienes envían y reciben las trasferencias, lo que permite identificar quiénes las realizan, las cifras manejadas, las épocas y destinación dada a los dineros, con lo que es posible rastrear su uso y evitar desvíos de estos.

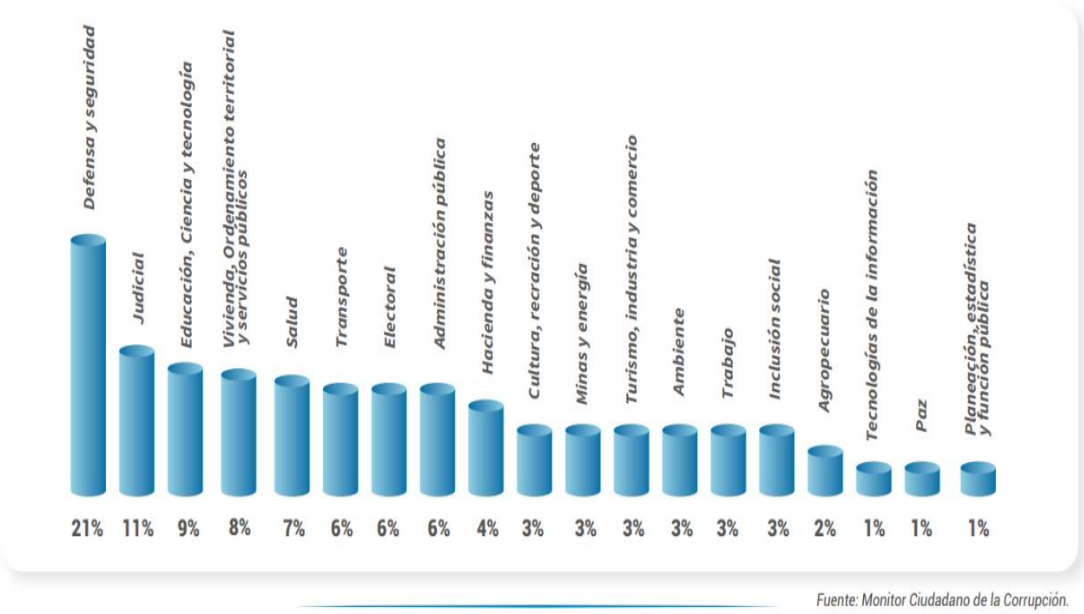
Ello se hace más relevante de reparar en las cifras presentadas por el Ministerio de Hacienda y Crédito Público con ocasión de la ley de Presupuesto General de la Nación para 2022, en las que se reflejan las apropiaciones a que se destinan los dineros del erario público son de gran envergadura y, por ende, su acceso efectivo de gran trascendencia, en tanto que los sectores a los que se dirige (educación, salud, justicia, defensa pública, inclusión social, salud, entre otros) son en extremo de vital importancia para el desarrollo del país, como se denota en la siguiente gráfica:



Fuente: Reproducido de [Proyecto de Ley PGN 2022 (minhacienda.gov.co)]

Y que en el mes de noviembre de este año se aprobó el Presupuesto del Sistema General de Regalías, que regirá entre el primero de enero de 2023 y el 31 de diciembre de 2024, por un monto de $31,3 billones, cifra equivalente a 2,1% del PIB, de los cuales asignó un presupuesto para la inversión de los territorios por $29 billones, de los cuales $7,5 billones serán asignados directamente para entidades territoriales productoras y puertos.

Es más, análisis en materia de corrupción de los últimos años, denotan que los sectores más afectados por circunstancias en las que se disipan los recursos públicos son precisamente aquellos a donde se dispersan dineros del erario, lo que necesariamente hacen aún más trascendente los controles que se imponen en su manejo y gestión. Así lo hizo ver un informe de Monitor Ciudadano que abarcó los años 2016 a 2020, en el que se refleja la afectación predominante a los sectores respecto de los cuales precisamente son asignados y girados dineros públicos para la provisión de bienes y servicios.



Fuente: Reproducido de https://www.monitorciudadano.co/documentos/hc-informes/2021/Radiografia-2016-2021.pdf

Capítulo II. Fraude Electrónico y Riesgo Cibernético en el Sistema Financiero Colombiano

La implementación de medios electrónicos para la realización de transacciones ha permitido no solo a la banca y los usuarios del sector financiero avanzar en el mundo digital, sino también se ha convertido en un desafío a la hora de garantizar la confianza de las operaciones pues debido a que requiere de un intercambio de información, crea un espacio propicio para la exposición al fraude electrónico, que según la doctrina especializada parte de la manipulación del sistema que facilita la sustracción de recursos, la obtención de datos personales o financieros confidenciales.

Estos espacios digitales, que propenden por la innovación y el uso de las tecnologías de la información, eliminando incluso barreras físicas en el manejo de los recursos, obligan no solo a las entidades que ofrecen productos financieros, a que los mismos sean eficientes, sostenibles y seguros, sino a los Estados a generar un ámbito de regulación propio, orientado a la prevención y mitigación oportuna de los riesgos que esto conlleva.

Lo anterior, se torna más relevante de reparar en que en tratándose de contratos de depósito como el que entraña el manejo de cuentas en que se administran dineros de un cuenta habiente, el artículo 1398 del código de comercio establece que todo banco es responsable por el reembolso de sumas depositadas que haga a persona distinta del titular de la cuenta o de su mandatario.

Bajo este parámetro, la jurisprudencia de la Sala Civil de la Corte Suprema de Justicia, especialmente en los últimos años ha venido decantando la naturaleza de la responsabilidad bancaria, donde las discusiones se han centrado en establecer si obedece realmente a un régimen

objetivo cuyo impacto directamente tiene relación con las condiciones que se establezcan en las pólizas que por cuenta de fraudes electrónicos puedan sufrir las entidades bancarias, aspecto que precisamente será materia de análisis a efectos de identificar si las pólizas que actualmente tienen las entidades financieras para estos eventos se ajustan a estas realidades.

Al efecto se dijo por esa Corporación en sentencia SC5176 del 18 de diciembre de 2020, trayendo a colación su línea frente al tema, que *"siendo la bancaria y la de intermediación financiera, actividades en las que (...) existe un interés público y son realizadas por expertos que asumen un deber de custodia de dineros ajenos, siéndole exigibles, según lo previsto por el Estatuto Orgánico del Sistema Financiero (Decreto 663 de 1993) y las Circulares Básica Contable y Financiera (100 de 1995) y Básica Jurídica (007 de 1996) unos altos y especiales cargas o cumplimiento de estándares de seguridad, diligencia, implementación de mecanismos de control y verificación de las transacciones e incluso de seguridad de la confiabilidad de la información y preservación de la confiabilidad, es natural que la asunción de tales riesgos no les corresponda a los clientes que han encomendado el cuidado de parte de su patrimonio a tales profesionales, de ahí que sea ellos quienes deban asumir las consecuencias derivadas de la materialización de esos riesgos. En ese orden de ideas, 'a la hora de apreciar la conducta de uno de tales establecimientos -ha dicho la Corte- es necesario tener presente que se trata de un comerciante experto en la intermediación financiera, como que es su oficio, que maneja recursos ajenos con fines lucrativos y en el que se encuentra depositada la confianza colectiva" (CSJ SC-076, 3 ago. 2004, Rad. 7447) y por tales razones se le exige "obrar de manera cuidadosa, diligente y oportuna en ejercicio de sus conocimientos profesionales y especializados en materia bancaria" para impedir que sean quebrantados los derechos patrimoniales de titulares de las cuentas de ahorros y corrientes de*

cuya apertura y manejo se encarga (CSJ SC, 3 feb. 2009, Rad. 2003-00282-01). De todo lo anterior deriva, necesariamente que en la materia impera un modelo particular de responsabilidad profesional del banco), (CSJ Sc, 15 dic. 2006, rad. 2002-00025-01).

(…)

Debido a las operaciones desplegadas inherentes a su objeto social, particularmente concernientes a la administración del ahorro del público, se enfatiza, las entidades bancarias, como profesionales del sector económico, tienen 17 Radicación n.° 11001-31-03-028-2006-00466-01 una carga especial de diligencia y prudencia tendientes a evitar daños suyos, a los ahorradores y a la comunidad. Cuando tales instituciones desatienden sus deberes de diligencia y cuidado, comprometen su responsabilidad (...). El profesionalismo, continuidad, trascendente función social y provecho pecuniario, entre otras características de la actividad bancaria, permiten suponer, no solo que cuentan con un conocimiento especializado, idoneidad y experiencia, sino que por el riesgo, de suyo creado con su ejercicio y la confianza pública generada, tienen diseñados y puestos en práctica procedimientos pertinentes y suficientes para garantizar la prevención, el control y la seguridad de las operaciones propias de su labor. Es por ello que a la hora de juzgar el cumplimiento de sus obligaciones, se impone hacerlo con mayor rigurosidad respecto de cualquier otro comerciante común o de gestión ordinaria, toda vez que la entidad bancaria, como organización empresarial de actividad especializada, debe estar preparada para precaver, evitar o controlar el darlo proveniente de su labor» (CSJ SC1230-2018, 25 abr.).”

2.1. Marco normativo en materia de ciberseguridad y riesgos cibernéticos en Colombia

En Colombia, el Consejo Nacional de Política Económica y Social CONPES, puntualmente a través de los documentos CONPES 3701 de 2011, CONPES 3854 de 2016 y CONPES 3995 de 2020 se emite un marco normativo y de política pública en ámbitos de ciberseguridad, ciberdefensa y mitigación de los diversos riesgos cibernéticos.

En el primer documento se define un plan de acción para la ejecución de la política pública en ciberseguridad y ciberdefensa, teniendo como antecedentes algunos ataques cibernéticos internacionales, el incremento del uso de las tecnologías en el país -particularmente del internet-, el aumento de denuncias por delitos informáticos, así como la falta de capacidad para enfrentar amenazas de este tipo y la necesidad de adoptar una política nacional de ciberdefensa que involucre todas las entidades del estado con la adhesión de Colombia a los diferentes instrumentos internacionales en la materia.

En el segundo de ellos, luego de analizar los avances obtenidos y la evolución de las amenazas cibernéticas se aborda la Política Nacional de Seguridad Digital, estableciendo a partir de parámetros y recomendaciones internacionales como los definidos por la OCDE, la necesidad de implementar un sistema de gestión de riesgos como uno de los elementos más importantes para abordar la seguridad digital, lo que impone la identificación, gestión, trata y monitoreo de los riesgos de seguridad digital, así como el fortalecimiento de la seguridad de los individuos y del Estado en el entorno digital.

Y en el tercero, se reevalúan los objetivos de la política trazada hasta el momento con miras a que la misma se enfoque a desarrollar la confianza digital a través de la mejora la seguridad digital de modo que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobierno en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Leyes como la 527 de 1999[1], la 599[2] y 600 de 2000[3], la 906 de 2004[4], la 1273 de 2009, la 1341de 2009[5], ley 1437[6], 1474[7], 1480[8], 1564 de 2011[9], la 1712 de 2012[10], la 1621 de 2013[11]; así como los decretos 019, 1704, 2364 y 2758 de 2012, 0032 de 2013, 1078 de 2015, las Resoluciones CRC 3066, 3067, 3502, la Resolución SIC 76434 DE 2012 y Circular Externa SIC 02 de noviembre de 2015, entre otras, son precisamente antecedentes y desarrollo de esa política pública.

Para su estructuración se ha tomado como referencia diferentes instrumentos internacionales como lo son el Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como en convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor

[1] Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
[2] Código Penal
[3] Código de Procedimiento Penal
[4] Código de Procedimiento Penal
[5] Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
[6] Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
[7] Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
[8] Estatuto de Protección al Consumidor
[9] Código General del Proceso
[10] Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
[11] Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones.

desde el 1° de julio de 2004; Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos; Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004; Consenso en materia de ciberseguridad(17) de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005; Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas (2009); Directiva 2006/24 de la Unión Europea; Marco de trabajo de estrategias nacionales de ciberseguridad. Manual de la OTAN; Declaración de la Cumbre de Gales de la OTAN en 2014; Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (celebrada el 20 de marzo de 2015); Declaración sobre Seguridad en las Américas de la OEA (México, 2003).

La Superintendencia Financiera de Colombia, en el año 2017, realizó un diagnóstico respecto de la capacidad de reacción a un evento de vulnerabilidad en materia de seguridad digital, documentando, a partir del análisis de 59 entidades encuestadas, encontrando que en ese año se afrontaron cerca de 40 millones de ataques cibernéticos, el 93% de aquellas tienen en cuenta estándares internacionales para la gestión de la seguridad de la información, todas implementaban comités para discutir temas de seguridad de la información y de seguridad digital, un 83% de las mismas tenían planes para fortalecer la gestión de la seguridad de la información y un 76% contaba con estrategias de comunicación y alianzas con organismos de defensa para brindar mayor solidez a sus esquemas de protección.

Sin embargo, también pudo determinar que a pesar de ese entorno positivo y de la implementación de herramientas de big data, blockchain, data analytics, machine learning, algorithmic trading, cloud computing, biometric, web services, API y de inteligencia artificial, el uso masivo de nuevas tecnologías incrementa la exposición a riesgos cibernéticos en el sector financiero, lo que conlleva un reto permanente, producto de lo cual la entidad de supervisión, el 5 de junio de 2018 la SFC expidió la Circular Externa 007 mediante la cual impartió instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

En este sentido se determinó como obligaciones generales en materia de ciberseguridad el que las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad, así como que aquellas deben adoptar, como mínimo lo siguiente:

- ✓ Establecer una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad en la entidad, la cual debe ser aprobada por la junta directiva, documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad; contener las funciones de la unidad de seguridad de la información y la ciberseguridad; determinar los principios y lineamientos para promover una cultura de ciberseguridad que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes dentro de la política de ciberseguridad. Todas las cuales deben realizarse periódicamente y pueden incluirse, en los cursos sobre riesgo operativo que realice la entidad.

- ✓ Establecer una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad, la cual debe tener al menos, las siguientes características y responsabilidades: a) Se debe conformar considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por la entidad. b). Debe realizar una gestión efectiva de la seguridad de la información y la ciberseguridad en la entidad. c) Debe reportar a la junta directiva y a la alta dirección, los resultados de su gestión, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, identificación de ciber amenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad. La periodicidad de los reportes debe ser, al menos, semestralmente. d) Debe actualizarse permanentemente y de manera especializada para que esté al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad. e) Debe sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciber amenazas. f) Ser la principal responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna. g). Asesorar a la alta gerencia y la junta directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones

adecuadas en esta materia. h) Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un SOC, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán. i) Sugerir los presupuestos de seguridad de la información y ciberseguridad. Dichos presupuestos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información. j) Verificar el cumplimiento de las obligaciones contenidas en el Capítulo I del Título II de la Parte I de la Circular Básica Jurídica, en lo que sea pertinente con sus funciones. K) Debe realizar las demás actividades que por su naturaleza les sean asignadas.

- ✓ Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (Information Security Forum), CIS Critical Security Controls (CSC) o Cobit 5 for Information Security, y sus respectivas actualizaciones.

- ✓ Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.

- ✓ Emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.

- ✓ Establecer procedimientos para la retención y destrucción final de la información, sin que se desconozca lo establecido en el Artículo 96 del EOSF y demás normas aplicables.

- ✓ Establecer una estrategia de comunicación e información que contemple los siguientes ejes, sin perjuicio de las obligaciones de reporte a la SFC y demás autoridades de acuerdo con la normatividad aplicable: a) Información que reportará a la SFC, sobre incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo. b) Información que reportará a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos, sobre incidentes cibernéticos. c) Información que reportará a los consumidores financieros, sobre incidentes cibernéticos que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para remediar la información.

- ✓ Incluir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y apps, que procesan la información confidencial de la entidad o de los consumidores financieros (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.

- ✓ +Incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.

- ✓ Verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas con relación a la inclusión en los contratos con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.

- ✓ Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.

- ✓ Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

- ✓ **Considerar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.**

2.2. Fraude por Medios Electrónicos

El uso del internet, como lo hemos venido refiriendo y el uso cada vez más frecuente de aplicaciones que facilitan la interacción de las personas, entre sí, con el comercio y con el sector financiero, han generado que se presenten amenazas a la seguridad de la información.

De acuerdo con la información reportada a la Superintendencia Financiera de Colombia, en el primer semestre de 2022 el sistema financiero colombiano realizó 6.667.629.172 operaciones: 2.957.987.392 monetarias por $5.328 billones y 3.709.641.780 no monetarias. Siendo los canales digitales los más utilizados y los que más recursos movilizan, como se denota en los datos, presentados en el Informe de operaciones del primer semestre del año que avanza por parte de esta entidad de supervisión.

Canal	Cantidad	Número total de operaciones	Monto de operaciones
Telefonía Móvil		3.840.373.865	204.239.117
Internet		954.084.934	2.473.061.383
Datáfonos	1.086.812	564.924.736	83.214.449
Cajeros Automáticos	16.012	419.077.584	158.707.908
Corresponsales Bancarios	250.344	370.671.646	144.028.009
Oficinas	5.641	235.864.089	1.286.843.952
Débito Automático		142.950.365	34.786.393
ACH		124.070.964	943.265.212
Audio Respuesta		15.610.989	786.958
Total		**6.667.629.172**	**5.328.933.381**

Fuente: Superintendencia Financiera de Colombia (superfinanciera.gov.co) / informe de operaciones enero-junio 2022.

Desde esta perspectiva, los usuarios del sector bancario y las entidades financieras enfrentan diferentes amenazas a la seguridad de su información, entre otras, las definidas por la ISO/IEC

27000:2009, en la Guía Técnica Colombiana, GTC- ISO27035 del Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), como:

- Evento de seguridad de la información: “presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad”.

- Incidente de seguridad: “evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información”.

- Ataques cibernéticos: que son eventos en los que se produce un bloqueo del servicio mediante códigos maliciosos con los que se busca sustraer información, destruirla, entre otras afectaciones a datos relevantes.

Según Asobancaria la banca ha sido uno de los sectores con mayor avance en digitalización, siendo cada vez mayor el número de clientes que accede a transacciones electrónicas monetarias y no monetarias, lo que necesariamente ha traído consigo nuevos riesgos que deben ser mitigados para evitar fraudes dentro de esa nueva economía digital.

Empero, como también lo refiere esa asociación, el sistema financiero resulta ser uno de los más afectados debido a delitos informáticos en Colombia, el cual, de acuerdo con sus cifras, para el

2018 se concentró principalmente en la categoría de tarjetas de crédito y cuentas de ahorro y corriente, mientras que para el año 2020 las modalidades más frecuentes de fraude electrónico fueron el phishing, con un 42%, la suplantación de identidad, con un 28%, el envío de malware, con 14%, y los fraudes en medios de pago en línea, con 16%" (Asobancaria, 2020, p. 1), con una tendencia al aumento de fraude por canales digitales que en un 183% desde diciembre de 2019 hasta abril de 2021(Asobancaria, 2021, p. 1).

Muestra de tal escenario, lo es el informe global sobre tendencias de fraude digital de TransUnion entre el segundo trimestre de 2020 y 2021, en el que se muestra la tasa de intentos de fraude digital en Colombia, distribuida atendiendo el tipo de fraude y la industria, el cual arrojó que:

Industria	**Variación porcentual**	**Principales tipos de fraude**
	Mayores incrementos	
Videojuegos	329%	Cultivo de oro en línea (MMO)
Viajes & Ocio	221%	Fraude con tarjeta de crédito
Comunidades en línea	*158%*	Falsificación del perfil

Mayores descensos		
Telecomunicaciones	-92%	Suplantación de identidad
Ventas minoristas	-40%	Abuso en promociones
Servicios Financieros	-32%	Robo de identidad

Fuente: reproducido de https://noticias.transunion.co/fraude-digital-concentra-su-enfoque-en-industrias-de-videojuegos-viajes-y-ocio/

- **Tipos de fraudes más comunes**

En el mundo, si bien aumenta la gestión de las empresas, entidades financieras y usuarios en general por el buen manejo de sus datos personales, lo que de alguna manera propende por la disminución de los índices de fraude digital, los defraudadores permanentemente también evolucionan en sus técnicas, siendo aún las más frecuentes y/o conocidas:

Phishing: se conoce por tal, al tipo de fraude en el que el cliente recibe un correo electrónico que le pide suministrar datos o actualizarlos utilizando una página web falsa.

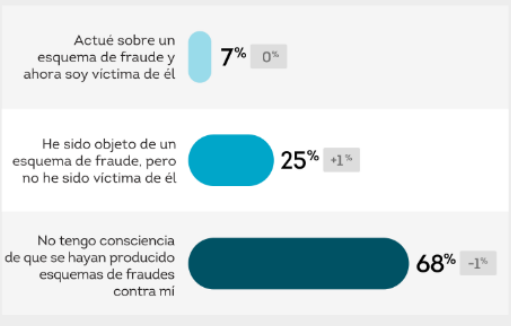
Vhishing: es aquel mecanismo de fraude con el que a través de una llamada, e-mail o un mensaje de texto que se envía a un teléfono móvil, se pide llamar a un sistema interactivo de voz falso en el que suministra información.

Pharming: permite que cuando el cliente intenta acceder a un URL se le lleve hacia un sitio fraudulento que se aprecia similar al original permitiendo que ingrese su usuario y contraseña obteniendo una respuesta de error y generar un intento nuevo, pero al generar nuevamente la operación al sitio legítimo, ya se cuenta con sus datos obtenidos de manera fraudulenta.

Ingeniería Social: este tipo de fraude parte de obtener información confidencial con la manipulación de usuarios legítimos y con engaños romper los procedimientos de seguridad tradicionales, manipulando para divulgar los datos de seguridad.

Eventos que según una encuesta de TransUnión, realizada en el presente año, se ha verificado en las siguientes proporciones en el uso de sistemas financieros, aunque con una variación porcentual con respecto al año anterior en el mismo espacio temporal.

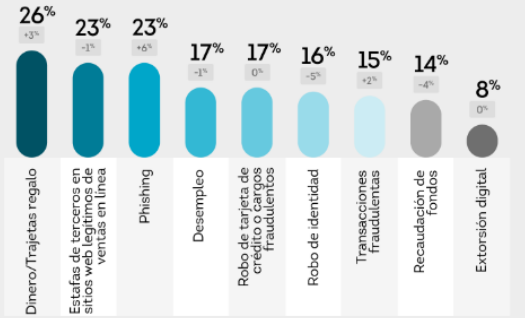
Figura 18. Experiencia personal con intentos de fraude digital en los últimos tres meses



X% Cambio en puntos porcentuales con respecto a T2 2022

Figura 19. Los esquemas de fraude más frecuentes contra los consumidores

(entre aquellos consumidores objeto o víctima de fraude digital)



X% Cambio en puntos porcentuales con respecto a T2 2022

Fuente: Reproducción de Comportamientos y perspectivas de los consumidores respecto a los presupuestos, gastos y deudas actuales y futuras de los hogares. Consumer Pulse ES CO Q3 2022 (transunion.com)

2.3. Riesgo cibernético en el sistema financiero e incidencia en el sector asegurador.

Según el Instituto de Gestión de Riesgos (Institute of Risk Management), el riesgo cibernético se define como *"cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información"*.

Sin embargo, el riesgo cibernético es un reto, que no parte de hechos aislados, sino de una suma de componentes humanos, procesos, tecnología y regulación, el cual constituye un desafío dada la variedad y complejidad que muestran, generan tensión económica y asimetría de información, fruto de ecosistemas digitales recientes que demandan un manejo interdisciplinario.

El sector financiero por la actividad misma que desarrolla y con la integración cada vez más necesaria de las tecnologías, ha generado un nuevo riesgo, o mejor, ha aumentado de manera significativa el riesgo de vulnerabilidad de ataques cibernéticos a esa transmisión de información que involucra fondos económicos (envío/recepción), lo cual es un tema de interés público, convirtiéndose en un tema de prioridad para autoridades financieras y entidades que se dedican al mercado financiero.

De ahí que la tendencia dentro de las entidades del sector necesariamente deba ser, aparte de implementar un programa de innovación digital, el mejorar la protección a la seguridad de datos, invertir en tecnologías de prevención de riesgo de crimen financiero que cubra estándares

internacionales, mecanismos de defensa idóneos para protegerse frente a los ataques cibernéticos y que sus análisis de vulnerabilidad les permitan identificar y corregir brechas de seguridad que podrían ser utilizadas para afectar la confidencialidad, integridad o disponibilidad de la información.

En este escenario se patentizan elementos como el manejo de un presupuesto de seguridad digital, adquisición e implementación de tecnología, capacitación y actualización del personal de seguridad de la información, contratación de servicios de consultoría, servicios de monitoreo y gestión de seguridad con terceros.

Igualmente, producto de esas amenazas a la seguridad de la información a la que se enfrentan quienes realizan operaciones electrónicas a través de sus portales o canales transaccionales, se cuestiona si, siendo estos potenciales eventos generadores de responsabilidad, en el caso de las entidades financieras se cuenta con un respaldo para responder por aquellos. Ello por cuanto, según el nivel de exposición o vulnerabilidad de los agentes involucrados se podrá determinar si están llamados a responder con ocasión de los daños que resulten.

Esto pues como hemos podido denotar, la realización de operaciones en el mundo digital como una constante y la importancia para las personas (clientes, usuarios, empresas, bancos, Estado) en obtener operaciones dotadas de integralidad y seguridad, es cada vez más relevante.

Empero, esta preocupación no solo es de las entidades financieras por cuenta de las reclamaciones que afrontan, sino también se convierte en un reto para el gremio asegurador, pues precisamente

esas nuevas formas de hacer negocios, las nuevas tecnologías, el manejo de la información y datos del usuario, imponen un mayor ejercicio profesional de su actividad, desde la implementación de herramientas nuevas o mejora de las existentes en punto de la venta de seguros, la tecnificación de la suscripción, emisión, fidelización de clientes e incluso pago de siniestros derivados de siniestros que involucran eventos tecnológicos.

Ciertamente, un fraude va desde el robo de información, identidad, recursos económicos o corporativos, uso de datos confidenciales, extorsión, espionaje corporativo o terrorismo cibernético, de allí que combatir los riesgos cibernéticos que afronta el mercado partirá del manejo propio de la seguridad de los asegurados, del conocimiento que estos tienen del uso de la tecnología y sus riesgos, de la información que se tenga de los seguros existentes en el mercado y su cubrimiento en punto de estos, así como la forma de usarlos, y de las gestiones que despliegan las aseguradoras en materia de información, prevención, diseño de seguros para cada necesidad, desde lo pequeño a lo macro, encaminados no solo a superar situaciones graves, sino como una herramienta de acompañamiento que se adapte a la constante evolución de los tipos de fraude.

En nuestro país, como lo puso de presente la Superintendencia Financiera de Colombia, en su publicación de los indicadores de seguridad de la información y ciberseguridad de los establecimientos bancarios del país, datos que hacen referencia a inversiones realizadas por los bancos en 2021 en esos rubros; además de la gestión de los incidentes y vulnerabilidades detectadas, y el monto que asumieron las entidades por los incidentes cibernéticos que afectaron a sus clientes, reportó que para esa anualidad la inversión en esta materia fue de $341 mil millones,

recibieron 1362 millones de ataques cibernéticos y debieron asumir $75 mil millones por incidentes cibernéticos que sufrieron sus clientes donde se hicieron operaciones no autorizadas.

En este campo entonces se muestra relevante el papel que juegan los contratos de seguros adquiridos por los partícipes de la relación económica y puntualmente la estructuración, de acuerdo con la legislación vigente y los parámetros del artículo 1045 del Código de Comercio, teniendo en cuenta los riesgos cibernéticos.

Frente al punto, la industria aseguradora desde hace algún tiempo, precisamente ante la aparición de estos fenómenos y la incidencia de la tecnología en el mundo financiero y de los negocios, ha venido estructurando productos especiales para la protección de los riesgos que ello representa y específicamente para el aseguramiento de los canales de pago que utiliza el sector financiero, los cuales buscan abarcar las necesidades del tomador según el riesgo que desea asegurar que por la misma naturaleza se muestran diversos.

Ha echado mano de metodologías para la clasificación de estos riesgos, desde el proceso de su formación -etapa de suscripción del seguro-, lo que se requiere para su emisión, dentro de lo cual se ha mencionado el identificar el incidente cibernético, el tipo de evento, las causas de ocurrencia y el actor, para a partir de allí, el tipo de impacto, su descubrimiento, cobertura y reclamación.

Sin embargo, los seguros se han visto por quien los adquiere como una forma de mitigación de daños más no como un elemento de previsión, por lo que para lo que a este trabajo se refiere, se muestra la importancia precisamente de esa clasificación de riesgos en tratándose de la actividad

financiera que involucra el manejo de depósitos en cuentas maestras, los daños y perjuicios causados a terceros y el derecho a reclamar una indemnización en caso de que se configuren siniestros con ocasión de un evento que altere las condiciones de seguridad y permita el fraude electrónico por la exposición a un riesgo cibernético.

Igualmente, si dado el tratamiento que tiene la responsabilidad bancaria en el manejo de los depósitos en cuentas, la entidad financiera debe contar con una póliza que le cubra riesgos de ese tipo, cuáles y en qué eventos o modalidades.

A la par, la entidad pública que deja a disposición los recursos en cuentas maestras no está exenta de contar también con una póliza que cubra el riesgo a que se somete el manejo a través de medios cibernéticos de esos dineros, más aún de reparar en las implicaciones fiscales que surgen para entidades y funcionarios derivado de tal omisión, como se verá en el siguiente capítulo.

Capítulo III. Control Fiscal en materia de los recursos depositados en cuentas maestras

3.1. Regulación general en materia de auditoria

Determinan los artículos 119 y 267 de la Constitución Política de Colombia, que le corresponde a la Contraloría General de la República ejercer la función pública de control fiscal, es decir, vigilar la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes de la Nación, lo cual incluye un control financiero, de gestión y de resultados, que está fundamentado en los principios de eficiencia, economía, equidad y valoración de los costos ambiental y que se realiza en forma posterior y selectiva, conforme a los procedimientos, sistemas y principios que establezca la ley.

En este sentido y para cumplir con esa función el Contralor ha de efectuar las tareas que aparecen en el artículo 268 de la Carta, modificado por el Acto Legislativo 04 de 2019, reglamentado por el Decreto 403 de 2020, como son:

i) exigir informes sobre su gestión fiscal a los empleados oficiales de cualquier orden y a toda persona o entidad pública o privada que administre fondos o bienes públicos;
ii) advertir a los servidores públicos y particulares que administren recursos públicos de la existencia de un riesgo inminente en operaciones o procesos en ejecución, con el fin de prevenir la ocurrencia de un daño, a fin de que el gestor fiscal adopte las medidas que considere procedentes para evitar que se materialice o se extienda, y ejercer control sobre los hechos así identificados;

iii) dictar normas generales para armonizar los sistemas de control fiscal de todas las entidades públicas del orden nacional y territorial; y dirigir e implementar, con apoyo de la Auditoría General de la República, el Sistema Nacional de Control Fiscal, para la unificación y estandarización de la vigilancia y control de la gestión fiscal;

iv) intervenir en los casos excepcionales previstos por la ley en las funciones de vigilancia y control de competencia de las Contralorías Territoriales, lo cual podrá ser solicitado por el gobernante local, la corporación de elección popular del respectivo ente territorial, una comisión permanente del Congreso de la República, la ciudadanía mediante cualquiera de los mecanismos de participación ciudadana, la propia contraloría territorial o las demás que defina la ley;

v) imponer sanciones desde multa hasta suspensión a quienes omitan la obligación de suministrar información o impidan u obstaculicen el ejercicio de la vigilancia y control fiscal, o incumplan las obligaciones fiscales previstas en la ley. Así mismo a los representantes de las entidades que, con dolo o culpa grave, no obtengan el fenecimiento de las cuentas o concepto o calificación favorable en los procedimientos equivalentes para aquellas entidades no obligadas a rendir cuenta, durante dos (2) períodos fiscales consecutivos,

vi) establecer la responsabilidad que se derive de la gestión fiscal, imponer las sanciones pecuniarias que sean del caso, recaudar su monto y ejercer la jurisdicción coactiva, para lo cual tendrá prelación,

vii) ejercer, directamente o a través de los servidores públicos de la entidad, las funciones de policía judicial que se requieran en ejercicio de la vigilancia y control fiscal en todas sus modalidades.

Y en cuanto al seguimiento al recurso público, se determinó que este sería permanente a los bienes, fondos, recursos o intereses patrimoniales de naturaleza pública, para el ejercicio del control concomitante y preventivo, el cual podrá realizarse mediante los mecanismos y ejercicios ordinarios o especiales de vigilancia fiscal, y especialmente mediante los siguientes:

a) Acceso y análisis de la información.
b) Trabajo articulado con el Control Social.
c) Trabajo de la mano con el Control Interno.
d) Acompañamiento en las instancias de asesoría, coordinación, planeación y decisión.
e) Acciones de especial seguimiento.
f) Asistencia con voz a las audiencias de conciliación ante la Procuraduría General de la Nación.
g) Las demás que determine el Contralor General de la República.

Adicionalmente, como lo contempla el artículo 107 de la ley 42 de 1993 "*Los órganos de Control Fiscal verificarán que los bienes del Estado estén debidamente amparados por una póliza de seguros o un fondo especial creado para tal fin, pudiendo establecer responsabilidad fiscal a los tomadores cuando las circunstancias lo ameriten"*.

Norma cuya aplicación se ve reflejada en el Decreto 1793 de 2021, por el cual se liquida el Presupuesto General de la Nación para la vigencia fiscal de 2022, se detallan las apropiaciones y se clasifican y definen los gastos, que fija en su artículo 45 que *"Las entidades estatales podrán constituir mediante patrimonio autónomo los fondos a que se refiere el Artículo 107 de la*

Ley 42 de 1993. Los recursos que se coloquen en dichos Fondos ampararán los bienes del Estado cuando los estudios técnicos indiquen que es más conveniente la cobertura de los riesgos con reservas públicas que con seguros comerciales. Cuando los estudios técnicos permitan establecer que determinados bienes no son asegurables o que su aseguramiento implica costos de tal naturaleza que la relación costo-beneficio del aseguramiento es negativa, o que los recursos para auto protección mediante fondos de aseguramiento son de tal magnitud que no es posible o conveniente su uso para tal fin, se podrá asumir el riesgo frente a estos bienes y no asegurarlos ni ampararlos con fondos de aseguramiento. También podrán contratar un seguro de responsabilidad civil para servidores públicos, mediante el cual se ampare la responsabilidad de los mismos por actos o hechos no dolosos ocurridos en ejercicio de sus funciones, y los gastos de defensa en materia disciplinaria, penal y fiscal que deban realizar; estos últimos gastos los podrán pagar las entidades, siempre y cuando exista decisión definitiva que exonere de toda responsabilidad y no sea condenada la contraparte a las costas del proceso. Esta disposición será aplicada en las mismas condiciones a las Superintendencias, así como a las Empresas Industriales y Comerciales del Estado y a las Sociedades de Economía Mixta asimiladas a estas".

Pudiendo así el Auditor General de la República y las contralorías territoriales solicitar al Contralor General de la República la activación de ejercicios puntuales de vigilancia y seguimiento permanente de los bienes, fondos, recursos o intereses patrimoniales de naturaleza pública cuando en el desarrollo de sus funciones observen riesgos inminentes de daño al patrimonio público.

Frente a la potestad reglamentaria del Contralor General de la República, la Corte Constitucional en sentencia C-384 de 2003 reseñó que la misma *"se limita a aquellos ámbitos expresamente*

mencionados en los numerales 1 y 12 del artículo 268 Superior, es decir, para la prescripción de los métodos y la forma de rendir cuentas los responsables del manejo de los fondos o de bienes de la Nación, indicar los criterios de evaluación financiera, operativa y de resultados que deben seguirse, así como a dictar las normas generales para armonizar los sistemas de control fiscal de todas las entidades públicas del orden nacional y territorial (….) la Constitución le ha atribuido al Contralor General de la República cierta potestad reglamentaria, a fin de que pueda desarrollar la función de vigilancia de la gestión fiscal, prescribiendo los métodos y la forma de rendir cuentas los responsables del manejo de fondos o bienes de la Nación, para que al rendir las cuentas a que están obligados lo hagan de una manera ordenada y sistemática, e indicar los criterios de evaluación que deberán seguirse, así como dictar normas generales para armonizar los sistemas de control fiscal de todas las entidades públicas del orden nacional y territorial, para facilitarles a las contralorías el ejercicio de su función".

En este marco, cumple un papel importante la información que reportan las entidades, así como la regulación propia del asunto a auditar, por eso la Contraloría debe atender no una sino múltiples normativas, reguladoras de la actividad que fiscaliza, como lo son, entre otras, los parámetros de la Ley 80 de 1993,[12] Ley 152 de 1994,[13] Ley 610 de 2000, modificada por el Decreto 403 de 2020,[14] Ley 599 de 2000,[15]. Ley 594 de 2000[16], Ley 1952 de 2019[17], Ley 87 de 1993,[18] Ley 1474

[12] Estatuto General de Contratación de la Administración Pública
[13] Ley Orgánica del Plan de Desarrollo
[14] Por la cual se fija el Trámite de los Procesos de responsabilidad fiscal de competencia de las Contralorías
[15] Código Penal
[16] Ley General de Archivos
[17] Código Disciplinario
[18] Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones

de 2011[19], Ley 1753 de 2015 Plan Nacional de Desarrollo 2014-2018, cuya vigencia no decayó con la Ley 1955 de 2019 (PND 2018-2022), Acto legislativo 04 de 2019,[20] Ley 1122 de 2007,[21] Ley 789 de 2002,[22] Ley 828 de 2003[23].

Al igual que el Decreto 111 de 1996,[24] la Ley 715 de 2001 contentiva de las Normas orgánicas en materia de recursos y competencias para organizar la prestación de los servicios de educación y salud, entre otros; Ley 819 de 2003 relativa a las Normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal; el Decreto 028 de 2008, estrategia de monitoreo, seguimiento y control integral al gasto que se realice con recursos del Sistema General de Participaciones, la Ley 1483 de 2011 que corresponde a las Normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal para las entidades territoriales.

La Normatividad Educación Calidad Matrícula y Calidad, el Decreto 1075 de 2015 Único Reglamentario del Sector Educación, la Guía para la Administración de los recursos financieros del Sector Educativo, Ley 115 de 1994 General de Educación, las Resoluciones del Ministerio de Hacienda y Crédito Público y Reglamentarias de las Cuentas Maestras de las entidades territoriales y sus entidades descentralizadas para la administración de los recursos del SGP de Propósito General, las Asignaciones Especiales y la Asignación para la Atención Integral a la Primera Infancia, entre otras no menos importantes.

[19] Normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
[20] Reforma el Régimen de Control Fiscal
[21] Modificaciones en el Sistema General de Seguridad Social en Salud
[22] Normas para apoyar el empleo y ampliar la protección social y modifican algunos artículos del Código Sustantivo de Trabajo
[23] Normas para el Control a la Evasión del Sistema de Seguridad Social
[24] Estatuto Orgánico de Presupuesto

3.2. Verificación de contratación de seguro por fraudes electrónicos en cuentas maestras desde la perspectiva de control fiscal

Ante la importancia que tiene el control fiscal que despliega la Contraloría a los recursos públicos, como función a través de la cual vigila la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes públicos, se radica en cabeza de ese ente público el establecer la responsabilidad que se derive de la gestión fiscal, imponer las sanciones pecuniarias que sean del caso, recaudar su monto y ejercer la jurisdicción coactiva, para lo cual tendrá prelación.

El objeto de la responsabilidad fiscal es precisamente el de lograr el resarcimiento de los daños ocasionados al patrimonio público como consecuencia de la conducta dolosa o gravemente culposa de quienes realizan gestión fiscal, o con ocasión de esta, mediante el pago de una indemnización pecuniaria que compense el perjuicio sufrido en la economía o patrimonio Estatal

A este respecto, la Corte Constitucional en Sentencia C-338 de 2014, explicó que: *"Esta responsabilidad tiene como finalidad o propósito específico la protección y garantía del patrimonio del Estado, buscando la reparación de los daños que éste haya podido sufrir como consecuencia de la gestión irregular de quienes tienen a su cargo el manejo de dineros o bienes públicos. Con base en el régimen jurídico vigente en cada momento, se han establecido una serie de características predicables de esta forma de responsabilidad. En la jurisprudencia constitucional se ha expresado que la responsabilidad fiscal i) es de naturaleza administrativa; es*

determinada a partir de un proceso de esta misma naturaleza, es decir, un proceso administrativo; iii) no tiene un carácter sancionatorio, sino eminentemente resarcitorio, pues busca recuperar el valor equivalente al detrimento ocasionado al patrimonio de una entidad estatal, teniendo esta suma como límite a exigir; y iv) en este proceso se deben observar las garantías sustanciales y adjetivas propias del debido proceso de manera acorde con el diseño constitucional del control fiscal".

De allí que como ya en sentencia C-735 de 2003 se indicó que: *"(…) Las entidades estatales deben velar porque sus bienes en general estén protegidos contra hechos futuros e inciertos que puedan causarle perjuicio o detrimento al funcionario público. En este sentido, los órganos de control fiscal deben verificar que los bienes públicos, se encuentren asegurados adecuadamente, es decir, que estos tengan la cobertura suficiente, con el fin de que el erario esté cubierto contra cualquier desmedro, que el hecho de un tercero o uno de sus funcionarios pueda ocasionarle, de manera tal que sea resarcido de los daños ocasionados por la ocurrencia del siniestro o riesgo asegurado (…)".*

En este sentido, se muestra de suma importancia las funciones atribuidas a la Contraloría y el deber de los entes que están administrando los bienes y recursos del estado de contar con mecanismos que les permitan evitar la pérdida o daño de aquellos, obligación que incluso está contemplada como uno de los eventos en que se presume responsabilidad fiscal bajo el rasero de la culpa grave (art. 118 de la ley 1471 de 2018).

Sin embargo, es lo cierto que el seguimiento que frente al tema de cuentas maestras en la que se mueven recursos públicos, debe hacerse por este ente público, no abarca o por lo menos así no se puede establecer, que las entidades que registran y manejan cuentas maestras cuenten con un específico aseguramiento frente a eventos cibernético que afecten los recursos, pues se parte de la necesidad de que existan garantías contratadas por las Entidades Territoriales, sin reparar en los amparos con que estas se adquieren y el cumplimiento de las exigencias que ello implica.

Es más, es cuando surgen los eventos que se verifica el tema, encontrando en esta investigación que ciertamente y seguramente por política fiscal, así como en cumplimiento de los deberes legales impuestos, las entidades que administran recursos públicos adquieren sendos productos del mercado asegurador, tal y como es posible consultar a través del aplicativo del plan anual de adquisiciones de cada ente territorial consultable por publicación que se hace en las páginas web oficiales de las mismas y los registros que de ello se hace en el SECOP - Sistema Electrónico para la Contratación Pública, que es el medio de información oficial de toda la contratación realizada con dineros públicos, dentro de los que se destaca, acorde a sus denominaciones los siguientes rangos:

1. Seguros de vida, salud y accidentes
2. Servicios de seguros para estructuras y propiedades y posesiones
3. Seguros de vida
4. Seguro de automóviles o camiones
5. Seguro de equipos electrónicos
6. Seguro de responsabilidad civil
7. seguros de asistencia médica y hospitalización
8. seguros de daños personales por accidente
9. seguros de edificios o del contenido de edificios
10. seguro de garantía de fidelidad
11. seguro de garantía

Sin embargo, el si estos seguros que se contratan incluyen un anexo para afrontar fraudes cibernéticos, no parece estar en la bandeja de prioridades más allá de que como también se muestran en dichas fuentes, las entidades invierten parte de los recursos del presupuesto en la protección de equipos, actualización de softwares y disposición de elementos de seguridad en el tema, siendo necesario que se contara con la citada protección y verificarse esto como un ítem de seguimiento en punto del manejo de cuentas maestras, lo cual debería estar contemplado en las licitaciones que para el efecto se realicen en este sentido.

Capítulo IV. Seguros tomados para la protección de los recursos públicos depositados en cuentas maestras

4.1. Entidades financieras

- Póliza global bancaria

La Póliza Global Bancaria o seguro global bancario, tiene sus orígenes en figuras como los *bankers blanket bonds,* denominados igualmente como *financials institution bonds,* desarrollados por el mercado Lloyd's de Londres y por las *American Bankers association* y *Surety Association* of *American*.

Según ha señalado la doctrina, está diseñada para proteger a las entidades financieras de los riesgos derivados de la infidelidad de sus propios empleados y actos fraudulentos por parte de terceros, caracterizándose porque en su generalidad opera sobre la base del descubrimiento y es como su nombre lo indica, global y de amparos múltiples.

Sin embargo, ese carácter no define por sí misma que esa cobertura lo sea respecto de riesgos no establecidos expresamente en el contrato de seguro, pues hay que recordar lo establecido por el artículo 1056 del Código de Comercio, que dispone la libertad del asegurador de asumir riesgos.

Sus amparos en Colombia van desde el de falsificación de monedas, cheques y títulos valores, infidelidad, daños a bienes propios de la sociedad, sobre los bienes transportados, pérdida dentro

de predios y en lo que a esta investigación importa el de fraude o crimen cibernético[25], que de cara a las cuentas maestras aperturadas en el sector financiero por entidades públicas se encuentra de gran relevancia, por la exposición que estas tienen a ser defraudadas y con ello afectar el dinero del erario público.

Lo anterior no se traduce en que esta póliza sea obligatoria, más allá de que la Superintendencia financiera contemple dentro de los requerimientos mínimos de seguridad el analizar si se requiere contratar un seguro para determinado riesgo, pues en estricto sentido no hay legislación que obligue a las entidades bancarias a contratarlas y dependerá de cada entidad, acorde a sus políticas adquirir las mismas, según lo previsto en el numeral 3º del artículo 185 del Estatuto Orgánico del Sistema Financiero que dispone que: *"En los seguros que tengan por objeto el amparo de los riesgos propios de la actividad financiera, se podrán asegurar, mediante convenio expreso, los hechos pretéritos cuya ocurrencia es desconocida por tomador y asegurador".*

Sin embargo, la misma tan solo de manera reciente comenzó a incluir en sus anexos los amparos encaminados a fungir como garantía en caso de fraudes electrónicos. Esto, por cuanto como se resalta por Jorge Eduardo Narváez Bonnet en su artículo 'Coberturas y tendencias del seguro global bancario', desarrollado en el marco del Congreso de ACOLDESE 2015, en cuanto la póliza global bancaria el "*desarrollo reciente de este tipo de productos en el mercado internacional a diferencia de lo que acontece en frente de las grandes corporaciones bancarias internacionales, en nuestro medio, suelen introducirse clausulados enteros impuestos por el reasegurador que*

[25] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercero, Subsección B, sentencia del 19 de julio de 2013. Rad. 25742. Consejero Ponente: Danilo Rojas Betancourth.

obedecen a formatos estándar, ante la exigencia para el asegurador que la póliza expedida al asegurado se adecue de la manera más fiel y cercana posible al reaseguro contratado. ***De manera que estos productos no resultan estructurados acorde con las exigencias de cada entidad bancaria o financiera, no son delineados a la medida de cada cliente…"*** (se resalta).

A lo que añade que "*Como las pólizas globales bancarias y las coberturas conexas fueron diseñadas para bancos comerciales,* ***otorgan protección respecto de los riesgos propios de la prestación de los servicios bancarios y claro está, no tienen la virtud de cubrir todos los riesgos que puedan estar presentes en el ámbito de las actividades de un banco comercial, porque este tipo de póliza no es más que un componente dentro de todo el programa de seguros****, que, ciertamente, contemplará otros amparos y, por ende, diversas tipos de coberturas de seguros".*

Es más, en ese mismo artículo se resalta *"que el origen de este tipo de pólizas se encuentra en la forma americana No. 24 que fue desarrollada por la American Banker's Association y la Surety Association of America, por lo cual es un referente ineludible cuando se cumple el examen de este tipo de productos; versión americana que ha sido materia de alteraciones, supresiones y adiciones de particular trascendencia, principalmente en el amparo de infidelidad de empleados; modificaciones que obedecen o se justifican, en pronunciamientos de los tribunales americanos que han conducido a los aseguradores a precisar el significado de los riesgos que se pretende amparar a través de ellas, como también, responden a la implantación casi generalizada de la tecnología en las actividades bancarias, con el correlativo aumento de la potencialidad de pérdidas, los cambios en los patrones de defraudación y que, suelen presentar como rasgos*

característicos: la alteración de registros encaminados a la apropiación de fondos; la simulación de operaciones, compras y préstamos".

Y respecto de la adaptación de estas pólizas, ante la realidad de la intervención de las tecnologías en la actividad bancaria, precisa que "*paradójicamente, si bien esa forma americana No. 24 influenció las versiones inglesas (que son precisamente las utilizadas en el mercado local),* ***éstas últimas no han tenido modificación en las últimas décadas.*** *Y como en la hora actual, en la actividad bancaria y financiera se identifican* ***como áreas de mayor exposición, las plataformas tecnológicas y la infidelidad de empleados, las modificaciones de la forma americana No. 24 han obedecido a esas mutaciones en la naturaleza de las operaciones bancarias y a las interpretaciones de algunos tribunales americanos que, en criterio de los aseguradores, desbordaron la finalidad y el propósito de la cobertura inicialmente prevista****"* (se destaca).

Siendo de relevancia para lo que importa a este análisis que como se expone por el citado tratadista "*…la revisión más reciente se cumplió en el año 2004; ocasión en que, entre otras cosas, se restringió la cobertura a transacciones derivadas de documentos físicos (paper transactions), de tal forma que las entidades que requirieran amparo para riesgos electrónicos, instrucciones fraudulentas de transferencias electrónicas y fraude a través de sistemas computarizados, adquirieran la protección a través de los correspondientes anexos".* Refiriendo el mismo doctrinante, que las entidades financieras *"para lograr una protección que resulte tanto integral como eficiente, suelen contratar el anexo de responsabilidad profesional bancaria, el seguro de directores y administradores, y el seguro de fraude por sistemas computarizados".*

Bajo ese contexto, se muestra necesaria la contratación de estos amparos como garantía en caso de fraudes electrónicos para la protección de cuentas maestras y cuyo desarrollo debe estar de la mano con la evolución constante de la tecnología y los riesgos que conlleva, pues precisamente en esta dinámica surgirán las potenciales reclamaciones que habrán de afrontarse de cara a buscar solventar el daño a través de la afectación de las pólizas globales bancarias.

Sobre este tópico tenemos que, como lo destaca el autor que hemos venido citando, el amparo de responsabilidad civil profesional bancaria otorga indemnización al asegurado frente a terceros en la realización de operaciones, cuando se presentan reclamaciones a título de resarcimiento o compensación de daños, lo cual aborda honorarios y gastos en que hubiera incurrido el reclamante.

Tal cubrimiento se muestra importante frente a la problemática que surge del fraude electrónico en la medida que si de lo que se trata es la protección de los dineros del erario público, la entidad está resguardando los rubros confiados en el desarrollo de su actividad y como profesional especialista en la materia, ante situaciones que pueden surgir por una falla propia del sistema operacional, errores u omisiones en que puedan incurrir sus funcionarios en el manejo de la plataforma, desatención de protocolos de seguridad en la realización de operaciones. Eventos que deben estar contemplados en el formulario de solicitud que hace parte del contrato de seguro, en procura que a la hora de acaecer el riesgo no se encuentren con el inconveniente de estar por fuera de las condiciones contratadas.

Precisamente, lo que promueve este estudio es evidenciar que no se trata de tener unos amparos contratados para reflejar que se está cumpliendo con la contratación de un seguro ante riesgos

financieros, sino que los mismos abarquen el riesgo cierto de la actividad y específicamente derivados de fraudes electrónicos que afectan indistintamente todo tipo de productos financieros, pero que frente a las cuentas maestras adquiere aun mayor relevancia dada la naturaleza de los recursos que se manejan a través de las mismas, para que en caso de un siniestro por esta razón no se vean desprovistos de una garantía real y efectiva que llevan al detrimento del erario público o que generen un desgaste ritualista y técnico frente al contrato de seguro contratado donde lo último que se espera es que se genere un debate acerca del cubrimiento o no de la póliza.

Por su parte y de manera paralela, como se sintetiza en el artículo en cuestión, al que hemos venido haciendo referencia, está el anexo de seguro de fraude por sistemas computarizados, el cual brinda cobertura con ocasión a actos dolosos de terceros cometidos contra el asegurado que resulten "*en transferencia, pago o entrega de dineros o de bienes, los cuales pueden obedecer a pagos realizados de la cuenta de un cliente por manipulación del sistema de cómputo del asegurado; por el ingreso fraudulento de datos o de instrucciones; o por destrucción de datos; o por la introducción de virus; o por haber confiado en comunicaciones electrónicas autorizando pagos o transferencias o la entrega de bienes, o dirigidas a un depósito centralizado de valores autorizando la compra, venta o pignoración de un título; o por razón de un tele-facsímil o por instrucciones verbales o telefónicas que aparezcan fraudulentamente realizadas por una persona autorizada".*

Este impone a la entidad financiera un ejercicio profesional importante, pues, se insiste, no se trata únicamente de contratar una póliza, sino de integrar procesos internos de verificación a sus sistemas de forma continua y rigurosa que le permitan establecer los riesgos que asume los

potenciales que surjan y la capacidad de respuesta que ha de tener, con lo cual garantiza en el caso del manejo de recursos públicos que no sufrirá pérdidas por reclamaciones derivadas de actos de defraudación a cuentas maestras o que estos podrán ser advertidos de manera oportuna, minimizando el riesgo en este sentido.

La relevancia del desarrollo de este tipo de amparos se muestra determinante para mitigar la defraudación a través de canales electrónicos, dado que como se resalta y reconoce en el medio asegurador los clausulados en materia de riesgos financieros han sido los mismos durante más de dos décadas, en donde la intermediación financiera era de prevalencia presencial y se ajustaba a los medios que en su momento eran novedosos, como giro de cheques, facsímiles, etc., los que con el desarrollo de las tecnologías tienen tendencia a su extinción. Y no podría ser de otra manera, si en cuenta se tiene que la aplicación de las tecnologías propicia una mayor y mejor funcionalidad en la prestación del servicio bancario que no puede detenerse, pero habrá de resguardarse al mismo ritmo, pues de lo contrario estaría desprovista de seguridad, que al fin y al cabo es el mayor pedimento de quienes acceden al sistema financiero.

Esa tendencia se ha hecho visible en decisiones que resuelven controversias jurisdiccionales, a manera de ejemplo: el laudo arbitral del 22 de diciembre de 2020, emitido dentro del Tribunal de Arbitramento promovido por Administradora Colombiana de Pensiones COLPENSIONES contra AXA COLPATRIA SEGUROS S.A., radicado 15943, en el que se señaló:

“el uso cada vez más frecuente de los servicios intermediación financiera y la creciente complejidad en el desarrollo de tales actividades, han generado un consecuente aumento de los

riesgos a los que se ven expuestos tanto los usuarios como las entidades prestadoras de esos servicios. Como estas se dedican de manera profesional al manejo de recursos del público, principalmente mediante operaciones de captación y colocación, enfrentan diversos riesgos relacionados con la administración de los respectivos capitales. Entre estos riesgos se encuentran, por ejemplo: los actos deshonestos de sus empleados; la pérdida de bienes que se encuentran dentro de las oficinas del asegurado; la pérdida de bienes que están siendo trasladados de un lugar a otro; o la falsificación de monedas, cheques u otros títulos valores, entre los más destacados. Es en este contexto que se han desarrollado los denominados 'seguros globales bancarios', que por regla general tienen por objeto proteger el patrimonio de entidades financieras en caso de que se concrete alguno de los riesgos que son inherentes al giro ordinario de sus negocios. Sin embargo, en la práctica, la contratación de estos seguros también se ha extendido para amparar la actividad de personas que administran o gestionan recursos del público pero que no son propiamente establecimientos de crédito (…)

Respecto de este tipo de seguro el Consejo de Estado ha señalado que debido a los diversos riesgos a los que están expuestas las entidades financieras 'el sistema asegurador mundial-incluido el Colombiano- creó y ofreció para la actividad bancaria un seguro que busca proteger a estas entidades de los riesgos que son propios de este tipo de negocios (…) esta póliza, si se analizan sus coberturas, cubre riesgos disímiles, no obstante que alcanzan a especializarse, en virtud de la experiencia adquirida por las aseguradoras en este campo, lo que hace que adquieran características propias diseñadas para ella'[26]*. Su finalidad es, entonces 'proteger los valores y ofrecer seguridad a la gestión ordinaria de los bienes y personas que se relacionan con el sistema*

[26] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Sentencia del 6 de julio de 2005. Rad. 11575. Consejero Ponente Alior Eduardo Hernández Enríquez.

financiero"[27]*. Como se puede observar, los riesgos que se amparan mediante los seguros globales bancarios son, en principio, aquellos que son propios o que están directamente relacionados con la actividad financiera y que puedan afectar patrimonialmente a la entidad asegurada. La principal característica que distingue a esta modalidad de seguro es que es 'global', es decir, comprende el amparo de una multiplicidad de riesgos, de ordinario, implicaría la celebración de múltiples contratos de seguro para ampararlo".*

Así mismo, la Sala de Casación Civil de la Corte Suprema de Justicia al referirse en su jurisprudencia sobre los orígenes y regulación de este tipo de seguro, ha señalado lo siguiente:

"2.1. en respuesta a las necesidades de garantía de las instituciones financieras entre las cuales se encuentran los almacenes generales de depósito, el mercado asegurador les ofrece pólizas conocidas con el nombre de 'globales bancarias'.

El adjetivo 'global' con el que se clasifica al indicado instrumento hace referencia a que su característica principal es la de contener varios y disímiles amparos que normalmente serían objeto de cobertura a través de pólizas independientes, los cuales, por ejemplo pueden ser (i) infidelidad de los empleados. Cubre los actos deshonestos de los empleados (…) (iii) falsificación de moneda, cheques y títulos valores (…) debido a las grandes cantidades de dinero que son objeto de aseguramiento se hizo necesaria la contratación de reaseguros con compañías multinacionales

[27] Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección B, Sentencia del 25 de septiembre de 2017. Rad. 34563. Consejero Ponente Estella Conto Díaz del Castillo.

las cuales han impuesto sus propias proformas, siendo las más utilizadas la No. 24 empleada en el mercado asegurador norteamericano, y los clausulados DHP, KFA, NMA y LSW.

El primero, en sus versiones 73, 75, 82 y 84, el segundo y el tercero en sus versiones 81 y 2626 respectivamente, aluden al amparo de infidelidad, en tanto los textos tipo LSW238 y 983 otorgan cobertura respecto de delitos electrónicos y por computador, y el clausulado MNA2273 es de responsabilidad civil profesional.

En razón a que el término global dio lugar a que se interpretara que la cobertura se extendía a riesgos no establecidos expresamente en ella, su denominación ha sido sustituida por otras como 'póliza de instituciones financieras', o 'de riesgos financieros'.

En Colombia, en lo concerniente a la infidelidad, las formas más utilizadas corresponden a las NMA2626, DHP84 y KFA81, que aluden a actos fraudulentos o deshonestos de empleados, cometidos por ellos directamente o en complicidad con otros, con la intención de ocasionar una pérdida a la asegurada o de obtener una ganancia propia indebida"[28]

Así entonces, este tipo de póliza si bien corresponde a un seguro de origen y construcción foránea, cuyos clausulados están estructurados y ajustados de manera regular a la operación del mercado, fue delineado en principio para amparar a los establecimientos financieros frente a riesgos

[28] Corte Suprema de Justicia Sala de Casación Civil. Sentencia SC18594-2016 del 19 de diciembre de 2016. MP. Ariel Salazar Ramírez.

relacionados con su actividad, pero su contratación no es exclusiva de aquellos, en tanto es posible que personas que no se dedican a tal actividad la contraten[29].

Sus amparos pueden ser instrumentados con el nombre de 'manejo y riesgos financieros' o 'infidelidad y riesgos financieros', cuyo fundamento normativo se encuentra en el artículo 23 de la ley 35 de 1993, recogido en el antes citado numeral 3º del artículo 185 del Estatuto Orgánico del Sistema Financiero (Decreto 663 de 1993) cuyo alcance fue fijado por el artículo 4º de la ley 389 de 1997 y el artículo 203 del anotado estatuto (EOSF).

En este sentido como se precisó en las decisiones judiciales que trajimos a colación en párrafos precedentes, puntualmente en cuanto a la naturaleza jurídica del seguro de riesgos financieros "…*pertenece al género de los seguros de daños, toda vez que está destinado a proteger el patrimonio del asegurado de menoscabos o detrimentos que pueda sufrir como consecuencia de circunstancias que sean materia de coberturas pactadas…"*[30], lo cual por demás se acompasa con las previsiones del artículo 1082 y siguientes del Código de Comercio.

- Coberturas en materia de riesgo electrónico

En lo que tiene que ver con las coberturas básicas de las pólizas globales bancarias, como se explicara en precedencia, han obedecido en el tiempo en general a las siguientes:

[29] Ver, por ejemplo: Tribunal arbitral de Whirpool Colombia S.A.S y Shubb Seguros S.A. laudo de 25 de noviembre de 2019. Arbitro único Jorge Eduardo Narváez Bonnet. Tribunal arbitral de Quala S.A. y Shubb de Colombia Compañía de Seguros S.A. Laudo 15 de noviembre de 2019. Arbitro único Carlos Ignacio Jaramillo Jaramillo.
[30] Op. Cit. 28

1. Infidelidad de empleados.
2. Predios.
3. Tránsito.
4. Falsificación.
5. Falsificación de moneda.
6. Responsabilidad profesional.

No obstante, el presente estudio está encaminado a destacar aquellas coberturas cuya relación está directamente relacionada con riesgos financieros por causa de fraudes electrónicos y específicamente en procura de salvaguardar los recursos públicos que se manejan a través de las cuentas maestras.

Para el efecto, previo a destacar lo pertinente es de reseñar que, realizada la investigación correspondiente, se advierte que en general las entidades financieras, trátense de Bancos denominados como de primer y segundo piso cuentan con una póliza global bancaria, pero ese no es el aspecto que se pretende aquí relievar, realmente lo perseguido con este análisis es destacar la necesidad de contar con unas coberturas que se incluyan en este tipo de aseguramiento para la protección de los dineros que se manejan en las cuentas maestras frente a la realidad de los avances tecnológicos e informáticos y que más allá de la rigurosidad establecida para la realización de operaciones financieras, no están exentos de verse afectados en algún momento por un fraude electrónico, el cual valga señalar no sería como el que sufriría cualquier cuentahabiente, no solo porque son dineros provenientes de los contribuyentes -dentro de los que forma parte el suscrito-, sino por su gran cuantía, que en caso de verse sustraídos producirían una afectación directa a

ámbitos como la salud, educación, asignación a territorios indígenas, entre otros, donde la generalidad obedece a población vulnerable cuya protección está en cabeza del Estado.

Es más, si de lo que se trata es que las cuentas maestras son un mecanismo para evitar que el flagelo de la corrupción principalmente se vea controlado, no puede, entonces, abrirse otra puerta donde los recursos recaudados por la sociedad para el ejercicio del bienestar general, queden expuestos ante terceros mal intencionados que se aprovechan de la novedad e inherente evolución de la informática y la tecnología, cuyo entramado delictual se dedica precisamente a encontrar esas brechas que pueden darse por negligencia de los funcionarios de las entidades financieras y públicas en el manejo de los sistemas electrónicos, fallas en los protocolos de seguridad, nuevos modelos de fraude electrónico, no actualización de los sistemas de seguridad, entre otros.

Así las cosas, según lo que se pudo determinar en el mercado, en el momento existen pólizas globales bancarias y anexos que se ajustan a la necesidad de proteger los recursos depositados en entidades financieras y especialmente en lo que tiene que ver con cuentas maestras que en el marco de este estudio considero deben tener los bancos en los que se aperturen este tipo de productos, sin perjuicio de las especiales consideraciones que se insertan en sus exclusiones, como ya tendré oportunidad de indicar.

De las entidades aseguradoras del país se encontró que la POLIZA DE SEGURO DE MANEJO GLOBAL BANCARIO que ofrece AXA COLPATRIA SEGUROS S.A. cuyo TOMADOR y

asegurado es SCOTIABANK COLPATRIA S.A. vigente para 2021 tiene contratados los siguientes amparos, discriminados en tres secciones:

Condiciones:

Sección 1: póliza global bancaria texto DHP 84 incluyendo infidelidad de empleados

Coberturas:

1. Infidelidad de empleados
2. En predios
3. En tránsito
4. Falsificación o alteración
5. Falsificación extendida
6. Moneda falsificada
7. Pérdidas de derechos de suscripción
8. Cajillas de seguridad. agradecemos que el asegurado confirme si en sus planes esta prestar este servicio a sus clientes, o indicar la razón por la cual requiere esta cobertura para proceder a su activación.

Sección 2: cláusula de pérdidas a través de sistemas de cómputo (LSW-983) cláusulas del 1 al 9 para los sistemas usados por el asegurado, haciendo parte del agregado anual.

Coberturas:

1. Sistemas computarizados
2. Operaciones de la oficina de servicios del asegurado
3. Instrucciones electrónicas por computador
4. Equipos y datos electrónicos
5. Virus de computador
6. Comunicaciones electrónicas
7. Transmisiones electrónicas
8. Títulos valores electrónicos
9. Telefacsímiles falsificados

Para el análisis que nos comporta, son de especial relevancia aquellos apartes que están incluidos en la sección dos, partiendo de las cláusulas y definiciones que se prevén para ellos.

I. Cláusulas de seguro

Cláusula de seguro 1 - sistemas de computación: En razón de que el asegurado haya transferido, pagado o entregado fondos o propiedad, establecido cualquier crédito, debitado alguna cuenta u otorgado cualquier valor como resultado directo de

(a) el ingreso fraudulento de datos electrónicos directamente en:

(i) el sistema de computación del asegurado, o
(ii) el sistema de computación de una oficina de servicios, o
(iii) cualquier sistema de transferencia electrónica de fondos, o
(iv) un sistema de comunicaciones del cliente; o

(b) la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados dentro o procesados dentro de cualquiera de los sistemas arriba indicados o durante una transmisión electrónica al sistema de computación del asegurado o al sistema de computación de una oficina de servicios; o

(c) el ingreso fraudulento de datos electrónicos a través de un sistema de banca telefónica, directamente al sistema de computación del asegurado

Y que tales actos fraudulentos hayan sido ordenados o cometidos por una persona con la intención de causar una pérdida al asegurado u obtener ganancia financiera para sí mismo o para cualquier otra persona.

Cláusula de seguro 2 - programas electrónicos de computación. En razón de que el asegurado haya transferido, pagado o entregado fondos o propiedad, establecido cualquier crédito, debitado alguna cuenta u otorgado cualquier valor como resultado directo de la preparación fraudulenta o la modificación fraudulenta de programas electrónicos de computación, y que tales actos fraudulentos hayan sido ordenados o cometidos por una persona que intentaba causar que el asegurado sufriera una pérdida, o que tratara de obtener una ganancia financiera para sí misma o para cualquier otra persona.

Cláusula de seguro 3 - datos y medios electrónico. En razón de:

(a) la alteración o destrucción maliciosa, o el intento de ella, de datos electrónicos por cualquier persona mientras los datos electrónicos se encuentran almacenados dentro del sistema de computación del asegurado o del sistema de computación de una oficina de servicios o mientras están registrados en medios electrónicos de procesamiento de datos dentro de las oficinas o predios del asegurado o en custodia de una persona designada por el asegurado para actuar como su mensajero (o de una persona que actúe como mensajero o custodio durante una emergencia que surja de la incapacidad de dicho mensajero designado), mientras que los medios electrónicos de procesamiento de datos sobre los cuales se encuentren registrados tales datos electrónicos estén en tránsito en cualquier parte, iniciando tal tránsito inmediatamente después del recibo de tales medios de procesamiento electrónico de datos por parte de dicho mensajero y finalizando inmediatamente después de la entrega de los mismos al destinatario designado o a su agente, previsto que el

asegurado sea el dueño de tales datos electrónicos o de tales medios electrónicos de procesamiento de datos, o sea legalmente responsable por su pérdida o daño;

(b) el extravío, daño o destrucción de medios electrónicos de procesamiento de datos como resultado directo de robo, hurto, latrocinio, extravío, desaparición misteriosa e inexplicable o acto malintencionado mientras los medios electrónicos se encuentran alojados o depositados dentro de oficinas o predios localizados en cualquier parte, o en custodia de una persona designada por el asegurado para que actúe como su mensajero (o de una persona que actúe como mensajero o custodio durante una emergencia que surja de la incapacidad de dicho mensajero designado), mientras que los medios electrónicos de procesamiento de datos sobre los cuales se encuentren registrados tales datos electrónicos estén en tránsito en cualquier parte, iniciando tal tránsito inmediatamente después del recibo de tales medios de procesamiento electrónico de datos por parte de dicho mensajero y finalizando inmediatamente después de la entrega de los mismos al destinatario designado o a su agente, previsto que el asegurado sea el dueño de tales datos electrónicos o de tales medios electrónicos de procesamiento de datos, o sea legalmente responsable por su pérdida o daño;

(c) alteración o destrucción malintencionada de programas electrónicos de computación mientras se encuentran almacenados dentro del sistema de computación del asegurado, previsto que el asegurado sea el propietario de tales programas electrónicos de computación o sea legalmente responsable por su pérdida o daño.

Cláusula de seguro 4 - virus de computación. En razón de:

(a) que el asegurado haya transferido, pagado o entregado fondos o propiedad, establecido cualquier crédito, debitado alguna cuenta u otorgado cualquier valor como resultado directo de la destrucción, o un intento de ella, de datos electrónicos del asegurado debido a un virus de computación causado por cualquier persona mientras que tales datos electrónicos se encuentren almacenados dentro del sistema de computación del asegurado o el sistema de computación de una oficina de servicios; y

(b) la destrucción, o un intento de ella, de los datos electrónicos del asegurado como resultado de un virus de computación causado por cualquier persona mientras tales datos electrónicos se encuentran almacenados dentro del sistema de computación del asegurado o el sistema de computación de una oficina de servicios.

Cláusula de seguro 5 - comunicaciones electrónicas y por fax. En razón de que el asegurado haya transferido, pagado o entregado fondos o propiedad, establecido cualquier crédito, debitado alguna cuenta u otorgado cualquier valor sobre la fe de cualquiera comunicación electrónica dirigidas al asegurado autorizando o reconociendo la transferencia, pago, entrega o recepción de fondos o propiedad, cuyas comunicaciones fueron transmitidas o parecieron haber sido transmitidas

(a) a través de un sistema electrónico de comunicación, ó

(b) por fax, telex, twx o medio similar de comunicación directamente al sistema de computación del asegurado o al terminal de comunicaciones del asegurado y que fraudulentamente aparenten haber sido enviadas por un cliente, cámara de compensación automática, una oficina del asegurado, u otra institución financiera pero que tales comunicaciones no fueron enviadas por dicho cliente, cámara compensadora automática, una oficina del asegurado, ni por otra institución financiera o fueron modificadas fraudulentamente durante el tránsito físico de los medios electrónicos de procesamiento de datos al asegurado o durante la transmisión electrónica al sistema de computación del asegurado o a la terminal de comunicaciones del asegurado.

Condición especial: Todo fax, telex, twx o medio similar de comunicación mencionado en el párrafo (b) anterior deberá ser probado o sujeto a una llamada de verificación (call-back) a una persona autorizada diferente de la persona que inició la solicitud de transferencia y también tal fax deberá portar una firma falsificada o alteración fraudulenta.

Cláusula de seguro 6 - transmisiones electrónicas. En razón de que un cliente del asegurado, una cámara de compensación automática u otra institución financiera haya transferido, pagado o entregado fondos o propiedad, establecido cualquier crédito, debitado cualquier cuenta o dado cualquier valor

(a) sobre la fe de cualquier comunicación electrónica que pretenda haber sido dirigida por el asegurado a su cliente, una cámara de compensación automática o una institución financiera, autorizando o reconociendo la transferencia, pago, entrega o recepción de fondos o propiedad cuyas comunicaciones fueron transmitidas o aparentan haber sido transmitidas a través de un sistema de comunicación electrónica, o por fax probado, telex probado, twx probado o método similar de comunicación cifrada directamente en un sistema de computación o una terminal de computación de dicho cliente, cámara de compensación automática o institución financiera e indiquen fraudulentamente haber sido enviadas por el asegurado o fueron el resultado directo de la modificación fraudulenta de datos electrónicos durante el tránsito físico de medios electrónicos de procesamiento de datos del asegurado o durante la transmisión electrónica de los sistemas de computación del asegurado o del terminal de comunicaciones del asegurado; o

(b) como resultado directo del ingreso fraudulento, la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados dentro de ó siendo procesados dentro del sistema de computación del asegurado o durante la transmisión electrónica del sistema de computación del asegurado al sistema de computación del cliente mientras el asegurado está actuando como oficina de servicios para dicho cliente;

Y por cuya pérdida el asegurado es legalmente responsable ante el cliente, la cámara de compensación automática o la institución financiera.

Cláusula de seguro 7 - títulos valores electrónicos. En razón de que un depositario central haya transferido, pagado o entregado fondos o propiedad o debitado alguna cuenta del asegurado, sobre la fe de cualquier comunicación electrónica que pretenda haber sido dirigidas por el asegurado al depositario central autorizando la transferencia, pago o entrega

de dichos fondos o propiedad, o el débito de la cuenta del asegurado en relación con la compra, venta, transferencia o prenda de un títulos valor electrónico, cuyas comunicaciones fueron transmitidas o aparentan haber sido transmitidas

(a) a través de un sistema de comunicación electrónica, o

(b) por fax probado, telex probado, twx probado o medio similar de comunicación probada directamente a un sistema de computación o un terminal de comunicaciones de dicho depositario central y que fraudulentamente pretenda haber sido enviado por el asegurado al depositario central pero cuyas comunicaciones no fueron enviadas por el asegurado al depositario central o fueron modificadas fraudulentamente durante el tránsito físico de medios electrónicos de procesamiento de datos desde los predios del asegurado o durante la transmisión electrónica del sistema de computación del asegurado o del terminal de comunicaciones del asegurado al depositario central y por cuya pérdida el asegurado es legalmente responsable ante el depositario central.

Cláusula de seguro 8 - instrucciones iniciadas por voz. En razón de:

(a) que el asegurado haya transferido cualesquiera fondos o entregado cualquier propiedad sobre la fe de instrucciones iniciadas por voz dirigidas al asegurado autorizando la transferencia de fondos o la entrega de cualquier propiedad en la cuenta de un cliente hacia otros bancos para acreditarlos a personas supuestamente designadas por el cliente y cuyas instrucciones fueron efectuadas por teléfono a aquellos empleados del asegurado específicamente autorizados para recibir dichas instrucciones en las oficinas del asegurado y que fraudulentamente pretendan haber sido efectuadas por una persona autorizada y designada por un cliente para solicitar telefónicamente la transferencia de tales fondos o la entrega de tales propiedades pero cuyas instrucciones no fueron efectuadas por dicho cliente ni por cualquier administrador, miembro de junta directiva , socio o empleado de dicho cliente o fueron efectuadas fraudulentamente por un administrador, miembro de junta directiva , socio o empleado de dicho cliente cuyas funciones, responsabilidades o autoridad no le permitían realizar, iniciar, autorizar, validar o autenticar las instrucciones iniciadas por voz del cliente, y actos fraudulentos que fueron cometidos por dicha persona con la intención de causar que el asegurado o el cliente sufriera una pérdida o para obtener una ganancia financiera para sí misma o para cualquier otra persona

(b) que el asegurado haya transferido cualesquiera fondos o entregado cualquier propiedad sobre la fe de instrucciones iniciadas por voz comunicadas supuestamente entre las oficinas del asegurado autorizando la transferencia de fondos o la entrega de cualquier propiedad en la cuenta de un cliente entre las oficinas del asegurado para acreditarlos a personas supuestamente designadas por el cliente y cuyas instrucciones aparentaban haber sido hechas supuestamente a través del teléfono entre las oficinas del asegurado a aquellos empleados del asegurado específicamente autorizados a recibir dichas instrucciones entre oficinas por teléfono, y que fraudulentamente pretendían haber sido realizadas por un empleado del asegurado autorizado a solicitar telefónicamente tal transferencia de fondos o la entrega de propiedad pero cuyos actos fraudulentos fueron cometidos por una persona, diferente de un empleado del asegurado, quien trató de causar que el asegurado o el cliente

sufrieran una pérdida o de obtener ganancia financiera para sí o para cualquier otra persona.

Coberturas que se ajustan al escenario de protección tantas veces reseñado en este documento respecto de cuentas maestras, sin perder de vista que como se destaca en la redacción de estas, tienen una especial relevancia el formulario de solicitud del seguro más cuando se trata de un producto tan parametrizado para la inscripción, registro y realización de las operaciones, el cual debería ajustarse al contexto exigido.

No obstante, dentro de las exclusiones que se consignan en este clausulado, como se destaca a continuación, resulta contradictorio que están eliminados de cobertura precisamente los riesgos inherentes al tipo de operación y canales utilizados para la recepción y dispersión de los recursos destinados a cuentas maestras.

En efecto, se lee de dicho clausulado, que le es aplicable a la sección 2 únicamente crimen por computador:

1. texto original de lloyd´s para delitos electrónicos LSW983 Se aclara que se incluyen las transacciones iniciadas por voz, sujeto a que exista segregación de funciones y que todas las llamadas sean grabadas.

2. la cobertura se extiende a incluir las operaciones por internet del asegurado según nma 2856, como se anexa.

3. se excluyen **pérdidas originadas por phishing e ingeniería social**.

4. anexo de costos de limpieza, según texto adjunto.

25/05/2000 NMA 2856 exclusión absoluta de phishing, pharming y eventos similares o relacionados

> Se excluyen las pérdida(s) proveniente(s) directa o indirectamente por razón de, o en conexión con, los sistemas de computadoras, equipo electrónico o redes de comunicación de propiedad o usados por los clientes del asegurado que hayan sido comprometidos y/o hackeados y/o objeto de phishing, afectados perjudicialmente o saboteados por terceros/defraudadores; y/o información sensitiva de clientes que haya sido filtrada y/o suministrada por los clientes a terceros o cualquier técnica de ingeniería social diseñada para engañar al usuario para que entregue información personal incluyendo, pero sin limitarse, a lo siguiente:
>
> a) la preparación o la modificación fraudulentas de programas de computadora electrónica dentro del sistema de computadoras de propiedad o usadas por un cliente del asegurado;
>
> b) la entrada fraudulenta de datos electrónicos directamente al sistema de computadoras de propiedad o usadas por un cliente del asegurado;
>
> c) la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados dentro o siendo corridos dentro del sistema de computadoras de propiedad o usados por un cliente del asegurado;
>
> d) un cliente del asegurado suministrando información del cliente a terceros como respuesta a comunicaciones electrónicas que fraudulentamente aparenten haber sido enviadas por el asegurado;
>
> e) un cliente del asegurado suministrando información del cliente a terceros mediante la entrada de la información del cliente en websites falsos que son designados para simular el website real del asegurado(s) y para engañar a los clientes para que entreguen información personal;
>
> f) un cliente del asegurado suministrando información a terceros como respuesta a técnicas de ingeniería social diseñadas para engañar a los clientes para que entreguen información personal.

Se destaca entonces, que esta póliza a pesar de sus cubrimientos su buen diseño y previsiones, no resultaría suficiente a la hora de verse enfrentada la entidad financiera a una reclamación por una operación producto de un ataque cibernético a una cuenta maestra. Y es por esta razón que como se abordará en el siguiente capítulo se hace necesario no solo que la entidad bancaria cuente con una cobertura respecto de fraudes electrónicos, sino que también lo tenga la entidad territorial que apertura una cuenta maestra.

Otra póliza que circula en el mercado asegurador, que se destaca por venir gestionando adaptaciones a la realidad financiera, es la ofrecida por CHUBB - FORMA DHP –84 AMPARO ADICIONAL DE CRIMEN POR COMPUTADOR LSW 983 MODIFICADO 14/09/2020-1305-P-13-CLACHUBB20160108-000I14/09/2020-1305-A-13, que cuenta con los siguientes amparos:

1. Sistemas de computadoras por que el asegurado haya transferido, pagado o entregado cualquier suma de dinero o propiedad, otorgado crédito, debitado cualquier cuenta o dado cualquier valor como resultado directo de:

1.1. El ingreso fraudulento de datos electrónicos directamente en:

i) el sistema informático del asegurado; o
ii) un sistema informático de la oficina de servicios; o
iii) un sistema electrónico de transferencia de fondos; o
iv) un sistema de comunicaciones del cliente.

1.2. La modificación o destrucción fraudulenta de datos electrónicos almacenados o siendo ejecutados dentro de cualquiera de los sistemas anteriores o durante la transmisión electrónica a través de líneas de comunicación de datos incluyendo enlaces satelitales al sistema informático del asegurado o un sistema informático de la oficina de servicios.
1.3. El ingreso fraudulento de datos electrónicos a través de un sistema de banca telefónica, directamente al sistema informático del asegurado siempre que tales actos fraudulentos sean cometidos por una persona con la intención de causar que el asegurado sufra una pérdida o para obtener una ganancia financiera para si mismo o para cualquier otra persona.

2. Programas electrónicos para computador: por razón de que el asegurado haya transferido, pagado o entregado cualquier suma o propiedad, establecido cualquier crédito, debitado cualquier cuenta o dado valor como resultado directo de una preparación fraudulenta o la modificación fraudulenta de programas electrónicos para computador cuyos actos fraudulentos fueron ordenados o cometidos por una persona cuya intención era la de causar que el asegurado soportara dicha pérdida o la obtención de una ganancia financiera para sí mismo o cualquier otra persona.

3. Equipos y datos electrónicos:

3.1. Por razón y como resultado de alteración o destrucción dolosa o intento o amenaza de tales datos electrónicos por cualquier persona mientras que los datos electrónicos estén guardados dentro del sistema de computadores del asegurado o en un sistema de una red

de servicios intercambiarios o mientras está siendo grabada en un sistema electrónico de procesamiento de datos dentro de las oficinas o los predios del asegurado o bajo la custodia de una persona designada por el asegurado para que actué como su mensajero (o una persona actuando como mensajero o que deba custodiar durante una emergencia que surja de la incapacidad de tal mensajero) mientras que el procesador electrónico de datos en el que tal información está siendo guardada se encuentre en tránsito deberá comenzar inmediatamente con la recepción del receptor designado o de su agente, dado que el asegurado sea el dueño de dicho procesamiento electrónico de datos o sea legalmente responsable por dicha pérdida o daño.

3.2. Por razón de que los equipos o datos electrónicos sean extraviados, dañados o destruidos como el resultado directo de hurto o desaparición misteriosa e inexplicable o acto malintencionado, desaparecimiento mientras que el procesador electrónico de datos es guardada o depositado dentro de las oficinas o predios localizados en cualquier parte, o en la custodia designada por el asegurado para actuar como su mensajero (o un apersona actuando como mensajero o custodiando durante una emergencia que surja como consecuencia de la incapacidad de dicho mensajero designado) mientras que los datos de procesamiento electrónico están en tránsito en cualquier lugar, dicho tránsito debe iniciar inmediatamente con la recepción de dichos datos de procesamiento electrónico por dicho mensajero, y deberá terminar inmediatamente con la entrega al correspondiente receptor o agente, dado que el asegurado sea el propietario de dicho procesamiento electrónico de datos o sea legalmente responsable por tal pérdida o daño; y

3.3. La adulteración o destrucción dolosa de programas electrónicos para computador mientras se encuentren almacenados dentro del sistema informatico del asegurado, previsto que el asegurado sea el dueño de tales programas electrónicos para computadoras o sea legalmente responsable por su pérdida o daño.

4. Virus informático:

4.1. Porque el asegurado haya transferido, pagado o entregado cualquier suma de dinero o propiedad, otorgado crédito, debitado cualquier cuenta o dado cualquier valor como resultado directo de la destrucción, o el intento de hacerlo, de los datos electrónicos del asegurado debido a un virus informático causado por cualquier persona mientras que tales datos electrónicos estén almacenados dentro del sistema informático del asegurado o un sistema informático de la oficina de servicios.

4.2. Por la pérdida de los datos electrónicos del asegurado como resultado de su destrucción, o el intento de hacerlo, debido a un virus informático causado por cualquier persona mientras que tales datos electrónicos estén almacenados dentro del sistema informático del asegurado o un sistema informático de la oficina de servicios.

6. Transmisiones electrónicas:

6.1. Porque un cliente del asegurado, una Cámara de compensación automatizada o una institución financiera haya transferido, pagado o entregado cualquier suma de dinero o

propiedad, otorgado crédito, debitado cualquier cuenta o dado valor confiando en cualquier comunicación electrónica pretendiendo haber sido dirigida por el asegurado a su cliente, una Cámara de compensación automatizada o una institución financiera autorizando o aceptando la transferencia, pago, entrega o recibo de suma de dinero o propiedad cuyas comunicaciones fueron transmitidas o aparenten haber sido trasmitidas:

A través de un sistema de comunicación electrónico; o Por tele facsímil probado, télex probado, twx probado o medios similares de comunicación probados. Directamente a un sistema informático o una terminal de comunicaciones de dicho cliente, Cámara de compensación automatizada o institución financiera y fraudulentamente parezcan haber sido enviadas por el asegurado o fueron el resultado directo de modificación fraudulenta de los medios de procesamiento electrónica de datos durante el transito físico de los medios de procesamiento electrónico de datos desde el asegurado o durante la transmisión electrónica desde el sistema informático del asegurado o la terminal de comunicaciones del asegurado; o

6.2. Como resultado directo del ingreso fraudulento, la modificación fraudulenta o la destrucción fraudulenta de datos electrónicos almacenados dentro de, o siendo procesados en el sistema informático del asegurado o durante la transmisión electrónica desde el sistema informático del asegurado hacia el sistema informático del cliente mientras el asegurado esté actuando como una oficina de servicios para dicho cliente; y por cuya pérdida el asegurado sea legalmente responsable ante el cliente, la cámara de compensación automatizada o la institución financiera.

Este Amparo adicional de Crimen por Computador según se lee del mismo, está diseñado para que sea una póliza acompañante para la Póliza Global de Instituciones Financieras del Asegurado, y su propósito es proveer cobertura contra delitos relacionados con computadores, los cuales no están amparados bajo la Póliza Global de Instituciones Financieras del Asegurado.

De modo expreso refiere que este amparo no cubre o excluye, entre otras circunstancias, las siguientes:

- Pérdida resultante de cualquiera de los riesgos cubiertos por la póliza global de entidades financieras a los que este amparo adicional se adhiere.
- Pérdida de datos electrónicos o medios de procesamiento electrónico de datos, excepto por lo establecido en la condición general (k).
- Pérdida resultante directa o indirectamente de:
    - Instrucciones o consejos escritos, o
    - Instrucciones o consejos telegráficos o por cable, o

    - Instrucciones o consejos por voz a través de teléfono, a menos que tales instrucciones estén cubiertas bajo el amparo 8, o
    - Instrucciones o consejos por tele facsímil a menos que tales instrucciones o consejos por tele facsímil están cubiertos bajo el amparo 5, 6, o 7.
- Pérdida resultante directa o indirectamente de instrumentos negociables, títulos valores, documentos o instrumentos escritos falsificados, alterados o fraudulentos, usados como fuente de documentación en la preparación de datos electrónicos o tecleados manualmente en una terminal de datos.
    - Pérdida resultante directa o indirectamente del acceso a cualquier información confidencial, incluyendo, pero no limitando a información de secretos comerciales, programas de computador o información de clientes.
    - Pérdida resultante de falla mecánica, construcción defectuosa, error de diseño, defecto latente, desgaste o rasgadura, deterioro gradual, perturbación eléctrica, falla o rotura de medios de procesamiento electrónico de datos o cualquier mal funcionamiento o error en programación o errores u omisiones en procesamiento.
    - Pérdida resultante directa o indirectamente de la preparación fraudulenta, modificación fraudulenta o destrucción de instrucciones electrónicas computarizadas, a menos que estén cubiertas bajos los amparos 2, 3, ó 4.
    - Pérdida por el ingreso de datos electrónicos en una terminal electrónica autorizada de un sistema electrónico de transferencia de fondos o un sistema de comunicaciones del cliente, por un cliente u otra persona que tenga acceso autorizado al mecanismo de autenticación del cliente.
    - Pérdidas resultantes de características fraudulentas contenidos en las instrucciones electrónicas de computadores desarrolladas para vender a o que sean vendidas a múltiples clientes al tiempo de su adquisición, por parte de un vendedor o consultor.
    - Pérdida resultante directa o indirectamente de cualquier virus de computador a menos que esté cubierta bajo el amparo 4.

De lo anterior, podemos extraer que sí existe un desarrollo frente a tener como riesgo el fraude a través de medios electrónicos. Sin embargo, la mayoría de los riesgos asociados a esta problemática están de una u otra forma limitados en su cubrimiento o definitivamente excluidos, con lo cual el panorama de protección se muestra incierto, amén que no se ofrece ninguna característica especial tratándose de recursos públicos.

Ahora bien, ante la realidad que se pone en evidencia en este trabajo, surge necesaria la adopción de medidas orientadas precisamente a contar desde el pliego de condiciones de la licitación siquiera una cobertura mínima frente a fraudes electrónicos que asegure que en caso de presentarse el

evento, pueda garantizarse que los recursos públicos encuentren una protección efectiva ante una realidad que día a día se trasforma y, por ende, hace más latente su acaecimiento.

4.2. Entidades Públicas

Como fue expuesto en el numeral precedente, según la Jurisprudencia del Consejo de Estado la póliza global no está limitada a ser adquirida por las entidades financieras, sino que a ella tienen acceso también quienes no ejercen esa actividad.

Partiendo de esta realidad, respecto a las pólizas que existen en el mercado como garantía en caso de fraudes electrónicos para entidades no financieras, dentro de la investigación adelantada se encontraron, entre otras, las siguientes:

Chubb Seguros Colombia S.A. tiene en su portafolio la póliza riesgos entidades no financieras – crime 14/09/2020-1305-P-13 - CLACHUBB20160012-000I-14/09/2020 - 1305-NT-13 P&CNTCHUBBSEG039. Dentro de cuyas consideraciones y dando la relevancia a los datos suministrados en el formulario de solicitud, elemento que se muestra de total relevancia a la ahora de la adquisición de este tipo de pólizas, como ya tuvimos oportunidad de anotar, así como en todas las demás manifestaciones e información suministrada por el asegurado, cuenta con los amparos de:

- Infidelidad de empleados: la compañía será responsable por pérdidas directas de dinero, títulos valores u otras propiedades, a causa de cualquier infidelidad o falsificación por parte de cualquier empleado de cualquier asegurado, que actúe solo o en concurso con otros.

- Predios: la compañía será responsable por pérdidas directas causadas por la destrucción real, desaparición, o hurto de dinero o títulos valores dentro o desde los predios, los predios bancarios; o hurto en las cajas fuertes cometidos por un tercero.

- Hurto por computador: la compañía será responsable de las pérdidas directas de dinero, títulos valores del asegurado causadas por hurto por computador cometido por un tercero.

- Fraude en transferencia de fondos: la compañía será responsable de las pérdidas directas de dinero o títulos valores del asegurado causadas por fraude en transferencia de fondos cometido por un tercero.

- Gastos por acceso no autorizado al sistema informático la compañía será responsable de los gastos por acceso no autorizado al sistema informático incurridos por un asegurado, que resulten de la pérdida directa cubierta por los amparos: 1. infidelidad de empleados, 7. hurto por computador y 11. pérdida a clientes.

Ahora bien, de estos amparos es importante destacar sus definiciones, así:

- Acceso no Autorizado al Sistema Informático significa: (A) La entrada no autorizada a los Datos, o borrar los Datos desde un Sistema de Computador, dirigido solamente contra el Asegurado; (B) Cambios no autorizados a un Sistema de Computador de los elementos de Datos o programas, los cuales se mantienen guardados en una maquina en un formato legible, dirigido solamente contra el Asegurado; o (C) La introducción no autorizada de instrucciones escritas, programación o de otra forma, los cuales se propaguen a través de un Sistema de Computador, dirigido solamente contra el Asegurado.

- Asegurado significa(n) aquella(s) organización(es) señalada(s) en la carátula de esta póliza.

- Fraude en Transferencia de Fondos significa: (A) Instrucciones fraudulentas electrónicas, telegráficas, por cable, por teletipo, o telefónicas, transmitidas a una Institución Financiera, indicando a tal institución debitar una cuenta, transferir, pagar o entregar Dinero o Títulos Valores desde tal cuenta, con instrucciones que pretenden haber sido transmitidas por el Asegurado, o Amparo 6. (Falsificación Extendida)) enviadas a una institución financiera, indicando a tal institución debitar una cuenta, transferir, pagar o entregar Dinero o Títulos Valores desde tal cuenta por medio de la utilización de un sistema electrónico de transferencia de fondos, a intervalos específicos o bajo instrucciones determinadas, y que tales instrucciones den a entender haber sido emitidas por el Asegurado.

- Hurto por Computador significa el acto de tomar intencionalmente Dinero o Títulos Valores debido a un Acceso no Autorizado al Sistema Informático mediante el uso de un computador localizado en el Predio del Asegurado, o en cualquier otra parte.

- Institución Financiera significa una de las siguientes entidades, en las cuales el Asegurado mantenga una Cuenta de Transferencia: (A) Establecimiento de crédito (establecimientos bancarios, corporaciones financieras y compañías de financiamiento comercial), (B) Sociedades de servicios financieros (sociedades fiduciarias, almacenes generales de depósito, sociedades administradoras de pensiones y cesantías), (C) sociedades de capitalización, (D) organismos cooperativos de grado superior de carácter financiero, y (E) comisionistas de bolsa, fondo mutuo o institución similar de inversión.

- Instrumento Financiero significa cheques, giros, pagarés, aceptación bancaria o promesa similar escrita, orden o instrucción de pagar una suma cierta en Dinero, hecha o girada por, o girada contra el Asegurado, o hecha o girada por alguien que esté actuando como agente del Asegurado, o que pretendan haber sido hechas o giradas como se menciona en la presente definición.

- Predios Bancarios significa el interior de aquella porción de cualquier edificio o edificios ocupados por algún banco, fiduciaria o sitios similares reconocidos como depósitos de seguridad.

- Sistema de Computador significa un computador o una red de computadores, incluyendo la entrada, salida, procesamiento, almacenamiento y equipos de comunicación; y también incluirá las bibliotecas de medios "off-line".

Otra póliza que también brinda amparos frente a riesgos financieros para entidades no financieras es la de Seguros Generales Suramericana S.A. – 23/11/2015- 13-18- p - 17 - f-01-21-002, dentro de la cual igualmente se hace énfasis en la confianza en los datos suministrados en el formulario de solicitud y todas las demás manifestaciones e información suministrada por el asegurado, se incluyen los siguientes en relación con fraudes electrónicos:

- Infidelidad de empleados. la compañía será responsable por pérdidas directas de dinero, títulos valores u otras propiedades a causa de cualquier infidelidad o falsificación por parte de cualquier empleado de cualquier asegurado que actúe solo o en concurso con otros.
- Predios. la compañía será responsable por pérdidas directas causadas por la destrucción real, desaparición, o hurto de dinero o títulos valores dentro o desde los predios, los predios bancarios o hurto en las cajas fuertes cometidos por un tercero.
- Hurto por computador. la compañía será responsable de las pérdidas directas de dinero, títulos valores o propiedad del asegurado causadas por hurto por computador cometido por un tercero.
- Fraude en transferencia de fondos. la compañía será responsable de las pérdidas directas de dinero o títulos valores del asegurado causadas por fraude en transferencia de fondos cometido por un tercero.

También está la póliza DE RIESGOS FINANCIEROS PARA ENTIDADES NO FINANCIERAS IRP-008-004 – PREVISORA 18/04/2018-1324-P-13-IRP008VERSIÓN004-D00I- 18042018-1324-NT-P-13-INFIDELIDAD00001, que contiene dentro de sus amparos el de hurto por computador y fraude en transferencia de fondos previsora se compromete a indemnizar al asegurado las pérdidas directas causadas por hurto por computador o por fraude en transferencia de fondos en dinero o en títulos valores.

Y relevante la cláusula tercera relativa a definiciones, se lee:

- Asegurado significa aquellas personas jurídicas señaladas en la carátula de esta póliza y/o sus condiciones particulares y/o especiales.
- Cuenta de Transferencias significa una cuenta mantenida por el Asegurado en una Institución Financiera desde la cual el Asegurado puede iniciar la transferencia, pago o entrega de Dinero o de Títulos Valores: i. Por medio de instrucciones electrónicas, telegráficas, por cable, por teletipo, por facsímil o telefónicas, comunicadas directamente o a través de un sistema electrónico de transferencia de fondos, o ii. Por medio de instrucciones escritas (diferentes a aquellas descritas en el Amparo previsto en el numeral 4 de la Cláusula Primera (amparos)), estableciendo las condiciones bajo las cuales tales transferencias van a ser iniciadas por tal Institución Financiera a través de un sistema electrónico de transferencia de fondos.
- Dinero significa solamente dinero efectivo, monedas, billetes y oro o plata en barras.
- Fraude en Transferencia de Fondos significa: i. Instrucciones fraudulentas electrónicas, telegráficas, por cable, por teletipo, o telefónicas, transmitidas a una Institución Financiera indicando a tal institución debitar una Cuenta de Transferencias y transferir, pagar o entregar Dinero o Títulos Valores desde tal Cuenta de Transferencias con instrucciones que pretenden haber sido transmitidas por el Asegurado pero que fueron de hecho fraudulentamente transmitidas por alguien distinto del Asegurado sin el conocimiento ni el consentimiento del Asegurado, o ii. Instrucciones fraudulentas escritas (diferentes a las descritas en el Amparo 4) enviadas a una Institución Financiera indicando a tal institución debitar una Cuenta de Transferencias y transferir, pagar o entregar Dinero o Títulos Valores desde tal Cuenta de Transferencias por medio de la utilización de un sistema electrónico de transferencia de fondos, a intervalos específicos o bajo instrucciones determinadas, y que tales instrucciones den a entender haber sido emitidas por el Asegurado pero fueron de hecho fraudulentamente emitidas, falsificadas o alteradas por alguien distinto del Asegurado y sin el conocimiento ni el consentimiento de éste.
- Hurto por Computador significa el acto de tomar intencionalmente Dinero o Títulos Valores mediante el uso de una computadora localizado en el Predio del Asegurado o en cualquier otra parte.

- Institución Financiera significa una de las siguientes entidades en las cuales el Asegurado mantenga una Cuenta de Transferencia: i. Establecimiento de crédito (Establecimientos Bancarios, Corporaciones Financieras, Corporaciones de Ahorro y Vivienda, Compañías de Financiamiento Comercial), ii. Sociedades de servicios financieros (Sociedades Fiduciarias, Almacenes Generales de Depósito, Sociedades Administradoras de Pensiones y Cesantías), iii. Sociedades de capitalización, iv. Organismos cooperativos de grado superior de carácter financiero, y v. Comisionistas de bolsa, fondo mutuo o institución similar de inversión.
- Predios significa aquella porción interior del edificio ocupado por el Asegurado en el desarrollo de sus negocios.
- Predios Bancarios significa el interior de aquella porción de cualquier edificio o edificios ocupados por algún banco, fiduciaria o sitios similares reconocidos como depósitos de seguridad.

Siendo estos referentes de pólizas que pueden cubrir riesgos por fraudes electrónicos en entidades no financieras, entre ellas, entidades públicas que tienen cuentas maestras para el manejo de los recursos asignados, lo que se evidencia es que el desarrollo que han presentado de cara a la protección de los dineros que pueden verse afectados ante la realidad de la implementación de la tecnología en la intermediación financiera, es realmente muy reciente y ninguno de ellos enmarcado en la relevancia de recursos públicos que circulan en cuentas aperturadas en entidades financieras.

Ahora, es importante en este punto, retomar un elemento que mencionamos al hablar de las pólizas tomadas por entidades financieras y la relevancia que tiene, cual es el formulario de solicitud, como parte integrante del contenido de estas pólizas, pues el desarrollo de este tipo de documento es a todas luces el que marca la pauta no solo para establecer la necesidad del seguro y su oferta, sino también en qué términos van a definirse las condiciones y las exclusiones, bajo el entendido que también la entidad financiera ya cuenta con otra póliza que brinda protección en caso de que productos financieros de esa naturaleza puedan verse afectados. Luego las circunstancias que

orienten ese formulario necesariamente, de así requerirse, habrán de ser trasladadas a los pliegos que para la contratación del mismo se publiquen en el marco de una licitación.

Desde esta perspectiva, en el que tanto las entidades públicas, que tienen una obligación fiscal que atender, y las entidades financieras un requerimiento mínimo de verificar la necesidad de contar con un seguro; surge claro que desde los dos extremos de esa relación en la que se entregan dineros para ser resguardados por un banco, es necesario que se liciten y oferten seguros que garanticen la no defraudación electrónica que pudieran sufrir esos recursos públicos al ser sometidos a una operación electrónica.

Conclusiones

- Panorama vs protección. Necesidad de contar con un seguro para la salvaguarda de los recursos depositados en las cuentas maestras, ante los riesgos inherentes derivados de la actividad financiera a través de canales electrónicos.
- No obstante, la reglamentación de las cuentas maestras si bien están delimitadas por unos procedimientos rigurosos para su constitución, uso y ejecución, no relacionan dentro de los mismos la necesidad de contar con un seguro por fraude electrónico, pese a que atendiendo el canal utilizado para las operaciones monetarias que cursan por las mismas, están expuestas, al tiempo que no se encuentra en el mercado bancario exigencia similar para el producto que ofrecen, mostrándose necesario el anexo de seguro de fraude por sistemas computarizados frente a los fraudes electrónicos en el manejo de cuenta maestras en Colombia, como salvaguarda de la naturaleza de los recursos allí depositados.

Bibliografía

Constitución Política de Colombia [Const]. 7 de julio de 1991 (Colombia)

Código de Comercio. [C. Cio]. Decreto 410 de 1971. Colombia.

Estatuto Orgánico del Sistema Financiero. [EOSF]. Ley 663 de 1993. Colombia

Rodriguez Azuero, S. (2009). *Contratos que Anteceden la Realización de Operaciones Pasivas*. En Contratos Bancarios (p. 283 a 370). Bogotá D.C. Colombia: LEGIS.

Jaramillo J. Carlos. (2021). Derecho De Seguros, II Edición. Colombia: TEMIS.

Ossa, Efrén. "Teoría General del seguro- El contrato- ", Segunda edición, Editorial Temis Ltda, Bogotá, 1991.

Narváez Bonnet, Jorge Eduardo. *El contrato de seguro en el sector financiero*. Editorial: Librería del Profesional, Bogotá, 2002, págs. 31-32

Narváez Bonnet, J. E. (2015). El contrato de seguro y los contratos de la actividad financiera: Coberturas y tendencias del seguro global bancario. *Revista Ibero-Latinoamericana De Seguros*, *24*(43). https://doi.org/10.11144/Javeriana.ris43.csaf

"Laudos arbitrales en materia de seguros", publicación de la Cámara de Comercio de Bogotá y Acoldese, Tomo II, Bogotá, 2004.

Clasificación de riesgos empresariales de Rodriguez, Eduardo *"Administración del Riesgo",* Editorial Alfaomega Colombiana S.A., Bogotá, 2002, página 43.

Laudo de 12 de noviembre de 2014 de Banco de la República contra Seguros Generales Suramericana S.A. y Allianz Seguros S.A.

ASOBANCARIA. (24 de julio de 2017). Cuentas maestras: una herramienta para la transparencia en las transacciones económicas. Semana Económica 2017, Edición 1099.

ASOBANCARIA. (2020). Amenazas Cibernéticas Post Covid. Perspectivas en Ciberseguridad, Edición 01, páginas 15.

CROforum org. (2021). Emerging Risks Initiative Major Trends and Emerging Risk Radar. 2021, de CROforum org Sitio web: https://www.thecroforum.org/wp-content/uploads/2021/06/ERI-Risk-Radar-2021.pdf

CROforum. (2021). The Three Lines Model. 2021, de CROforum Sitio web: https://www.thecroforum.org/wp-content/uploads/2021/05/CRO-WG-Governance-.pdf

ENISA (2020). Panorama de Amenazas de la ENISA. 2020. etl2020-phishing-ebook-en-es.pdf (europa.eu)

Asociación Colombiana de Ingenieros de Sistemas (ACIS). (2019, junio). XIX Encuesta Nacional de Seguridad informativa. Lecciones aprendidas y prospectiva de futuro. Vista de Núm. 151 (2019): Ciber riesgo: Un riesgo sistémico (acis.org.co). Sitio web: https://sistemas.acis.org.co/index.php/sistemas/issue/view/4/1

Signorino Barbat, A. (2020). Ciber riesgos: Su dimensión social, funcional y ética. Recuperado 4 de mayo de 2022, de https://revistas.javeriana.edu.co/, website: https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/29017

Zaharia, A. (2022). 300+ Estadísticas aterradoras de cibercrimen y ciberseguridad. Recuperado de https://www.comparitech.com website: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Headline_cybercrime_statistics_for_2019-2022

TransUnion. (julio 21 de 2020). *TransUnion mejora la solución de verificación de documentos a medida que una nueva investigación encuentra que el fraude de identidad está en el centro de muchas estafas digitales COVID-19*. https://www.transunion.com//business Recuperado de https://newsroom.transunion.com/transunion-enhances-document-verification-solution-as-new-research-finds-identity-fraud-at-center-of-many-digital-covid-19-scams/

TransUnion. (23 de septiembre de 2021). *Fraude digital concentra su enfoque en industrias de videojuegos, viajes y ocio*. https://www.transunion.com//business Recuperado de https://noticias.transunion.co/fraude-digital-concentra-su-enfoque-en-industrias-de-videojuegos-viajes-y-ocio/

TransUnion. *Comportamientos y perspectivas de los consumidores respecto a los presupuestos, gastos y deudas actuales y futuras de los hogares.* Recuperado de: Consumer Pulse ES CO Q3 2022 (transunion.com)

TransUnion. *Tendencias de Fraude – Análisis Trimestral*. Fraude Digital en 2022. Recuperado de: INT-LATAM-22-2190377-TU-Q2-2022-FraudTrends-Infographic-v2 (transunion.com)

Reunión Anual de Davos 2022 - Global Cybersecurity Outlook - Original. (23 de mayo de 2022). *El informe Global Cybersecurity Outlook del Foro Económico Mundial* . https://www.weforum.org/ Recuperado de https://www.weforum.org/videos/davos-annual-meeting-2022-global-cybersecurity-outlook-original

Superintendencia Financiera de Colombia. (marzo 2022). *Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CS)*. www.superfinanciera.gov.co Recuperado de https://www.superfinanciera.gov.co/jsp/10110733

Superintendencia Financiera de Colombia. (Enero-Junio 2022). *Informe de Operaciones*. https://www.superfinanciera.gov.co. Recuperado 30 de octubre de

https://www.superfinanciera.gov.co/inicio/informes-y-cifras/cifras/establecimientos-de-credito/informacion-periodica/semestral/informe-de-operaciones-61066

Superintendencia Financiera de Colombia. (noviembre 2022). Consulta condiciones generales pólizas de seguro. Recuperado de: Superintendencia Financiera de Colombia (superfinanciera.gov.co)

Así se mueve la corrupción. *Radiografía de los hechos de corrupción en Colombia 2016-2018*. (2019). Recuperado 8 de marzo de 2022, de www.monitorciudadano.com website: https://www.monitorciudadano.co/documentos/hc-informes/asi_se_mueve_la_corrupcion.pdf

Así se mueve la corrupción. *Radiografía de los hechos de corrupción en Colombia 2016-2020*. (2021). Recuperado 8 de marzo de 2022, de www.transparenciacolombia.org y www.monitorciudadano.com website: radiografia-2016-2021-02-11-21.pdf (transparenciacolombia.org.co) y Radiografia-2016-2021.pdf (monitorciudadano.co)

Proyecto de ley Presupuesto General de la Nación 2022. *Presentación del ministro de Hacienda*. Recuperado julio de 2022 de www.minhacienda.gov.co. Proyecto de Ley PGN 2022 (minhacienda.gov.co)

Anexo Mensaje Presidencia, Proyecto de ley Presupuesto General de la Nación 2023 website: www.minhacienda.gov.co Proyecto de Ley PGN 2023 (minhacienda.gov.co)