ASOBANCARIA

Semana Económica 2016

Edición 1062

Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas

03 de octubre de 2016

- Los constantes avances tecnológicos han generado enormes retos en materia de defensa y seguridad, buena parte asociados a los riesgos de afectación a nivel nacional y a los que se ven enfrentados empresas y personas en diversos ámbitos. Es por esto, que las organizaciones privadas y el Estado se han visto obligados a invertir una mayor cantidad de recursos en fortalecer sus capacidades en la lucha contra los ciberataques.

- Para poder abordar las nuevas amenazas cibernéticas, es necesario definir y aplicar regulaciones que establezcan las bases para la protección del ciberespacio, así como fortalecer las capacidades de los diferentes actores que puedan considerarse sustanciales en la prevención, detección e investigación de ciberdelitos.

- Se resaltan dos iniciativas gubernamentales que se convierten en importantes herramientas para mitigar riesgos de ilícitos, particularmente informáticos. La primera, desde el ámbito macro, hace referencia al CONPES 3854 “Política nacional de seguridad digital” aprobado en abril de este año. La segunda, como ejemplo de una herramienta puntual, está relacionada con los lineamientos para las terminales de áreas financieras de entidades públicas, que pretenden que los dispositivos desde los cuales las entidades públicas realizan operaciones bancarias cuenten con unos requisitos mínimos de seguridad, tanto físicos como lógicos.

- De la iniciativa de los lineamientos se resalta, en primer lugar, el trabajo coordinado entre el sector público y el sector privado en la consecución de un interés común: mitigar el riesgo de fraude sobre recursos públicos. En segunda instancia, es un documento con lineamientos claros y específicos y no meramente indicativo. El tercer aspecto a resaltar radica en que hace parte de una estrategia gubernamental más amplia en seguridad y privacidad de la información. En cuarto lugar, la guía tiene cobertura para organismos tanto del orden nacional como territorial. Tiene, a su vez, un componente de monitoreo y seguimiento para dar cuenta de las acciones desarrolladas. Por último, ofrece incentivos para su cumplimiento.

- El ejercicio realizado por los bancos y Asobancaria, en conjunto con el MINTIC, es una herramienta puntual que si es implementada por las entidades gubernamentales indudablemente ayudará en la mitigación de los riesgos de fraudes bancarios con recursos públicos. Es necesario, por lo tanto, seguir trabajando de manera articulada y mediante acciones concretas para avanzar en la protección digital de los diversos actores de la economía.

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

Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas

Los constantes avances tecnológicos han generado enormes retos en materia de defensa y seguridad, buena parte de ellos asociados a los riesgos de afectación a nivel nacional y a los que se ven enfrentados empresas y personas en diversos ámbitos. Asuntos como la ciberdefensa tienen al mundo repensando estrategias para hacer frente a las complejas estructuras criminales que con diferentes propósitos, sobre todo monetarios, se convierten en amenazas latentes para la estabilidad económica y la protección de los bienes de los ciudadanos.

En este contexto, han surgido dos importantes iniciativas por parte del Gobierno para mitigar estos riesgos. La primera, desde el ámbito macroeconómico, hace referencia al documento CONPES 3854 mediante el cual se establece la "Política Nacional de Seguridad Digital", aprobado en abril de este año y que actualizó la política pública establecida mediante el CONPES 3701 de julio de 2011 que definía los lineamientos de ciberseguridad en el país.

La segunda, como ejemplo de una herramienta puntual, relacionada con los *Lineamientos para las terminales de áreas financieras de entidades públicas*, recientemente publicada, que pretende que los dispositivos desde los cuales las entidades públicas realizan operaciones bancarias cuenten con unos requisitos mínimos de seguridad, tanto física como lógica.

En esta Semana Económica se recopilan los principales desafíos provenientes de las amenazas tecnológicas. Analiza la estrategia de política pública en ciberdefensa y resalta las políticas que han resultado efectivas en la mitigación de los riesgos tecnológicos.

Amenazas tecnológicas: desafíos cambiantes y a la orden del día

La interconexión que experimenta el mundo hoy en día, se manifiesta en la masificación de los servicios de las tecnologías de la información y ha tenido como consecuencia la profundización de la economía digital. El aumento en la oferta de servicios asociados a tecnologías de la información beneficia positivamente a las economías, permitiendo un aumento significativo en la competitividad y posibilitando el desarrollo de diferentes esquemas de negocio (Katz 2015a; Katz 2015b)[1]. Aprovechando estas ventajas, las empresas y los gobiernos han empleado las TICs para impulsar su productividad, cobertura y eficacia.

[1] Katz, Raúl. (2015a). El Ecosistema y la Economía Digital en América Latina. Telefónica, CEPAL, CAF, Cet.la y Ariel. Recuperado de: http://repositorio.cepal.org/bitstream/11362/38916/1/ecosistema_digital_AL.pdf
Katz, Raúl & Callorda, Fernando (2015b). Impacto de arreglos institucionales en la digitalización y el desarrollo económico de América Latina. Proceedings of the 9th CPR LATAM Conference, Cancun, Mexico, July 14-15st, 2015. Recuperado de: http://www.teleadvs.com/wp-content/uploads/Katz-Callorda-2015-version-final.pdf

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Gina Pardo Moreno
Manuel Serna Botero
Hernan Ramírez Rozo
Nataly González Molano

A pesar de las ventajas que pueda traer esta nueva realidad en muchos aspectos (económicos, sociales y/o financieros), esta situación también ayuda a incrementar los riesgos de ataques informáticos. Es por esto, que los delincuentes han encontrado en internet una herramienta para robar datos e información que represente alguna ganancia económica, y/o que ayude a perseguir algún interés político, dado que favorece el anonimato por la dificultad de rastrear el origen de sus actividades.

Los informes sobre ataques informáticos manifiestan que el número y la variedad de ataques en los últimos años se han magnificado, a pesar que desde hace algunos años la conciencia sobre la seguridad informática se ha incrementado. Según el Informe Global de Seguridad 2015 de Trustwave, las amenazas informáticas siguen en aumento, las pérdidas son cuantiosas y han sido también numerosos los recursos invertidos para protegerse de esos peligros (Cuadro 1).

Conforme a esta realidad, las organizaciones privadas han empezado a invertir una mayor cantidad de recursos en fortalecer sus capacidades contra ciberataques mientras que los gobiernos enfrentan aún más retos en materia de ciberseguridad. Cada vez son mayores las amenazas de carácter de seguridad nacional, lo que implica mayores desafíos y el desarrollo de estrategias transversales que involucren un amplio conjunto de sectores económicos.

Dos aspectos se hacen fundamentales para abordar estas nuevas amenazas: (i) definir y aplicar regulaciones que establezcan las bases para la protección del

Cuadro 1. Estadísticas en materia de ciberdefensa y ciberseguridad[2]

	Descripción
1.	Más de 169 millones de registros personales fueron expuestos en 2015 como producto de las 781 infracciones publicitadas por los sectores financieros, de negocios, educación, gobierno y salud (Reporte de brechas totales ITRC – *Identity Theft Resource Center*).
2.	El costo global promedio por cada registro perdido o robado que contiene datos confidenciales y sensibles fue de USD 154. (Costo de las brechas de información: Análisis Global | IBM / Ponemon).
3.	En 2015, se registró un 38% más de incidentes de seguridad detectados que en el 2014. ("Encuesta sobre el Estado Global de Seguridad de la Información 2016" | Price Waterhouse Cooper).
4.	En 2015, incluso un menor número de pequeñas y medianas empresas (29%) utilizaron herramientas estándar como la configuración y parches para evitar violaciones de la seguridad, en comparación con el 39% que lo hizo en 2014. ("Informe Anual de Seguridad 2016 " | Cisco).
5.	La mediana del número de días que los atacantes se quedan en estado latente dentro de una red antes de la detección es más de 200. ("Analíticas de las amenazas avanzadas " | Microsoft).
6.	Al menos el 52% de los encuestados consideró que un ataque cibernético exitoso contra su red se llevaría a cabo dentro del año. ("Informe de Defensa frente a Ciberamenazas 2015" | Grupo CyberEdge).
7.	El 70% de los ataques cibernéticos utilizan una combinación de técnicas de *phishing* y piratería e implican una víctima secundaria. ("Violación de datos Informe 2015 Investigaciones" | Verizon).
8.	El 74% de los directores de seguridad están preocupados por los empleados que roban información confidencial de la empresa. ("SANS 2015 Encuesta sobre Ejecutivas Amenazas" | SpectorSoft).
9.	Sólo el 38% de las organizaciones globales afirman que están preparadas para manejar un ciberataque sofisticado. (“Informe de situación sobre Ciberseguridad Global 2015” | ISACA Internacional).
10.	La mayoría de las víctimas de violación de datos encuestadas, el 81%, no cuentan con un sistema o servicio de seguridad para asegurarse de la detección de las violaciones de datos sino que confía en la notificación de un agente externo a pesar del hecho de que las violaciones ‘autodetectadas’ tardan sólo 14,5 días para contener un ataque a partir de la fecha de intrusión, mientras que las infracciones detectadas por un agente externo toman un promedio de 154 días. (“Informe Global de Seguridad 2015 de Trustwave" | Trustwave).

Fuente: Elaboración Asobancaria.

[2] Recuperado de: http://swimlane.com/10-hard-hitting-cyber-security-statistics/

ciberespacio y (ii) fortalecer las capacidades de los diferentes actores que puedan considerarse sustanciales en la prevención, detección e investigación de ciberdelitos.

Hacia una política pública de ciberseguridad

Actualmente, se reconoce que una estrategia de ciberseguridad nacional integral debe involucrar acciones en todo el territorio que incluyan a todos los actores nacionales, que se articulen con las autoridades en materia de capacidades de ciberdefensa y ciberdelitos y que tenga en cuenta actividades de cooperación internacional.

En Estados Unidos múltiples agencias vienen desarrollando acciones en este sentido. Por ejemplo, el Departamento de Seguridad Nacional trabaja con otras instituciones en investigaciones criminales de alto impacto para: (i) frenar el actuar de los delincuentes cibernéticos, (ii) dar prioridad a la contratación y formación de expertos técnicos, (iii) desarrollar métodos estandarizados y (iv) compartir las mejores prácticas y herramientas de respuesta cibernética.

En 2013 se creó en Europa el Centro Europeo para el Cibercrimen, cuyo objetivo consiste en reforzar la respuesta a la delincuencia informática en la Unión Europea y ayudar a proteger a los ciudadanos europeos, las empresas y los gobiernos. Su establecimiento era una prioridad en la Estrategia de Seguridad Interior de la UE.

Por su parte, los países emergentes como Colombia, según Control Risks (2015)[3], han visto incrementos importantes en la presencia de amenazas cibernéticas debido a su creciente riqueza y posición geográfica privilegiada. De esta forma, una estrategia en ciberseguridad se hace cada vez más importante para empresas y gobiernos de las economías emergentes que deseen masificar la prestación de sus servicios por canales virtuales.

En este contexto, vale la pena resaltar que el Gobierno colombiano desde hace algunos años ha venido orientando sus esfuerzos a realizar una política pública para atender las necesidades de ciberseguridad en el país, así como promover la seguridad de la información a lo largo de todos los sectores de la economía.

En este contexto, vale la pena resaltar que el Gobierno colombiano desde hace algunos años ha venido orientado sus esfuerzos a realizar una política pública para atender las necesidades de ciberseguridad en el país, así como promover la seguridad de la información a lo largo de todos los sectores de la economía.

El primer acercamiento de la ciberseguridad como política pública en Colombia nace a partir del CONPES 3701 de 2011, con el que se esperaba fortalecer las capacidades del país en esta materia, aclarando que la seguridad de la información era un objetivo nacional por cuanto Colombia había sido un foco importante de ataques dirigidos tanto hacia el Gobierno como hacia las empresas. Este mayor fortalecimiento se esperaba lograr a través del cumplimiento de 3 objetivos específicos:

i) 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.

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

iii) 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.

Además, tenía un gran componente de articulación institucional tanto al interior de las agencias estatales como con otras instituciones privadas.

El problema central identificado en 2011 radicó en la carencia de un Centro de Respuesta a Emergencias Cibernéticas (CERT) a nivel nacional, lo que imposibilitaba una buena articulación, disponibilidad de soluciones y el cierre de brechas regulatorias para hacer frente a amenazas cibernéticas en el país. La política pública diseñada como respuesta se orientó a fortalecer las capacidades del Estado en ciberseguridad y, a la vez otorgar espacio para articular a las organizaciones

[3] Amenazas cibernéticas al sector financiero mexicano. Informe Control Risks 2015.

del Estado responsables de la atención de incidentes a través del desarrollo de un CERT para el país.

Así las cosas, se creó el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCert), como organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa. Éste debería prestar su apoyo y colaboración a las demás instancias nacionales, tales como el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOC) (Cuadro 2).

Cuadro 2. Ejes temáticos de la política pública en ciberseguridad - CONPES 3701 de 2011

CONPES 3701 de 2011	
Objetivos	• Brindar capacitación y ampliar líneas de investigación. • Fortalecer capacidades del Estado. • Fortalecer la legislación y la cooperación internacional.
Institucionalidad	• Comando Conjunto Cibernético. • ColCERT. • Centro Cibernético Policial. • Comisión Intersectorial.

Fuente: Documento CONPES 3701 de 2011. Elaboración Asobancaria.

El ColCert sería un grupo adscrito al Ministerio de Defensa Nacional, que recibiría lineamientos de la comisión intersectorial y su objetivo central sería la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional (Gráfico 1).

Cambiando la política pública: hacia la seguridad digital basada en un enfoque de riesgos

El CONPES 3701 de 2011 se constituyó como un valioso aporte para posicionar al país como líder regional en ciberseguridad 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 han 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.

Si bien el principal logro alcanzado por la política de ciberseguridad y ciberdefensa fue el fortalecimiento de la institucionalidad, la evaluación realizada en el CONPES 3854 concluyó que “los resultados no pueden interpretarse

Gráfico 1. Modelo relacional ColCERT

Fuente: Gráfico tomado del documento CONPES 3701.

como una capacidad suficiente, integral y efectiva de preparación y respuesta ante ataques cibernéticos"[4]. Además, se evidenció la necesidad de incorporar nuevos elementos porque en la política existente no se tuvieron en cuenta objetivos relacionados con la prosperidad económica y social, los cuales pueden ser logrados garantizando un entorno digital seguro y abierto en aras de fortalecer la economía digital.

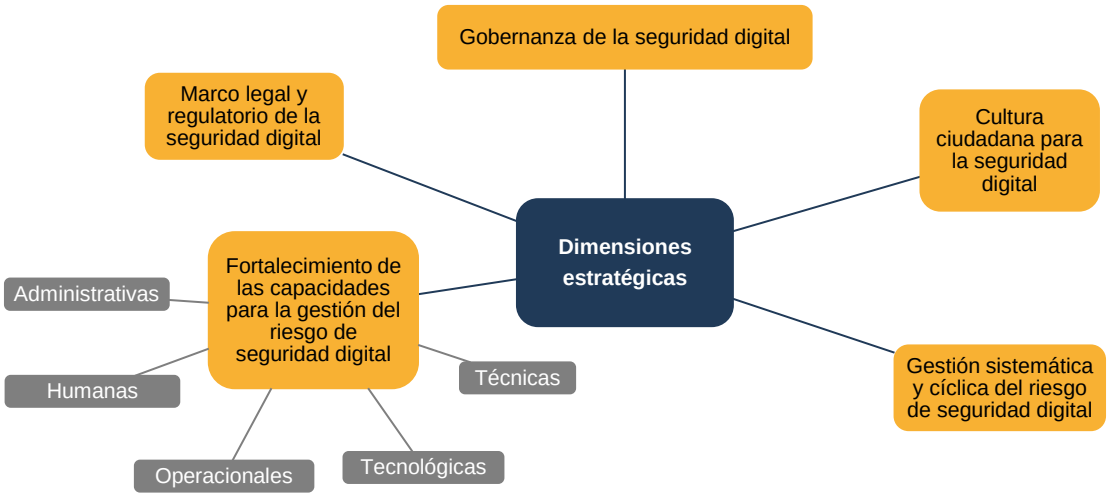
Según el mismo documento CONPES, diferentes estudios "coinciden en que los gobiernos deben adoptar un enfoque de política que se adapte a los cambios del mercado y permita que las organizaciones y los ciudadanos entiendan, evalúen y tomen medidas correctas para manejar las incertidumbres y los riesgos en el entorno digital"[5].

Además, se reconoció que el ColCert era un coordinador de la ciberdefensa y la ciberseguridad, más no "…una visión global y estratégica en torno a la seguridad digital"[6] porque a pesar de tener amplios resultados en materia de detección y atención a incidentes, su capacidad se veía reducida por cuanto la información a la que acudía era externa y no suministrada por la sociedad de manera coordinada. Además, se requería establecer una visión global y estratégica en torno a la seguridad digital para evitar la dispersión que se venía observando de los esfuerzos realizados por cada entidad en el cumplimiento de sus funciones y competencias.

Por su parte, se evidenció la ausencia de una instancia de orientación superior que emitiera lineamientos generales a nivel nacional y definiera los objetivos nacionales en términos de seguridad digital. En este sentido, el internacionalmente reconocido enfoque de riesgos frente a la política pública sobre la ciberseguridad se logró establecer en el primer semestre de este año mediante el CONPES 3854 de 2016, con el que se busca diseñar estrategias incluyentes, de carácter colaborativo y donde se compartan responsabilidades que solventen los vacíos del CONPES de 2011 y se reoriente la política nacional en torno a cinco dimensiones estratégicas.

Al contemplar esta visión multidimensional, se observa una política pública más robusta y con un panorama más amplio para abordar las complejas amenazas informáticas. Además, se espera que un mayor número de actores económicos hagan uso de las ventajas de las TICs para que se incorporen a la economía y contribuyan a la prosperidad económica nacional (Gráfico 2).

Gráfico 2. Dimensiones estratégicas de la estrategia en seguridad digital - CONPES 3854 de 2016



Fuente: CONPES 3854 de 2016. Elaboración Asobancaria.

[4] CONPES 3854 de 2016 (p.17).
[5] CONPES 3854 de 2016 (p.19).
[6] CONPES 3854 de 2016 (p.33).

De otro lado, existe la expectativa de contribuir con un entorno digital más seguro y reducir las prácticas inseguras de sus usuarios y sus posibilidades de ser víctimas de delitos. Adicionalmente, deberían reforzarse las capacidades de los organismos de previsión e investigación de incidentes, quienes se enfrentan a un número creciente de estrategias delictivas a través del cumplimiento de cinco objetivos centrales (Gráfico 3).

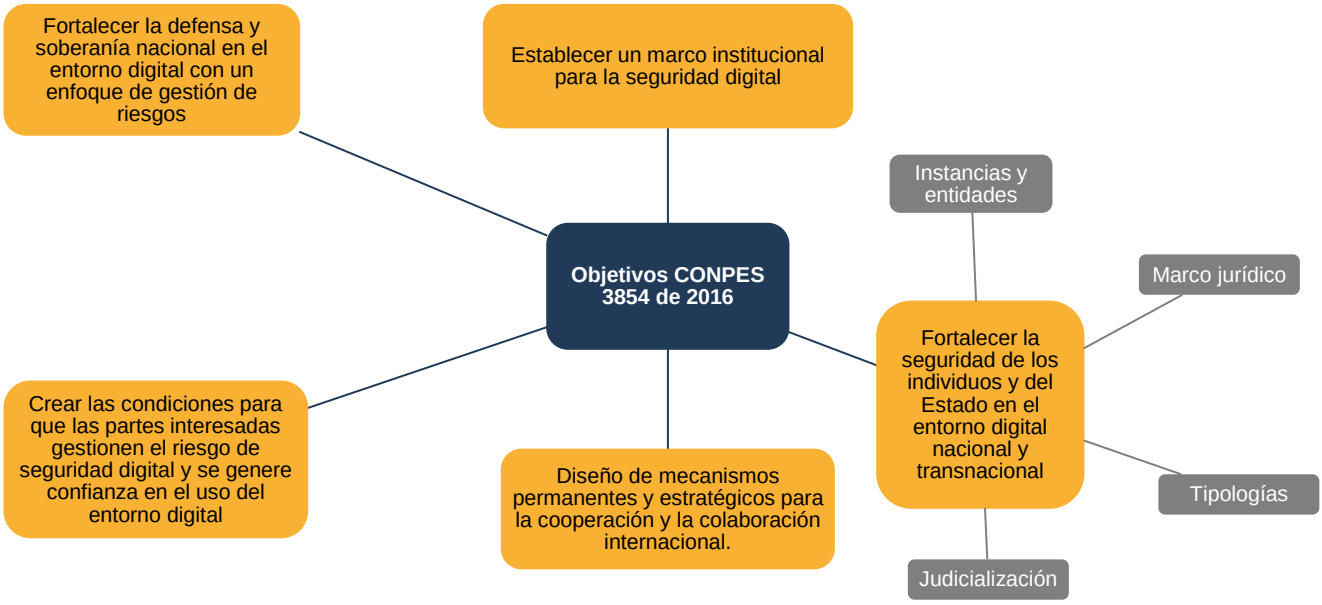
Con el esquema propuesto en este documento se espera alcanzar el logro de esos objetivos, fortaleciendo las capacidades de todos los interesados en seguridad informática en el país (no solo el Estado). De esta forma, al promover un entorno digital (nacional y transnacional) se permitirá aprovechar todas las oportunidades de crecimiento económico que ofrecen las TICs, promover la cultura de la ciberseguridad en los ciudadanos y ampliar el goce de los derechos humanos.

Asimismo, esta política pública espera mejorar la oferta, avanzar en la confianza de los servicios gubernamentales a través de las TICs, y contribuir al fortalecimiento de las capacidades del país en materia de ciberdefensa y ciberseguridad. Lo anterior se constituye como una importante medida de seguridad para hacer frente a un entorno de delitos informáticos atractivo para defraudadores en búsqueda de la creciente riqueza del país.

Desde el sector financiero, cualquier esfuerzo que se realice en seguridad informática es deseado debido a que los retos en esta materia y las amenazas de defraudaciones a las que se ven enfrentados los bancos y sus usuarios, requieren del trabajo articulado de actores públicos y privados.

Sin embargo, los desafíos que surgen después de expedida la política pública son aún mayores que los enfrentados para su construcción. Si bien es cierto que el cambio hacia un enfoque de riesgos es un avance sustancial y que, tal vez, la implementación y el fortalecimiento de un adecuado arreglo institucional es el mayor reto al que se enfrenta el Estado en esta materia, en el concepto de Asobancaria, es necesario avanzar hacia la definición y ejecución de herramientas y hacia la materialización de acciones puntuales que permitan obtener resultados en el corto y mediano plazo.

Gráfico 3. Objetivos centrales de la política de ciberseguridad - CONPES 3854 de 2016



Fuente: CONPES 3854 de 2016. Elaboración Asobancaria.

Lineamientos de seguridad para las terminales de las áreas financieras de entidades públicas: un ejemplo de cómo llevar la política a acciones concretas de prevención y mitigación de riesgos

El Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) viene trabajando desde hace varios años en el fortalecimiento de la gestión de tecnologías de la información del Estado. Con el Modelo de Seguridad para las entidades del Estado publicado este año, el MINTIC entrega una guía para que puedan construir su Sistema de Gestión de Seguridad de la Información (SGSI). Este modelo está compuesto de 24 guías que contienen diversos elementos relacionados con estos asuntos y que son herramientas de gran utilidad para las instituciones públicas tanto del orden nacional como del territorial.

Hace tres años, Asobancaria realizó un acercamiento con el MINTIC para plantear la preocupación del sector acerca del inadecuado seguimiento de las recomendaciones y los mecanismos de seguridad en la realización de transacciones financieras por parte de diversas entidades públicas, lo que generaba un alto riesgo en la utilización de los canales virtuales por parte de instituciones gubernamentales del orden nacional, pero especialmente del ámbito territorial.

Si bien los bancos invierten cuantiosos recursos en el fortalecimiento de sus plataformas tecnológicas o en la disposición de herramientas para robustecer la seguridad en las operaciones financieras, estos esfuerzos se ven debilitados si el cliente no toma unas medidas mínimas de precaución.

Por lo anterior, en su momento se elaboró un documento que contó con la participación de las entidades bancarias, Asobancaria y el MINTIC, que contiene los lineamientos de seguridad que deben tener los equipos y/o terminales desde donde se realizan transacciones financieras con recursos públicos (Cuadro 3). El objetivo es que los dispositivos desde los cuales las entidades públicas

Tabla 3. Resumen de los lineamientos para terminales de áreas financieras de entidades públicas

Lineamientos para terminales de áreas financieras de entidades públicas	
Lógica	• Solicitar la autenticación de credenciales. • Controlar los tiempos de inactividad del usuario - bloqueo automático del equipo. • Restringir los archivos que no sean necesarios para las actividades del cargo. • Hacer limpieza regular del equipo (cookies, historial de navegación y descargas).
Física	• Restringir el acceso al área donde se realizan transacciones financieras al personal no autorizado. • Limitar el uso de las terminales móviles al interior de la entidad. • Contar con cámaras de video.
En la Red	• Restringir el acceso a correos personales, redes sociales, y a sitios no asociados con las funciones del funcionario. • Definir mecanismos de autenticación. • Establecer buenas condiciones y estándares de las redes inalámbricas (WIFI). • Aislar y segmentar las redes inalámbricas (WIFI) para invitados.
Frente a la entidad financiera	• Asignar una dirección IP fija. • Garantizar la protección de las claves y dispositivos de acceso al equipo. • Validar que la identificación y autenticación del equipo de la entidad sea de forma única y personalizada. • Establecer montos y horarios para la realización de operaciones.
Seguimiento y monitoreo	• El área financiera de la Entidad y las áreas de TI y/o de seguridad de la información elegirán el responsable de verificar el cumplimiento de las condiciones de seguridad del equipo. • El responsable del área financiera y el funcionario designado para la respectiva verificación firmarán un documento para darle cumplimiento a los lineamientos.

Fuente: MINTIC. Elaboración Asobancaria.

realizan operaciones bancarias cuenten con unos requisitos mínimos de seguridad, tanto físicos como lógicos. Finalmente, el documento fue publicado como la Guía 21 del Modelo de Seguridad de TI y fue denominada como *"lineamientos terminales de las áreas financieras de entidades públicas".* Esta disposición está organizada bajo 5 elementos: (i) seguridad lógica, (ii) seguridad física, (iii) seguridad de la red, (iv) frente a la entidad financiera y (v) seguimiento y monitoreo de controles. La guía contiene lineamientos que, si son cumplidos adecuadamente por las entidades públicas, pueden contribuir a mitigar el riesgo de fraudes bancarios sobre los recursos que administran.

Varios aspectos se deben resaltar de esta guía. En primer lugar, es el resultado del trabajo mancomunado entre los sectores público y privado en una iniciativa de interés común: mitigar el riesgo de fraude sobre recursos públicos. En segunda instancia, es un documento con lineamientos claros y específicos y no meramente indicativo. El tercer aspecto a resaltar radica en que hace parte de una estrategia gubernamental más amplia: seguridad y privacidad de la información. En cuarto lugar, la guía tiene cobertura para organismos tanto del orden nacional como del territorial. Tiene, a su vez, un componente de monitoreo y seguimiento para dar cuenta de las acciones desarrolladas. Por último, ofrece incentivos para su cumplimiento.

Conclusiones y consideraciones finales

Las constantes y cambiantes amenazas tecnológicas que enfrentan las naciones y sus diferentes agentes hacen que las capacidades de respuesta tengan que revaluarse y adecuarse constantemente. Así las cosas, la nueva política nacional de seguridad digital establecida en el CONPES 3854 de abril de 2016 es una muestra de los avances del Estado en la política pública y en el cambio de enfoque necesario para adaptarse a los desafíos digitales considerando una visión multidimensional y la necesidad de continuar con el fortalecimiento institucional en estas materias.

Sin embargo, seguramente el mayor reto está en materializar la política pública en acciones concretas a implementar por los diferentes actores de la sociedad. Un ejemplo de que esto es posible es la publicación de los lineamientos de seguridad para las terminales de las áreas financieras de las entidades públicas. Este ejercicio realizado por los bancos y Asobancaria, en conjunto con el MINTIC, es una herramienta puntual que si es implementada por las entidades gubernamentales indudablemente ayudará en la mitigación de los riesgos de fraudes bancarios con recursos públicos. Es necesario, por lo tanto, seguir trabajando de manera articulada y mediante acciones concretas para avanzar en la protección digital de los diversos actores de la economía.

Colombia
Principales Indicadores Macroeconómicos

	2013	2014					2015					2016		
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total**	T1	T2	**Total Proy.**
PIB Nominal (COP MM)	**710,5**	186,8	188,2	190,4	192,0	**757,5**	193,8	198,2	201,9	207,0	**800,8**	209,5	213,6	**…**
PIB Nominal (USD Billones)	**368,7**	95,1	100,0	93,9	80,3	**316,6**	75,2	76,7	64,7	65,7	**254,3**	69,3	73,2	**…**
PIB Real (COP MM)	**493,8**	127,9	128,3	129,4	129,9	**515,5**	131,3	132,3	133,4	134,3	**531,4**	134,7	134,9	**545,4**
Crecimiento Real														
PIB Real (% Var. interanual)	**4,9**	6,5	4,1	4,2	3,5	**4,6**	2,8	3,0	3,2	3,3	**3,1**	2,5	2,0	**2,3**
Precios														
Inflación (IPC, % Var. interanual)	1,9	2,5	2,8	2,9	3,7	**3,7**	4,6	4,4	5,4	6,8	**6,8**	8,0	8,6	**6,8**
Inflación básica (% Var. interanual)	**2,2**	2,5	2,5	2,4	2,8	**2,8**	3,9	4,5	5,3	5,9	**5,9**	6,6	6,8	**…**
Tipo de cambio (COP/USD fin de periodo)	**1927**	1965	1881	2028	2392	**2392**	2576	2585	3122	3149	**3149**	3022	2916	**2962**
Tipo de cambio (Var. % interanual)	**9,0**	7,3	-2,5	5,9	24,2	**24,2**	31,1	37,4	53,9	31,6	**31,6**	**17,3**	**12,8**	**-5,9**
Sector Externo (% del PIB)														
Cuenta corriente	**-3,3**	-4,3	-4,3	-5,0	-7,2	**-5,2**	-7,0	-5,2	-7,6	-6,1	**-6,5**	-5,6	-4,8	**-6,0**
Cuenta corriente (USD Billones)	**-12,1**	-4,0	-4,2	-4,9	-6,4	**-19,5**	-5,3	-4,2	-5,3	-4,2	**-18,9**	-3,5	-2,8	**-16,1**
Balanza comercial	**-0,7**	-1,8	-1,9	-2,5	-5,9	**-3,0**	-8,7	-6,6	-11,7	-11,0	**-6,2**	-9,1	-6,5	**-4,7**
Exportaciones F.O.B.	**17,7**	16,7	16,9	17,3	16,4	**16,9**	22,2	22,6	24,6	23,5	**15,6**	21,4	21,9	**-2,1**
Importaciones F.O.B.	**18,4**	18,5	18,8	19,8	22,3	**19,9**	30,9	29,2	36,3	34,5	**21,7**	30,6	28,4	**2,1**
Servicios	**-1,6**	-1,5	-1,7	-1,8	-2,1	**-1,8**	-2,3	-2,3	-2,5	-1,6	**-1,4**	-1,8	-1,9	**0,4**
Renta de los factores	**-3,7**	-3,6	-3,4	-3,6	-2,8	**-3,4**	-3,4	-3,7	-3,1	-1,5	**-2,1**	-2,5	-2,5	**0,4**
Transferencias corrientes	**1,2**	1,1	1,0	1,1	1,5	**1,2**	2,1	2,2	3,3	3,0	**1,7**	3,2	3,0	**0,1**
Inversión extranjera directa	**4,3**	4,1	5,1	3,7	4,3	**4,3**	6,0	7,5	4,9	5,3	**4,2**	11,6	7,6	**-0,4**
Sector Público (acumulado, % del PIB)														
Bal. primario del Gobierno Central	**0,0**	0,5	1,1	1,4	-0,2	**-0,2**	0,0	0,8	1,0	-0,5	**-0,5**	0,2	…	**…**
Bal. del Gobierno Central	**-2,4**	0,1	0,1	-0,5	-2,4	**-2,4**	-0,4	-0,2	-1,0	-3,0	**-3,0**	-0,9	…	**-3,9**
Bal. estructural del Gobierno Central	**-2,3**	…	…	…	…	**-2,3**	…	…	…	…	**-2,2**	…	…	**-2,1**
Bal. primario del SPNF	**1,4**	0,9	2,4	2,3	0,2	**0,7**	0,6	1,8	1,7	-0,6	**-0,6**	1,0	…	**0,9**
Bal. del SPNF	**-0,9**	0,5	1,4	0,5	-2,0	**-1,4**	0,2	1,3	-0,4	-3,4	**-3,4**	0,2	…	**-2,6**
Indicadores de Deuda (% del PIB)														
Deuda externa bruta	**24,2**	25,1	25,6	26,1	26,8	**26,8**	36,4	36,9	37,4	37,9	**37,9**	42,2	…	**…**
Pública	**13,7**	14,3	15,0	15,4	15,8	**15,8**	21,7	22,1	22,3	22,7	**22,7**	25,3	…	**…**
Privada	**10,5**	10,8	10,6	10,7	11,0	**11,0**	14,7	14,8	15,1	15,2	**15,2**	16,9	…	**…**
Deuda del Gobierno Central	**37,2**	35,8	35,5	36,9	40,0	**40,5**	39,8	40,5	45,3	45,1	**45,1**	41,5	…	**…**

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*

	jul-16 (a)	jun-16	jul-15 (b)	Variación real anual entre (a) y (b)
Activo	**524.076**	**522.252**	**369.456**	**30,2%**
Disponible	34.739	35.286	23.357	36,5%
Inversiones y operaciones con derivados	95.920	98.165	75.627	16,4%
Cartera de crédito	371.704	367.998	256.511	33,0%
Consumo	100.049	99.157	68.806	33,4%
Comercial	214.066	211.871	149.066	31,8%
Vivienda	47.010	46.452	30.807	40,0%
Microcrédito	10.580	10.518	7.832	24,0%
Provisiones	17.113	16.759	11.207	40,1%
Consumo	6.410	6.246	4.225	39,2%
Comercial	8.504	8.349	5.521	41,4%
Vivienda	1.448	1.416	887	49,9%
Microcrédito	739	736	574	18,2%
Pasivo	**454.065**	**452.133**	**320.190**	**30,1%**
Instrumentos financieros a costo amortizado	390.750	389.205	275.439	30,2%
Cuentas de ahorro	152.563	153.712	113.865	23,0%
CDT	124.703	121.632	76.769	49,1%
Cuentas Corrientes	45.406	45.718	36.172	15,2%
Otros pasivos	2.944	2.679	2.196	23,0%
Patrimonio	**70.011**	**70.119**	**49.266**	**30,4%**
Ganancia / Pérdida del ejercicio (Acumulada)	7.907	7.308	4.485	**61,8%**
Ingresos financieros de cartera	23.219	19.671	14.485	47,1%
Gastos por intereses	9.436	7.882	4.554	90,2%
Margen neto de Intereses	13.566	11.635	9.661	28,9%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	3,22	3,02	2,98	**0,24**
Consumo	4,95	4,80	4,60	0,35
Comercial	2,44	2,19	2,27	0,17
Vivienda	2,15	2,09	1,91	0,25
Microcrédito	7,23	7,16	6,41	0,82
Cubrimiento**	143,2	150,7	146,7	**3,55**
Consumo	129,4	131,1	133,3	-3,95
Comercial	162,9	180,2	163,3	-0,45
Vivienda	143,0	145,5	151,0	-8,01
Microcrédito	96,6	97,7	114,3	-17,76
ROA	2,60%	2,82%	2,10%	0,5
ROE	20,13%	21,93%	15,44%	4,7
Solvencia	14,96%	15,44%	15,17%	N.A

* Cifras en miles de millones de pesos.
** No se incluyen otras provisiones. El cálculo del cubrimiento tampoco contempla las otras provisiones.