ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Semana Económica 2018

Edición 1148

Retos de Colombia en ciberseguridad a propósito de la adhesión al "Convenio de Budapest"

06 de agosto de 2018

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Jonathan Malagón González
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

- La evolución constante de la tecnología ha generado que las personas y empresas migren la realización de sus actividades diarias a tecnologías digitales y a que también las transacciones se realicen, cada vez más, a través de servicios en línea. En el caso particular de Colombia, el Gobierno ha realizado importantes esfuerzos para conectar a la población del país a plataformas digitales, especialmente en las regiones más apartadas del territorio.

- La mayor conectividad también ha provocado un aumento en los ataques cibernéticos. De acuerdo con el Centro Cibernético Policial de la DIJIN, en 2017, el cibercrimen en el país registró un aumento del 28,3% respecto al 2016. A nivel sectorial, la industria financiera en Colombia es la más atacada por los ciberdelincuentes dados los recursos y la información que maneja, registrando 214.000 ataques por día, el 39,6% del total de ciberataques.

- El Gobierno Nacional ha realizado esfuerzos importantes para combatir el cibercrimen. El avance más reciente de política pública para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, fue la adhesión de Colombia al Convenio de Budapest. Esto supone un importante progreso regulatorio en varias direcciones al interior de un Estado que busca facilitar la judicialización del cibercrimen y crímenes conexos.

- Asobancaria se encuentra en el proceso de crear el Centro de Respuesta a Incidentes de Seguridad (CSIRT) del sector financiero que permita establecer un enfoque organizado y estructural de la gestión de incidentes digitales y desarrollar una gestión proactiva de las amenazas cibernéticas.

- Para lograr una correcta implementación del Convenio de Budapest, el Estado deberá fijar una hoja de ruta clara para armonizar su legislación interna a las exigencias penales y judiciales internacionales con el fin de combatir la amenaza de la ciberdelincuencia. Deberá, a su vez, fortalecer los mecanismos de cooperación y la articulación del sector privado y de las autoridades mediante la intercomunicación de CSIRT existentes.

Para suscribirse a Semana Económica, por favor envíe un correo electrónico a semanaeconomica@asobancaria.com

Retos de Colombia en ciberseguridad a propósito de la adhesión al "Convenio de Budapest"

Editor

Germán Montoya Moreno
Director Económico

Participaron en esta edición:

Jaime Rincón Arteaga
Andrés Quijano Díaz
Felipe Ramírez Rozo
Camila Barrera Neira

La dinámica de la tecnología ha propiciado que las personas y empresas migren la realización de sus actividades diarias a tecnologías digitales y a que las transacciones se realicen, cada vez más, a través de servicios en línea. En Colombia, el Gobierno ha realizado valiosos esfuerzos para conectar a la población con plataformas digitales, especialmente en las regiones más apartadas del territorio.

Sin embargo, esta mayor conectividad ha provocado también un aumento en los ataques cibernéticos. Por esta razón, el Estado debe garantizar un adecuado marco legal que habilite la judicialización de delitos, adhiriéndose a lineamientos técnicos para servicios en la nube e Infraestructuras Críticas Cibernéticas (ICC) y tipologías de delitos informáticos como el robo de identidad, el ciberterrorismo y los crímenes a través de *malware* y *phishing*.

Así mismo, esta nueva realidad de integración tecnológica supone una nueva era para el terrorismo y el crimen, que obliga a los Estados a implementar los mecanismos de política pública más adecuados para lograr un esquema regulatorio eficaz en materia de ciberseguridad.

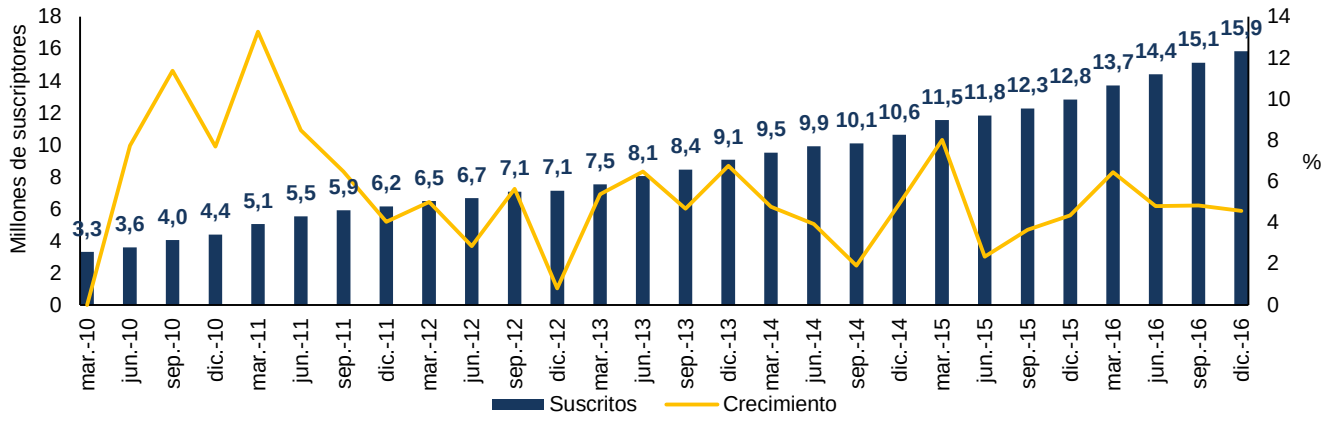
Un aspecto fundamental para judicializar y reducir los incentivos hacia el crimen resulta de una buena cooperación. Es por esto que el convenio de Budapest se constituye en el instrumento de regulación internacional más destacado frente al ciberdelito.

En este escenario, esta Semana Económica muestra las principales ventajas que trae la adhesión del país al convenio de Budapest frente a la cooperación internacional, la judicialización del cibercrimen y el fortalecimiento de la infraestructura de seguridad digital. Así mismo, señala los retos que supone, para el sector financiero y para el país, la adhesión al Convenio.

Panorama actual del ciberdelito a nivel nacional e internacional

Según cifras del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el país se han multiplicado significativamente las conexiones por banda ancha en los últimos años, pasando de 213 millones en el 2010 a 15.850 millones de conexiones en 2016 (Gráfico 1). Esta dinámica representó, en 2016, un incremento equivalente en la penetración en conectividad de 32,5% a nivel nacional, 1,5 pp más

Gráfico 1. Total de suscriptores a internet en Colombia 2010 - 2016



Fuente: Elaboración Asobancaria con datos del MinTIC.

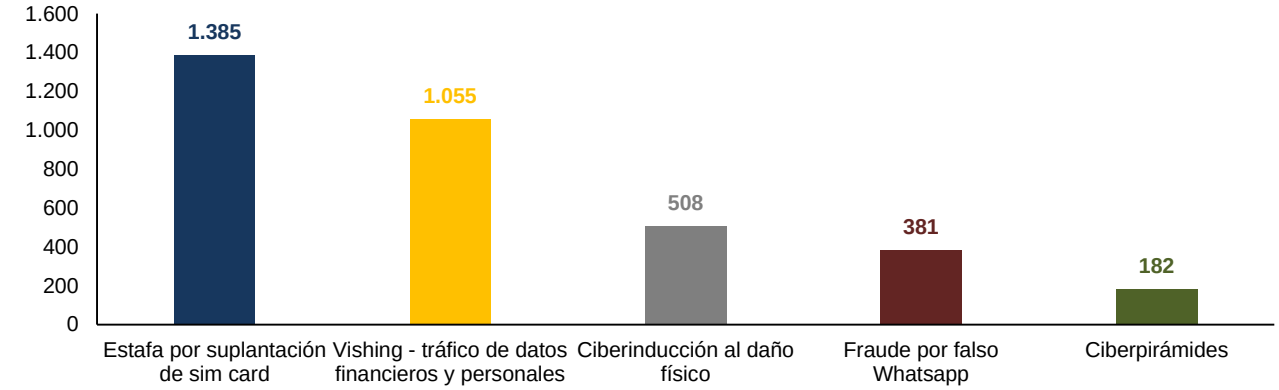
que en 2015, cuando registró un crecimiento de 31%. Hoy, gracias a este dinamismo, el 98% de los municipios en Colombia cuentan con conexiones de red, asegura MinTIC.

No obstante, este aumento en la conectividad ha venido aparejado de un incremento en el número de delitos cibernéticos. De acuerdo con el Centro Cibernético Policial de la DIJIN, en 2017 el cibercrimen en el país registró un aumento del 28,3% respecto al 2016. En el informe se descastan amenazas nuevas como la estafa por suplantación de *simcard* y el engaño por teléfono (*vishing*[1], Gráfico 2).

A nivel global, las cifras de este fenómeno resultan alarmantes. De acuerdo con McAfee – CSIS (2018)[2], el cibercrimen le costó al mundo 600.000 millones de dólares en 2017, es decir, 0,8% del PIB mundial. Esto posiciona al cibercrimen como el tercer flagelo económico global más importante, después de la corrupción gubernamental y el narcotráfico.

Por su parte, de acuerdo con Lagarde, C. (2018)[3], las entidades bancarias a nivel mundial cuentan con detrimentos anuales de 100.000 millones de dólares a causa de ataques cibernéticos, cifra que representa alrededor el 9% de los ingresos netos del sector. Esto es

Gráfico 2. Número de casos reportados de nuevas amenazas presentadas en el 2017 en Colombia



Fuente: Elaboración Asobancaria con datos del Centro Cibernético Policial.

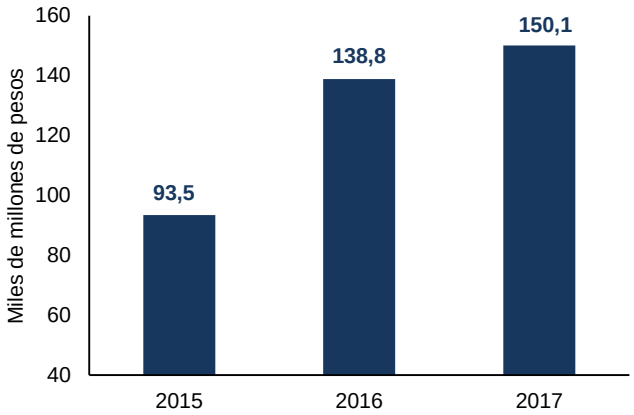
[1] Engaño a personas para obtener información personal durante llamadas telefónicas
[2] *Economic Impact of Cybercrime - No Slowing Down',* 2018.
[3] Lagarde, C. (2018). Estimación del riesgo cibernético en el sector financiero. Obtenido de https://blog-dialogoafondo.imf.org/?p=9460.

alarmante, si se tiene en cuenta que en algunos casos las pérdidas representan la mitad de las utilidades netas de las entidades crediticias.

Situación local: el caso del sistema financiero colombiano

En Colombia, el sector financiero es el más atacado por los ciberdelincuentes, un hecho atribuible a los recursos y la información que maneja. El sector registra cerca de 214.000 ataques por día, el 39,6% del total de ciberataques[4], lo que representa pérdidas cercanas a los $411 millones de pesos diarios. Según cálculos de Asobancaria, el fraude a través de canales electrónicos ha crecido cerca de 60,6% de 2015 a 2017, pasando de $93.452 millones a $150.060 millones (Gráfico 3).

Gráfico 3. Fraude a través internet y banca móvil



Fuente: Cálculos Asobancaria.

Estas cifras resultan ser solo una pequeña muestra de la actual tendencia criminal a nivel global, en la cual la mayor parte de delitos está migrando al mundo digital. En este contexto, garantizar la seguridad de los sistemas informáticos y los cibercriminales se ha convertido en un imperativo que ha terminado profesionalizando la forma de investigar, detectar y prevenir los ataques, todo ello en un contexto en el que los cibercriminales constantemente crean ataques más sofisticados y con mayor alcance y rapidez.

Convenio de Budapest para hacer frente al cibercrimen

Orígenes

La Convención sobre Ciberdelincuencia del Consejo de Europa (CETS No.185), conocido también como la Convención de Budapest, surge en 2001 como resultado del trabajo de expertos en ciberseguridad del Consejo de Europa, orientado a desarrollar marcos jurídicos nacionales que puedan hacer frente a los nuevos retos de la criminalidad asociados con los delitos informáticos.

El origen de la convención se remonta a 1985, con la existencia del comité de expertos en fraudes computacionales y las primeras regulaciones sobre cibercrimen hacia 1995 en la Unión Europea. Sin embargo, solo hasta 1996 el Comité Europeo de Problemas del Crimen recomendó que el Consejo de Europa estableciera un comité de expertos sobre cibercrimen[5].

En particular, desde 1997 y hasta 2005, el Consejo de Europa trabajó en el análisis de los cambios que la innovación digital y el internet podrían traer a la seguridad y los derechos de la ciudadanía, concluyendo que estos cambios suponen nuevos retos en materia de seguridad. A partir de allí, el Consejo Europeo analizó las dificultades prácticas en la persecución del crimen para establecer principios generales que favorecieran su judicialización[6], concluyendo que el aparato judicial de cada país debe adaptarse para lograr una persecución efectiva del delito y asegurar la confianza en la economía digital.

Hacia 2003, un nuevo apartado del convenio se puso bajo consideración de los países miembro. Este buscaba incorporar las preocupaciones sobre el acoso en internet y que no fueron abordadas en la etapa original del mismo, específicamente aquellas relacionadas con acoso político y racialmente dirigido (a la fecha, este apartado no ha sido de aceptación generalizada entre los Estados miembros).

Desde el punto de vista de la política pública, la nueva realidad de integración tecnológica supuso una nueva era para el terrorismo y el crimen. Esto condujo a que los

[4] Informe de Ciberseguridad Digiware 2017.
[5] Vatis, M. (2010). The Council of Europe Convention on Cybercrime. En C. o. Options (Ed.), *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. National Research Council.
[6] Gillespie, A. (2015). *Cybercrime: Key Issues and Debates*. Routledge.

Estados buscaran los mecanismos de política pública más adecuados para lograr un esquema regulatorio eficaz en materia de ciberseguridad. Finalmente, se logró reconocer que la cooperación resulta ser un aspecto fundamental para judicializar y reducir los incentivos hacia el crimen. Como resultado, el Convenio de Budapest se ha convertido en uno de los instrumentos de cooperación internacional más destacados frente al ciberdelito.

En efecto, los retos en materia de seguridad resultan muy desafiantes. El crimen y el terrorismo se transformaron de manera radical con las oportunidades del internet y la mayor integración de las plataformas tecnológicas, migrando desde crímenes tradicionales (narcotráfico, hurto, estafa, etc.) hacia el cibercrimen, que posee mayores ganancias y menores riesgos[7]. Sumado a lo anterior, las ventajas de la conectividad también condujeron al recrudecimiento de la incidencia del crimen, traspasando fronteras, lo que aumenta la dificultad en la judicialización a causa de los cambios jurisdiccionales entre territorios.

¿Qué busca el Convenio de Budapest y por qué es importante?

La adhesión al convenio supone un importante avance regulatorio en varias direcciones al interior de un Estado que busca facilitar la judicialización del cibercrimen y crímenes conexos.

Por un lado, los Estados deben armonizar su legislación interna a las exigencias penales y judiciales de los demás países adheridos al Convenio, con el fin de garantizar un flujo apropiado de información y evidencias entre países en el marco de las investigaciones judiciales. Por otro lado, los Estados deben garantizar un adecuado marco legal que habilite la judicialización de delitos, adhiriéndose a lineamientos técnicos para tipologías de delitos informáticos como el robo de identidad, ciberterrorismo, crímenes a través de *malware*, *phishing* y para el caso de servicios en la nube e Infraestructuras Críticas Cibernéticas. Esto se logra al institucionalizar un lenguaje común para la penalización de actividades ilegales, lo que facilita la identificación crímenes y penas entre países. Para lograrlo, los países deben desarrollar esquemas de cooperación claros y expeditos entre autoridades, lo que supone el desarrollo de capacidades técnicas y cambios institucionales en favor de una mejor gestión de las investigaciones. Esto permite que las investigaciones en materia de cibercriminalidad que involucran varias jurisdicciones logren fluir fácilmente y contribuyan a mejorar la política criminal.

En materia legislativa, el Convenio de Budapest propone modificaciones sustantivas en lo penal y en lo procesal. Desde el punto de vista penal, los países que buscan adherirse deben regular varios delitos contra la confiabilidad, disponibilidad, integridad de los datos y de los sistemas informáticos, así como aquellos vinculados al fraude informático y los referentes a las posibles violaciones a la propiedad intelectual en un contexto digital. En lo procesal, los Estados deben desarrollar capacidades idóneas (infraestructuras, instituciones y protocolos) para registrar y confiscar los datos almacenados, así como obtener en tiempo real los datos relativos al tráfico e interceptar los datos relativos al contenido digital. Finalmente, el Convenio incluye un apartado sobre las jurisdicciones y las fronteras de acción, lo que atiende al hecho que el crimen organizado moderno es transnacional y evita los problemas típicos de distintas jurisdicciones para penalizar el delito[8].

A lo anterior se suman otros aspectos relevantes. Por ejemplo, el Convenio reconoce el equilibrio entre derechos humanos y penales, por lo que respeta las leyes de *habeas data* y datos personales vigentes. La implementación del Convenio al interior de cada país debe respetar estos lineamientos. A su vez, los países quedan comprometidos a programas de cooperación internacional, así como a esquemas de vigilancia por parte de las autoridades internacionales.

Países miembros y contenido del acuerdo

En la actualidad se han adherido al convenio más de 56 países de todo el mundo. En Latinoamérica ya forman parte Chile, Costa Rica, República Dominicana, Panamá y Argentina.

El Convenio está compuesto por tres ejes principales. El primer eje tipifica los delitos y los clasifica de la siguiente manera:

• Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: aquellos en los que la tecnología es el fin como, por

[7] Koops, B.-J. (2016). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. En B. Akhgar, & B. Brewster (Edits.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Springer.*
[8] Op. cit. Gillespie, A. (2015).

ejemplo, lograr el acceso ilícito a un sistema informático que ponga en riesgo datos confidenciales..

• Delitos informáticos: aquellos en los que la tecnología es el medio, como la alteración, borrado o introducción ilegitima de datos informáticos que dé lugar a datos no auténticos.

• Delitos relacionados con el contenido: define delitos relacionados con la producción, oferta, difusión, adquisición y posesión de pornografía infantil.

• Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines: define delitos como la reproducción y difusión sin autorización, en internet, de contenidos protegidos por derechos de autor.

El segundo eje establece las instrucciones para manipular y proteger la evidencia digital, con el fin de conservarla adecuadamente y utilizarla como prueba. Finalmente, el tercer eje dispone las reglas o normas de cooperación internacional para las investigaciones que requieran de evidencia digital.

Consideraciones para Colombia

El 1 de agosto de 2017 el Gobierno Nacional, en cabeza de la Cancillería y los Ministerios de Justicia, Defensa y Tecnologías de la Información y las Comunicaciones (TIC), presentó al Congreso de la República el Proyecto de Ley para que Colombia se adhiriera al Convenio de Budapest. Dicho Proyecto fue aprobado de manera unánime tanto en la plenaria del Senado como en la Cámara de Representantes.

Finalmente, el 24 de julio del presente año, el presidente de la República sancionó la Ley 1928 “por medio de la cual se aprueba el «Convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest”. Actualmente, la Ley se encuentra en proceso de examen automático de constitucionalidad.

Marco normativo

De manera complementaria a las exigencias estipuladas en el convenio de Budapest, relativa a los temas de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual y responsabilidad de las personas jurídicas, Colombia ha modificado de forma progresiva su legislación interna en materia de seguridad informática.

En este escenario, se han desarrollado instrumentos normativos para combatir el cibercrimen. Entre los más relevantes, se destaca la Ley 1273 de 2009, por medio de la cual se modificó el Código Penal y se creó un nuevo bien jurídico tutelado: “la protección de la información y los datos”, mediante la inclusión de 9 tipos penales:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación.
3. Interceptación de datos informáticos.
4. Daño informático.
5. Uso de *software* malicioso
6. Violación de datos personales
7. Suplantación de sitios web para capturar datos personales.
8. Hurto por medios informáticos y semejantes
9. Transferencia no consentida de activos.

Así mismo, la Ley 1581 de 2012 dispuso de mecanismos de protección para salvaguardar los datos personales registrados en cualquier base de datos que permitan llevar a cabo operaciones de recolección, almacenamiento, uso y tratamiento por parte de entidades públicas o privadas.

Por su parte, la Ley Estatutaria de Inteligencia y Contrainteligencia (1621 de 2013) fortaleció el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir con su misión constitucional al establecer los límites y fines de dichas actividades, así como los principios que las rigen, los mecanismos de supervisión y control y la cooperación y coordinación entre organismos y entidades públicas y privadas.

Política pública

Luego de un proceso de evaluación, se encontró que el país contaba con un marco normativo disperso en torno a la seguridad digital, con normas expedidas bajo condiciones diferentes a las actuales.

El Gobierno Nacional diseñó e implementó una estrategia integral de ciberseguridad nacional materializada en la hoja de ruta que inició en 2011, con la aprobación del CONPES 3071. Este documento definió la política pública para fortalecer las capacidades del Estado en ciberseguridad y, a la vez, definió espacios y mecanismos de articulación de las diferentes instituciones estatales y

privadas para su promoción. Esta política ayudó a que el país avanzara en la institucionalidad necesaria para enfrentar las amenazas cibernéticas y logró mitigar de manera activa los ataques a nivel nacional. No obstante, los resultados obtenidos evidenciaron que aún no se contaba con la "capacidad suficiente, integral y efectiva de preparación y respuesta ante ataques cibernéticos"[9].

Así las cosas, el Gobierno actualizó la política de ciberseguridad a través de un nuevo documento, el CONPES 3854, expedido en 2016, el cual buscó diseñar estrategias incluyentes de carácter colaborativo donde se compartan responsabilidades para reorientar la política nacional en torno a cinco dimensiones estratégicas: (i) gobernanza de la seguridad digital, (ii) marco legal y regulatorio de la seguridad digital, (iii) fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital, (iv) cultura ciudadana y (v) gestión de riesgos de seguridad digital.

La Política Nacional de Ciberseguridad contempla, en varios de sus componentes, la creación de Centros de Respuesta a Incidentes de Seguridad (CSIRT) para una mejor gestión y atención de ciberincidentes en los sectores más importantes del país que se consideran infraestructuras críticas, destacando la Estrategia 4.4 del CONPES 3854, que apoya la creación de CSIRT sectoriales para fortalecer el esquema de identificación, prevención y gestión de incidentes digitales con la participación de las múltiples partes interesadas.

Actualmente, Asobancaria se encuentra en el proceso de crear un CSIRT del sector financiero mediante el cual se busca establecer un enfoque organizado y estructural de la gestión de incidentes digitales y desarrollar una gestión proactiva de las amenazas cibernéticas. Adicionalmente, el paso más reciente de política pública para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, fue la adhesión de Colombia al Convenio de Budapest.

Implementación de programas de concientización sobre la seguridad digital

De manera complementaria, resulta fundamental alinear el marco normativo existente para combatir el ciberdelito con estrategias que permitan alcanzar una cultura de prevención y denuncia de los delitos informáticos. Esto se logrará mediante una política pública que permita generar conciencia acerca de la responsabilidad que tenemos todos en el uso de las TIC (tanto personas como empresas) y en el cuidado de los datos.

Fortalecimiento institucional

Se debe procurar el fortalecimiento de las capacidades institucionales que se encargan de la investigación y la judicialización de estas conductas criminales. Si bien cada vez más los profesionales que imparten justicia comprenden mejor los delitos informáticos, aún falta mucho por trabajar en este sentido. Estas tipicidades, como están consagradas en la ley, no son sencillas de comprender. La evidencia digital difiere de otro tipo de pruebas físicas y, en ocasiones, se requiere de la comprensión de terminología técnica para percibir el accionar de los delincuentes. Por su parte, una gran parte de las denuncias asociadas a estas tipicidades están dispersas en oficinas de fiscales de todo el país, muchos de los cuales tienen una enorme carga procesal y no cuentan con el conocimiento adecuado para investigar estas conductas criminales tan particulares.

Frente a delitos informáticos es clave conservar la evidencia digital, lo cual representa un gran reto, teniendo en cuenta que esta puede desaparecer o ser alterada rápidamente, por lo que las investigaciones deben ser expeditas y precisas. Para ello, debe existir un proceso penal ágil y eficiente que cuente con la cooperación de diferentes países. En este sentido, cobra especial importancia la intercomunicación entre los equipos de respuesta a incidentes de seguridad –CSIRT– sectoriales, los cuales deben contar con recursos suficientes, personal capacitado y entrenado y las herramientas para llevar a cabo las actividades que puedan dar solución a los eventos inesperados.

Esfuerzos del sistema financiero

En el sector financiero se destacan los avances en la estandarización de reportes de información que realizan las entidades de la mano con la Fiscalía General de la Nación (protocolo para compartir información). Este mecanismo define un modelo de conexión virtual entre la Fiscalía General de la Nación y las entidades bancarias, a la vez que estandariza cada uno de los documentos necesarios para solicitar información. Este protocolo contribuye a una gestión más oportuna de la

[9] CONPES 3854 de 2016 (p.17).

evidencia judicial y es un hito en la región para la política criminal.

El sector financiero también ha fortalecido sus esquemas de vigilancia y protección a ICC. Gracias al trabajo conjunto entre el Comando Conjunto Cibernético (CCOC) y distintas entidades del sector financiero (bancos, comisionistas, aseguradores, administradores de pensiones, etc.), se ha avanzado en la identificación de tipologías y mecanismos de protección a ICC ante distintos niveles de ataques informáticos. Esto no solo permite analizar las interdependencias propias de las ICC y propender hacia estrategias para mitigar sus riesgos, sino que además permite establecer las modalidades delictivas que subyacen y consecuentemente contribuyen a la judicialización.

Consideraciones finales

Asobancaria resalta los esfuerzos realizados por el Gobierno en la elaboración e implementación de la Política Nacional de Seguridad Digital, necesaria para adaptarse a los nuevos desafíos y amenazas tecnológicas que enfrentan las naciones. Consideramos que, para lograr una correcta implementación del Convenio de Budapest, el Estado deberá fijar una hoja de ruta clara para armonizar su legislación interna a las exigencias penales y judiciales internacionales con el fin de combatir la amenaza de la ciberdelincuencia. De igual manera, deberá fortalecer los mecanismos de cooperación y la articulación del sector privado y de las autoridades mediante la intercomunicación de CSIRT existentes.

Es preciso recordar que, a pesar de los importantes avances que representa el acuerdo, algunos países que se han adherido no han iniciado una hoja de ruta clara para dar cumplimiento a los compromisos que se estipulan en el articulado del Convenio. En este sentido, la voluntad política de los Estados resulta fundamental para lograr una adecuada implementación de los acuerdos.

Colombia
Principales Indicadores Macroeconómicos

	2015					2016					2017					2018*	
	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	**Total**
Producto Interno Bruto**																	
PIB Nominal (COP Billones)	194,3	196,9	204,1	209,4	**804,7**	211,3	214,7	215,2	222,7	**863,9**	225,0	230,1	234,0	239,0	**928,1**	243,6	**985,6**
PIB Nominal (USD Billones)	75,4	76,2	65,4	66,5	**255,5**	67,5	71,7	73,6	74,0	**287,0**	76,5	75,7	79,7	80,1	**311,0**	87,6	**344,6**
PIB Real (COP Billones)	197,4	199,6	202,9	204,7	**804,7**	204,7	204,8	203,4	207,6	**820,5**	206,3	208,7	209,5	210,6	**835,2**	212,1	**856,9**
PIB Real (% Var. interanual)	3,0	3,3	3,8	1,8	**3,0**	3,7	2,6	0,2	1,4	**2,0**	0,8	1,9	3,0	1,4	**1,8**	2,8	**2,6**
Precios																	
Inflación (IPC, % Var. interanual)	4,6	4,4	5,4	6,8	**6,8**	8,0	8,6	7,3	5,7	**5,7**	4,7	4,0	4,0	4,1	**4,1**	3,1	**3,1**
Inflación sin alimentos (% Var. interanual)	3,9	4,5	5,3	5,9	**5,2**	6,2	6,3	5,9	5,1	**5,1**	5,1	5,1	4,7	5,0	**5,0**	4,1	**3,5**
Tipo de cambio (COP/USD fin de periodo)	2576	2585	3122	3149	**3149**	3129	2995	2924	3010	**3010**	2941	3038	2937	2984	**2984**	2780	**2860**
Tipo de cambio (Var. % interanual)	31,1	37,4	53,9	31,6	**31,6**	21,5	15,8	-6,3	-4,4	**-4,4**	-6,0	1,5	0,4	-0,9	**-0,9**	-5,5	**-4,2**
Sector Externo (% del PIB)																	
Cuenta corriente	-7,3	-5,6	-7,3	-5,2	**-6,3**	-5,6	-3,7	-4,8	-3,2	**-4,2**	-4,7	-3,2	-3,6	-2,0	**-3,3**	-3,5	**-3,0**
Cuenta corriente (USD Billones)	-5,4	-4,3	-5,0	-3,8	**-18,5**	-3,4	-2,6	-3,5	-2,6	**-12,0**	-3,4	-2,5	-2,8	-1,7	**-10,4**	-2,8	**-11,4**
Balanza comercial	-6,4	-4,6	-7,6	-6,5	**-6,2**	-6,2	-3,9	-4,6	-3,5	**-4,5**	-3,5	-3,3	-3,1	-1,6	**-2,8**	-2,2	**-3,2**
Exportaciones F.O.B.	15,9	15,6	16,5	14,5	**15,7**	14,7	14,9	14,9	14,5	**14,8**	15,3	14,9	15,6	15,1	**15,2**	15,6	**...**
Importaciones F.O.B.	22,3	20,2	24,1	21,0	**21,9**	20,9	18,8	19,5	18,0	**19,3**	18,8	18,2	18,7	16,7	**18,1**	17,8	**...**
Renta de los factores	-2,5	-2,6	-1,9	-0,8	**-2,0**	-1,7	-1,8	-2,1	-1,8	**-1,8**	-3,1	-2,0	-2,6	-2,6	**-2,6**	-3,4	**-2,3**
Transferencias corrientes	1,6	1,6	2,2	2,0	**1,9**	2,2	2,0	1,9	2,1	**2,1**	1,9	2,1	2,2	2,2	**2,1**	2,0	**1,8**
Inversión extranjera directa	4,4	5,3	3,2	2,9	**4,0**	7,7	5,2	3,1	4,1	**4,9**	3,4	3,3	6,3	4,6	**4,4**	2,7	**...**
Sector Público (acumulado, % del PIB)																	
Bal. primario del Gobierno Central	0,0	0,8	1,0	-0,5	**-0,5**	-0,2	0,3	0,1	-1,1	**-1,1**	-0,7	0,2	0,6	-0,8	**-0,8**	...	**-0,2**
Bal. del Gobierno Central	-0,4	0,2	-0,8	-2,0	**-3,0**	-0,8	-1,0	-2,5	-4,0	**-4,0**	-1,1	-1,2	-2,0	-3,6	**-3,6**	...	**-3,1**
Bal. estructural del Gobierno Central	...	...	...	...	**-2,2**	...	...	...	...	**-2,2**	...	...	...	...	**-1,9**	...	**-1,9**
Bal. primario del SPNF	0,6	1,8	1,8	-0,6	**-0,6**	1,0	2,1	1,8	0,9	**0,9**	-0,1	1,2	2,0	0,5	**0,5**	...	**0,6**
Bal. del SPNF	0,2	0,7	-0,4	-3,4	**-3,4**	0,3	0,6	-0,7	-2,4	**-2,4**	-0,7	-0,3	-0,8	-2,7	**-2,7**	...	**-2,4**
Indicadores de Deuda (% del PIB)																	
Deuda externa bruta*	36,5	37,1	37,5	37,9	**37,9**	40,4	41,2	41,1	42,5	**42,5**	39,0	39,1	40,2	40,2	**40,2**	36,7	**...**
Pública	21,8	22,2	22,4	22,7	**22,7**	24,2	24,8	24,8	25,2	**25,2**	23,3	22,8	23,4	23,2	**23,2**	21,2	**...**
Privada	14,7	14,9	15,1	15,2	**15,2**	16,2	16,3	16,3	17,2	**17,2**	15,7	16,2	16,8	17,0	**17,0**	15,4	**...**
Deuda bruta del Gobierno Central	39,6	40,3	45,1	45,0	**42,1**	43,1	43,9	44,5	46,0	**43,9**	43,6	44,1	45,6	46,6	**44,9**	...	**...**

* Proyecciones para el cierre de 2018. ** Datos corregidos por efectos estacionales y de calendario - DANE, base 2015.
Fuente: PIB y Crecimiento Real – DANE, proyecciones Asobancaria. Sector Externo – Banco de la República, proyecciones MHCP y Asobancaria. Sector Público – MHCP. Indicadores de deuda – Banco de la República, Departamento Nacional de Planeación y MHCP.

Colombia
Estados financieros del sistema bancario*

	may-18 (a)	abr-18	may-17 (b)	Variación real anual entre (a) y (b)
Activo	**586.106**	**584.635**	**565.681**	**0,4%**
Disponible	36.486	36.056	39.969	-11,5%
Inversiones y operaciones con derivados	106.561	106.736	98.026	5,4%
Cartera de crédito	427.125	424.396	404.619	2,3%
Consumo	118.895	117.920	109.857	4,9%
Comercial	238.658	237.666	231.880	-0,2%
Vivienda	57.577	56.870	51.648	8,1%
Microcrédito	11.995	11.940	11.235	3,5%
Provisiones	25.881	25.479	20.736	21,0%
Consumo	9.531	9.423	7.748	19,2%
Comercial	13.499	13.230	10.522	24,4%
Vivienda	1.999	1.979	1.635	18,6%
Microcrédito	840	835	819	-0,5%
Pasivo	**511.698**	**510.752**	**493.277**	**0,6%**
Instrumentos financieros a costo amortizado	446.088	445.052	428.781	0,9%
Cuentas de ahorro	162.659	165.380	155.725	1,3%
CDT	155.121	153.713	147.380	2,0%
Cuentas Corrientes	49.346	49.884	46.962	1,9%
Otros pasivos	3.268	3.263	3.120	1,5%
Patrimonio	**74.408**	**73.883**	**72.404**	**-0,4%**
Ganancia / Pérdida del ejercicio (Acumulada)	**3.419**	**2.875**	**3.423**	**-3,2%**
Ingresos financieros de cartera	18.161	14.480	18.702	-5,9%
Gastos por intereses	6.588	5.279	8.144	-21,6%
Margen neto de Intereses	12.055	9.591	11.114	5,2%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,88**	**4,87**	**4,14**	**0,74**
Consumo	5,90	6,08	5,78	0,12
Comercial	4,65	4,55	3,54	1,12
Vivienda	3,12	3,13	2,56	0,55
Microcrédito	7,69	7,79	7,93	-0,24
Cubrimiento	**124,2**	**123,2**	**123,7**	**-0,51**
Consumo	135,8	131,5	122,0	13,84
Comercial	121,5	122,4	128,3	-6,77
Vivienda	111,4	111,2	123,4	-12,07
Microcrédito	91,1	89,8	91,8	-0,78
ROA	1,41%	1,48%	1,46%	-0,1
ROE	11,39%	12,13%	11,73%	-0,3
Solvencia	15,71%	15,78%	16,07%	-0,4

* Cifras en miles de millones de pesos.
Fuente: Superintendencia Financiera de Colombia.

Edición 1148

Colombia

Principales indicadores de inclusión financiera

	2015	2016					2017					2018
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1
Profundización financiera - Cartera/PIB (%) EC	**49,9**	49,8	50,0	50,2	50,2	**50,2**	49,9	50,4	49,9	49,6	**49,6**	49,28
Efectivo/M2 (%)	**12,53**	12,72	12,76	12,69	12,59	**12,59**	12,39	12,24	12,19	12,18	**12,18**	12,40
Cobertura												
Municipios con al menos una oficina, un corresponsal bancario o un cajero automático (%)	**100**	100	100	100	100	**100**	100	100	100	-	**-**	
Municipios con al menos una oficina (%)	**66,2**	66,3	66,1	66,4	66,4	**66,4**	66,2	66,5	66,5	66,5	**66,5**	66,5
Municipios con al menos un corresponsal bancario (%)	**98,6**	98,7	98,5	98,4	98,3	**98,3**	98,6	98,8	98,8	-	**-**	
Acceso												
Productos personas												
Indicador de bancarización(%) SF*	**76,30**	77,10	77,30	77,40	77,30	**77,30**	77,10	78,50	79,10	80,10	**80,10**	
Indicador de bancarización (%) EC**	**75,40**	76,20	76,40	76,50	76,40	**76,40**	77,20	77,60	78,25	79,20	**79,20**	
Adultos con: (en millones)												
Cuentas de ahorro EC	**23,01**	23,38	23,53	23,63	23,53	**23,53**	24,05	24,35	24,68	25,16	**25,16**	
Cuenta corriente EC	**1,75**	1,75	1,74	1,71	1,72	**1,72**	1,72	1,72	1,71	1,73	**1,73**	
Cuentas CAES EC	**2,81**	2,82	2,83	2,83	2,83	**2,83**	2,82	2,83	2,83	2,97	**2,97**	
Cuentas CATS EC	**0,103**	0,103	0,103	0,103	0,103	**0,103**	0,103	0,103	0,103	0,103	**0,103**	
Otros productos de ahorro EC	**0,582**	0,612	0,626	0,646	0,769	**0,769**	0,767	0,779	0,777	0,781	**0,781**	
Crédito de consumo EC	**8,28**	8,53	8,51	8,63	8,74	**8,74**	8,86	8,99	9,04	9,17	**9,17**	
Tarjeta de crédito EC	**8,94**	9,12	9,20	9,37	9,58	**9,58**	9,81	9,96	10,00	10,27	**10,27**	
Microcrédito EC	**3,50**	3,59	3,57	3,52	3,56	**3,56**	3,69	3,63	3,63	3,68	**3,68**	
Crédito de vivienda EC	**1,31**	1,34	1,35	1,36	1,39	**1,39**	1,40	1,41	1,41	1,43	**1,43**	
Crédito comercial EC	**-**	-	-	-	-	**1,23**	1,00	0,992	0,985	1,02	**1,02**	
Al menos un producto EC	**24,66**	25,02	25,20	25,35	25,40	**25,40**	25,77	26,02	26,33	27,1	**27,1**	
Uso												
Productos personas												
Adultos con: (en porcentaje)												
Algún producto activo SF	**64,5**	64,6	65,4	66,0	66,3	**66,3**	67,1	67,4	67,6	68,6	**68,6**	
Algún producto activo EC	**63,5**	63,5	64,3	65,0	65,1	**65,1**	66,1	66,3	66,5	66,9	**66,9**	
Cuentas de ahorro activas EC	**71,7**	67,8	69,8	71.6	72,0	**72,0**	73,4	73,7	72,9	71,8	**71,8**	
Cuentas corrientes activas EC	**86,3**	85,2	85,4	84,8	84,5	**84,5**	84,5	83,8	83,9	83,7	**83,7**	
Cuentas CAES activas EC	**87,3**	87,5	87,5	87,5	87,5	**87,5**	87,7	87,5	87,5	89,5	**89,5**	
Cuentas CATS activas EC	**96,5**	96,5	96,5	96,5	96,5	**96,5**	96,5	96,5	96,5	96,5	**96,5**	
Otros productos de ahorro activos EC	**53,1**	55,1	65,8	65,9	66,6	**66,6**	65,1	65,6	64,3	62,7	**62,7**	
Créditos de consumo activos EC	**82,4**	82,5	82,4	82,7	82,8	**82,0**	83,0	83,2	83,4	83,5	**83,5**	
Tarjetas de crédito activas EC	**92,0**	92,2	92,2	92,3	92,3	**92,3**	91,7	91,1	90,8	90,1	**90,1**	
Microcrédito activos EC	**70,8**	70,5	99,0	66,3	66,2	**66,2**	71,8	71,0	71,4	71,1	**71,1**	

Edición 1148

Colombia

Principales indicadores de inclusión financiera

	2015	2016					2017					2018
	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1
Créditos de vivienda activos EC	**79,1**	78,4	79,1	79,4	79,3	**79,3**	79,2	79,3	79,2	78,9	**78,9**	
Créditos comerciales activos EC	**-**	84,2	83,3	84,2	84,9	**85,3**	85,6	85,5	85,1	84,7	**84,7**	
Acceso												
Productos empresas												
Empresas con: (en miles)												
Al menos un producto EC	**726,8**	730,3	729,3	725,9	751,0	**751,0**	751,0	756,8	759,2	775,2	**775,2**	
Cuenta de ahorro EC	**475,5**	480,7	480,4	481,0	500,8	**500,8**	500,8	507,0	508,7	522,7	**522,7**	
Cuenta corriente EC	**420,4**	419,6	419,2	412,0	420,9	**420,9**	420,9	424,5	425,5	430,7	**430,7**	
Otros productos de ahorro EC	**11,26**	11,39	11,70	13,39	15,24	**15,24**	15,24	14,37	14,13	14,12	**14,12**	
Crédito comercial EC	**223,2**	236,9	228,8	229,7	242,5	**242,5**	242,5	247,0	240,1	243,6	**243,6**	
Crédito de consumo EC	**96,65**	97,66	97,77	98,09	98,72	**98,72**	98,72	100,4	101,1	102,5	**102,5**	
Tarjeta de rédito EC	**77,02**	76,32	77,10	78,51	79,96	**79,96**	79,96	84,24	84,74	94,35	**94,35**	
Al menos un producto EC	**726,7**	730,3	729,3	725,9	751,0	**751,0**	751,0	756,8	759,1	775,1	**775,1**	
Uso												
Productos empresas												
Empresas con: (en porcentaje)												
Algún producto activo EC	**75,2**	70,6	74,9	74,5	74,7	**74,7**	74,7	74,5	73,2	73,3	**73,3**	
Algún producto activo SF	**75,2**	70,6	74,9	74,5	74,7	**74,7**	74,7	74,0	73,2	73,3	**73,3**	
Cuentas de ahorro activas EC	**49,1**	39,3	48,7	48,1	49,1	**49,1**	49,1	49,7	46,9	47,2	**47,2**	
Otros productos de ahorro activos EC	**45,3**	45,4	55,6	56,1	57,5	**57,5**	57,5	-	52,5	51,2	**51,2**	
Cuentas corrientes activas EC	**90,5**	89,0	89,3	89,0	89,1	**89,1**	89,1	88,4	88,5	88,5	**88,5**	
Microcréditos activos EC	**60,8**	60,6	61,7	63,0	63,2	**63,2**	63,2	63,1	63,0	62,0	**62,0**	
Créditos de consumo activos EC	**84,8**	84,3	84,8	85,1	84,9	**84,9**	84,9	85,1	85,4	85,1	**85,1**	
Tarjetas de crédito activas EC	**85,6**	88,4	88,8	88,7	88,6	**88,6**	88,6	88,8	88,3	89,4	**89,4**	
Créditos comerciales activos EC	**89,2**	90,4	89,9	90,3	91,3	**91,3**	91,3	91,3	90,4	90,8	**90,8**	
Operaciones												
Total operaciones (millones)	**4.333**	-	2.390	-	2.537	**4.926**	-	2.602	-	2.860	**5.462**	
No monetarias (Participación)	**44,7**	-	48,0	-	48,1	**48,0**	-	49,8	-	50,7	**50,3**	
Monetarias (Participación)	**55,3**	-	52,0	-	51,9	**52,0**	-	50,2	-	49,3	**49,7**	
No monetarias (Crecimiento anual)	**33,3**	-	30,4	-	15,4	**22,22**	-	12,9	-	18,9	**16,01**	
Monetarias (Crecimiento anual)	**6,09**	-	8,3	-	5,4	**6,79**	-	5,2	-	7,1	**6,14**	
Tarjetas												
Crédito vigentes (millones)	**13,75**	13,84	14,30	14,43	14,93	**14,93**	14,79	14,75	14,71	14,89	**14,89**	14,91
Débito vigentes (millones)	**22,51**	23,22	23,83	24,61	25,17	**25,17**	25,84	26,39	27,10	27,52	**27,52**	28,17
Ticket promedio compra crédito($miles)	**215,9**	202,5	204,5	188,9	205,8	**205,8**	200,9	199,5	187,9	201,8	**201,8**	194,1
Ticket promedio compra débito ($miles)	**137,4**	123,8	129,4	125,6	138,3	**138,3**	126,1	127,5	121,6	133,4	**133,4**	121,2

*EC: Establecimientos de crédito; incluye Bancos, Compañías de financiamiento comercial, Corporaciones financieras, Cooperativas financieras e Instituciones Oficiales Especiales.
**SF: Sector Financiero; incluye a los Establecimientos de crédito, ONG y Cooperativas no vigiladas por la Superintendencia Financiera.
Fuente: Profundización – Superintendencia Financiera y DANE. Cobertura, acceso y uso - Banca de las Oportunidades. Operaciones y tarjetas – Superintendencia Financiera.