ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Semana Económica 2018

Edición 1133

La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones

23 de abril de 2018

• La creciente trasformación digital ha promovido el aumento del uso de las tecnologías de la información y las comunicaciones en todos los aspectos de la dinámica económica y social. Esta situación también ha traído consigo nuevos riesgos asociados con la confidencialidad y protección de información, así como frente al resguardo de las infraestructuras cibernéticas que soportan los negocios.

• El aumento de los ataques cibernéticos es inminente. Según *Kaspersky*, en América Latina crecieron en un 59% entre 2016 y 2017. Además, cada vez son más diversos, sofisticados, potentes y con mayor alcance e impacto. En Colombia, de acuerdo con un informe del Centro Cibernético Policial, el cibercrimen en el país aumentó 28,3% en 2017.

• En Colombia, el Estado ha avanzado en la definición de una política pública de ciberseguridad y en el fortalecimiento institucional. Sin embargo, debido a los enormes impactos que podría tener un incidente cibernético, no solo en términos netamente monetarios sino en pérdida de información y amenaza sobre la reputación, todas las instituciones públicas y privadas deben trabajar en el fortalecimiento de sus capacidades para anticiparse a las ciberamenazas.

• El sector financiero es uno de los que más invierte en materia de protección de los datos y de los sistemas de información. Ha venido incorporando, además, prácticas internas de ciberseguridad y seguridad de la información. No obstante, es pertinente seguir fortaleciendo las capacidades empresariales para anticiparse a estos riesgos.

• Recientemente la Superintendencia Financiera publicó para comentarios un proyecto que busca impartir instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. En este documento se destaca: (i) la inclusión del enfoque de riesgos frente a los temas de ciberseguridad y seguridad de la información y (ii) el ascenso de las responsabilidades de aprobar y monitorear las acciones por parte de los mayores órganos de dirección.

• Es previsible que la expedición de esta regulación acelere los avances en la constitución de un sistema de gestión de riesgos de ciberseguridad e implique reorganizaciones al interior de cada institución para fortalecer sus capacidades frente a las amenazas cibernéticas.

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Jonathan Malagón
Vicepresidente Técnico

Germán Montoya
Director Económico

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

Edición 1133

La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones

La creciente importancia que han adquirido las tecnologías de la información en los procesos productivos ha conducido a importantes ventajas económicas y financieras, pero también ha conllevado nuevos riesgos asociados con la confidencialidad y protección de datos e información, así como con las infraestructuras cibernéticas que sustentan los negocios.

El crecimiento de las amenazas cibernéticas es irrefutable. En los últimos años se ha evidenciado que los ataques son cada vez más diversos, sofisticados, potentes y con mayor alcance e impacto. La materialización de una ciberamenaza puede traer consecuencias enormes, desde pérdidas económicas directas y de información confidencial, hasta daños a la reputación.

Este panorama hace que todas las instituciones, públicas y privadas, deban concentrar importantes esfuerzos en generar las capacidades necesarias para detectar las amenazas, identificar los ataques y prevenir que se materialicen en una afectación de sus sistemas y/o de la información.

En relación con el Estado colombiano, uno de los adelantos más importantes es el fortalecimiento de la capacidad institucional. En la actualidad existen diversas instancias estatales que buscan responder a las necesidades de las diferentes aristas que requiere tener un modelo de prevención y gestión de incidentes cibernéticos.

Por su parte, el sector financiero es uno de los que más invierte en materia de protección de los datos y de los sistemas de información. Además, ha venido incorporando prácticas internas de ciberseguridad y seguridad de la información. Sin embargo, es clara la necesidad que tienen las organizaciones de seguir fortaleciendo sus capacidades para anticiparse a las amenazas cibernéticas.

La Superintendencia Financiera expidió recientemente para comentarios un proyecto de Circular Externa con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. Seguramente la expedición de una regulación en este sentido acelerará los avances en la constitución de un sistema de gestión de riesgos de ciberseguridad, sobre el que varias entidades financieras vienen trabajando, e implicará reorganizaciones al interior de cada institución para reforzar sus capacidades frente a las amenazas cibernéticas.

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Ginna Pardo Moreno
Andrés Quijano Díaz
Hernán Felipe Ramírez
Camila Barrera Neira

Sin embargo, es necesario avanzar también en la articulación de los diferentes actores y sectores, no solo pensando en fortalecer la capacidad de respuesta ante la materialización de eventos de ciberseguridad sino también para robustecer el modelo de riesgo de amenazas del país y continuar con la consolidación de las habilidades propias para anticiparse al actuar delictivo cibernético.

Esta Semana Económica presenta un panorama frente a los ataques cibernéticos y aborda los avances del sector público colombiano en materia de ciberseguridad. Muestra las perspectivas y avances del sector financiero en estos temas y señala aspectos importantes desde el punto de vista regulatorio dada la reciente expedición de un proyecto de normatividad por parte de la Superintendencia Financiera sobre el particular.

Los ataques cibernéticos, una creciente amenaza

La trasformación digital que se ha venido presentando en los últimos años alrededor del mundo ha promovido el aumento del uso de las tecnologías de la información y comunicaciones en todos los aspectos de la vida. Según el reporte *Digital in 2018* de *Hootsuite*[1], en 2017 hubo un total de 8.485 millones de dispositivos conectados a internet, despertando en las empresas y personas la necesidad de utilizar el ciberespacio[2].

En este contexto, la delincuencia también ha encontrado importantes ventajas, toda vez que desde el anonimato se facilita la realización de ataques cibernéticos desde cualquier lugar del mundo y se reduce la probabilidad de que estos sean anticipados y descubiertos.

El 2017 fue un año complejo en términos de cibercriminalidad en el mundo, particularmente porque se evidenciaron ataques más diversos, sofisticados, potentes y con mayor alcance e impacto a lo largo de todo el mundo. Dentro de los incidentes cibernéticos más importantes se encuentra el *Ransomware*[3] "*WannaCry*", el cual afectó algo de más de 360.000 dispositivos en más de 180 países y generó a sus creadores más de USD 100.000 dólares en rescates. También se destacaron incidentes como el *hackeo* a la compañía de televisión *HBO*, el cual derivó en la filtración de uno de los episodios de la cuarta temporada de la serie *Game of Thrones* y la exigencia de USD 6 millones en *Bitcoins* a cambio de otra información robada a esta empresa.

En la Séptima Cumbre Latinoamericana de Analistas de Seguridad realizada en septiembre de 2017 en Argentina, *Kaspersky* reveló que América Latina tuvo un aumento de 59% en el número de ciberataques en 2017. Se identificaron 677 millones de ataques cibernéticos entre enero y agosto del último año, es decir, 33 ataques por segundo y 117 ataques por hora con afectaciones principalmente en Brasil, México y Colombia[4].

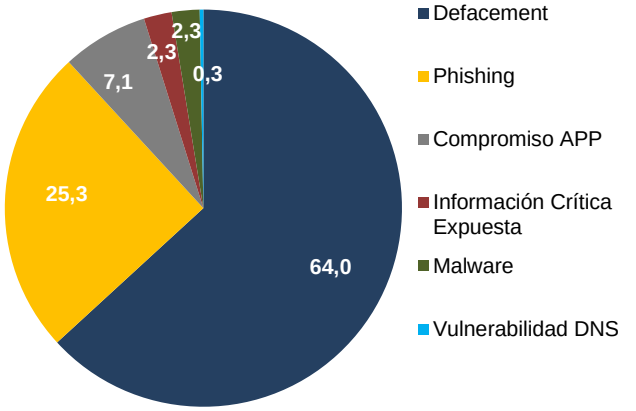
De acuerdo con el informe *Balance Cibercrimen en Colombia 2017* del Centro Cibernético Policial, el cibercrimen en el país aumentó 28,3% en 2017 frente a los resultados de 2016 y 446 empresas reportaron haber sido víctimas de ciberataques[5]. Según el reporte, las amenazas cibernéticas que más se presentaron en el país el año pasado fueron *ransomware*, ataques a entidades estatales, la suplantación de correo corporativo, el *carding*[6] y las estafas por internet. Por otro lado, se detectaron nuevas amenazas como la ciberinducción al daño físico, la estafa a través de suplantación de *Sim*

[1] Hootsuite. El ámbito digital en el 2018 y su situación mundial desde Argentina hasta Zambia. Digital in 2018. Consultado en https://hootsuite.com/es/pages/digital-in-2018
[2] Entorno complejo que resulta de la interacción de las personas, software y servicios a través de Internet por medio de dispositivos tecnológicos y redes conectados al mismo, que no existe en forma física alguna. (ISO 27032).
[3] "Ese término se refiere, de manera amplia, a algunos tipos de malware empleados para extorsionar digitalmente a víctimas a cambio de un pago. Es decir, hace referencia a clases específicas de software malicioso que realiza un encriptado sobre la data para luego solicitar un "rescate" para "liberar" la información". Para mayor información sobre el tema se puede consultar la Semana Económica No. 1091 Secuestro de información o "ramsonware": una amenaza para todos. https://sabermas.s3.amazonaws.com/asobancaria/1091.pdf
[4] Kaspersky. (12 de septiembre de 2017). 33 ataques por segundo: Kaspersky Lab registra un aumento de 59% en ataques de malware en América Latina. Obtenido de https://latam.kaspersky.com/blog/33-ataques-por-segundo-kaspersky-lab-registra-un-aumento-de-59-en-ataques-de-malware-en-america-latina/11265/
[5] Centro Cibernético Policial. (diciembre de 2017). Informe: Balance Cibercrimen en Colombia 2017. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf
[6] Modalidad de fraude mediante la cual los ciberdelincuentes comercializan los datos de tarjetas de crédito y débito, cuentas bancarias e información financiera sustraída a las víctimas con fines fraudulentos. Tomado del Informe: Balance Cibercrimen en Colombia 2017 del Centro Cibernético Policía. Para mayor información sobre esta modalidad se puede consultar el portal Por una Red Segura de la Policía Nacional, Incocrédito y Asobancaria. http://www.porunaredsegura.com/index.php/carding

Cards, el *Vishing*[7], fraude por *WhatsApp* y las ciberpiramides. La autoridad también llama la atención acerca de la consolidación del *Crime as a Service*, modalidad en la cual el delincuente pone a disposición servicios, generalmente a través de la web, para que cualquier persona sin conocimientos profundos en tecnología los pueda contratar.

Por su parte, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –Colcert– ha dado a conocer las estadísticas sobre los tipos de incidentes presentados durante 2017, de las que se evidencia que el 64% correspondieron a eventos de *defacement*[8] seguidos por los ataques de *phishing* con un 23% (Gráfico 1).

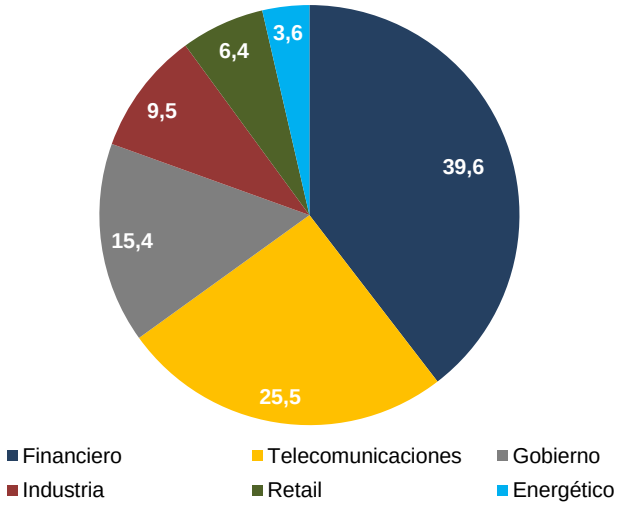
Gráfico 1. Tipos de incidentes cibernéticos en Colombia en 2017 (%)



Fuente: Colcert. Elaboración Asbancaria

En relación con los sectores económicos, el sector financiero es uno de los más apetecidos por los ciberdelincuentes, dados los recursos y la información que maneja, esta última cada vez más valiosa. La compañía de ciberseguridad *Digiware* mostró, en el evento *Information Security Trends Meeting* realizado en septiembre de 2017 en Bogotá, que los sectores más afectados por ciberataques en Colombia son el financiero, con 214.000 ataques por día (39,6%) y el de telecomunicaciones, con 138.329 ataques por día (25,50%)[9] (Gráfico 2).

Gráfico 2. Distribución de los ataques cibernéticos por sectores económicos (%)



Fuente: Digiware. Elaboración Asobancaria.

La materialización de una ciberamenaza, es decir, cuando se convierta en un ciberincidente, puede traer consecuencias enormes. Según *Karspersky*, para la industria bancaria los costos monetarios de un ciberdelito pueden alcanzar, en promedio, los USD 1,8 millones. Adicionalmente, el 61% de este tipo de eventos trae consigo otros costos que incluso pueden generar mayores impactos, como la pérdida de reputación y de información confidencial[10].

En esta línea, un ejemplo de ello es el reciente caso de *Facebook*, en el cual se identificó el uso indebido de datos de 87 millones de usuarios de la red social por parte de una empresa durante las campañas presidenciales de

[7] Es una modalidad de cibercrimen relativa al uso de llamadas telefónicas con el objetivo de obtener información personal y bancaria para luego cometer robos y fraudes.
[8] Defacement es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.
[9] Dinero. (26 de septiembre de 2017). Los sectores económicos más impactados por el cibercrimen en Colombia. Consultado en https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321
[10] Kaspersky. (14 de junio de 2017). Online banking security incidents come with a $1.8 million price tag for banks. Consultado en https://www.kaspersky.com/about/press-releases/2017_online-banking-security-incidents-come-with-a-18-million-price-tag-for-banks

2016 en Estados Unidos. El impacto negativo sobre las acciones de la compañía bordeó el 6% y el CEO de la compañía tuvo que comparecer ante el Congreso de ese país asumiendo compromisos para aumentar la protección de la información personal de sus usuarios. Esta situación ha llevado incluso a abrir el debate sobre la conveniencia de la expedición de una regulación en esta materia en EE.UU.

Este panorama hace que todas las instituciones, públicas y privadas, deban concentrar importantes esfuerzos para generar capacidades de detectar las amenazas, identificar los ataques y prevenir que se materialice en una afectación de sus sistemas y/o de la información.

Avances del sector público en la elaboración de una política de ciberseguridad en Colombia

Los países emergentes, como Colombia, han visto cómo las amenazas cibernéticas se han incrementado significativamente debido a su potencial de desarrollo. De esta forma, una estrategia en ciberseguridad[11] se hace cada vez más importante para empresas y gobiernos de economías emergentes que deseen masificar la prestación de sus servicios por canales virtuales.

Así las cosas, el Gobierno viene trabajando desde hace algunos años en el diseño e implementación de una estrategia de ciberseguridad nacional integral. Particularmente, en 2011 se aprobó el CONPES 3701 que definió la política pública orientada a fortalecer las capacidades del Estado en ciberseguridad y, a la vez, establecer espacios y mecanismos de articulación de las diferentes instituciones estatales y privadas en este sentido. En dicha política se establecieron tres objetivos:

1. Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional.

2. Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad nacional.

3. Fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

La definición de esta política pública 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, a pesar de que se fortalecieron las acciones del país en estos asuntos, para 2016 solo se había consolidado el 79% de las iniciativas allí estipuladas, por lo que aún hay un importante espacio para el mejoramiento de las capacidades del Estado y de la sociedad para enfrentar estas crecientes amenazas[12].

Además, la evaluación del cumplimiento del CONPES 3701 estableció que los resultados obtenidos no podían entenderse como una "capacidad suficiente, integral y efectiva de preparación y respuesta ante ataques cibernéticos"[13]. 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 y donde se comparten 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.

Esta última dimensión es quizás el mayor avance entre los dos documentos de política pública. Cambiar el enfoque hacia uno de gestión de riesgos podría ser adecuado para adaptarse al entorno cambiante en materia de las diversas amenazas cibernéticas.

Por su parte, uno de los adelantos más importantes desde el Gobierno es el fortalecimiento de la capacidad institucional. En la actualidad existen diversas instancias estatales que buscan responder a las necesidades de las diferentes aristas que requiere tener un modelo de

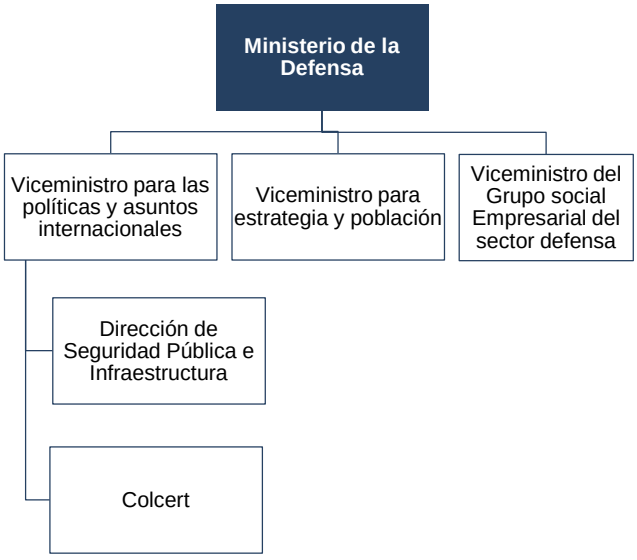
[11] Preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio. (ISO 27032)
[12] Asobancaria, Semana Económica Edición 1062, "Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas", 3 de octubre de 2016
[13] CONPES 3854 de 2016 (p.17).

prevención y gestión de incidentes cibernéticos. Dentro de estas instituciones se destacan:

Centro Cibernético Policial – CCP: es la dependencia de la Dirección de Investigación Criminal e *INTERPOL* encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

Colcert: es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, que se encarga de brindar colaboración activa en la resolución de incidentes cibernéticos. Además, brinda servicios de asistencia técnica al sector público y privado. El Colcert es el punto focal para el reporte de incidentes y hace parte de la estructura del Ministerio de Defensa (Esquema 1).

Esquema 1. Posición del Colcert dentro del organigrama del Ministerio de Defensa



Fuente: Ministerio de Defensa. Elaboración Asobancaria.

CCOC: Es una Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea) que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperar las amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto soportado en un marco jurídico y/o la Constitución Nacional[14].

El caso del *ramsonware "Wannacry"* sucedido el año pasado mostró que los reportes de las entidades públicas o privadas presentados directamente a una sola autoridad podrían desbordar la capacidad de respuesta de la misma. Por este motivo, el Ministerio de las Tecnologías y las Comunicaciones está trabajando en la implementación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) para entidades gubernamentales que sirva como receptor de los incidentes cibernéticos de dichas instituciones y que ayude en la gestión de los mismos cuando se considere necesario.

Hacer frente a los problemas de ciberseguridad requiere, por lo tanto, de una permanente comunicación y coordinación entre las diferentes entidades públicas y privadas de diferentes países y organizaciones. En este sentido, el Gobierno también ha diseñado un modelo nacional de gestión de incidentes (Esquema 2) que permita establecer mecanismos de actuación y articulación en caso de materializarse una amenaza cibernética en el país.

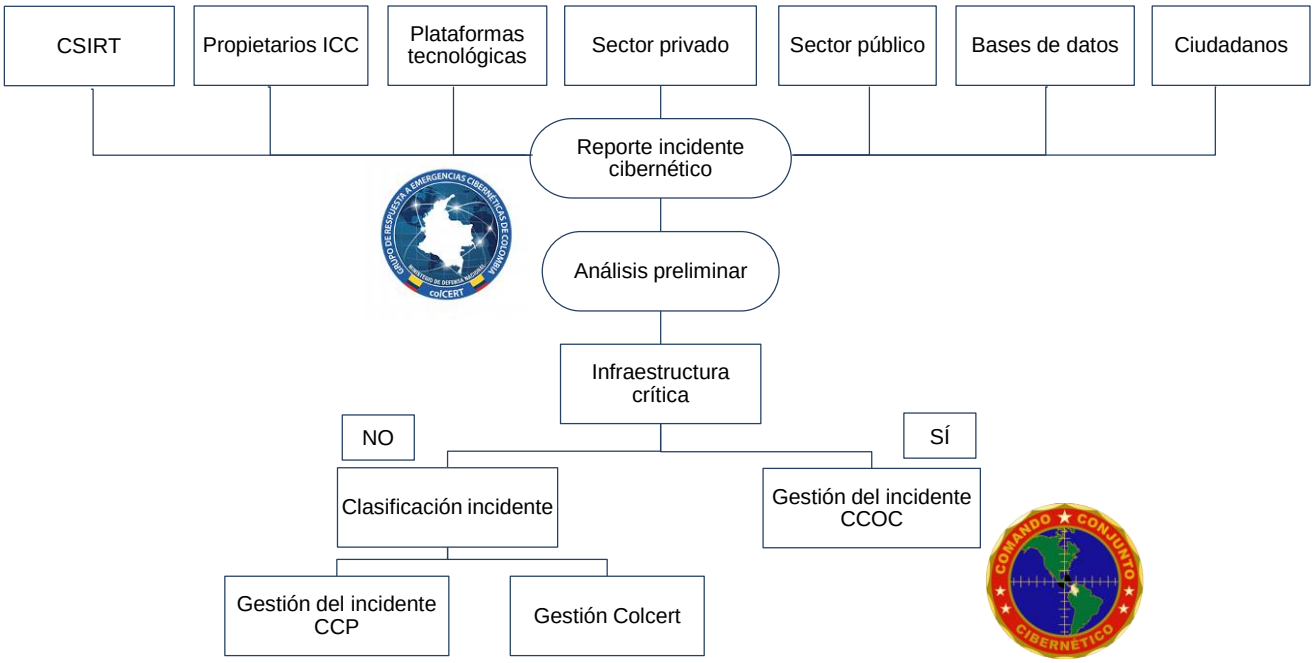
¿Y el sector financiero?

El sector financiero es, sin lugar a dudas, uno de los que más invierte en materia de protección de datos y sistemas de información (plataformas y medios tecnológicos). Según el más reciente estudio de la OEA y el MINTIC acerca del impacto económico de los incidentes digitales en Colombia durante 2016[15], entre las empresas que asignaron mayor presupuesto para la seguridad digital[16] se destacan las pertenecientes al sector de servicios y al sector financiero.

En materia de enfoque, tradicionalmente las entidades financieras han venido incorporando prácticas internas de ciberseguridad y seguridad de la información coherentes con la creciente integración de servicios esenciales mediante tecnologías de la información. Más allá de la

[14] Guía para la Identificación de Infraestructura Crítica CIbernética (ICC) de Colombia (2015). Comando General Fuerzas Militares.
[15] Estudio Impacto de los incidentes de seguridad digital en Colombia 2017, elaborado por el BID, la OEA y MinTIC. Consultado en: www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf
[16] La mediana del presupuesto en relación a las ventas fue de aproximadamente el 0,3%.

Esquema 2. Modelo Nacional de Gestión de Incidentes



Fuente: Ministerio de las Telecomunicaciones. Elaboración Asobancaria.

gestión de los riesgos operacionales, tradicionalmente vinculada con la gestión de eventualidades y el diseño de controles de contingencia, las áreas dedicadas a la seguridad de la información cuentan con un panorama técnico que articula acciones preventivas y tácticas no estrictamente vinculadas con la gestión del riesgo operativo.

En la mayoría de las entidades, la estrategia interna ha sido el fortalecimiento de la arquitectura de seguridad digital orientada sobre todo a generar capacidades para defender y anticipar las amenazas digitales con el propósito de conseguir resiliencia en la operación y proteger la reputación. En esta línea, la estrategia de seguridad digital actual se basa en promover la confidencialidad, la integridad y la disponibilidad de los servicios mediante lo que se denomina *Security as a Service (SECaaS).* Este esquema privilegia la flexibilidad de los esquemas de seguridad para adaptarlos principalmente a las necesidades de los usuarios y la armonización de objetos y funciones organizacionales, particularmente aquellas alojadas en la nube[17].

No pueden desconocerse los esfuerzos de las entidades del sector en la protección de su información e infraestructura tecnológica. En efecto, en intervenciones recientes de la Superintendencia Financiera, si bien se menciona un número importante y creciente de ataques cibernéticos contra el sistema financiero colombiano (39'145.253 en 2016 y 17'821.293 en el primer semestre del 2017), se ha reconocido que los ataques recibidos fueron detectados y contenidos, sin tener conocimiento de afectaciones a la operación, el servicio, ni a la reputación de las entidades[18].

No obstante, los riesgos asociados a la confidencialidad y protección de datos e infraestructuras tecnológicas que sustentan el negocio han promovido a nivel mundial la conformación de modelos de gestión particulares para afrontar los riesgos cibernéticos (MGRC). Estos riesgos (ciberseguridad, seguridad de la información, protección perimetral, etc.) son de naturaleza distinta a los riesgos operaciones tradicionales. Como lo sugiere *Accenture*, "las instituciones financieras (IF) quieren establecer controles para gestionar el riesgo cibernético de arriba hacia abajo.

[17] Cloud Security Alliance, Security as a Service Working Group (2012). Consultado en https://cloudsecurityalliance.org/group/security-as-a-service/#_overview
[18] Intervención del doctor Jorge Castaño, Superintendente Financiero de Colombia, en el 16º Congreso de Riesgo Financiero de Asobancaria, Cartagena, 16 de noviembre de 2017. Presentación disponible en https://www.superfinanciera.gov.co/publicacion/10096506

Sin embargo, aunque las IF están familiarizadas con los aspectos básicos de los cortafuegos, el *malware* y el *phishing*, tienen dificultades para asociar los aspectos técnicos de la ciberseguridad con las personas y procesar los riesgos que el riesgo operacional está diseñado para monitorear y controlar."[19]

Esta aparente contradicción tiene su origen en la dificultad para medir y gestionar los riesgos digitales. Un ejemplo de ello es la forma de abordar un ataque cibernético que no es catastrófico. Los directores de riesgos (CRO) y de seguridad de la información (CISO) son conscientes de sus responsabilidades, pero el mismo evento no siempre está en el alcance de las funciones de uno u otro. Es decir, en muchos casos, la ciberseguridad se gestiona por medio de conjuntos de controles internos dentro de los procesos de Tecnología de Información (TI), separados de los deberes y procesos requeridos para la gestión o cumplimiento del riesgo operacional.

Avances y desafíos regulatorios de la ciberseguridad

La regulación en materia de ciberseguridad busca que las organizaciones adquieran las capacidades suficientes para hacer frente a los riesgos de ciberseguridad derivados de la exposición de las organizaciones en el entorno digital. Actualmente cada país cuenta con un conjunto de regulaciones en torno a la seguridad digital, más o menos heterogénea entre sí, que obedece a distintas realidades legales, económicas y sociales, así como a realidades de costo y oportunidad frente a la regulación[20].

Las primeras regulaciones asociadas a la seguridad digital se vincularon principalmente hacia la protección de datos, buscando proteger la información de personas y empresas de los cibercriminales. Este es el caso de la *Data Protection Directive* de 1995 para la Unión Europea, la cual se ha venido actualizando permanentemente. Otras regulaciones se enfocan sobre todo en la Infraestructura Crítica Cibernética[21], siendo el caso de los lineamientos implementados por ENISA (*European Union Agency for Network and Information Security*) de la mano con los estados europeos[22].

Avances significativos en materia de judicialización del cibercrimen en Estados Unidos fueron realizados por medio de la *Computer Fraud and Abuse Act* de la *Federal Trade Comission Act* en materia de protección de datos así como de la protección de infraestructuras críticas provistas por NIST (*National Institute of Standars and Technology*) y articuladas con el *Department of Homeland* Security. También se ha avanzado en iniciativas de vigilancia y protección en ambientes digitales asociadas principalmente a la defensa nacional y, mediante la *Federal Information Security Management Act,* sobre terceros contratistas del gobierno americano. Finalmente están los avances en las leyes sobre privacidad de datos vinculadas a la protección de la identidad digital en suelo americano[23].

Por su parte, los estándares y marcos de referencia internacional juegan un papel fundamental dentro del proceso de gestión de la seguridad digital. En el contexto de la seguridad digital, los estándares contribuyen a definir lineamientos y buenas prácticas para la gestión de los incidentes dentro y entre distintas organizaciones[24]. Entre las más conocidas están las familias de las ISO 27000, *Cobit* 5, los esquemas de NIST y ENISA, o del WEF, los estándares ISF, los SANS Top 20 CIS y, finalmente, los IT *Capability Maturity Framework.*

En Colombia se encuentra la Ley 1273 de 2009 que nace para ampliar el alcance de la política nacional del país que no había tipificado delitos de carácter informático en la normativa penal, dificultando el papel de autoridades para

[19] Accenture, The Convergence of Operational Risk and Cyber Security. Consultado en https://www.accenture.com/t20160212T030611__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf

[20] Kobayashi, B. (2006). Private versus Social Incentives in Cybersecurity: Law. En M. Grady, & F. Parisi (Edits.), The Law and Economics of Cybersecurity. Cambridge University Press.

[21] Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa.

[22] Rishikof, H., & Sullivan, C. (2018). Legal and Compliance. En D. Antonucci (Ed.), The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity. Wiley.

[23] Kosseff, J. (2016). Cybersecurity Law. Wiley.

[24] Deutscher, S., & Yin, W. (2016). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity. En D. Antonucci (Ed.), Standards and Frameworks for Cybersecurity. Wiley.

perseguir y de las víctimas para denunciar ciberdelitos. Para este fin, la ley crea nuevas formas penales, orientadas hacia la protección de los datos y la confidencialidad siguiendo los estándares del Criminal *Investigative Training Assistance Program* (ICITAP).

En esta misma línea, se está tramitando actualmente el proyecto de ley que busca implementar el Convenio de Budapest en el país. Este convenio es el único estándar multilateral para la judicialización de delitos informáticos y busca hacer frente al crimen organizado y transnacional de manera articulada, asociando al sector público y privado en torno a la lucha contra el cibercrimen. Para este fin, los países que implementan el Convenio tienen la obligación de armonizar su legislación interna a las exigencias penales y judiciales de los demás países, a la vez que deben mejorar los procesos para favorecer el flujo de información.

Puntualmente, frente a la regulación dirigida a las entidades financieras, el Capítulo XXIII de la Circular Básica Contable y Financiera de la Superintendencia Financiera reglamenta el Sistema de Atención al Riesgo Operacional (SARO), la cual incorpora los primeros lineamientos referentes a la seguridad de la infraestructura y los procesos informáticos. En materia de seguridad de la información, en el Capítulo I del Título II de la Parte I de la Circular Básica Jurídica, "Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros", se establecen los requisitos que deben cumplir las entidades financieras en este sentido.

No obstante, en razón a que el supervisor financiero considera necesario avanzar en la consolidación de un modelo de madurez de la gestión de la Seguridad de la Información y la Ciberseguridad, dicha entidad publicó recientemente para comentarios un proyecto de Circular Externa "por medio de la cual se imparten instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad"[25]. Se resaltan dos aspectos sobre el documento: (i) la inclusión del enfoque de riesgos frente a los temas de ciberseguridad y seguridad de la información y (ii) el ascenso de las responsabilidades de aprobar y monitorear las acciones por parte de los mayores órganos de dirección.

En particular, el proyecto establece la obligatoriedad de crear procedimientos y políticas de gestión de riesgos de ciberseguridad que deben ser aprobados y monitoreados por la Alta Dirección y la Junta Directiva de cada entidad. Adicionalmente, promueve la profesionalización del conocimiento y de la cultura en torno a la ciberseguridad. Asimismo, establece la obligatoriedad de estructurar una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad que cada entidad deberá conformar considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes y servicios prestados.

Seguramente la expedición de esta regulación por parte de la Superintendencia acelerará los avances en la constitución de un sistema de gestión de riesgos de ciberseguridad sobre el que varias entidades financieras vienen trabajando e implicará reorganizaciones al interior de cada institución para fortalecer sus capacidades frente a las amenazas cibernéticas.

Sin embargo, es necesario seguir avanzando también en la articulación de los diferentes actores y sectores en el marco del modelo nacional de gestión de incidentes cibernéticos, no solo pensando en contar con capacidades de respuestas ante la materialización de eventos de ciberseguridad, sino también para fortalecer el modelo de riesgo de amenazas del país y continuar con la consolidación de las habilidades propias para anticiparse al actuar delictivo cibernético.

Consideraciones finales

El escenario hiperconectado digitalmente en el que se desarrollan cada vez más las actividades de los individuos y las organizaciones trae consigo nuevos riesgos relacionados con la protección de información y de las infraestructuras cibernéticas que sustentan los negocios.

La cibercriminalidad viene en aumento y los ataques son cada vez más sofisticados y con mayores alcances. Las implicaciones de un incidente cibernético son enormes pues no solo generan costos económicos para superarlo, sino que pueden afectar activos tan importantes para las organizaciones como su reputación. Es por esto que las instituciones públicas y privadas deben trabajar con mayor esfuerzo en el mejoramiento de sus capacidades para enfrentarse a estas amenazas digitales.

En Colombia, el Estado ha avanzado en la definición de una política pública de ciberseguridad y en el fortalecimiento institucional. Por su parte, el sector

[25] Proyecto No. 04 -2018. Consultado en https://www.superfinanciera.gov.co/publicacion/proyectos-de-norma-10082380

financiero ha venido incorporando prácticas internas de ciberseguridad y seguridad de la información. Sin embargo, tanto en el sector público como en el privado es necesario continuar con los esfuerzos por diseñar estrategias y competencias para anticiparse a los ataques cibernéticos. Además, es preciso avanzar en la articulación de los diferentes actores y sectores, no solo para fortalecer la capacidad de respuesta ante la materialización de eventos de ciberseguridad, sino también para administrar el riesgo de ciberamenazas del país y consolidar las habilidades necesarias para anticiparse a las actuaciones de los ciberdelincuentes.

Colombia
Principales Indicadores Macroeconómicos

	2015	2016					2017				2018	
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total Proy.**	**Total Proy.**
PIB Nominal (COP Billones)*	**799,3**	209,3	214,0	216,2	223,1	**862,7**	224,5	227,2	229,84	232,0	**913,5**	**970,1**
PIB Nominal (USD Billones)*	**253,8**	66,9	71,5	73,9	74,1	**286,6**	76,3	74,8	78,3	77,7	306,1	326,9
PIB Real (COP Billones)*	**531,3**	134,6	135,2	135,5	136,8	**542,1**	136,6	137,5	138,6	139,0	**551,7**	**566,0**
Crecimiento Real*												
PIB Real (% Var. interanual)	**3,1**	2,5	2,4	1,5	1,8	**2,0**	1,5	1,7	2,3	1,6	**1,8**	**2,6**
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**
Inflación sin alimentos (% Var. interanual)	**5,9**	6,6	6,8	6,7	6,0	**6,0**	5,6	5,1	2,2	4,0	**4,0**	**3,5**
Tipo de cambio (COP/USD fin de periodo)	**3149**	3129	2995	2924	3010	**3010**	2941	3038	2937	2984	**2984**	**2968**
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**	**-0,5**
Sector Externo (% del PIB)*												
Cuenta corriente	**-7,4**	-5,1	-3,8	-4,8	-3,4	**-4,3**	-4,1	-3,6	-3,3	-2,4	**-3,4**	**-3,6**
Cuenta corriente (USD Billones)	**-18,7**	-3,6	-2,8	-3,6	-2,6	**-12,5**	-3,2	-2,7	-2,6	-1,9	**-10,4**	**-11,4**
Balanza comercial	**-7,3**	-5,4	-3,9	-4,7	-4,2	**-4,6**	-3,4	-3,9	-3,1	-1,9	**-3,1**	**-3,2**
Exportaciones F.O.B.	**17,9**	12,9	13,9	14,0	14,9	**13,9**	14,0	14,8	15,3	16,6	**15,2**	…
Importaciones F.O.B.	**25,1**	18,4	17,8	18,7	19,1	**18,5**	17,5	18,7	18,6	18,4	**18,3**	…
Renta de los factores	**-2,2**	-1,6	-1,8	-1,9	-1,4	**-1,7**	-2,5	-1,9	-2,3	-2,9	**-2,4**	**-2,3**
Transferencias corrientes	**2,1**	1,9	1,9	1,8	2,2	**1,9**	1,8	2,2	2,2	2,4	**2,1**	**1,8**
Inversión extranjera directa	**4,6**	6,8	5,0	2,9	4,1	**4,7**	3,3	3,6	6,3	4,9	**4,5**	…
Sector Público (acumulado, % del PIB)												
Bal. primario del Gobierno Central	**-0,5**	0,2	…	…	…	**-1,1**	0,6	…	…	…	**…**	**0,4**
Bal. del Gobierno Central	**-3,0**	-0,8	-1,0	-2,7	-3,9	**-4,0**	-1,1	-1,2	…	…	**-3,6**	**-3,1**
Bal. estructural del Gobierno Central	**-2,2**	…	…	…	…	**-2,2**	…	…	…	…	**-2,0**	**-1,9**
Bal. primario del SPNF	**-0,6**	1,0	2,1	1,8	0,9	**0,9**	-0,1	1,2	…	…	**0,0**	**0,5**
Bal. del SPNF	**-3,4**	0,3	0,6	-0,6	-2,6	**-2,4**	-0,7	-0,3	…	…	**-3,2**	**-2,7**
Indicadores de Deuda (% del PIB)*												
Deuda externa bruta*	**37,9**	40,4	41,2	41,1	42,5	**42,5**	39,0	39,1	40,2	40,2	**40,2**	**…**
Pública	**22,7**	24,2	24,8	24,8	25,2	**25,2**	23,3	22,8	23,4	23,2	**23,2**	**…**
Privada	**15,2**	16,2	16,3	16,3	17,2	**17,2**	15,7	16,2	16,8	17	**17,0**	**…**
Deuda bruta del Gobierno Central	**45,1**	43,2	44,0	44,6	46,1	**46,0**	44,3	44,9	46,4	47,4	**45,8**	**…**

*La sección de Precios, PIB, Sector externo y Indicadores de deuda presentan datos observados hasta diciembre de 2017, no proyecciones.
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*

	ene-18 (a)	dic-17	ene-17 (b)	Variación real anual entre (a) y (b)
Activo	**579.011**	**581.459**	**550.246**	**1,5%**
Disponible	37.494	37.929	36.585	-1,2%
Inversiones y operaciones con derivados	107.005	103.738	98.064	5,2%
Cartera de crédito	416.734	418.604	392.711	2,4%
Consumo	116.043	116.007	106.700	4,9%
Comercial	233.605	235.696	225.261	0,0%
Vivienda	55.257	55.094	49.745	7,1%
Microcrédito	11.829	11.806	11.006	3,7%
Provisiones	24.395	23.871	19.285	22,0%
Consumo	9.007	8.800	7.177	21,0%
Comercial	12.629	12.362	9.727	25,2%
Vivienda	1.893	1.860	1.582	15,4%
Microcrédito	854	837	786	4,9%
Pasivo	**502.657**	**505.403**	**476.849**	**1,7%**
Instrumentos financieros a costo amortizado	441.714	441.714	416.482	2,3%
Cuentas de ahorro	166.445	166.445	156.625	2,5%
CDT	144.308	144.308	139.305	-0,1%
Cuentas Corrientes	53.145	53.145	47.914	7,0%
Otros pasivos	3.201	3.290	2.491	24,0%
Patrimonio	**76.354**	**76.056**	**73.397**	**0,3%**
Ganancia / Pérdida del ejercicio (Acumulada)	**529**	**7.712**	**706**	**-27,8%**
Ingresos financieros de cartera	3.656	44.665	3.755	-6,1%
Gastos por intereses	1.354	18.142	1.525	-14,3%
Margen neto de Intereses	2.354	27.305	2.133	6,4%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,52**	**4,26**	**3,66**	**0,86**
Consumo	5,92	5,74	5,04	0,88
Comercial	3,99	3,64	3,10	0,89
Vivienda	3,12	3,01	2,40	0,72
Microcrédito	8,04	7,78	7,57	0,47
Cubrimiento**	**129,4**	**134,0**	**134,1**	**4,70**
Consumo	131,1	132,1	133,4	-2,25
Comercial	135,6	144,1	139,4	-3,82
Vivienda	109,9	112,1	132,6	-22,69
Microcrédito	89,8	91,1	94,3	-4,56
ROA	1,10%	1,33%	1,55%	-0,5
ROE	8,63%	10,14%	12,18%	-3,5
Solvencia	15,55%	15,89%	15,18%	0,4

* Cifras en miles de millones de pesos.
** No se incluyen otras provisiones.