“Banca abierta y ciberdelitos, un reto de gestión para el derecho financiero”

Autor: Dr. Iván Danilo Ortiz Alulema

Junio, 2025

Banca abierta y ciberdelitos, un reto de gestión para el derecho financiero

Resumen

La innovación en los mecanismos de servicios e interacción a través de plataformas virtuales y la crisis producto de la pandemia, han acelerado la transformación digital generando nuevos modelos de negocio que han interpuesto desafíos a los distintos actores de control y juzgamiento del delito tecnológico, ya que el advenimiento de la era digital es una realidad presente que demanda un marco regulatorio bancario y financiero ágil y eficiente que incorpore una comprensión y evaluación integral objetiva por parte de los sujetos obligados, supervisores y sistemas de justicia de los países de la región.

El ciberdelito se ha convertido en una de las mayores amenazas para la sociedad, por ello las innovaciones criminales asociadas a estos actos antijurídicos plantean retos y desafíos para la industria financiera, como es la adaptación y comprensión de estas nuevas tecnologías disruptivas para su gestión de protección a los derechos vulnerados de las víctimas. Por lo que resulta clave entender el contexto funcional del riesgo cibernético o ciberriesgos que afectan a las partes inmersas en esta coyuntura tecnológica, asociadas a la amenaza de los ciberataques que se derivan en delitos económicos que puede tener múltiples consecuencias, cuya gravedad dependerá de cada caso y de la intención de las organizaciones delictivas, que atenta al derecho de la privacidad de las personas, pérdidas monetarias, la integridad sicológica que pueden vulnerar o atentar hasta la vida de las

víctimas, cuya perspectiva según los estudios especializados muestran que esta crisis se profundizará en los próximos años.

La alta tecnología en la época actual es capaz de vulnerar los sistemas informáticos para la comisión de delitos transnacionales, por lo que se debe adoptar estrategias legales y de control regionales a través del fortalecimiento de la cooperación internacional, la alineación de políticas públicas y regulaciones complementarias comunes entre países, considerando que estos ciberdelitos se asocian y conllevan a otros delitos penales asociados.

Los delitos tecnológicos provocan la vulnerabilidad de diversos actores del ecosistema financiero que generan enormes conflictos a las partes, sin que la doctrina del derecho tenga en muchos casos lineamientos uniformes para enfrentar y regular estas amenazas, principalmente por la falta de una visión holística del problema.

La falta de estandarización y uso efectivo de leyes que permitan comprender, perseguir y sancionar estos ciberdelitos provocan impunidad a los responsables, ya que estos actos antijurídicos muchas veces no se circunscriben a un país o territorio, lo que dificulta la situación para identificar y recuperar recursos patrimoniales de las víctimas, que pese a la existencia de leyes fiscales de ubicación de capitales locales en el extranjero y leyes de extinción de dominio, que pueden ayudar a la recuperación de capitales de origen antijurídico, son procesos complejos y que aún no son aplicados con todo su alcance de control y facultad sancionatoria.

Tabla de contenido

Tabla de Gráficos

Introducción

El año 2020 quedará en los anales de la historia como un punto de quiebre que a causa de la pandemia generó más incidentes de seguridad informática que nunca y más digitalización de negocios e interacción de acceso virtual a la gestión de servicios públicos y privados. La pandemia hizo posible la aceleración de una época de cambios tecnológicos que estaba siendo impulsada intrínsecamente por la corriente disruptiva del avance digital de la industria financiera, en especial el sector bancario, ya que estas tecnologías se afianzaron para que una gran mayoría de procesos de interacción a través de canales digitales y virtuales terminen de incorporarse en la relación "cliente - proveedor" e incluso fue más allá, ya que puso a prueba la capacidad digital de nuestras sociedades, economías y gobiernos, a la vez la proliferación acelerada de cambios tecnológicos dio también lugar al aparecimiento de actores hostiles, brindándoles nuevas y numerosas oportunidades de actuar para generar delitos relacionados a las nuevas tecnologías (ciberdelitos).

Este contexto de transformación de los modelos de negocio incrementa los riesgos emergentes que en su diversidad y complejidad en la actualidad son los problemas más graves que enfrenta el sector bancario y la sociedad en esta etapa de transición digital. El nuevo escenario pospandemia, las nuevas tecnologías de información y comunicación, las redes sociales, la aparición de nuevos mercados de inversión (criptoactivos), el comercio electrónico y la globalización de la economía dirigida a fomentar la circulación de los capitales que se transfieren de un lado al otro con apoyo de las redes tecnológicas al rededor del mundo, han abierto un espacio de incertidumbre de enormes dimensiones, que así mismo sirve de escenario perfecto para la evolución y

desarrollo de nuevos factores de riesgo asociados a los ciberdelitos de alcance transnacional, cuyas consecuencias impactan principalmente en las estructuras de control y recursos de las organizaciones y personas afectadas.

En el plano regional de América Latina y el Caribe muchas de las condiciones de estos avances tecnológicos, así como el deterioro social y el menoscabo de los valores éticos que imperan a través de la ejecución de actividades ilícitas relacionadas a la materialización de estos riesgos, que en esencia atentan contra la propiedad que representa el bien jurídico protegido amparado por la Constitución de clientes y entidades financieras de los diferentes países de la región, provocan pérdidas monetarias, fuga de datos, acceso no autorizado a información confidencial de usuarios y organizaciones y hasta pueden atentar a los derechos humanos fundamentales de las víctimas, todos estos eventos interrelacionados y sistematizados terminan alineándose en un orden antijurídico que sirven de estructura ideal para sostener con mucha eficacia el escenario de complejidad de los nuevos riesgos tecnológicos.

CAPITULO UNO: COMPRENSIÓN DEL ENTORNO TECNOLÓGICO

1.1 Cambios disruptivos en el modelo de negocio bancario

El avance digital provoca cambios en los esquemas de negocio, que obliga literalmente a la evolución de la administración de los riesgos que estas innovaciones tecnológicas generan, entre ellos el riesgo legal y reputacional; sin embargo, este avance no está acompañado de un marco jurídico que apoye su desarrollo y control regulatorio, ya que las diferentes legislaciones actuales de la región de América Latina y el Caribe se enfrentan a limitaciones por la inexistencia o ambigüedad de las normas sobre nuevas tecnologías, sobre todo si analizamos la desigual evolución de estas leyes especializadas en la región, divergentes en la uniformidad, alcance, tipos de controles y sanciones aplicables a las partes infractoras inmersas en esta coyuntura legal y tecnológica de los diversos esquemas y tipologías de estos delitos extraterritoriales, los cuales incluyen a diversos actores tales como: las organizaciones públicas y privadas, los usuarios afectados, los organismos de supervisión y administración de justicia y los ciberdelincuentes.

El incremento marcado de estos delitos se observa a partir de la postpandemia, ya que según la consultora Axur el número de casos de phishing (obtención de contraseñas) en América Latina durante el primer semestre de 2021 es de 14.083 casos registrados, 4.279 fueron identificados en Brasil, el país con el mayor número de casos de phishing; 2.5 millones de protocolos de seguridad de Certificados SSL (datos cifrados), 687 mil intentos de fraudes con tarjetas de crédito y débito; la ciberdelincuencia tiene segmentos preferidos para los ciberataques tales como: e-commerce, Saas y

Web Mail y entidades financieras (Moura, 2021), cuya tendencia incremental a partir de esta etapa va en un aumento vertiginoso.

Con el desarrollo de estas tecnologías, paralelamente la ciberdelincuencia ha desarrollado sofisticadas formas para vulnerar las seguridades de los sistemas informáticos para la comisión de variados delitos en el ciberespacio, al tomar ventaja de la vulnerabilidad y falta de controles preventivos de las organizaciones, así como el aprovechamiento de los vacíos legales y falta de uniformidad de la doctrina jurídica en esta materia en los diversos países de la región.

El concepto macro de ciberseguridad entendido como el control de la seguridad informática de una entidad o espacio virtual, toma relevancia ante el aumento de uso del ciberespacio como un lugar para la creciente interacción social alrededor del mundo, la gran cantidad de datos virtuales que se generan en dicho espacio posibilitan almacenar y manejar gran cantidad de información con diversos propósitos, justamente apoyados de estas nuevas tecnologías tales como la inteligencia artificial (IA), la conectividad de empresas de tecnología financiera (Fintech), el uso de activos virtuales, entre otros.

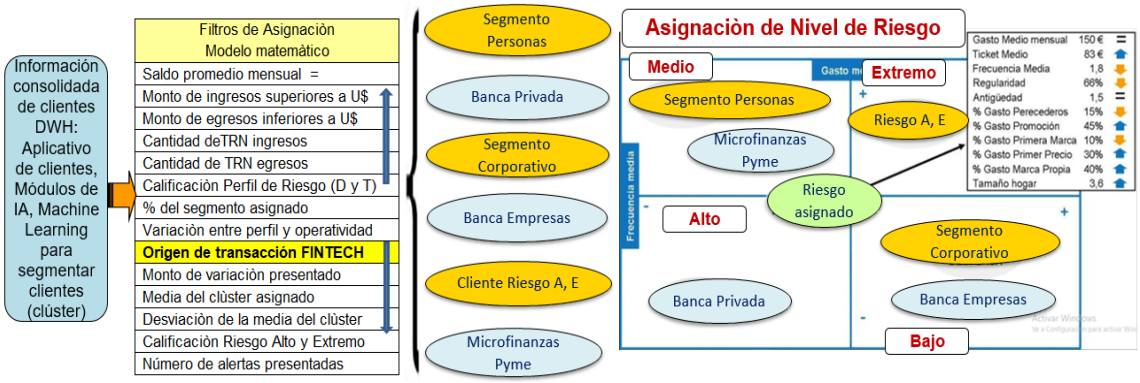
1.1.1 Uso de la Inteligencia Artificial para monitoreo y control de datos

En la práctica la inteligencia artificial incorporada en distintas aplicaciones sobre todo en la industria bancaria es fundamental en el funcionamiento operativo de las entidades y sus clientes o usuarios, por lo que las organizaciones deben supervisar y reforzar sus plataformas operativas de ciberseguridad con apego a la normatividad legal emitida para el efecto.

La inteligencia artificial es una tecnología de big data (datos procedentes de una nueva fuente de datos) que maneja grandes volúmenes de información

acumulada de las operaciones de los clientes, tanto de la información que él provee, como de datos históricos y sobre todo el comportamiento que muestra con base al uso de sus productos y servicios, toda esa inteligencia artificial se aplica para establecer grupos de perfiles homogéneos entre sí, e identificar tendencias u operaciones atípicas que salen fuera de un perfil comercial asignado, para gestionar y conocer el origen de tales desviaciones o inusualidades, las cuales deben pasar procesos de validación y justificación de las operaciones alertadas del comportamiento transaccional o conductual de los clientes o usuarios.

Gráfico 1: Inteligencia Artificial en procesos de Cumplimiento



Fuente y elaboración propia del autor

Esta tecnología facilita la adecuada segmentación de los clientes mediante filtros de asignación con modelos o algoritmos matemáticos, que ayuda a realizar un monitoreo más eficiente, reduce las alertas (falsos positivos) por mala segmentación de clientes. Depura los segmentos de clientes y le asigna un segmento acorde a la calificación de riesgo tomando aspectos del nivel de riesgo, los controles definidos y los filtros comerciales, permite identificar clientes y transacciones provenientes de empresas de

tecnología financiera o intermediarios Fintech con los que opera la entidad bancaria.

La mayor incidencia en el uso de herramientas de big data con apoyo de inteligencia artificial aplicadas sobre todo a uno de los sectores más vulnerables como son las entidades financieras, permite un profundo conocimiento de tendencias y comportamientos con la interacción con la base de clientes, así como la identificación de posibles fuentes de riesgos asociados a una diversidad de ciberdelitos, fraudes internos o externos y en general a la exposición al riesgo tecnológico inherente al giro operativo de cada entidad. Un ejemplo de estas aplicaciones en la banca es el software de monitoreo de prevención de lavado de activos que desarrolla e incorpora estos conceptos de inteligencia artificial en sus nuevas versiones; otra valiosa aplicación es la minería de datos que facilita la segmentación automática de la cartera de clientes y la asignación de características comunes u homogéneas para dotar de información valiosa para la gestión comercial o actividades de control de acuerdo a los parámetros automatizados establecidos.

Dentro de este contexto de transformación digital y la aparición de nuevos riesgos tecnológicos se destaca el hecho y la relevancia que representa la aplicación necesaria de un marco jurídico acorde a este nuevo escenario de los actuales modelos de negocio de la industria, como soporte y acorde a la operatividad de dichos modelos, sobre todo la aplicación de normas relativas a la protección de datos personales del cliente, ciberseguridad, contrato de operatividad o contrato inteligente[1] (smart contracts) para transmisión de datos,

[1] Un contrato inteligente es un acuerdo entre dos personas o entidades en forma de código informático programado para ejecutarse de forma automática para intercambiar activos (valores), registros de información y su almacenamiento, sin necesidad de intermediarios

gestión y prevención de riesgos, sobre todo el de fraude cibernético y el blanqueo de capitales, como los principales riesgo que en la práctica afectan los sistemas de control interno de las instituciones financieras.

1.1.2 Incursión de empresas de tecnología financiera (Fintech)

Esta innovadora corriente tiene una repercusión notable en la competitividad del servicio y el bienestar del usuario o beneficiarios de un servicio, además plantea un reto de comprensión y control para las áreas legal y operativa de las entidades financieras, los reguladores y entes judiciales, más si se considera que la normativa regional no contempla todos los aspectos legales de acuerdo al entorno y necesidades que demanda su propia jurisdicción, menos aún los estándares internacionales en esta materia, por lo que es indispensable conocer la evolución de estas nuevas corrientes, medir el impacto de las Fintech en el incremento de los ciberdelitos, así como los riesgos y el nivel de cumplimiento de la normatividad aplicable, ya que no todas las legislaciones de los países contemplan y regulan en todo o en parte el amplio espectro de estas innovaciones, principalmente de servicios financieros que ya son una realidad y cuyas plataformas están siendo utilizados para vulnerar las seguridades físicas y lógicas para la comisión de delitos informáticos.

Los operadores de justicia y reguladores deben considerar que estas tecnologías ya son parte del convivir social y mercantil, las principales áreas de negocio donde se plasma el concepto de las Fintech y se generan riesgos son: pagos y transacciones, finanzas personales, asesoría para inversiones y alternativas de financiación entre particulares y empresas; que incluyen actividades como: crowdfunding, crowlending (financiación por varios

inversores), criptomonedas[2], mercado de divisas, transferencias de fondos, préstamos p2p (préstamos en línea entre particulares), asesoramiento financiero, trading o mercado de criptos, entre otros.

Al igual que estos nuevos avances tecnológicos facilitan y simplifican tiempos para la concreción de una serie de procesos operativos y transacciones financieras por medio de plataformas digitales o aplicaciones móviles (App); así también generan inmensas brechas relacionadas a la falta de seguridad en su ejecución, operaciones irregulares y fuga de información sensible sin consentimiento del usuario o de la entidad vulnerada en sus controles de seguridad, que confluyen en innumerables casos de fraudes y delitos informáticos, que provocan pérdidas monetarias y hasta potenciales riesgos relacionados al lavado de activos, financiamiento del terrorismo y otros delitos conexos, cuya materialización se pueden enmarcar en delitos de tipo penal.

1.1.3 Activos virtuales: desafíos para la investigación de ciberdelitos

El control preventivo se ha convertido en una prioridad para el sector bancario y financiero debido al creciente uso de estos activos digitales en operaciones financieras globales. La naturaleza descentralizada, pseudoanónima y sin fronteras de los criptoactivos plantea desafíos significativos para la identificación y seguimiento de estas transacciones, lo que los convierte en una herramienta potencialmente atractiva para redes criminales involucradas en actividades ilegales en el uso de estas tecnologías.

[2] Criptomoneda, criptodivisa o criptoactivo es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones financieras, controlar la creación de unidades adicionales y verificar la transferencia de activos, las criptomonedas son un tipo de divisa.

Las criptomonedas son parte de los activos virtuales que representan un activo digital que emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones, desde que apareció el bitcoin se han creado un sinnúmero de monedas virtuales cuya principal característica es el respaldo en activos que posean (stablecoins). Dentro de esta categoría de criptomonedas existen una variedad de ciberamenanzas que provocan innumerables pérdidas, estafas y fraudes, que tanto los bancos y el sistema judicial debe gestionar.

Este mercado virtual en la actualidad es poco transparente, sin una adecuada regulación o supervisión en la región; aún hasta en las legislaciones más desarrolladas como el mercado estadounidense o la Unión Europea se registran varios delitos derivados de estas tecnologías. Para comprender de mejor forma estas ciberamenazas, en la práctica se debe considerar y analizar el entorno, las características y señales de alerta más comunes en la ocurrencia de estos riesgos asociadas a las criptomonedas, tales como:

1) Plataformas que crean su propio contenido para promocionar y dar la apariencia de legitimidad, rentabilidad y seguridad da las inversiones tranzadas en este mercado.
2) Organizaciones delictivas que reclutan a sus propios blogueros (persona que administra un sitio web o red social) quienes promocionan y hablan bien de un sitio web para adquirir una buena reputación, aceptación y una aparente seguridad.
3) Empresas nuevas legalmente constituidas para ofrecer portafolio de inversiones exclusivas en bitcoin a través de plataformas web que gestionan tales inversiones.

4) Casas de cambio falsas (Exchange) para que los usuarios incautos adquieran las criptomonedas, al existir una elevada cantidad de casas de cambio es difícil establecer la legalidad de todas y cada una de estos intermediarios que suministran servicios a los inversores, y sobre todo porque se encuentran alrededor de todo el mundo, sin una mayor regulación.
5) Aplicaciones móviles falsas de intercambio de criptomonedas, que inducen al usuario a realizar depósitos o pagos para obtenerlas, pero que nunca fueron entregadas a los adquirentes, cuya finalidad es la apropiación indebida de fondos.

El mundo virtual del ciberespacio plantea grandes retos para las áreas de control de las instituciones financieras y posteriormente las investigaciones judiciales para salvaguardar el bien jurídico protegido y los derechos de las partes afectadas, la dificultad de establecer los nexos y grado de participación de estas organizaciones requiere muchas veces acciones y engorrosos procesos de asistencia penal internacional para poder perseguir y sancionar a los responsables.

Con este antecedente, las entidades bancarias en cumplimiento a las disposiciones de Basilea III para reforzar la regulación, la supervisión y la gestión de riesgo de los bancos, sobre el control del riesgo operacional que incluye estas nuevas tecnologías y el control preventivo, en lo referente a “el riesgo operacional de un banco aumenta a un ritmo creciente según lo hacen sus ingresos” (Basilea, 2019), deben establecer toda una filosofía corporativa de cambio para el control y mitigación de los nuevos riesgos emergentes, más aún si en su jurisdicción aún no se ha desarrollado una doctrina y marco

jurídico para la administración efectiva y eficiente de sus riesgos financieros, o en su defecto adoptar los lineamientos de las mejores prácticas universales de control preventivo, puesto que el cambio tecnológico y los modelos de negocio avanzan con mayor celeridad con relación al marco legal, en especial el derecho financiero que norma y regula la actividad financiera de las personas físicas como de los entes jurídicos .

CAPITULO DOS: EL MODELO DE BANCA ABIERTA

2.1 Actualización del modelo de negocio bancario

Las organizaciones deben adaptar sus procesos y modelos de negocio hacia estas nuevas tecnológicas disruptivas; para esta transición se debe crear una estrategia y modelo de negocio donde se integre la transformación digital. El nuevo modelo de banca abierta (Open Banking) parte como eje central y prioriza al cliente, toda la transformación digital de la organización debe estar centrada en la reinvención del modelo de negocio en función de la experiencia del cliente.

Para la transformación digital hacia este modelo es indispensable definir directrices generales con objetivos específicos para estos procesos de cambio, tales como:

1) ¿*Qué vamos a transformar*?: uso de nuevas tecnologías y su impacto en el modelo de negocio en la banca.
2) ¿*Cómo lo haremos*?: con base a la Identificación de los nuevos riesgos emergentes y nuevos actores en el modelo de banca abierta.
3) ¿*Cómo identificamos el riesgo*?: con base a un análisis de todos y cada uno de los factores de riesgo en función del nuevo modelo operativo de negocio a implementar.
4) ¿*Qué generamos*?: Confianza, cultura de cambio y generación de valor agregado entre todos los stakeholders inmersos en la transición digital.

La banca abierta no es solo exponer y administrar datos, sino aprovechar todas las ventajas de un ecosistema abierto con el objetivo de mejorar la experiencia del cliente o usuario. Las organizaciones están agresivamente implementando nuevas tecnologías para transformar el “modelo

de negocio” para lograr crecimiento en el mercado, mejorar eficiencias operativas e incrementar valor para los accionistas.

Entender la transformación digital en el sector financiero, las oportunidades y desafíos de las Fintech, brindan un marco conceptual de la evolución de los modelos de negocio. La premisa principal es que los clientes *son los dueños de la data* y se puede compartir su información con otras entidades financieras y terceros (Fintech o intermediarios) bajo su consentimiento, para lo cual el modelo demanda la apertura de las plataformas de conectividad tecnológica de las instituciones financieras para compartir datos e información de clientes con su autorización.

2.2 Proceso general del modelo de banca abierta

En la banca tradicional (Pre-Open Banking) de la cual estamos migrando, los clientes se conectan con sus entidades bancarias mediante canales digitales, en especial a través de portales web o la Interfaz de Programación de Aplicaciones (APIs por sus siglas en inglés) para realizar sus requerimientos de servicios y transacciones.

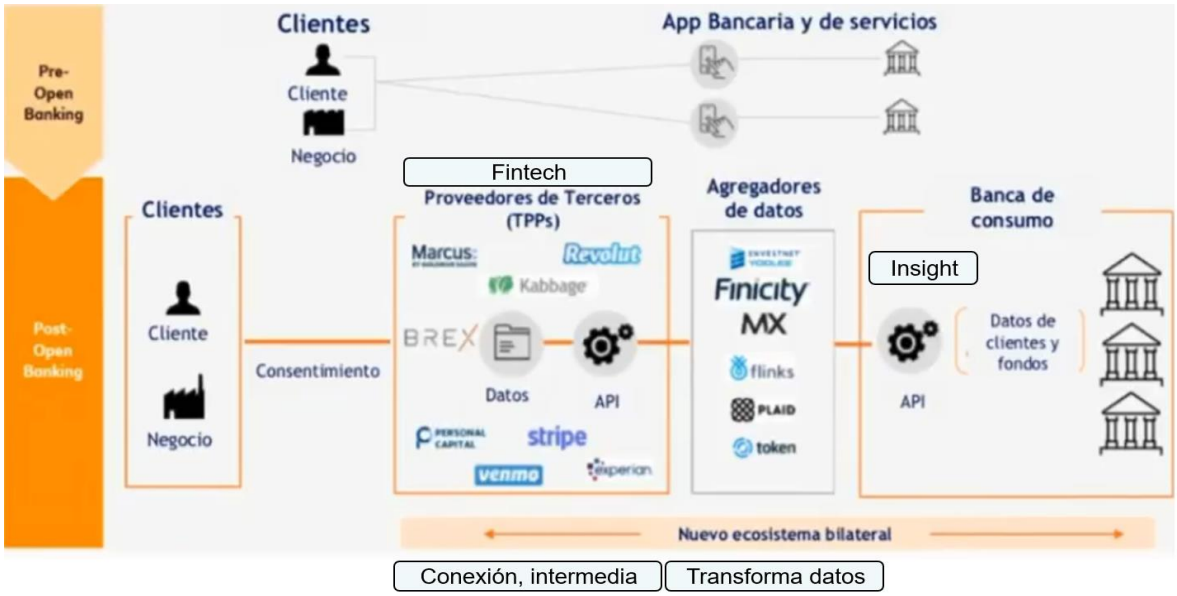
El esquema general de la transición hacia este nuevo modelo incluye las siguientes etapas:

- En la etapa de Post Open Banking el cliente previo su “consentimiento” autoriza compartir su información con otras entidades bancarias y/o terceros.
- Con el apoyo operativo de las Fintech y/o Proveedores de Servicios Virtuales (PSAV) se compila la información compartida, cuyas plataformas de conectividad se alimentan de una serie de entradas de información que son procesadas e integradas en sus plataformas tecnológicas con base a

inteligencia artificial que utilizan filtros y algoritmos matemáticos y operativos para el manejo de datos, la aplicación de controles técnicos y comerciales.

- Con base a criterios analíticos de negocio los intermediarios Fintech a través de los agregadores de datos pueden entregar información a otros bancos mediante las APIs o plataformas de visualización y plataformas de ciencia de datos.
- La información procesada del cliente es compartida con otras entidades bancarias o terceras partes del sector del retail para consumir y explotar comercialmente la información del cliente.

Gráfico 2: Banca abierta fortalece la relación entre bancos y clientes



Fuente: Risk Consulting

Desde el punto de vista de la “experiencia del cliente”, este modelo de negocio facilita y agiliza los servicios bancarios, aparte que puede obtener productos personalizados, una mayor oferta se servicios, reducción de costos, simplificación de tiempos, transparencia y control, entre otros. En tanto que

para las funciones de control surgen nuevos riesgos y desafíos respecto a la gestión de riesgos sobre la conectividad, seguridad y privacidad de los datos, medidas sólidas de protección y autenticación para proteger y transmitir la información confidencial de los clientes, cumplir con las regulaciones de prevención de lavado de activos y protección de datos personales (PDP) de clientes, entre otros.

Un factor crítico a considerar es que las empresas Fintech suelen tener clientes de todo el mundo que están sujetos a diferentes jurisdicciones legales. Por tanto, es posible que deban cumplir múltiples normas anti lavado de dinero, tributarias, fiscales y de protección de datos, que pueden ser difíciles de alinear, implementar y más de cumplir.

El derecho financiero al regular las relaciones y actividades financieras entre particulares constituye un apoyo para los participantes en el modelo, que facilita, administra y armoniza estas relaciones contractuales de conectividad y operatividad, más aún cuando se generan conflictos entre las partes intervinientes en el modelo de banca abierta.

2.3 Debida diligencia para empresas Fintech en el modelo de negocio

Un proceso sólido de debida diligencia ayuda a gestionar y mitigar los riesgos operativos, legales y financieros de estos intermediarios operativos tecnológicos, que al ser parte de esta la industria bancaria requieren cumplir procedimientos de control, entre los cuales se pueden mencionar la revisión y cumplimiento de los siguientes puntos de control hacia las Fintech:

- Procesos on-line para *verificar la identidad* de clientes (claves de acceso).
- Entender las *actividades de monitoreo* de la operatividad de clientes.

- Procesos de Debida Diligencia (DD) y Debida Diligencia Reforzada (DDR) para sus clientes.
- Registro de autorizaciones y licencias vigentes, emitidas por el ente regulador (local o internacional).
- Control en línea de listas restrictivas de la Oficina de Control de Activos Extranjeros[3] (OFAC por sus siglas en inglés) en las interfaces operativas y de conexión y transmisión de datos.
- Conocer condiciones de las alianzas *estratégicas operativas* y *comerciales* del cliente u operador con los agregadores de datos (App) y bancos.
- Revisión de los balances auditados por el auditor externo e informe de cumplimiento normativo (si aplica).
- Conocimiento y validación del modelo operativo para el manejo de la Protección de Datos de clientes propios como de aquellos transferidos.
- Evaluar las funciones definidas del Oficial de Protección de Datos de acuerdo a los objetivos de las regulaciones vigentes.
- En el caso de la aplicabilidad de la inteligencia artificial en los procesos de "Conocimiento del Cliente", evaluar su alcance y funcionalidad práctica.
- Identificar y evaluar la seguridad de las interfaces de intercambio o transmisión de datos e información entre las partes.
- Revisión del Programa de Cumplimiento que incluye la DDC, monitoreo continuo de transacciones procesadas y Reporte de Operaciones Sospechosas.

[3] OFAC es una oficina del Tesoro de E.U. que administra e impone sanciones económicas y comerciales basadas en la política exterior estadounidense y sus objetivos de seguridad nacional contra ciertos países extranjeros, terroristas y narcotraficantes internacionales, y aquellos que participan en actividades relacionadas con la proliferación de armas de destrucción masiva.

- Conocimiento y aplicación de leyes anti lavado de dinero que aplican las Fintech y sus actualizaciones, en función de los tipos de servicio ofertados.
- Uso de la tecnología para ayudar con el cumplimiento normativo y de control preventivo, incluido el análisis de datos para rastrear el comportamiento del cliente y autenticación biométrica para verificar la identidad del cliente.
- Capacitación a los empleados sobre el programa de cumplimiento y acciones para asegurar de que comprendan la importancia de seguirlo.
- Cooperación con reguladores y los mecanismos para proporcionar la información solicitada.
- Verificar la aplicabilidad a la Fintech de los controles emitidos por el GAFI respecto a los mecanismos de control de las nuevas tecnologías, identificación del cliente, monitoreo continuo, mantenimiento de registros, cooperación y mecanismos de reporte.

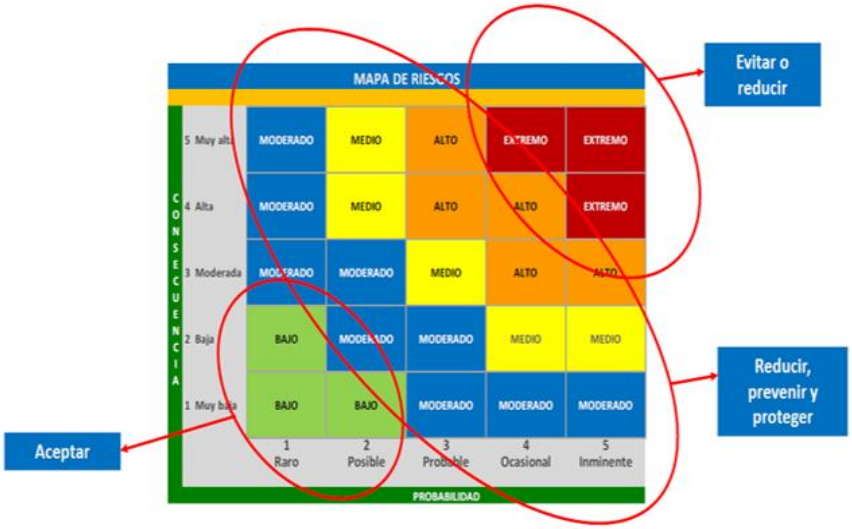
2.4 Alianza operativa y estratégica con las Fintech

Para los procesos de debida diligencia de este tipo de intermediarios Fintech, es de suma importancia para los bancos identificar el rol dentro del modelo, Una Fintech puede ser un "*Cliente*" o un "*Aliado Operador*" de una entidad financiera. Los dos roles sobre el tipo de Fintech, deben ser objeto de procesos de conocimiento del cliente y debida diligencia ampliada en función de la relación comercial y/o contractual, tomando en consideración:

1) Un operador Fintech puede ser sólo *cliente* del banco, sólo un *operador* contractual del banco, o ambos a la vez.
2) En el caso que se trate de un "cliente", éste debe ser segmentado y calificado como de riesgo alto o extremo y sujetos a procesos de control y

debida diligencia reforzada para evitar o reducir la materialización de los riesgos, sin caer en el de-risking[4].

Gráfico 3: Matriz de Evaluación de Riesgo para procesos de Debida Diligencia



Fuente y elaboración proía del autor

3) Si es un “operador intermediario” del banco dentro del modelo de banca abierta debe ser sujeto de exhaustivos procesos de prospección, control y debida diligencia ampliada.

Por parte de la entidad bancaria y para documentar el proceso de revisión hacia la Fintech, ya sea como cliente, operador o ambas circunstancias es importante elaborar el informe de revisión, exposición al riesgo y viabilidad de este tipo de clientes o aliados estratégicos operativos, descritos en el punto anterior (2.3 Debida diligencia para empresas Fintech en el modelo de negocio).

[4] Se refiere a la práctica de instituciones financieras de reducir o eliminar relaciones comerciales con ciertos clientes o categorías de clientes para evitar el riesgo, en lugar de gestionarlo activamente

CAPITULO TRES: LOS DELITOS DE ALTA TECNOLOGÍA

3.1 Identificación de los actores de la amenaza de los ciberdelitos

El Centro Criptológico Nacional (CCN) del Ministerio de Defensa de España, identifica dentro del esquema de estos delitos a los siguientes actores asociados a la amenaza propiamente dicha de los ciberataques: el Estado, la ciberdelincuencia, el hacktivismo y los actores internos (CCN, 2021, 13).

1) *El Estado o sector gubernamental:* son uno de los principales blancos de amenaza, de hecho los entes públicos son los que sufren ciberataques, principalmente los sectores relacionados a seguridad nacional y defensa, centros de investigación, telecomunicaciones, energía, industria farmacéutica, comercio internacional, inclusive han sido identificados ataques en temas de coyuntura política como las elecciones de dignidades, es decir el límite de ataques no restringe sector alguno para la ciberamenaza que ciertas ocasiones tienen hasta injerencia e intereses geopolíticos.
2) *Ciberdelincuencia:* se refiere las organizaciones delictivas o ciberdelincuentes, que utilizan todo tipo de ransomware (secuestro de datos) para extorsionar a sus víctimas para obtener un beneficio económico ilícito, así como el envío de campañas masivas de phishing para obtener datos privados de acceso a cuentas financieras o datos sensibles de los usuarios mediante internet, a través de un conjunto de técnicas que inducen al engaño o estafa para acceder a dicha información confidencial.

   Dentro de esta categoría de delitos, el sector bancario es uno de los más afectados por estas amenazas, ya que por la naturaleza del giro de negocio sobre el manejo de esquemas de seguridad para protección de la información financiera, esquemas operativos de transferencia de información

sensible, protección de datos personales de clientes, entre otros, este sector es un blanco atractivo para los hackers u organizaciones delictivas para materializar delitos relacionados con el acceso indebido de información confidencial, fraudes informáticos, sustracción irregular de recursos, entre otros, lo que expone a las entidades financieras a un sin número de problemas legales con las partes afectadas por la ocurrencia de estos riesgos.

3) *Hacktivismo*: relacionados con ataques de extracción no autorizada de información para su publicación en fuentes públicas, suspensión o desconfiguración para que ciertos sitios web no estén disponibles (principalmente sitios estatales). Uno de los principales ejemplos de esta corriente de filtración de información sensible es el grupo Anonymous, en tanto que una de las principales plataformas para distribuir información filtrada a nivel mundial de movimientos hacktivistas es la plataforma X (antes twitter), por lo que es importante la utilización responsable y el límite de datos personales o corporativos que se exponen para interactuar en estas plataformas.

4) *Actores Internos*: constituyen los funcionarios internos, quiénes por negligencia de seguridad, con conocimiento de causa o de manera involuntaria pueden ser víctimas de campañas phishing, que permiten accesar a los sistemas informáticos internos, por lo que se debe adoptar medidas de prevención a través de programas de capacitación sobre los riesgos legales y consecuencias. Estas filtraciones deben ser analizadas desde la perspectiva del grado de participación de los actores internos, quienes por acción u omisión permiten que la amenaza ingrese en los

sistemas, pudiendo llegar a establecer impactos negativos como el sabotaje, el espionaje o el fraude que terminan por lo general en un perjuicio económico, cuyas responsabilidades pueden ser asociadas a varios tipos de delitos penales.

Dentro de un contexto integral de los actores, se debe mencionar además a las partes encargadas de la investigación, determinación y juzgamiento, una vez que estos ciberdelitos se presentan. En esta instancia, el Estado a través del sistema de justicia tiene el gran reto y responsabilidad de garantizar el debido proceso para juzgar y sentenciar –si el caso amerita– estos delitos tecnológicos, que con el aparecimiento de los canales de interacción virtuales y en especial en la etapa de postpandemia se incrementaron de manera acelerada.

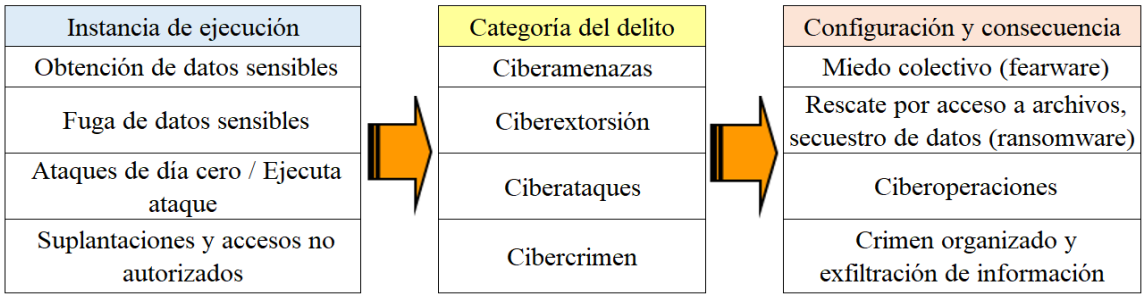
3.1.1 Riesgo cibernético en el contexto funcional del sector público y privado

Es fundamental para los profesionales inmersos en las funciones de control y juzgamiento de estos delitos, conocer las principales características y esquemas del riesgo cibernético para actuar con conocimiento de causa dentro de esta problemática, que en términos generales y por la experiencia en el campo legal y la investigación de estos delitos de alta tecnología estos casos se relacionan con: la instancia de ejecución del delito, la categorización del delito y la configuración y consecuencia.

Más allá de la labor de los pofesionales o peritos expertos que apoyan la investigación especializada de estos delitos, el esquema general de las instancias del delito (Gráfico 4) permite tener una visión global e integral de las fases y las conexiones de estos actos ilegales, que facilitan a los funcionarios

de control y de seguridad de la información de los bancos una auditoría informática forense objetiva para poder establecer y reportar la ocurrencia de estos potenciales delitos, en tanto que a los órganos supervisores y autoridades judiciales le permite obtener un criterio técnico para elaborar y sustentar una teoría del caso y obtener una sentencia según su competencia, con fundamento para establecer responsabilidades y grado de participación de las partes responsables en estos actos antijurídicos dentro de un proceso judicial.

Gráfico 4: Esquema integral de las instancias del delito cibernético



Fuente y elaboración propia del autor

Una de las deficiencias a nivel regional es la falta de coordinación y cooperación interinstitucional de los organismos estatales a nivel local para compartir información de los sujetos procesales con agilidad y celeridad, con la reserva de la información que demanda el debido proceso, muchas veces la confusión o falta de claridad de los esquemas de estos delitos constituyen los principales factores de retrazo de dichos procesos; más aún tratándose de delitos de alcance extraterritorial es necesario utilizar los convenios de control del cibercrimen para obtener cooperación a través de una asistencia penal interancional que requiere la colaboración de entidades de control y judiciales del exterior; sin embargo, en esta instancia surge un problema debido a que

pese a exisitir estos convenios de cooperación multilateral, en ocasiones la legislación de cada país se contrapone o es contradictoria y no está en concordancia con tales convenios, por lo que el reto para el Ministerio Público en la región es la de armonizar y coordinar de manera urgente estos convenios con las leyes existentes en la actualidad.

3.1.2 Perspectiva de la evolución de los delitos de alta tecnología

El informe Global Digital Trust Insights 2025, elaborado por Price Waterhouse Coopers (PwC) a partir de una encuesta a 4.042 directivos y responsables de tecnología de compañías de 77 países, revela que existen importantes brechas o puntos débiles que las empresas deben mejorar para llegar a ser ciberresilientes (PwC, 2025), cuyas deficiencias generales se describen a continuación:

1) *Brechas en la puesta en marcha de iniciativas*: sólo el 2% de los ejecutivos afirma que su empresa ha puesto en marcha iniciativas para alcanzar la ciberresiliencia dentro de su organización.
2) *Brechas en el nivel de preparación***:** Las empresas se sienten menos preparadas para hacer frente a las ciberamenazas más preocupantes, como los riesgos relacionados con la nube y los problemas de seguridad de terceros.
3) *Brechas a la hora de involucrar al Director de Seguridad de la Información* (CISO por sus siglas en inglés)**.** Menos de la mitad de los ejecutivos afirma que sus CISO están realmente involucrados en la planificación estratégica, en el reporte al Consejo y en la supervisión de los desarrollos tecnológicos.
4) *Brechas en el cumplimiento normativo*: los Directores Ejecutivos y de Seguridad de la Información, tienen niveles de confianza diferentes acerca

de su capacidad para cumplir con la regulación, especialmente, en lo que respecta a la inteligencia artificial y las infraestructuras críticas

5) *Brechas en la medición de los ciberriesgos***:** Aunque los ejecutivos reconocen la importancia de medir estos riesgos, menos de la mitad lo hace de manera efectiva, y solo el 15% mide el impacto financiero de manera significativa.

Las perspectivas de esta problemática se van a profundizar para los próximos años, lo que se reflejará en el aumento de estos delitos sino existe en gran parte acciones concretas para solventar y cerrar las brechas para lograr un equilibrio entre la normatividad y estos avances tecnológicos, así como una actualización constante de la legislación financiera acorde a estos avances disruptivos, puesto que éstas herramientas automatizadas están siendo utilizadas por un mayor número de plataformas y modelos de negocios para la transformación digital, cuya finalidad es proveer una mayor cobertura de servicios con menor tiempo de ejecución.

El ejemplo emblemático de este cambio se da en la industria financiera, ya que en ciertos países de América Latina están concluidas o en proceso de desarrollo las interfaces para la adopción del modelo de “banca abierta” cuya principal característica es la *conectividad* entre clientes o usuarios, intermediarios operativos (Fintech y procesadores de datos) y las entidades bancarias para la apertura de la conectividad tecnológica de las entidades financieras para compartir datos de clientes con su autorización, este nuevo esquema obliga a los países de la región a alinear las regulaciones nacionales en concordancia con las leyes de protección de datos, conectividad y de

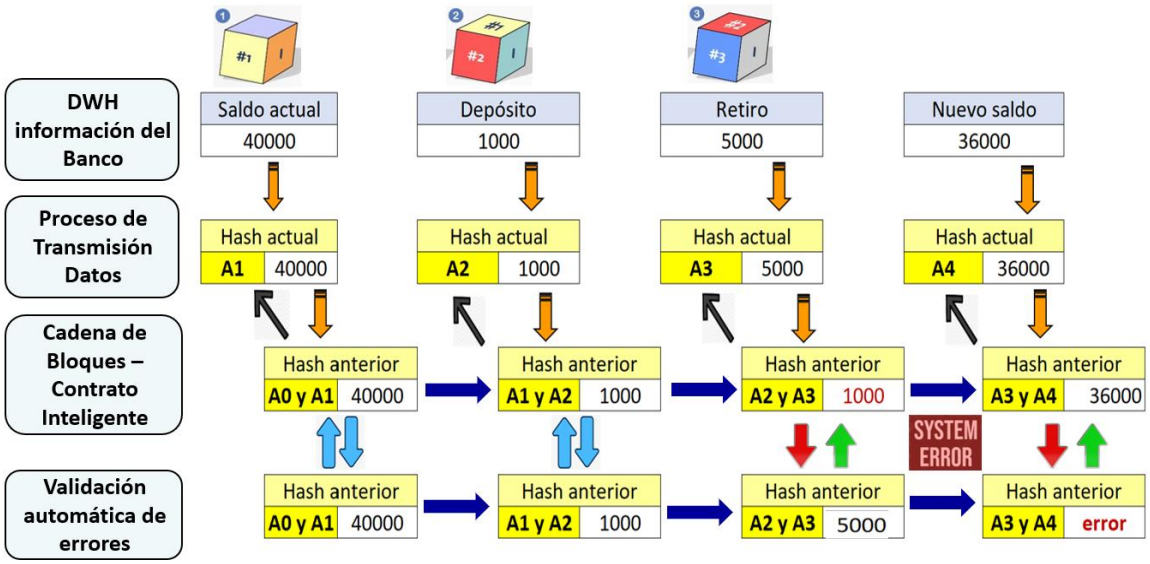
ciberseguridad que surgen por el incremento de las vulnerabilidades informáticas en cada jurisdicción.

3.1.3 Ejemplo de la tecnología blockchain en transmisión de datos

La parte clave del modelo de banca abierta está en la transmisión de información y seguridad de los datos de los clientes entre los bancos y las Fintech; si bien es cierto que para el personal informático que desarrolla las interfaces de comunicación son tareas tecnológicas rutinarias, para los profesionales del derecho en cambio es necesario comprender la funcionalidad operativa, ya que de la experiencia en caso de litigios legales cuando se generan conflictos entre las partes es necesario que todos los intervinientes en estos reclamos o conflictos tengan un criterio o visión uniforme del problema para ayudar a solventarlo.

A continuación, se describe de forma didáctica un esquema práctico del funcionamiento del blockchain en el envío de datos de clientes hacia una Fintech:

Gráfico 5: Generación y estructura de la cadena de bloques



Fuente y elaboración propia del autor

1) El proceso inicia con la identiificación y extracción de los datos a transmitir que se encuentran en el repositorio centralizado de datos del banco (DWH por sus siglas en inglés). En este caso se va a enviar datos numéricos sobre el saldo actual (US$ 40.000), operaciones de depósito (US$ 1.000) y retiro (US$ 5.000) y el nuevo saldo (US$ 36.000).

2) Se ejecuta el proceso de transmisión de información, donde a cada dato se seudonimiza u ofusca y se le asigna un hash[5] actual alfanumérico para identificarlo, así tenemos: A1: saldo actual (US$ 40.000), A2: depósito (US$ 1.000), A3: retiro (US$ 5.000) y A4: el nuevo saldo (US$ 36.000).

3) Se forma la cadena de bloques, cada bloque se compone del dato alfanumérico del hash actual, más el dato del hash alfanumérico anterior, así tenemos: A0 y A1: saldo actual (US$ 40.000), A1 y A2: depósito (US$ 1.000), A2 y A3: retiro (US$ 5.000) y por último A3 y A4: el nuevo saldo (US$ 36.000).

4) En el caso que se llegare a modificar o alterar un dato una vez transmitido el mismo, como en el presente ejemplo de la operación de retiro de US$ 5.000 por U$ 1.000, el sistema de transmisión alerta un error.

5) En la fase de validación automática de errores, de existir la posibilidad de alterar información de alguno de los datos de los bloques, el control preventivo de validación en línea alerta del error individualizado en el campo alertado y subsiguientes, ya que para alterar toda la cadena de bloques (blockchain) se debería alterar el resto de bloques que conforman la red descentralizada.

[5] Un hash es un código alfanumérico que representa un conjunto de datos. Se genera a partir de una función matemática que transforma los datos de entrada en una cadena de caracteres de longitud fija.

La característica fundamental de esta tecnología es la inmutabilidad de los datos; sin embargo, en la práctica bancaria para evitar discrepancias e inconvenientes, los contratos se servicios con las Fintech deben contener cláusulas o alternativas sobre aspectos donde pudieren darse vacíos legales y operativos no definidos por las partes, que el derecho bancario y financiero deben poner especial atención en considerar y normar, esto es:

- ¿Qué datos se capturarán en cada bloque?
- ¿Cuáles son los requisitos regulatorios pertinentes para las partes y cómo se cumplen o pueden cumplir?
- ¿Cómo se gestionan los datos de identidad? ¿Están cifradas las cargas útiles en bloque? ¿Cómo se gestionan y revocan las claves?
- ¿Cuál es el plan de recuperación de desastres para los participantes de blockchain? ¿Existieron adecuadas pruebas en sandbox (ambiente de prueba) para evaluar su óptimo funcionamiento?
- ¿Cuál es la lógica para resolver las colisiones de bloques de blockchain?
- ¿Cuál es el plan de continuidad para la interrupción del servicio de la plataforma de bloques de blockchain?
- ¿Cómo se valida las cargas automáticas y continuas de transmisión de datos en la plataforma blockchain?

Un entendimiento integral del esquema de negocio permite solventar cualquier divergencia legal u operativa a las partes, sobre todo en llegar a consensos en circunstancias de incertidumbre, cambios o ambigüedad de la doctrina jurídica en estas nuevas tecnologías disruptivas, con base al principio “ganar, ganar”, tanto para entidades bancarias como para operadores o intermediarios financieros Fintech.

3.1.4 Obtención de evidencia digital en casos de delitos informáticos

Estos delitos ocurren y se propagan a una velocidad asombrosa y su evidencia que consiste en información digital puede modificarse o eliminarse con la misma rapidez; por tanto, es un reto para los funcionarios de control de las instiuciones financieras, fiscales e investigadores informáticos recopilar y preservar la prueba digital, para su uso en los procesos judiciales.

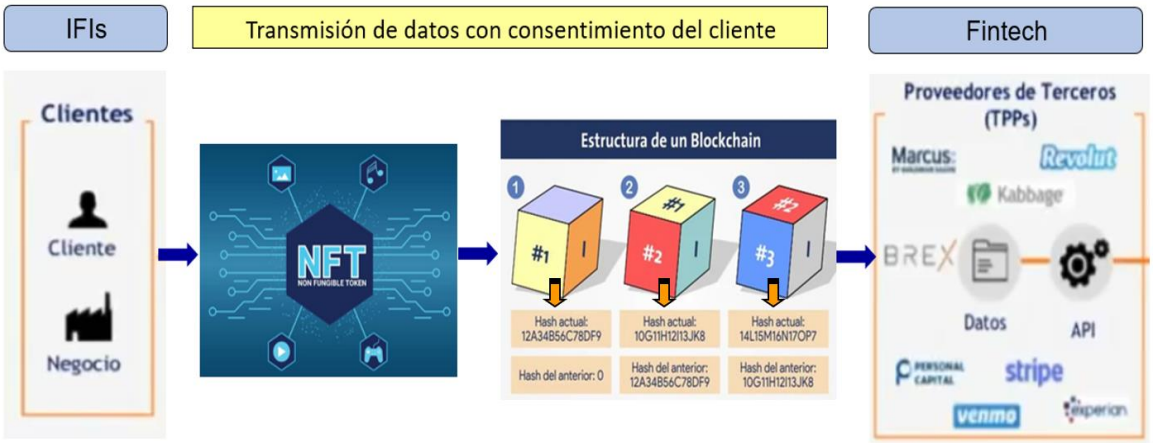
Al igual que las tecnológicas disruptivas son aprovechadas con fines fraudulentos para la ejecuión de ciberdelitos, en cambio junto con las partes afectadas y autoridades judiciales en la fase investigativa se pueden apoyar y explotar las herramientas tecnológicas disponibles para obtener pruebas de la comisión de estos delitos para sustentar en la instancia judicial pertintene.

Una de las tecnologías que crece y revolucionará la variedad y tiempos de ejecuión de las transacciones financieras y procesos operativos iterativos es la denominada tecnología a base de cadenas de bloques de información denominada “blockchain” que va a dinamizar los procesos, pero a su vez deja pistas o bitácoras de evidencia tencnológica de la ejecución de operaciones, sin cambios en sus protocolos e inmutabilidad de la ejecución original, útil para efecto de la recolección y tratamiento de las pruebas en materia de delitos informáticos.

La banca fue la primera en incorporar la cadena de bloques a sus procesos operativos, ya que esta tecnología nació en un entorno de transacciones. Blockchain es un conjunto de tecnologías que permiten llevar un registro seguro descentralizado, sincronizado y distribuido de las operaciones digitales, sin necesidad de la intermediación de terceros. La cadena de bloques, como una base de datos distribuida facilita el registro de

transacciones o documentación, creada para evitar que la información se pueda modificar una vez esta sea publicada, haciendo que se vuelva incorruptible (Hayes, 2025).

Gráfico 6: Funcionalidad del blockchain en transmisión de datos



Fuente y elaboración propia del autor

El proceso de transmisión de datos e información de clientes dentro de la banca abierta, donde se comparte información de clientes, es el siguiente:

1) A medida que se produce una transacción, se registra como un bloque de datos, estos muestran el movimiento de un activo, que puede ser tangible o intangible. El bloque de datos puede registrar la información que desee: ¿quién, qué, cuándo, dónde, cuánto?.
2) Una vez que unos datos han sido registrados dentro de una cadena de bloques, se hace imposible modificarlos y esto se debe a su compleja estructura.
3) Cada bloque está conectado al bloque anterior y al posterior, estos *bloques forman una cadena de datos a medida que el activo se mueve* de un lugar a otro o la propiedad cambia de manos. Los bloques confirman el tiempo exacto y la secuencia de las transacciones, y los bloques se encadenan de

forma segura para evitar que ningún bloque sea modificado o que se inserte un bloque entre dos bloques existentes.

4) Las transacciones se unen y forman una cadena irreversible llamada blockchain. Cada bloque adicional refuerza la verificación del bloque anterior y por lo tanto toda la cadena de bloques (blockchain). Esto hace que la cadena de bloques no se pueda manipular, ofreciendo la fuerza clave de la inmutabilidad.

De acuerdo al Foro y Observatorio Blockchain de la Unión Europea en su informe “Desmitificando los tokens no fungibles” (NFT por sus siglas en inglés) referente a la gestión de contraseñas electrónicas de acceso a la información, ilustra una serie de casos de uso interesante que pueden ser aprovechados para la investigación financiera por parte de los bancos y el sistema y judicial para la obtención de evidencia digital de estos delitos, gracias a la tecnología blockchain se pueden rastrear y verificar las operaciones y transacciones de los tokens no intercambiables. Además, suponen una prueba de propiedad y veracidad de las acciones oficiales que garantizan la ejecución de un proceso (Comisión Europea, 2021, 25).

Con la obtención de estas pruebas es imprescindible que éstas sean manejadas y tratadas de acuerdo a los protocolos de seguridad y cadena de custodia pertinentes que no invaliden este medio de prueba digital que sustentarán el caso judicial, por lo que es vital conservar copias para el trabajo investigativo y para los sujetos procesales que lo requieran y puedan obtenerlas para sus fines de defensa, en apego al debido proceso.

El rol que desempeñan las entidades bancarias dentro de los procesos de control interno es de suma importancia, ya que en principio son las

responsables del monitoreo primario de transacciones en plataformas tecnológicas, y los que pueden alertar oportunamente sobre la ocurrencia de operaciones inusuales o sospechosas asociadas a los fraudes o ejecución de transacciones con señales de alerta, que demandan una revisión profunda y procesos de debida diligencia para establecer la razonabilidad y justificación de las mismas.

3.2 Estrategias legales frente a los delitos de alta tecnología

En mayor o menor grado los países se han dedicado a desarrollar estrategias legales que les permitan hacer frente a las ciberamenazas para disminuir la confluencia de estos delitos en perjuicio del propio Estado y la sociedad, sin vulnerar derechos y principios en las políticas públicas de prevención y control. Pues bien, la disyuntiva está en cómo hacer frente a una ciberdelincuencia que no se conoce su identidad, ni tampoco su ubicación geográfica, ya que la administración de justicia no es suficiente para persuadirla (González, 2021, 88).

El Convenio del Consejo de Europa sobre cibercriminalidad firmado en Budapest el 23 de noviembre del 2001, es uno de los acuerdos que tiene una adhesión de varios países para lograr una mayor cooperación entre los Estados, con un desarrollo armónico de las leyes para regular y controlar este tipo de delincuencia organizada.

A continuación, se expone ciertas estrategias comunes para enfrentar estos delitos:

- Disponer de un análisis jurídico de la normativa local e internacional sobre esta materia, para fomentar un debate de reformas jurídicas orientado a estandarizar y recoger las mejores prácticas de la región.

- Fomentar acuerdos y consensos en la medida de lo posible sobre el enfoque y tratamiento de amenazas comunes que afrontan los Estados, que les permitan armonizar el orden jurídico y coordinar planes de acción conjuntos.
- Fortalecer y entender el derecho internacional con una visión holística, para lograr consensos en la elaboración de los convenios internacionales, que permita la acción ágil y oportuna en la administración de justicia.
- Consolidar y estandarizar los mecanismos preventivos de control en el uso de las diferentes tecnologías de la información y comunicación, como elemento estratégico de control preventivo.

La educación preventiva es clave como estrategia para precautelar y disminuir los ciberdelitos, ya que gran parte de las medidas de seguridad dependen del propio usuario de las tecnologías que utiliza en su desempeño profesional y personal, por lo que se enfatiza en la importancia de cumplir tales medidas de prevención y protección.

3.3 Cooperación internacional

La cooperación jurídica internacional es un mecanismo esencial para el desarrollo de los sistemas de justicia y la consolidación del estado de derecho que en la región debe fortalecerse, para ello los Estados deben procurar la adhesión a convenios y tratados relativos a la efectiva gestión jurídica del ciberdelito, por lo que además es prioritario generar un diálogo con el sector privado, ya que en poder de los proveedores de servicios informáticos y financieros en el exterior se encuentra mucha de la información imprescindible para facilitar las investigaciones judiciales en esta materia.

Tal como fue el compromiso de cooperación acordada en la XXX Reunión Especializada de Ministerios Públicos del Mercosur celebrada el 23 de septiembre de 2021 en Brasilia sobre “Cooperación Internacional en el Combate a la Criminalidad Cibernética y a la Desinformación Online” cuya declaración central indica:

> El firme compromiso de los Ministerios Públicos en actuar, por medio de la cooperación internacional, para el combate a los delitos cibernéticos y a otros delitos cometidos por medios electrónicos, para una mayor eficiencia en la preservación, recolección y uso de las evidencias electrónicas, necesarias a la resolución de casos, y para el enfrentamiento a la desinformación online, que sea compatible con el Estado de Derecho y en armonía con los derechos fundamentales (Ministerio Público, 2021, 1).

3.3.1 Competencia legal de delitos tecnológicos y sus ganancias ilícitas

Al tratarse de delitos que no se circunscriben a un solo territorio y el accionar de las organizaciones delictivas frecuentemente operan en varios países, en ciertas ocasiones resulta difícil establecer con certeza la procedencia del origen de los ataques cibernéticos, esto por la diversa gama de servicios -muchas veces en la nube- cuyos servidores para el procesamiento y almacenamiento de datos se pueden contratar al rededor del mundo.

Esta situación genera una dualidad entre el delito tecnológico per se y la obtención de ganancias ilícitas que genera el mismo, que pueden ocultarse en otro país o territorio distinto al del ataque, principalmente en jurisdicciones con laxos o mínimos controles; surge entonces una controversia jurisdiccional para establecer el origen de los hechos fácticos que origina el delito previo y el delito de ocultamiento de las ganancias que pueden ser asociados por ejemplo a un ciberdelito o a un delito de lavado de activos en otro país o jurisdicción diferente donde ocurre la comisión y el ocultamiento de las ganancias ilícitas del delito.

La mayoría de legislaciones nacionales de América Latina y el Caribe incluyen en la norma penal como un hecho punible el lavado de activos procedente de un delito cometido en el extranjero (común en los delitos tecnológicos), para evitar problemas de interpretación, la aplicación de esta cláusula debe respetar el discutido principio de doble incriminación que supone que los comportamientos susceptibles de ser calificados como delitos previos deben estar sancionados penalmente tanto en el lugar de comisión como en el lugar de realización del delito, en este caso el lavado de activos. No es suficiente que se trate de un hecho contra el cual sólo se establecen sanciones administrativas, sino que la sanción ligada al mismo debe tener un carácter penal (Blanco, 2018, 131).

Cuando se materializan esto delitos tecnológicos, no sólo se produce un delito aislado, sino que se derivan otros delitos penales conexos que generalmente son asociados a perjuicios y pérdidas monetarias.

3.4 Controles emitidos por el Grupo de Acción Financiera Internacional

Dentro de las 40 recomendaciones del GAFI[6] existe la No 15: Nuevas tecnologías, que indica que los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir sobre: "…el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes…" (GAFI, 2012, 17).

En virtud de esta recomendación los países deben aplicar medidas preventivas a los activos virtuales (bienes, productos, fondos y otros activos de

[6] Organismo intergubernamental de 37 miembros para el desarrollo y la promoción de políticas, a nivel internacional, combate el lavado de activos y la financiación del terrorismo, incluye la Comisión Europea.

valor equivalente) y a los proveedores de servicios de activos virtuales, es decir este estándar mundial sugiere mantener controles preventivos acorde al avance tecnológico, mismos que deben ir alineados a la legislación local.

Los principales riesgos sobre los delitos relacionados con el desarrollo de la tecnología están dirigidos al control de delitos cibernéticos en compras en línea, transmisión de datos de clientes, intermitencia y vulneración de seguridades de los sistema de control interno, la falta de comprensión integral del entorno virtual de interacción de usuarios, disparidad de normatividad en transacciones extraterritoriales, entre otros, esto conlleva a adaptaciones rápidas y eficientes del marco jurídico en lo que respecta a la regulación de la interacción virtual y comercio electrónico a fin de dar atención a los derechos vulnerados de las víctimas.

Las actualizaciones en el año 2023 de estas recomendaciones regulatorias universales y sin fronteras del GAFI se encuentran enfocadas a contrarrestar los posibles problemas delictivos derivados de los activos virtuales y en general con las nuevas tecnologías financieras y sus riesgos inherentes, éstas han puesto énfasis en:

- Monitoreo estricto obligatorio de actividades posiblemente sospechosas con activos virtuales a través de bancos, servicios de cambio, empresas de tarjeta de crédito y otras instituciones financieras.
- Definición de los activos virtuales convertibles como “dinero”, a fin de facilitar la aplicación de la “regla de viaje” (travel rule).
- Extender la jurisdicción de entidades que pertenecen y operan dentro de un país a entidades que operan en dicho país, pero que proporcionan servicios a nivel internacional.

3.4.1 Actualización de las reglas de viaje en transacciones con criptos

La implementación de la Travel Rule del GAFI marca un antes y un después en la regulación de las transacciones con criptoactivos, esta norma exige a los Proveedores de Servicios de Activos Virtuales (PSAV) o Fintech compartir información sobre remitentes y destinatarios de transferencias cripto para reforzar la lucha contra el lavado de activos y financiamiento del terrorismo, factores a considerar por parte del sector bancario cuando tienen clientes que operan con este tipo de servicios o los propios PSAV o Fintech son clientes de las entidades bancarias (Sergeenkov, 2024).

Los principales desafíos que enfrentan los PSAV, Fintech y otros actores del ecosistema cripto, es la interoperabilidad entre plataformas, la adopción de estándares tecnológicos y las implicaciones de cumplimiento normativo en jurisdicciones con marcos regulatorios dispares. Adoptar estrategias prácticas para garantizar el cumplimiento de esta normativa, los riesgos asociados a su implementación parcial o inadecuada y el impacto que tendrá en la transparencia y trazabilidad de las transacciones con criptoactivos, más aún si no se dispone de una legislación fuerte que respalde el modelo de negocio financiero.

3.5 Leyes de protección de datos

La tendencia legal en la región alrededor de la privacidad y la protección de datos personales induce a pensar constantemente sobre las preocupaciones respecto a la vulnerabilidad de éstos con los ciberataques, esta protección para estos datos, nace del derecho a la libertad y del consentimiento para proteger su privacidad ante terceros.

El derecho a la protección de datos personales corresponde al derecho derivado de la vida privada y la intimidad de las personas que se vio amenazada con la aparición de nuevas tecnologías acompañadas de la innovación digital (Espinosa, 2021, 7), que modificaron la forma de almacenar y distribuir la información que debía ser resguardada, no obstante, el hacktivismo vulnera y atenta contra este derecho fundamental, que el Estado debe garantizar y priorizar en su política pública.

Los reglamentos de protección de datos establecen la obligación de gestionar el riesgo para los derechos y libertades de las personas, suponen un tratamiento sensible. El riesgo surge por el tratamiento automatizado de datos, su procesamiento manual, elementos humanos y por los recursos implicados; surge por los fines del tratamiento, su naturaleza, por su alcance y su contexto.

La protección de derechos evalúa el impacto que tienen sobre la persona afectada al tratamiento, como el impacto social que genera y ocasiona para el titular de los datos que se están tratando, además de todos los colectivos afectados (AEPD, 2021).

3.6 Recuperación de fondos provenientes de actividades ilícitas

Los delitos tecnológicos aparte de ocasionar una serie de problemas a las partes afectadas, sean éstos los clientes o las instituciones financieras, en la mayor parte de casos persiguen la obtención de ganancias o un beneficio económico de origen ilegal, es decir se genera un “delito punitivo” que según la ley merece una sanción.

Las organizaciones delictivas dedicadas a la ciberdelincuencia o hackeo de información confidencial sujeta a reserva, una vez que obtienen un rédito económico con esta actividad ilegal, tratan de ocultar el origen ilícito de estas

ganancias, que constituyen capitales o fondos de origen antijurídico, que bien pueden ser tratados como un delito precedente para otros delitos conexos tales como el lavado de activos, enriquecimiento ilícito, divulgación de información no autorizada, estafa, fraude, extorsión, entre otros, que la mayor parte de las legislaciones penales la contemplan y sancionan. Surge entonces el problema de la ubicación de estos fondos de origen ilegal, que en la mayor parte de casos se encuentran en el exterior, es decir en una jurisdicción diferente donde se originan estos delitos.

Los delitos subyacentes asociados a los ciberdelitos, tales como enriquecimiento ilícito, abuso de funciones, blanqueo de capitales y el encubrimiento de bienes producto del blanqueo de capitales, son parte de los delitos tipificados por el Grupo de Enlaces Institucionales para la Recuperación de Activos (GEIRA) para la gestión de recuperación de activos (STAR, 2023).

La Organización de las Naciones Unidas a través del Foro Económico Mundial estima que el costo de la corrupción es de al menos US$ 2,6 billones, o el 5% del PIB bruto mundial (ONU, 2018). Estos capitales de origen ilícito que circulan alrededor del mundo pueden ser identificados con el apoyo del Grupo EGMONT[7] para realizar las acciones legales de recuperación de estos capitales tan indispensables en época de crisis, en concordancia con las leyes de extinción de dominio con injerencia sobre los activos ubicados en el extranjero, que fueron generados por una actividad ilegal precedente en el país de origen y que estas leyes facultan incautar para resarcir en parte los daños causados al Estado afectado.

[7] Organización internacional que facilita la cooperación e intercambio de información entre unidades nacionales de inteligencia financiera para investigar y prevenir el lavado de dinero y el financiamiento del terrorismo, que cobija a 151 países, incluye a ALC-UE.

3.6.1 Principales mecanismos fiscales de ubicación de capitales locales en el extranjero

Existen diversos mecanismos que los Estados pueden aprovechar para identificar y gestionar el retorno de capitales privados del extranjero, aprovechando las regulaciones fiscales universales y a la vez obtener indicios o alertas sobre la licitud de los fondos mantenidos en el exterior por los contribuyentes, entre los principales mecanismos de apoyo del marco legal regional para recopilar información de cuentas y capitales, se encuentran:

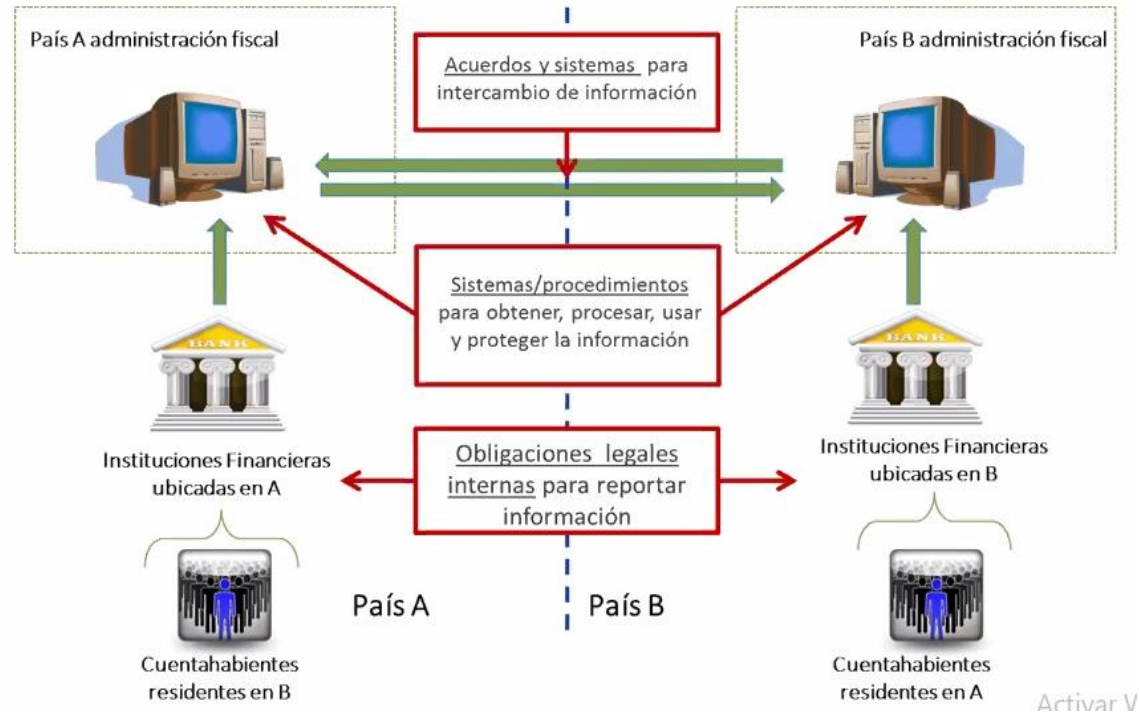
1) *Estándar Común de Reporte*: consiste el intercambio de información financiera de los sujetos pasivos por parte de las autoridades tributarias de los países que integran y se rigen con base al Acuerdo Multilateral de Autoridades Competentes sobre el intercambio automático de información de cuentas financieras a través del Estándar Común de Reporte[8] (CRS por sus siglas en inglés) para conocer los capitales e inversiones que sus contribuyentes locales o connacionales mantienen en el exterior; este intercambio de información se ejecuta con fines tributarios para reducir la evasión fiscal de los contribuyentes, a la vez que permite identificar señales de alerta sobre su origen o sus titulares y beneficiarios finales (contribuyentes).

2) *Ley de Cumplimiento Tributario en el Extranjero*: Es la ley fiscal (FATCA por sus siglas en inglés) que establece que las instituciones financieras de otros países informen al Servicio de Impuestos Internos (IRS por sus siglas en inglés) sobre las cuentas e ingresos de sus clientes sean personas o entidades de Estados Unidos (EE.UU), contribuyendo así a

[8] Acuerdo aprobado por el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) del cual son miembros 137 países que incluyen a los de ALC-UE.

evitar el fraude fiscal y en la transparencia de identificar los beneficiarios finales de cuentas o fondos en el extranjero. Aplica a ciudadano o residentes en EE.UU., nacidos o con nacionalidad de EE. UU., los que cuenten con dirección postal o número telefónico de EE. UU., empresas constituidas con dirección postal en EE.UU. o personas o empresas que mantengan un agente residente en EE. UU.

Gráfico 7: Esquema operativo y funcional de FATCA y CRS



Fuente: Internal Revenue Services

Las leyes FATCA y CRS son bastante similares en su esencia fiscal y operativa, ya que las entidades financieras son las encargadas de realizar procesos internos para ubicar dentro de su base de clientes o cuentahabientes que cumplan las indicias o que tengan responsabilidad tributaria en una jurisdicción local, para centralizar y transmitir la información tamizada a la autoridad tributaria nacional, quien con base a los acuerdos establecidos

reporta la información a la autoridad tributaria en el exterior, estos procesos periódicos de intercambio de información se ejecuta en doble vía, entre pares de autoridades fiscales.

Dentro de estos mecanismos de obtención de información, el rol que desempeñan las instituciones bancarias y financieras de todo el mundo para el cumplimiento de estas leyes es muy importante, ya que en principio son los encargados de detectar indicias y cambios de circunstancias de los clientes respecto a la identificación de cuentas o recursos en sus jurisdicciones para proceder reportar esta información al IRS a través de las autoridades tributarias locales.

Estos mecanismos internacionales avalados por acuerdos de cooperación multilaterales en materia económica y financiera, se deben aprovechar para tratar de actualizar y ajustar el marco jurídico del derecho financiero de los países, con relación a los lineamientos de las leyes fiscales, leyes de extinción de dominio para la recuperación de activos o capitales ubicados en el extranjero; más si se considera que ayudan a ubicar dichos capitales y a los potenciales responsables de delitos que provienen de actos ilícitos.

3.7 Impacto y efectos de los delitos de alta tecnología en la sociedad

El entorno virtual donde se desenvuelve los usuarios internautas para gestionar sus actividades está expuesto a factores y amenaza de riesgos, muchas veces por el desconocimiento de una cultura básica de ciberseguridad, que desembocan directa o indirectamente en la afectación de los derechos humanos de las víctimas, ya que no solo se incrementan los delitos tecnológicos asociadas a pérdidas monetarias de clientes e instituciones

financieras, sino lo más grave, un alto número de éstos se vinculan a delitos que atentan no solo al patrimonio, sino contra la privacidad, la integridad sicológica y hasta la vida o el pudor de las personas que caen víctimas de estos ciberdelitos, por ejemplo el más común denominado secuestro virtual, asociado a la extorsión bajo amenazas de atentar contra la vida o revelar circunstancias personales de la víctima o su entorno.

Las amenazas del ciberespacio pueden generar vulneración a los derechos humanos, si bien se han realizado diversas estrategias para implementar y dar seguimiento al tema de la ciberseguridad en los modelos de negocios financieros, en algunas ocasiones ante la falta de experiencia y conocimientos especializados sobre el tema, las estrategias restringen o vulneran los derechos de los usuarios bajo el argumento de brindarles seguridad en el ciberespacio (Canizales, Tapia, Vega, 2021, 150), por lo que el rol del Estado debe delimitar objetivamente la regulación de este denominado ciberespacio, capaz que pueda garantizar una razonable seguridad pero sin coartar derechos de la libertad y privacidad de las personas o usuarios del entorno virtual.

4. CONCLUSIONES

- El cambio digital de una banca tradicional hacia el nuevo modelo de banca abierta, abre una serie de riesgos y oportunidades para desarrollar estrategias de renovación tecnológica y resiliencia para las organizaciones, que puede enfrentar dificultades por ciertas incertidumbres y barreras regulatorias y una serie de riesgos prudenciales, así como la falta de una gobernanza adecuada del proceso de transición.
- Con la llegada de Open Banking, la regulación bancaria está destinada al cliente, su protección y ofrecerle una mejora en los servicios financieros, mediante la utilización de las nuevas tecnologías y dentro de un entorno protegido.
- La apertura transparente de la información y datos de los clientes y productos financieros a todos los participantes del modelo (para fomentar la sana competencia), sobre la base de la reciprocidad entre bancos e intermediarios Fintech, reconocen al cliente como propietario exclusivo de su información bancaria para posibilitar que, con su consentimiento, puedan hacer fluir y compartir esa información en la búsqueda de mejores opciones de servicios financieros.
- El derecho financiero es un mecanismo fundamental de regulación y control que todas las legislaciones de los países de la región, deben reforzar y aplicar para administrar y mitigar los riesgos tecnológicos de los nuevos modelos de negocio, que por su naturaleza y alcance las instituciones financieras deben observar.
- Existen numerosos desafíos, retos y oportunidades que surgirán del aumento de la materialización de los delitos cibernéticos, en las estrategias

de gobierno corporativo de las empresas para gestionar con políticas efectivas el tratamiento de estos riesgos, sobre todo en la adopción de políticas y normas de control, sin coartar derechos de los usuarios acorde a la evolución de estas corrientes innovadoras.

- Enfrentar el ciberdelito requiere especialización, en este sentido el sector bancario, los Ministerios Públicos y supervisores financieros de la región deben fortalecer los programas de capacitación en materia de control preventivo, cooperación internacional y evidencia digital, para compartir las mejores prácticas y estandarizar los conocimientos de los funcionarios de control de las instituciones financieras, órganos reguladores, fiscales y agentes investigadores.
- La gobernabilidad de todo sistema político requiere controlar y gestionar la seguridad del ciberespacio como condición del bienestar colectivo, la institucionalidad como medio eficaz de gestión pública y el desarrollo como objetivo de apoyo a los procesos de transformación digital.
- Los Estados deben propender el diseño de adecuadas estrategias que permitan que los diferentes actores públicos y privados se adapten al mundo digital, promoviendo el uso de las nuevas tecnologías como soporte fundamental para las actuaciones de control.
- Esta nueva realidad de cambios tecnológicos demanda el apoyo de un renovado orden jurídico orientado a proteger los derechos de las partes vulneradas, que incluyen al propio Estado, así como regular y mitigar estos riesgos que generan variadas y complejas discrepancias legales, una vez que se materializan los riegos.

- La revolución digital no tiene reversa y el sector bancario tiene la oportunidad de abrir nuevos mercados, ampliar la inclusión financiera y reducir costos, siempre y cuando realice una adecuada transición al modelo de banca abierta.

5. BIBLIOGRAFÍA

AEPD. (2021). *Gestión del riesgo y evaluación de impacto en tratamiento de datos personales*. Publicado por la Agencia Española de Protección de Datos. Madrid, junio 2021.

Basil Committee. (2017). Marco regulador internacional para los bancos. https://www.bis.org/bcbs/publ/d424_hlsummary.pdf Consulta el 14 de junio de 2025.

Blanco, I. (2018). *Combate al lavado de activos desde el sistema judicial.* Publicado por el Departamento contra la Delincuencia Organizada Transnacional de la Secretaría de Seguridad Multidimensional de la Organización de los Estados Americanos. 5ta. edición. Washington, D.C., Global Printer.

Canizales R., Tapia H., Vega, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual, *Revista Misión Jurídica*. pp. 142-158. https://doi.org/10.25058/1794600X.1912 Consulta el 15 de mayo de 2025.

Centro Cristológico Nacional. (2021). Agentes de la amenaza. *Ciberamenazas y Tendencias*. Edición octubre 2021. Madrid, Ministerio de Defensa. pp. 13-20.

Comisión Europea. (2021). Desmitificando los tokens No Fungibles (NFTs). *Foro y Observatorio Blockchain de la Unión Europea*. https://www.eublockchainforum.eu/sites/default/files/reports/DemystifyingNFTs_November%202021_2.pdf Consulta 29 de abril de 2025.

Espinosa, X. (2021). La privacidad y la protección de datos personales. *Asobanca Law Journal*. Edición noviembre 2021. pp. 6-7.

GAFI. (2012). Estándares Internacionales contra el lavado de activos y el financiamiento del terrorismo: *Las Recomendaciones del GAFI*. p.17 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf Consultada el 27 de mayo de /2025.

González, J. (2020). Estrategias legales frente de las cibermamenazas. *Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y comunicación*. pp. 85-125. Madrid, Ministerio de Ciencia e Innovación.

Hayes, A (2025). Datos sobre blockchain: qué es, cómo funciona y cómo se puede utilizar. https://www.investopedia.com/terms/b/blockchain.asp Consultada e 21 de junio de 2025.

Ministerio Público. (2021). Cooperación Internacional en el Combate a la Criminalidad Cibernética y a la Desinformación Online. https://www.rempm.org/archivos/Reuniones/30/Especializada/Anexo_V_Declaraci%C3%B3n_de_Brasilia_ESP.pdf Consultada el 29 mayo de 2021.

Moura, H. (2021). Principales datos. *Actividad criminal en línea en América Latina, 1er semestre / 2021*. p. 3.

Organización de Naciones Unidas. (2018). El costo global de la corrupción es al menos el 5% del Producto Interno Bruto mundial. https://press.un.org/en/2018/sc13493.doc.htm Consultada el 13 de mayo de 2025.

PwC (2025). Cómo impulsar la ciberresilencia en tu empresa una guía para la alta dirección. https://www.pwc.es/es/consultoria/soluciones-seguridad-

negocio/global-digital-trust-insights-2025.html. Consultado el 25 de mayo de 2025.

Sergeenkov, A. (2024). ¿Qué es la regla de viaje de las cripto? https://www.coindesk.com/es/learn/whats-the-crypto-travel-rule-and-what-does-it-mean-for-you Consultada el 20 de junio de 2025.

Stolen Assest Recovery Initiative (2023). *Curso práctico de Restitución de Activos*. 31 de enero al 2 de febrero 2023, Quito.