ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Semana Económica 2019

Edición 1178

Riesgo cibernético y el futuro de la estabilidad financiera

26 de marzo de 2019

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

- El sistema financiero realiza funciones fundamentales para la actividad económica, como recaudar ahorro, asignar créditos, facilitar pagos, transferir riesgos, proporcionar liquidez y mediar en la asignación de precios. El deterioro significativo de cualquiera de estas funciones puede causar inestabilidad financiera.

- Según el Foro Económico Mundial, el riesgo de ciberataques puede llegar a ser tan probable y con el mismo nivel de impacto que los desastres naturales. Además, resulta más probable y con mayor impacto que los riesgos de ataques terroristas.

- Los choques financieros y las políticas económicas se originan en su mayoría por fallas de mercado, contrario a lo que ocurre con los choques cibernéticos. Estos son realizados y programados de manera premeditada con el objetivo de deshabilitar, destruir, corromper o comprometer el funcionamiento del mercado, lo que puede generar inestabilidad financiera.

- Colombia cuenta con un marco de política pública y un desarrollo institucional sólido, así como con Planes Sectoriales de Defensa de Infraestructura Crítica, incluido el sector financiero. Esto permite tener capacidades de gestión del riesgo y ciberresilencia acorde a los niveles de criticidad y ciberamenazas actuales.

- Asobancaria lidera, a través del Equipo de Respuesta a Incidentes de Ciberseguridad - CSIRT, los esfuerzos del sector para compartir los incidentes de ataques cibernéticos. En este equipo, la colaboración es el mejor mecanismo para enfrentar este nuevo reto en el sistema financiero.

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

Edición 1178

Riesgo cibernético y el futuro de la estabilidad financiera

Editor

Germán Montoya Moreno
Director Económico

Participaron en esta edición:

Jaime Rincón Arteaga
Andrés Quijano Díaz
Daniel Tocaría Díaz

El sector financiero es uno de los grandes determinantes del crecimiento económico. Las actividades que el sector realiza al recaudar ahorro, asignar créditos, facilitar pagos, transferir riesgos, proveer liquidez y mediar en la formación de precios, son fundamentales para el desempeño económico y productivo.

Teniendo en cuenta que el sector financiero es fundamental para el desarrollo y desempeño de las economías y la creciente importancia que han adquirido los ataques cibernéticos, el análisis acerca del impacto que el riesgo cibernético puede tener sobre el futuro de la estabilidad financiera es hoy una tarea crucial.

Esta Semana Económica analiza los canales por donde los riesgos cibernéticos y financieros interactúan y generan crisis financieras. Así mismo, muestra los avances institucionales, en regulación y técnicos alrededor del mundo diseñados para gestionar el riesgo cibernético. En este contexto, es preciso sensibilizar acerca de la importancia de incorporar los riesgos cibernéticos dentro de los modelos de estabilidad financiera.

En primer lugar, se hace una descripción de los aportes teóricos y empíricos del Centro de Análisis y Resiliencia del Sistema Financiero de Estados Unidos y de la Escuela de Asuntos Internacionales de la Universidad de Columbia. En segundo lugar, se describen las vulnerabilidades que tradicionalmente generan inestabilidad financiera y cómo las amenazas de ciberseguridad pueden influir. En tercer lugar, se muestran escenarios de crisis financieras causados por choques cibernéticos y los desarrollos institucionales y de política pública diseñados para atenderlas. Por último, se describen algunos retos y recomendaciones en materia de ciberdefensa para la gestión del riesgo.

Antecedentes

El Foro Económico Mundial, a través de su informe anual de Riesgos Globales, ha venido mostrando la creciente importancia que han adquirido los ataques cibernéticos, el fraude y robo de datos dentro de los riesgos globales con mayor probabilidad e impacto (Cuadro 1).

Por su parte, en 2016, el gobierno de Estados Unidos creó el Centro de Análisis y Resiliencia del Sistema Financiero (FSARC) para identificar el riesgo sistémico del sistema financiero ante las amenazas actuales y emergentes de ciberseguridad. El

Cuadro 1. Evolución de los riesgos globales en términos de probabilidad

	2015	2016	2017	2018	2019
1	Conflicto interestatal con consecuencias regionales	Migraciones involuntarias a gran escala	Cambio climático extremo	Cambio climático extremo	Cambio climático extremo
2	Cambio climático extremo	Cambio climático extremo	Migraciones involuntarias a gran escala	Grandes desastres naturales	Falla en la mitigación y adaptación del cambio climático
3	Fallas de gobernanza nacional	Falla en la mitigación y adaptación del cambio climático	Grandes desastres naturales	Ciberataques	Grandes desastres naturales
4	Crisis de Estados	Conflicto interestatal con consecuencias regionales	Ataques terroristas a gran escala	Robo de datos y fraude	Robo de datos y fraude
5	Alto desempleo estructural o informalidad	Grandes catástrofes naturales	Incidente masivo de robo de datos	Falla en la mitigación y adaptación del cambio climático	Ciberataques

Económicos | Ambientales | Tecnológicos | Sociales | Geopolíticos

Fuente: Foro Económico Mundial.

FSARC surgió como respuesta a la necesidad de identificar entidades financieras a las cuales un incidente cibernético pudiera generarles un impacto significativo.

En los últimos años el FSARC y la Escuela de Asuntos Internacionales de la Universidad de Columbia han realizado esfuerzos por mejorar el marco de análisis que permita comprender y mitigar el riesgo de los ataques cibernéticos y su impacto en la estabilidad financiera. Estos avances teóricos y conceptuales han sido relevantes en la generación de conocimiento y de sensibilización acerca de los ataques cibernéticos.

Vulnerabilidades tradicionales que generan inestabilidad financiera

El Fondo Monetario Internacional (FMI) define la Estabilidad Financiera como la capacidad del sistema financiero para facilitar y mejorar transacciones económicas, administrar riesgos y absorber choques[1].

En este sentido, la estabilidad es un interés constante de los gobiernos y creadores de política pública y demanda el diseño de estrategias de prevención y gestión de los ciclos sistémicos que puedan afectar el desempeño económico. Históricamente, las vulnerabilidades del sistema financiero han conducido a recesiones o crisis económicas, periodos de deflación, bajo crecimiento económico y desempleo.

Existen tres características tradicionales del sistema financiero que crean vulnerabilidades:

a. **Apalancamiento.** Altos niveles de endeudamiento están relacionados con altos niveles de vulnerabilidad sistémica. Un alto apalancamiento y una disminución del valor de los activos pueden causar una caída en el patrimonio de las instituciones financieras, así como en la capacidad para absorber los choques externos, lo que desencadena dificultades financieras de insolvencia.
b. **Maduración y transformación del riesgo.** Los sistemas financieros transforman activos ilíquidos de largo plazo y de alto riesgo (como las hipotecas de alto riesgo) en activos más seguros y líquidos. De haber un choque en el precio de los activos ilíquidos de riesgo, pueden darse retiros de fondos y venta de activos. Esto puede conducir a iliquidez y contagio de instituciones, una crisis sistémica.

[1] Schinasi, Garry J. (2004). *Defining Financial Stability*. IMF Working Paper No. 04/187. http://www.imf.org/en/Publications/WP/Issues/2016/12/31/Defining-Financial-Stability-17740.

c. **Prociclicidad del riesgo.** La prociclicidad interactúa con el apalancamiento y la transformación del riesgo para potenciar los auges y caídas de los precios de los activos. Por ejemplo, la caída de los precios de los activos hace que baje el valor de la garantía de los deudores (es decir, su valor neto) y suba el costo del endeudamiento (primas de riesgo y tasas de interés). Al aumentar el riesgo para los prestamistas, esta dinámica deprime aún más los precios de los activos de riesgo, creando un ciclo en donde a menor financiación, mayores pérdidas y mayores primas de riesgo.

¿Cómo y cuánto puede afectar el riesgo de ciberseguridad la estabilidad financiera?

Los ataques cibernéticos pueden comprometer los ingresos netos del sistema bancario. Un estudio del FMI[2], a través de modelaciones de riesgo financiero y con una muestra de 7.947 entidades bancarias de todo el mundo, señala que se pueden comprometer desde el 9% al 62% de los ingresos netos de las entidades (USD$97.000 millones a USD$ 642.000 millones) por ataques cibernéticos (Cuadro 2).

Cuadro 2. Estimación de pérdidas agregadas a entidades bancarias por riesgo cibernético

	Línea base		Escenario severo	
Independencia				
	Ingresos netos (%)	**$USD *BN***	**Ingresos netos (%)**	**$USD *BN***
Promedio	9	97	26	268
VaR (95%)	14	147	34	352
ES (95%)	18	187	40	409
VaR (99%)	19	201	41	427
ES (99%)	27	281	52	539
Asumiendo 20% de independencia*				
Promedio	12	127	34	351
VaR (95%)	18	184	43	446
ES (95%)	22	229	49	509
VaR (99%)	24	248	51	529
ES (99%)	32	329	62	642

***** Se asume contagio. El ciberataque tiene 20% de probabilidad de afectar dos o más firmas.
VaR: Valor en Riesgo. ES: Pérdida Esperada.
Fuente: FMI (2018) con datos de ORX News y SNL.

El estudio asume dos escenarios a partir del número de ataques, la posibilidad de riesgo de contagio y metodologías de cálculo de riesgo financiero. En el escenario de línea base e independencia, se asumen el número de ataques registrados en 2013 y sin riesgo de contagio. Bajo estos supuestos se pueden comprometer del 9% de los ingresos netos (USD$97.000 millones), hasta el 19% (USD$201.000 millones). Si se asume riesgo de contagio, los ingresos comprometidos pueden ser desde el 12% de los ingresos (USD$97.000 millones) hasta el 32% (que representa cerca de USD$329.000 millones).

El escenario dos asume que la cantidad de ataques cibernéticos es dos veces la registrada en 2013. Con el supuesto de independencia, sin riesgo de contagio, se pueden comprometer desde el 26% de los ingresos (USD$268.000 millones) hasta el 52% (USD$539.000 millones). Si se asume riesgo de contagio, los ingresos comprometidos ascienden desde el 34% de los ingresos (USD$351.000 millones) hasta el 62% (USD$642.000 millones). Además de una estimación promedio, en el Cuadro 1 se muestran metodologías de Valor en Riesgo (VaR) y Perdida Esperada (ES) con probabilidades del 95% y 99%, ambas técnicas estadísticas para estimar el nivel de riesgo.

Es importante señalar los determinantes en los que se crean vulnerabilidades que pueden comprometer los ingresos netos de las entidades bancarias y generar inestabilidad. Según la Oficina de Investigación Financiera (OFR) del Departamento del Tesoro de Estados Unidos, los incidentes de ciberseguridad generan riesgos de contagio, financiamiento y liquidez. Estos son los cuatro canales a través de los cuales los riesgos pueden ser transmitidos:

a. **Pocos actores sustitutos.** El sistema financiero está altamente interconectado y relacionado con empresas de sectores como servicios públicos, sistemas de comercio electrónico y cámaras de compensación, que desempeñan funciones vitales para toda la sociedad. La industria de servicios financieros, sin embargo, basa su infraestructura en el uso de Tecnología de la Información y las Comunicaciones para realizar transacciones y pagos. En el caso de una afectación sistémica, habría pocas alternativas, instituciones y empresas de servicios públicos.

[2] Bouveret, Antoine. (2018). *Cyber Risk for the Financial Sector: A framework for Quantitative Assesment*. IMF Working Paper WP/18/143.

b. **Pérdida de confianza y reputación.** Una campaña de ataques cibernéticos podría generar una pérdida de confianza y reputación significativa. Por ejemplo, ataques a cajeros automáticos, denegación de servicio a una o más instituciones financieras, fallas en los sistemas inducidos y fugas de información sensible de los banqueros o reguladores, podrían provocar pérdidas de confianza sistémicas.
c. **Integridad de los datos.** Los impactos sistémicos pueden surgir a partir de incidentes que afectan la calidad de los datos del mercado y el consumidor. Los casos recientes de ataques cibernéticos como WannaCry han mostrado que la restauración de los datos puede demorar más de lo esperado y causar una pérdida de integridad de los datos.
d. **Pocos proveedores.** La computación y el almacenamiento del mundo se concentra en pocos proveedores de servicios en la nube; las empresas de TI corporativas tienden a ser similares y ejecutan los mismos sistemas operativos y aplicaciones. Los casos recientes a menudo revelan dependencias que interrumpen el correcto funcionamiento de industrias enteras o zona geográficas.

Diferencias entre los choques cibernéticos y financieros tradicionales

Según la OFR, existen tres diferencias entre los choques cibernéticos y financieros que pueden crear inestabilidad financiera sistémica: planeación (*timing*), complejidad e intención adversa[3].

- **Planeación de los ataques (*timing*).** Los determinantes típicos que desencadenan inestabilidad financiera se caracterizan por no estar programados. En cambio, los ataques cibernéticos requieren una planeación para su ejecución. En algunos casos, los ciberdelincuentes se infiltran en un sistema meses antes de ejecutar el ataque, con el fin de planear la mejor manera de causar una interrupción.

- **Complejidad.** El ciberespacio es un sistema complejo a nivel físico, de red y cognitivo. Tradicionalmente, estos sistemas están altamente interconectados y estrechamente acoplados, por lo que las interrupciones pueden conectarse en cascada fácilmente. Este riesgo correlacionado es la razón por la cual el ciberespacio es capaz de tener eventos muy impredecibles y de consecuencias altas. Pese a que el sector financiero también es complejo, al menos en finanzas, esta complejidad es el objeto de un estudio intenso por parte de especialistas en riesgos que utilizan modelos avanzados y maduros. Modelos como estos no existen en el mismo grado para la gestión del riesgo cibernético.
- **Intención de los ciberdelincuentes.** Los riesgos cibernéticos generalmente se diseñan y ejecutan por intenciones voluntarias de los ciberdelincuentes con objetivos maliciosos. En contraste, los choques financieros pueden surgir de externalidades, fallas de mercado y de la subestimación del efecto de políticas macroeconómicas. Los choques financieros no son causados con intenciones maliciosas y premeditadas. Los ataques cibernéticos, por su parte, son dirigidos y programados para deshabilitar, destruir y corromper el mercado, generando inestabilidad financiera.

Tipos de crisis financieras generadas a partir de riesgos cibernéticos

Los delincuentes cibernéticos pueden causar tres tipos de crisis:

a. **Crisis de combustión lenta.** Se producen cuando un ciberdelicuente usa las capacidades cibernéticas para causar fricción a largo plazo, pérdida de confianza e interrupción de los servicios.

b. **Crisis exacerbadas.** Ocurren cuando una crisis financiera ya está en progreso, o una nación está al borde de una, y un adversario intencionalmente le da un empujón con un ataque cibernético.

c. **Crisis premeditadas.** Surgen cuando los ciberdelincuentes utilizan capacidades para crear desde cero una crisis financiera. Ejemplo de ello son los ataques a una infraestructura financiera crítica cibernética, como sistemas de pago.

Los ataques cibernéticos, como ya se explicó, difieren de los choques financieros y de políticas tradicionales tanto en la intención como en el momento. Si bien ningún ataque hasta la fecha ha generado inestabilidad financiera, el impacto potencial de un ataque cibernético programado para desestabilizar las funciones y vulnerabilidades de los canales tradicionales del sistema financiero no se ha examinado lo suficiente.

[3] U.S. Treasury Department Office of Financial Research. (2017). *Cybersecurity and Financial Stability: Risks and Resilience*.

Escenarios de ataques cibernéticos que pueden afectar la estabilidad financiera

La defensa cibernética debe ser atendida de manera integral, teniendo en cuenta la multiplicidad de actores, quienes deben usar herramientas técnicas y legales disponibles y pueden desarrollar nuevas si es necesario. Así mismo, este enfoque debe promover la cooperación internacional y los avances en materia de regulación. Según el Instituto de Finanzas Internacionales (IFF) los siguientes cuatro escenarios de riesgo cibernético pueden afectar la estabilidad financiera[4].

1. Ataque cibernético a sistemas de pago al por mayor y minoristas. Un ataque a estos sistemas puede interrumpir la prestación de servicios esenciales durante períodos de tiempo prolongados.
2. Robos a gran escala de datos. Ataques cibernéticos dirigidos a Depósitos de Centrales de Valores pueden generar cambios en la estabilidad financiera.
3. Ataques a la infraestructura de la que depende el sistema financiero como la red eléctrica.
4. Ataques a consumidores minoristas y la sociedad en general. Provocaría desconfianza en la seguridad y la solidez de las partes del sistema financiero, debido a unos pocos ataques cibernéticos muy significativos o muchos ataques menores muy frecuentes y exitosos contra instituciones financieras o infraestructuras de mercados financieros.

Capacidades de protección, resiliencia y desarrollos institucionales y de política pública

En Estados Unidos, en el año 2013, el Departamento de Seguridad diseñó una política pública para identificar infraestructuras que pudieran verse afectadas por ataques cibernéticos como el sistema de salud pública, seguridad económica y seguridad nacional. A partir de esto, ocho de los bancos decidieron, a nivel de CEO, unirse para crear el Centro de Resistencia y Análisis Sistémico Financiero (FSARC), ahora una subsidiaria del FS-ISAC.

Los miembros fundadores - Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street y Wells Fargo - crearon el FSARC para "identificar, analizar, evaluar y coordinar de manera proactiva las actividades para mitigar el riesgo sistémico para el sector financiero estadounidense. Además, crearon el Sistema de Amenazas de Seguridad Cibernética actuales y emergentes a través de operaciones enfocadas y una mejor colaboración entre las firmas participantes, socios de la industria y el gobierno de los Estados Unidos[5]".

Dentro de esos sistemas se realizan ejercicios de ataques cibernéticos en los sectores público y privado, que desempeñan un papel importante en la identificación de brechas y puntos débiles para una posible explotación. Sheltered Harbor, una organización encargada de proteger la confianza del público en el sistema financiero de Estados Unidos, fue el resultado directo de las lecciones aprendidas de estos ejercicios cibernéticos. Trimestralmente, los principales actores de la industria bancaria se someten a un ejercicio que simula un escenario de ataque diferente. En el caso del FS-ISAC y el Consejo de Riesgos de Pagos los ejercicios son anuales y simulan un ciberataque contra los procesos de pago.

De acuerdo con la National Automated Clearance House Association (NACHA), estas simulaciones ayudan a identificar brechas en los planes de respuesta a incidentes, fortalecer las relaciones del equipo de respuesta a incidentes, desarrollar la comprensión de las vulnerabilidades del sistema e impulsar la exploración de mejoras en la respuesta.

De hecho, en 2015, los gobiernos británico y estadounidense realizaron un ejercicio conjunto con el sector privado para mejorar el entendimiento entre el gobierno y la industria en el intercambio de información, la respuesta a incidentes y las comunicaciones públicas. Los esfuerzos hasta la fecha se han centrado en los Estados Unidos. Sin embargo, en 2013, el FSISAC amplió su estatuto para incluir a instituciones financieras globales en regiones como Asia, Europa, América del Norte y del Sur.

Principales retos

El sistema financiero ha logrado un gran progreso en la defensa cibernética, tanto a nivel nacional como

[4] Boer, Martin, and Jaime Vazquez. (2017). *Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System*. Institute of International Finance, p. 9. Retrieved from www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf
[5] Office of Financial Research. (2016). *2016 Financial Stability Report*. Tomado de https://www.financialresearch.gov/financial-stability-reports/files/OFR_2016_Financial-Stability-Report.pdf

transfronterizo. Actualmente, se están realizando ejercicios de simulación de crisis cibernética, se están mapeando los riesgos de ciberseguridad y se pueden detectar las vulnerabilidades en las redes. Sin embargo, hay tres retos principales que persisten:

a. Ciberdelincuentes. Los ciberdelincuentes son cada vez más informados y sofisticados, lo que podría apuntar deliberadamente a la inestabilidad financiera (o involuntariamente causarla). La complejidad de la dependencia tecnológica ha generado una preocupación relacionada y creciente. Incluso actores poco sofisticados pueden ser capaces de desencadenar efectos sistémicos[6].

b. Mayor entendimiento. Existe una escasez de información y análisis sobre las posibles interacciones de los riesgos cibernéticos, los canales de contagio financiero y los posibles "amplificadores" dentro de esos canales, como los puntos únicos de falla. El trabajo adicional aquí es crucial para comprender cómo el riesgo cibernético se relaciona con los flujos y decisiones empresariales cuando los mercados y las instituciones están bajo presión.

c. Uso de nuevas tecnologías. A pesar de que el sistema financiero ya es altamente complejo, continúa transformándose, especialmente con el crecimiento explosivo de las fintech. Algunas de estas tecnologías tendrán un impacto sistémico, otras acelerarán el riesgo y otras lo reducirán. Por ejemplo, la tecnología blockchain puede reducir el riesgo al disminuir los puntos únicos de falla, mientras que la computación en la nube reduce la mayoría de los riesgos cibernéticos, pero aumenta la dependencia de algunos proveedores clave. Será especialmente difícil desarrollar controles ante una mayor complejidad financiera y tecnológica.

Recomendaciones y consideraciones finales

Teniendo en cuenta estos retos, las siguientes recomendaciones resaltan la necesidad de tener una mayor comprensión compartida de las dos disciplinas, la estabilidad financiera y el riesgo cibernético, así como las acciones para armonizar los enfoques de resiliencia en todo el sector financiero:

a. Armonizar las regulaciones internacionales que fomenten la resistencia a los ataques cibernéticos y mitiguen el riesgo en caso de un ataque. Este enfoque regulatorio y de supervisión debe tener la suficiente elasticidad para evolucionar con los cambios tecnológicos y la sofisticación del adversario.

b. Llevar a cabo investigaciones adicionales para identificar datos y facilitar el diseño de modelos para medir o cuantificar el riesgo cibernético, incluido el desarrollo de un léxico compartido o taxonomía para discutir este tipo de riesgo como un factor en la estabilidad financiera. El esfuerzo del Consejo de Estabilidad Financiera del G20 (FSB), iniciado en julio de 2018, en Estados Unidos, es un gran avance para crear un léxico de seguridad cibernética y la resistencia cibernética a través de su proceso consultivo. Sin embargo, aún se debe compartir un léxico entre las comunidades cibernéticas y de estabilidad financiera, no solo en beneficio de los expertos financieros, sino para fomentar una mayor comunicación y resistencia en ambos sentidos. Por ejemplo, el léxico omitió "riesgo" y "ataque", que tienen diferentes significados en las comunidades cibernéticas y de estabilidad financiera y podrían llevar a malentendidos en el contexto de una crisis.

c. Compartir y desarrollar aún más los mapas de las estructuras críticas del mercado, así como los procesos y convenciones del mercado (tanto los esfuerzos recientes del sector público como el privado) y desarrollar mapas adicionales para comprender mejor la superposición del riesgo cibernético en la plomería de los mercados e instituciones. Se debe prestar especial atención a cómo el contagio de la tecnología cibernética puede interactuar con las decisiones comerciales y las respuestas financieras, lo que a su vez puede inducir el contagio financiero. Desarrollar planes de acción basados en esta comprensión y uso de estos mapas.

d. Realizar más ejercicios de simulación de incidentes cibernéticos, a nivel nacional y transfronterizo. Las partes interesadas deben incluir ejecutivos de la alta dirección de compañías de seguridad cibernética, reguladores, bancos y bancos centrales. Los ejercicios deberían incluir cada vez más a todos los

[6] Villeneuve, Nart. (2010). *Inside a Crimeware Network*. Infowar Monitor Technical Report No. JR04-2010 https://citizenlab.ca/wp-content/uploads/2017/05/koobface.pdf

centros financieros y reguladores globales para que coincidan con la naturaleza global del ciberespacio y las finanzas.

Cada año, los ataques cibernéticos se vuelven más severos y los adversarios más arriesgados. El sector financiero global ha sido un objetivo de los ciberdelincuentes a escalas mucho más grandes y sofisticadas. Estos ataques podrían haber tenido un impacto sistémico si no hubiera sido por los decididos esfuerzos de los tecnólogos y líderes. Sin embargo, los adversarios, por diseño o por accidente, realizarán algún día un ataque que esté más allá de la capacidad de estos defensores. Por lo tanto, nunca ha sido más importante continuar el trabajo de reconciliar y mitigar los riesgos cibernéticos para la estabilidad financiera.

Sobre el fortalecimiento de las capacidades de ciberdefensa y ciberseguridad de Colombia, se resalta de manera muy positiva que los últimos gobiernos hayan orientado sus esfuerzos en implementar una política pública dirigida a atender las necesidades de ciberseguridad en todos los sectores de la economía.

Desde Asobancaria resaltamos la importancia del Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia que lidera el Comando Conjunto Cibernético - CCOC, el cual define los lineamientos generales que deben adoptar los diversos actores, dueños y operadores de las infraestructuras críticas cibernéticas del país. Este conjunto de actores está compuesto por entidades del sector público y privado que pertenecen a sectores que brindan servicios esenciales, como el energético, telecomunicaciones, de servicios financieros, entre otros.

Sin lugar a dudas, esta iniciativa contribuye a definir una hoja de ruta para trabajar de manera conjunta con el Gobierno ante ataques cibernéticos e incidentes que afecten la prestación de servicios esenciales. Es decir, ataques contra aquellos servicios necesarios para el mantenimiento de las funciones sociales básicas como la salud, la educación, la seguridad y el bienestar social y económico de la población, los cuales son prestados y soportados en su operación por la Infraestructura crítica de la Nación y que sustentan a la sociedad colombiana.

De igual forma, destacamos la adhesión de Colombia al Convenio de Budapest en 2018, mediante la aprobación de la Ley 1928 del 24 de julio de 2018, siendo el avance regulatorio más importante de colaboración internacional para la investigación y judicialización de los delitos informáticos. A partir de ahora, el país debe fijar una hoja de ruta clara para armonizar su legislación interna a las exigencias penales y judiciales internacionales para combatir la amenaza de la ciberdelincuencia.

Para cumplir con este y otros objetivos, Asobancaria ha venido desarrollando e implementando una serie de estrategias gremiales. En Colombia, es la Asobancaria, quien a través del Equipo de Respuesta a Incidentes de Ciberseguridad – CSIRT, lidera los esfuerzos de colaboración en el sector para compartir los incidentes de ataques cibernéticos. Es a través de la colaboración que mejor se puede enfrentar este nuevo reto del sector financiero.

Colombia
Principales indicadores macroeconómicos

	2015	2016					2017					2018					2019*
	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	Total
Producto Interno Bruto**																	
PIB Nominal (COP Billones)	**804,7**	209,0	213,5	218,6	222,8	**863,8**	224,3	228,4	231,6	235,9	**920,2**	240,5	242,9	245,3	247,4	**976,1**	**1043,6**
PIB Nominal (USD Billones)	**255,5**	66,8	71,3	74,7	74,0	**287,0**	76,3	75,2	78,9	79,0	**308,4**	86,5	82,9	82,5	76,1	**300,3**	**325,0**
PIB Real (COP Billones)	**804,7**	192,0	199,5	206,1	223,8	**821,5**	194,4	202,2	209,4	226,6	**832,6**	198,4	208,2	215,0	233,0	**854,7**	**882,1**
PIB Real (% Var. interanual)	**3,0**	3,1	1,9	1,4	2,0	**2,1**	1,1	1,9	1,4	1,0	**1,8**	2,2	2,6	2,9	2,9	**2,7**	**3,2**
Precios																	
Inflación (IPC, % Var. interanual)	**6,8**	8,0	8,6	7,3	5,7	**5,7**	4,7	4,0	4,0	4,1	**4,1**	3,1	3,2	3,2	3,2	**3,2**	**3,6**
Inflación sin alimentos (% Var. interanual)	**5,2**	6,2	6,3	5,9	5,1	**5,1**	5,1	5,1	4,7	5,0	**5,0**	4,1	3,8	3,7	3,5	**3,5**	**3,6**
Tipo de cambio (COP/USD fin de periodo)	**3149**	3129	2995	2924	3010	**3010**	2941	3038	2937	2984	**2984**	2780	2931	2972	3250	**3250**	**3211**
Tipo de cambio (Var. % interanual)	**31,6**	21,5	15,8	-6,3	-4,4	**-4,4**	-6,0	1,5	0,4	-0,9	**-0,9**	-5,5	-3,5	1,2	8,9	**8,9**	**-1,2**
Sector Externo (% del PIB)																	
Cuenta corriente	**-6,4**	-5,6	-3,7	-4,7	-3,2	**-4,3**	-4,7	-3,3	-3,7	-1,9	**-3,3**	-3,5	-3,7	-3,7	-4,8	**-3,8**	**-3,6**
Cuenta corriente (USD Billones)	**-18,6**	-3,4	-2,6	-3,5	-2,6	**-12,1**	-3,5	-2,5	-2,8	-1,7	**-10,4**	-2,8	-3,1	-3,1	-3,7	**-12,7**	**-12,8**
Balanza comercial	**-6,3**	-6,2	-3,9	-4,6	-3,5	**-4,6**	-3,5	-3,3	-3,1	-1,4	**-2,9**	-1,9	-2,6	-2,8	-4,1	**-2,8**	**-1,2**
Exportaciones F.O.B.	**15,8**	14,8	14,9	14,8	14,6	**14,9**	15,1	14,9	15,7	15,4	**15,5**	15,8	15,9	16,3	18,1	**16,3**	**13,2**
Importaciones F.O.B.	**22,1**	21,0	18,9	19,4	18,1	**19,5**	18,6	18,2	18,8	16,8	**18,3**	17,8	18,6	19,1	22,2	**19,1**	**14,5**
Renta de los factores	**-2,0**	-1,7	-1,8	-2,1	-1,8	**-1,9**	-3,2	-2,1	-2,7	-2,7	**-2,6**	-3,5	-3,2	-3,3	-3,7	**-3,4**	**-3,2**
Transferencias corrientes	**1,9**	2,2	2,0	1,9	2,1	**2,1**	1,9	2,1	2,2	2,2	**2,2**	2,0	2,1	2,3	2,9	**2,3**	**2,3**
Inversión extranjera directa (pasivo)	**4,0**	7,7	5,2	3,1	4,1	**4,9**	3,4	3,3	6,4	4,6	**4,7**	2,6	4,3	3,0	3,5	**3,3**	**3,8**
Sector Público (acumulado, % del PIB)																	
Bal. primario del Gobierno Central	**-0,5**	-0,2	0,3	0,1	-1,1	**-1,1**	-0,7	0,2	0,6	-0,8	**-0,8**	-0,1	-0,3	...	...	**-0,2**	**...**
Bal. del Gobierno Central	**-3,0**	-0,8	-1,0	-2,5	-4,0	**-4,0**	-1,2	-1,2	-2,0	-3,6	**-3,6**	-0,6	-1,5	...	...	**-3,1**	**-2,4**
Bal. estructural del Gobierno Central	**-2,2**	...	...	...	...	**-2,2**	...	...	...	...	**-1,9**	...	...	...	...	**-1,9**	**...**
Bal. primario del SPNF	**-0,6**	1,0	2,1	1,8	0,9	**0,9**	-0,1	1,2	2,0	0,5	**0,5**	0,5	0,8	...	...	**0,6**	**0,5**
Bal. del SPNF	**-3,4**	0,3	0,6	-0,7	-2,4	**-2,4**	-0,5	-0,3	-0,8	-2,7	**-2,7**	0,0	-0,5	...	...	**-2,4**	**...**
Indicadores de Deuda (% del PIB)																	
Deuda externa bruta*	**38,2**	40,8	41,3	41,2	42,5	**42,5**	38,5	38,5	39,6	39,6	**39,6**	36,5	36,5	...	...	**...**	**...**
Pública	**22,6**	24,1	24,7	24,6	25,1	**25,1**	22,9	22,4	23,0	22,8	**22,8**	21,2	20,9	...	...	**...**	**...**
Privada	**15,6**	16,7	16,6	16,6	17,4	**17,4**	15,6	16,0	16,6	16,7	**16,7**	15,3	15,5	...	...	**...**	**...**
Deuda bruta del Gobierno Central	**40,8**	43,1	43,9	44,5	46,0	**42,5**	43,6	44,1	45,6	46,6	**43,1**	43,7	46,1	...	...	**...**	**...**

* Proyecciones. ** PIB Real: 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*

	ene-19 (a)	dic-18	ene-18 (b)	Variación real anual entre (a) y (b)
Activo	**624.806**	**627.253**	**581.264**	**4,2%**
Disponible	42.594	45.918	37.494	10,1%
Inversiones y operaciones con derivados	118.793	116.155	107.005	7,6%
Cartera de crédito	440.763	443.737	416.734	2,5%
Consumo	126.663	126.225	116.043	5,8%
Comercial	239.707	243.508	233.605	-0,5%
Vivienda	62.165	61.801	55.257	9,1%
Microcrédito	12.227	12.203	11.829	0,2%
Provisiones	27.770	27.461	24.395	10,4%
Consumo	9.793	9.724	9.007	5,4%
Comercial	14.847	14.655	12.629	14,0%
Vivienda	2.196	2.166	1.893	12,5%
Microcrédito	934	915	854	6,0%
Pasivo	**541.028**	**544.296**	**502.657**	**4,3%**
Instrumentos financieros a costo amortizado	466.362	469.764	441.714	2,4%
Cuentas de ahorro	174.328	176.914	166.445	1,5%
CDT	152.033	149.284	144.308	2,1%
Cuentas Corrientes	52.060	56.352	53.145	-5,0%
Otros pasivos	5.771	4.269	3.201	74,8%
Patrimonio	**83.779**	**82.957**	**76.354**	**6,4%**
Ganancia / Pérdida del ejercicio (Acumulada)	**851**	**9.668**	**529**	**56,1%**
Ingresos financieros de cartera	3.735	43.873	3.656	-0,9%
Gastos por intereses	1.285	15.574	1.354	-8,0%
Margen neto de Intereses	2.493	29.289	2.354	2,7%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,71**	**4,51**	**4,52**	**0,19**
Consumo	5,27	5,17	5,92	-0,65
Comercial	4,65	4,36	3,99	0,67
Vivienda	3,25	3,17	3,12	0,13
Microcrédito	7,63	7,37	8,04	-0,42
Cubrimiento	**133,7**	**137,3**	**129,4**	**-4,26**
Consumo	146,8	149,1	131,1	15,70
Comercial	133,1	138,0	135,6	-2,52
Vivienda	108,7	110,5	109,9	-1,28
Microcrédito	100,2	101,7	89,8	10,40
ROA	1,65%	1,54%	1,10%	0,5
ROE	12,90%	11,65%	8,63%	4,3
Solvencia	15,44%	15,58%	15,55%	-0,1

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

Edición 1178

Colombia

Principales indicadores de inclusión financiera

	2015	2016					2017					2018				
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**
Profundización financiera - Cartera/PIB (%) EC	**49,9**	49,9	50,2	50,3	50,2	**50,2**	49,8	50,2	49,9	49,6	**49,6**	49,4	49,3	48,8	50,3	**50,3**
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	12,07	12,27	13,09	**13,09**
Cobertura																
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,9**	100	100	99,9	99,7	**99,7**	100	100	99,9	100	**100**	99,9	100	…	…	…
Municipios con al menos una oficina (%)	**75,3**	73,8	73,7	74,0	73,9	**73,9**	73,7	74,0	73,9	73,9	**73,9**	74,0	74,1	74,2	…	…
Municipios con al menos un corresponsal bancario (%)	**99,6**	99,7	99,6	99,6	99,5	**99,5**	99,8	100	99,9	100	**100**	99,9	100	…	…	…
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**	80,10	80,8	81,3	…	…
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**	79,00	79,70	80,4	…	…
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**	25,00	25,3	25,6	…	…
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**	1,74	1,81	1,8	…	…
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**	3,00	3,02	3,02	…	…
Cuentas CATS EC	**0,10**	0,10	0,10	0,10	0,10	**0,10**	0,10	0,10	0,10	0,10	**0,10**	0,10	0,10	0,10	…	…
Otros productos de ahorro EC	**0,58**	0,61	0,63	0,65	0,77	**0,77**	0,77	0,78	0,78	0,78	**0,78**	0,78	0,81	0,82	…	…
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**	7,23	7,37	7,47	…	…
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**	9,55	9,83	9,98	…	…
Microcrédito EC	**3,50**	3,59	3,57	3,52	3,56	**3,56**	3,69	3,63	3,63	3,68	**3,68**	3,41	3,50	3,49	…	…
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**	1,34	1,37	1,38	…	…
Crédito comercial EC	**-**	-	-	-	-	**1,23**	1,00	0,99	0,98	1,02	**1,02**	0,65	0,67	0,66	…	…
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**	26,8	27,2	27,5	…	…
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**	67,1	68,0	68,4	…	…
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**	65,7	66,6	67,1	…	…
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**	67,7	68,4	68,4	…	…
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**	84,4	85,0	85,1	…	…
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**	89,7	89,8	89,8	…	…
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**	96.5	95,2	96,5	…	…
Otros pdtos. 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**	62,0	62,5	62,1	…	…
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**	82,0	81,5	81,8	…	…
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**	88,9	88,9	88,7	…	…
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**	71,2	70,4	69,4	…	…

Edición 1178

Colombia

Principales indicadores de inclusión financiera

	2015	2016					2017					2018				
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**
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**	78,2	77,7	77,8	…	…
Créditos comerciales activos EC	**-**	84,2	83,3	84,2	84,9	**85,3**	85,6	85,5	85,1	84,7	**84,7**	59,2	58,7	57,6	…	…
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**	944,3	947,8	946,6	…	…
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**	649,7	647,7	648,9	…	…
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**	488,9	505,2	502,4	…	…
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**	14,4	14,1	14,0	…	…
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**	265,3	272,2	276,5	…	…
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**	104,4	106,7	105,3	…	…
Tarjeta de crédito EC	**77,02**	76,32	77,10	78,51	79,96	**79,96**	79,96	84,24	84,74	94,35	**94,35**	102,1	104,4	105,1	…	…
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**	944,3	947,8	946,6	…	…
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**	71,6	71,9	71,6	...	...
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**	71,7	71,9	71,6	...	...
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**	48,1	47,7	48,2	…	…
Otros pdtos. de ahorro activos EC	**45,3**	45,4	55,6	56,1	57,5	**57,5**	57,5	53,6	52,5	51,2	**51,2**	50,8	49,5	49,5	…	…
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**	88,5	88,2	88,6		
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**	58,5	58,5	57,2		
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**	83,7	83,4	83,7	…	…
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**	90,6	89,8	90,0		
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**	91,0	91,1	91,4	…	…
Operaciones (semestral)																
Total operaciones (millones)	**4.333**		- 2.390		- 2.537	**4.926**		- 2.602		- 2.860	**5.462**		- 2.926		- 3.406	**6.332**
No monetarias (Participación)	**44,7**		- 48,0		- 48,1	**48,0**		- 49,8		- 50,7	**50,3**		- 52,5		- 55,6	**54,2**
Monetarias (Participación)	**55,3**		- 52,0		- 51,9	**52,0**		- 50,2		- 49,3	**49,7**		- 47,4		- 44,3	**45,8**
No monetarias (Crecimiento anual)	**33,3**		- 30,4		- 15,4	**22,22**		- 12,9		- 18,9	**16,01**		- 18,66		- 30,9	**25,1**
Monetarias (Crecimiento anual)	**6,09**		- 8,3		- 5,4	**6,79**		- 5,2		- 7,1	**6,14**		- 6,30		- 7,0	**6,7**
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	15,03	15,17	15,28	**15,28**
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	28,68	29,26	29,57	**29,57**
Ticket promedio compra crédito ($miles)	**215,9**	202,5	204,5	188,9	205,8	**205,8**	200,9	199,5	187,9	201,8	**201,8**	194,1	196,1	183,1	194,4	**194,4**
Ticket promedio compra débito ($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	123,2	120,3	131,4	**131,4**

*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.