ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Semana Económica 2017

Edición 1091

Secuestro de información o "*Ramsonware*": una amenaza para todos

30 de mayo de 2017

- Los avances tecnológicos han traído consigo un sin número de ventajas y facilidades a la vida moderna. Sin embargo, la digitalización de la información también ha traído importantes riesgos en materia de seguridad informática. La infraestructura tecnológica sobre la que se soportan las funcionalidades digitales hace necesario considerar las amenazas de seguridad a las que se puede estar expuesto.

- Debido a que existen datos que por su naturaleza desean ser conservados (sean personas naturales o instituciones que dependen de ellos para operar) y que ahora se encuentran almacenados de forma digital, la criminalidad informática ha encontrado un nuevo nicho para operar.

- Desde hace algún tiempo, modalidades como el *Ransomware* se han convertido en los mayores retos en materia de ciberdelincuencia. 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.

- En las últimas semanas ha sido noticia mundial un tipo de ataque de *Ransomware* denominado *Wanna Cry* que, según los análisis, ha logrado infectar y secuestrar de manera masiva la información de más de 200.000 sistemas operativos de equipos en empresas, entidades gubernamentales, hospitales, bancos y universidades de 120 países. Este tipo de ataques masivos y de gran impacto no deben generar un pánico generalizado sino, por el contrario, un aprendizaje de las personas y organizaciones frente a la necesidad de tener una mayor conciencia en relación con la importancia de la seguridad de la información.

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

Secuestro de información o "*Ramsonware*": una amenaza para todos

Los avances en las tecnologías de la información han traído innumerables ventajas y facilidades a la vida moderna. Su consolidación ha promovido la productividad y eficiencia en los procesos productivos y ha contribuido de manera fundamental a la investigación y al avance de la ciencia en ámbitos tan importantes para el ser humano como la medicina y las comunicaciones. En materia financiera, las tecnologías han promovido facilidades en el uso de canales transaccionales, beneficios en costos y acceso y han contribuido con el alcance de logros en inclusión financiera.

No obstante, la digitalización de la información ha traído consigo importantes riesgos en materia de seguridad informática. La infraestructura sobre la que se soportan los datos y las funcionalidades tecnológicas acarrean amenazas de seguridad debido a que presentan vulnerabilidades inherentes. Los ataques informáticos revisten ventajas frente a los fraudes "físicos" o estafas comunes debido a que se facilitan el anonimato, contribuyen a generar economías de escala en los ataques y cuentan con un amplio abanico de técnicas de hurto y daño.

En este contexto, aparecen modalidades como el *Ransomware,* que consiste en "secuestrar" la información de una persona u organización para luego pedir un rescate para "liberarla". En las últimas semanas ha sido noticia mundial el ataque de un software malicioso denominado *Wanna Cry*, que según los análisis, corresponde a un caso de R*amsomware* que ha logrado expandirse rápidamente y afectar a personas e instituciones (públicas y privadas) en todo el mundo.

El propósito de esta Semana Económica está orientado a dar una explicación integral del *Ransomware* con el fin de que se tenga un mejor entendimiento de esta amenaza informática y se identifiquen recomendaciones y buenas prácticas para prevenir ser víctimas.

El valor de los datos

Actualmente vivimos en un mundo complejo y de aceleradas transformaciones en todos los ámbitos de la sociedad, donde personas y dispositivos cada vez más conectados están creando huellas digitales[1]. Para prosperar, las organizaciones se enfrentan a la necesidad de medir en forma más precisa el verdadero valor de la información y obtener datos en tiempo real. Se ha evidenciado que los datos que almacenan las empresas les permiten detectar nuevas oportunidades de negocio y en ocasiones obtener una ventaja competitiva en su industria o en la economía digital.

De acuerdo con el informe global de 2015 *"Big & Fast Data: The Rise of Insight Driven Business"* de *Capgemini* y *EMC Corporation*[2], el 65% de las organizaciones reconocen la importancia de implementar nuevas soluciones de análisis de datos para no perder competitividad en su industria. Hay un reconocimiento generalizado de

[1] Marca que deja el uso y tratamiento de nuestra identidad en internet.
[2] Este informe encuestó a más de 1.000 altos ejecutivos que participan en la toma de decisiones, en Norteamérica, América del Sur, Europa y Asia Pacífico.

Editor

Germán Montoya
Director Económico

Participaron en esta edición:

Ginna Alexandra Pardo Moreno
Andrés Quijano Díaz
Hernán Felipe Ramírez

que los datos se están convirtiendo en un componente central de valor de mercado. De hecho, para algunas empresas, la información se ha convertido hoy en un elemento de igual importancia que sus productos y servicios tradicionales.

Para convertirse en una empresa que participe en la economía digital, las organizaciones deben aprovechar los datos que se encuentran dentro y alrededor de sus negocios. La experiencia digital del cliente se centra en entender sus necesidades y preferencias, con lo cual se deben aprovechar todas las fuentes de información, relacionándolas a fuentes externas como las redes sociales.

Si bien muchas de las grandes corporaciones han realizado cuantiosas inversiones en el desarrollo de iniciativas de *Big Data*[3] y hoy reconocen su importancia, un gran número de organizaciones no han incorporado estas iniciativas en sus operaciones. En ese sentido, algunas de las barreras más importantes que enfrentan las empresas continúan asociadas a: i) una administración de información muy dispersa y ubicada en distintos sistemas de almacenamiento, ii) una coordinación ineficaz de iniciativas analíticas, iii) la falta de un caso claro de negocio para justificar la inversión y iv) la dependencia en sistemas anticuados para procesar y analizar datos.

De acuerdo con la encuesta realizada por *Capgemini Consulting "Big Data Survey 2014"*[4], el 79% de las organizaciones no han integrado completamente sus fuentes de datos a sus áreas o unidades de negocio. Lo anterior significa que los directores en muchas ocasiones carecen de un criterio unificado acerca de la información que tiene la compañía, lo que impide tomar decisiones de manera acertada y oportuna.

Un esquema de análisis de datos es efectivo cuando las organizaciones lo asocian a su modelo operativo, el cual requiere incorporar elementos asociados a una estructura organizacional definida, a planes de implementación sistemáticos y a un buen liderazgo.

Gracias al creciente valor que ha venido adquiriendo la información, las vulneraciones cibernéticas a gran escala han incrementado su frecuencia, elevando las pérdidas financieras para buena parte de las organizaciones. Vale la pena tener en cuenta que, debido a la estrecha conectividad en la actualidad, ninguna entidad se encuentra a salvo de una violación de datos. Por lo tanto, independientemente de los sistemas de protección con los que cuente o los estándares de seguridad implementados, es muy difícil controlar y neutralizar todas las amenazas internas y externas a las que una empresa está constantemente expuesta.

En este sentido, los ataques cibernéticos impactan la operación de cualquier compañía y los perjuicios que se pueden generar repercuten tanto en la productividad de la empresa como en los costos legales, pérdidas de propiedad intelectual y daños a la reputación de la misma. Como en muchas ocasiones el valor real de la información es mucho mayor a lo que las organizaciones habitualmente identifican, es imprescindible tomar las decisiones necesarias para enfrentar ataques cibernéticos que intenten sustraerla.

Hasta hace algún tiempo los delincuentes centraron su accionar hacia el robo de información financiera (usuarios y claves) o de medios de pago (tarjetas débito o crédito) para obtener sus ingresos de operaciones fraudulentas contra clientes bancarios. No obstante, las grandes y constantes inversiones del sector financiero en mejorar los mecanismos de seguridad y autenticación de los usuarios hicieron que la delincuencia viera oportunidad de obtener ganancias atacando también a otros sectores. Debido a que existen datos que por su naturaleza desean ser conservados (sean personas naturales o instituciones que dependen de ellos para operar), la criminalidad informática encontró en ese valor de la información un nuevo nicho donde operar. Así las cosas, desde hace algún tiempo, modalidades como el *Ransomware* se han convertido en los mayores retos en materia de ciberdelincuencia.

¿Qué es el *Ransomware*?

De acuerdo con Liska y Gallo (2017)[5], el *Ransomware* es un término amplio que se refiere a algunas tipologías de *malware*[6] empleadas para extorsionar digitalmente a

[3] Cerca de $31mil millones de dólares es 2013 y se predice que ascenderá los 114$ mil millones de USD para 2018, de acuerdo con el *ABI Research, "Unlocking the Value of Big Data in Enterprises"*, September 2013.
[4] Dirigida a 226 ejecutivos expertos en tecnología de la información de Europa, Norte América y Asía Pacífico de diferentes industrias de la economía (Servicios financieros, retail, manufacturero, energía y farmacéuticas).
[5] Liska, A., & Gallo, T. (2017*). Ransomware: Defending against digital extortion.* O'Reilly.
[6] El *malware* se refiere a *software* malicioso.

víctimas a cambio de un pago. Por su parte, Gazet (2010)[7] establece que *Ransomware* hace referencia a clases específicas de software malicioso que realiza un encriptado sobre la data para luego solicitar un "rescate" para "liberar" la información.

Es relevante mencionar que existe un conjunto amplio de *malwares* empleados para el *Ransomware*, los cuales se denominan *criptomalwares*. Su funcionamiento es en muchas ocasiones elemental, pero suele estar acompañado de cierto grado de sofisticación cuando el *malware* logra comunicarse con el atacante y recibir instrucciones de este.

Como campo de estudio técnico, los códigos maliciosos que encriptan información son estudiados por la criptovirología, así los *Ransomwares* son denominados como criptovirus empleados para hacer extorsión. El origen de este tipo de ataques puede situarse hacia 1986, cuando un código malicioso encriptaba carpetas mediante el *reboot* de algunos directorios, amenaza que resultaba sencilla y podía ser fácilmente eliminada con antivirus primitivos.

El *Ransomware* creció rápidamente en los años 90, pero hacia 2005 aumentó de manera exponencial convirtiéndolo en el centro de las preocupaciones mundiales en seguridad informática, proceso marcado por un incremento en la complejidad de los mecanismos de encriptado y claramente por la evolución de los sistemas informáticos modernos. En 2016, los ataques de R*ansomware* ya eran las formas más comunes de ataques informáticos a las organizaciones y sistemas informáticos.

Su rápido crecimiento se produjo principalmente por tres factores fundamentales. En primer lugar, la consolidación del *Crime as a Service (CaaS),* que se refiere a que se ha encontrado una forma lucrativa de negocio en la masificación de los instrumentos de ataques cibernéticos. De esta manera, el *Ransomware as a Service (RaaS)* – una derivación natural del *CaS*- se ha convertido en una empresa altamente lucrativa generando un incentivo para que el crimen organizado busque la manera de masificar estos ataques.

Sobre el *RaaS* es importante mencionar que actualmente es una empresa criminal altamente rentable, debido a que se ha adaptado para poder hacerse de un mercado con diferentes segmentos delictivos al ofrecer diferentes tipos de *cryptomalware.* De esta manera se ha llegado a codificar tipos de malware con propiedades específicas dedicadas a explotar vulnerabilidades en conocimiento de los ciberdelincuentes.

El segundo factor es la disponibilidad masiva de criptomonedas, que garantiza el anonimato en los pagos. Por este motivo son cada vez más frecuentes los casos de secuestro de información mediante *Ransomware* pagados mediante *bitcoins* y otras criptomonedas[8]. Por último, los servicios de DNS[9] dinámicos también suelen ser víctimas de vulnerabilidades, en particular porque los cibercriminales aprovechan el anonimato de estas tecnologías que migran la información entre diferentes direcciones IP y permiten que los criminales muevan sus centrales de comando. De esta manera, los códigos *cryptomalware* que reciben órdenes del atacante sí pueden comunicarse para ejecutar el programa, mientras que las autoridades no pueden encontrar rastros de dicha comunicación.

En este sentido, los cibercriminales han puesto sobre el campo de juego dos tendencias importantes. En primer lugar, para ejecutar un *Ransomware* ya no es necesario ser un cibercriminal técnicamente dotado para poder secuestrar datos importantes, ya que basta acudir al crimen organizado para poder acceder al código malicioso que es elaborado de acuerdo con las necesidades de su cliente. En segundo lugar, el objetivo de los ataques cibernéticos se ha ampliado considerablemente debido a que los ataques no necesitan reconocer actores particulares, por el contrario, en gran parte de los casos buscan afectar a la mayor proporción de dispositivos.

Anatomía de un ataque de *Ransomware*

La anatomía de un ataque de *Ransomware* (Gráfico 1) inicia con el despliegue del *cryptomalware* por el ciberatacante. En múltiples ocasiones no tiene un objetivo específico -el mayor número de infectados-, pero en otras

[7] Gazet, A. (2010). *Comparative analysis of various ransomware virii. Journal in Computer Virology*, 6(1), 77-90.
[8] Es importante anotar que si bien muchas criptomonedas permiten la trazabilidad de los datos, no es sencillo encontrar la ruta de dineros hurtados.
[9] DNS es la abreviatura del inglés de Servicio de Nombres de Dominio y permite controlar la configuración de correo electrónico y sitio web de un nombre de dominio. Así las cosas, cuando los visitantes se dirigen en la web a un nombre de dominio, la configuración de DNS controla a cuál servidor de la empresa se dirigen.

buscan explotar un público objetivo. Para esto emplea diferentes tipos de canales que buscan aprovechar el desconocimiento y las vulnerabilidades y acudir al engaño. Hay diferentes mecanismos para el despliegue del malware y los siguientes son los más frecuentes:

- *Download–by driven:* instalan automáticamente el malware en desconocimiento del usuario.
- *Strategic web compromise:* son análogos a los casos de *watering hole*[10], donde se busca lograr un ataque sobre elementos específicos a sabiendas que las potenciales víctimas van a acceder a ellos.
- *Phishing:* por su naturaleza puede tener objetivos múltiples o muy específicos.
- Explotar vulnerabilidades en red: búsqueda de vulnerabilidades en web para explotarlas y no depende de acciones posteriores del usuario.

Una vez se ha esparcido el *cryptomalware,* inicia la segunda fase del proceso que consiste en su instalación. Para este fin se hace uso de diferentes mecanismos, uno de ellos es el *download dropper methodology,* donde el archivo de instalación es pequeño, no es detectado por los antivirus y permite la comunicación del malware con el ciberatacante. En esta fase, el dispositivo ya está infectado, pero seguido a la instalación, se requiere que el *cryptomalware* reconozca el sistema operativo y permita la comunicación con el atacante.

La tercera etapa depende de que el ciberatacante logre establecer un sistema de mando y control sobre las acciones del *cryptomalware.* Estas instrucciones hacen que el malware recopile información sobre los datos que dispone el dispositivo y sus medidas de seguridad, con lo que caracteriza el dispositivo del usuario y le permite al ciberatacante extraer más valor de los datos capturados. El mecanismo de comunicación depende de la familia de malware y pueden ser canales seguros o no seguros.

Una vez el *cryptomalware* logra establecer el enlace para el mando y control por parte del ciberatacante, se envía la orden de encriptar un conjunto de información. Los archivos preferidos para la captura por su valor son fotos y archivos de trabajo, aunque no hay preferencias cuando se trata de extorsionar. En este sentido, vale la pena señalar que algunos ataques no roban solo información, sino que buscan secuestrar o anular funcionalidades del dispositivo atacado.

El mecanismo de encriptado actual es más complejo que hace algunos años, aunque su complejidad depende del objetivo del ataque. Lo importante del mecanismo de encriptado es que evite que los usuarios puedan tener acceso a sus archivos e incluso a alguna medida de mitigación, obligándolo a pagar el rescate que se solicita.

El pago por los datos capturados depende de si la extorsión es creíble. Por este motivo, se ha refinado la técnica de llevar a cabo la extorsión perfeccionando el encriptado de la información. Otros rasgos particularmente importantes en la actualidad es que el pago de rescates por *Ransomware* es solicitado mediante *bitcoins* y otras criptomonedas, lo que favorece el anonimato, dificulta el seguimiento de los recursos productos del fraude y complica los procesos de judicialización.

Por último, es importante mencionar que, en muchos casos, los ataques de *Ransomware* no buscan recibir el

Gráfico 1. Flujograma de un ataque de *Ransomware* típico

Fuente: Elaboración propia con base en Liska y Gallo (2017)

[10] "*Watering hole"* es el término usado para nombrar una poza donde los animales acuden a beber, por ejemplo en la sabana africana. El nombre del ataque pretende representar a los leones que, en vez de salir a buscar a sus presas, las esperan agazapadas cerca de la charca. Saben que tarde o temprano acudirán a repostar en ella y ahí, cuando las víctimas se relajan, se preparan para perpetrar el ataque. En seguridad informática, la poza es una web especializada a la que suele acudir la víctima. Por ejemplo un foro de programación. La comprometen de forma que puedan subir un código propio, y así intentan explotar alguna vulnerabilidad en el navegador del usuario. Esto contrasta con los ataques "dirigidos" comunes hoy en los que el atacante envía específicamente por email u otros medios documentos o enlaces muy concretos y personalizados a diferentes organizaciones, con la esperanza de que los abran y aprovechen alguna vulnerabilidad". Consultado en: http://blog.elevenpaths.com/2013/10/watering-hole-nuevos-terminos-para.html

rescate monetario. Son muchos los casos en los que oculta otros tipos de ataques más sofisticados o simplemente busca materializar un objetivo políticamente guiado.

Las diversas familias de *Ransomware*

A pesar que la anatomía de *malware* es sencilla, existe un conjunto amplio de *cryptomalware* que poseen ciertas funcionalidades que favorecen los objetivos del ciberatacante y de su perfil de ataque. A continuación, se muestran los más frecuentes.

- **Tesla Crypt:** es uno de los más antiguos *cryptomalwares*, aunque dejó de ser funcional a mediados de 2016 cuando se reveló la llave privada de encriptado y se desarrolló una herramienta gratuita de desencriptado.

- **CryptXXX:** es una variedad de *cryptomalware* que surge para explotar una vulnerabilidad específica. Sin embargo, las etapas tempranas de este código malicioso podían ser contrarrestadas porque su mecanismo de encriptado no era complejo. Las versiones posteriores del malware desarrollaron un mecanismo de encriptado más robusto.

- **CryptoWalles:** el *cryptomalware* más famoso, fue empleado por hackers rusos en campañas de SPAM. No obstante, evolucionó para lograr tener acceso a sitios legítimos y hacer despliegues en sus plataformas. Su popularidad lo ha hecho estar muy presente en los análisis de especialistas de seguridad y se han desarrollado diferentes medidas para contenerlo.

- **Locky o Rock Loader:** Es frecuente asociarlos a campañas de SPAM, aprovechando el engaño sobre documentos descargables que incorporan el virus. Suele esconderse en ejecutables de JAVA que no son analizados por antimalwares tradicionales. En los ataques de esta variedad, suelen verse otros *cryptomalwares* complementarios. Fue famoso por ser parte de la campaña de antivirus falsos.

- **Ranscam:** Este es un *cryptomalware* que se distancia de los tradicionales, debido a que no acude solo a la extorsión, sino que en general finaliza borrando toda la información capturada. Aunque el usuario pague la extorsión, se borra la información y debido al pánico de la víctima, se suele pagar incluso un segundo rescate.

Aunque las anteriores son las familias de malware más frecuentes, se deben visibilizar los riesgos ocultos que se derivan de las variedades más desconocidas y la mutación constante que se hace a partir de códigos maliciosos que traen consigo nuevas vulnerabilidades.

El *Ransomware* del siglo XXI

De la mano con la consolidación de la cuarta revolución industrial, se ha modernizado la forma de realizar *Ransomware.* Los ataques buscan una mayor eficiencia en el proceso de infección a usuarios y, por lo tanto, las amenazas han cambiado fundamentalmente. Si bien en sus orígenes los *cryptomalwares* eran frecuentes en dispositivos del hogar, hoy en día las empresas se han convertido en un blanco de ataques que deja amplias ganancias.

Otro componente que se suma a la avanzada del cibercriminal está ligada a mejorar la estrategia de despliegue y conocimiento de la víctima. Los ciberdelincuentes hacen uso de las Amenazas Avanzadas Persistentes (APT, por sus siglas en inglés), para poder evitar los mecanismos de protección informáticos –más popularizados hoy en día- y también mejorar la estrategia de extorsión. Otras estrategias están ligadas a encubrir ataques informáticos, en las que una práctica infrecuente consiste en realizar ataques de *cryptomalware* como una forma de encubrir ataques reales y severos al desviar la atención de los equipos de seguridad, estrategia similar a algunos casos de Ataques de Denegación de Servicio (DDoS por sus siglas en inglés).

Finalmente, la evolución de los códigos maliciosos también es una importante forma de innovación para el cibercrimen. En efecto, el más reciente ataque cibernético de *Ransomware* denominado *Wanna Cry* (realizado el 12 de mayo de 2017) pone de manifiesto la creciente amenaza global a la que se expone el mundo digital, al haber infectado y secuestrado de manera masiva la información de más de 200.000 sistemas operativos de equipos en empresas, entidades gubernamentales, hospitales, bancos y universidades de 120 países.

Wanna Cry compromete las versiones de Windows más recientes, desde la XP en adelante, que no estén debidamente actualizadas. En los equipos infectados por este *Ransomware* se puede observar un mensaje (Gráfico 2) que exige un pago de $300 dólares en *bitcoins* para desencriptar la información del disco duro.

De acuerdo con el Centro de Control Cibernético de la Policía Nacional, en Colombia se han recibido a la fecha

7.400 reportes por posibles afectaciones del *Ransomware Wanna Cry* y entre las entidades afectadas por este tipo de ataque han identificado varias que hacen parte del sector público. Vale la pena resaltar que, frente a este ataque puntual, los teléfonos celulares no están en riesgo dado que manejan otros sistemas operativos.

Gráfico 2, Ventana de exigencia de pago *Ransomware – "WannaCry"*

Fuente: Policía Nacional de Colombia. Consultado en: https://caivirtual.policia.gov.co/contenido/cai-virtual-0

Estrategias y recomendaciones ante variantes de los ataques de *Ransomware – "WannaCry"*

Como parte del conjunto de estrategias para enfrentar la amenaza de *Ransomware* se pueden enumerar las siguientes: i) protección a servidores y equipos, ii) protección sobre el equipo de trabajo e iii) inteligencia sobre el ataque. Es importante señalar que si el *Ransomware* llega a infectar algún dispositivo de la organización es porque deben existir fallas en los componentes de seguridad. A pesar de que en la actualidad se cuenta con una comprensión profunda de las formas de ataques informáticos mediante *cryptomalware,* la mayor parte de estrategias que se han logrado son del lado preventivo.

Otras acciones que no suelen considerarse como fundamentales tienen que ver con conocer la motivación y perfil del ciberatacante y es necesario avanzar en este sentido. Como lo señala Gazet (2010), conocer la forma que usa el ciberatacante puede ser beneficioso ya que esto permite identificar fragilidades del código malicioso que permitan obviar el proceso de encriptado. Reconocer al atacante permite identificar las rutas específicas que emplean los *cryptomalwares,* lo que da paso a simplificar el proceso de prevención de vectores de ataque.

Desde el año 2016, la Policía Nacional de Colombia participa en la iniciativa de nomoreransomware.org que cuenta con más de 160.000 llaves para descifrar información encriptada, en donde 2.500 víctimas han podido recuperar su información sin pagar a los cibercriminales. El Gobierno Nacional, a través del Ministerio de Defensa, el Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic), la Policía Nacional y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) entregan una serie de recomendaciones para enfrentar las nuevas variantes de esta amenaza[11]:

1. Tener una copia de respaldo de su información.

2. Hacer las actualizaciones de los sistemas operativos. Para que estas sean efectivas el software debe ser legal. Particularmente es importante consultar el catálogo de actualizaciones para Microsoft.

3. Para las entidades o empresas que tengan equipos con sus sistemas operativos sin actualizar lo mejor es desconectarlos de Internet.

4. Evitar abrir correos electrónicos con archivos adjuntos sospechosos que aparentemente alerten sobre cobros jurídicos, demandas o similares.

5. Si se recibe un mensaje de alguna entidad bancaria o ente gubernamental, verifique que el dominio o *link* de la página web que se encuentre en el mensaje realmente sea el que represente oficialmente a la entidad o persona que se referencie.

[11] En caso de presentarse esta situación, las autoridades colombianas piden reportar los casos en: contacto@colcert.gov.co; incidentes-seginf@mintic.gov.co y caivirtual@correo.policia.gov.co. También se puede solicitar mayor información a través de la línea gratuita 01 8000910742 opción 4.

6. Nunca compartir información personal ni financiera solicitada a través de correos electrónicos, llamadas telefónicas, mensajes de texto o redes sociales.

7. No abrir mensajes ni archivos adjuntos de remitentes desconocidos.

8. Tener cuidado con los sitios web que visite, desconfiar de los dominios que no conozca.

9. No descargar software de sitios no confiables.

10. No descargar contenido multimedia por redes de intercambio tales como Ares.

11. Evitar conectar dispositivos extraíbles que no sean confiables.

Recomendaciones y consideraciones finales

Los desarrollos tecnológicos han traído consigo eficiencias y facilidades en todos los sectores. La posibilidad de almacenar, procesar y aprovechar los datos de forma digital ha abierto unas enormes oportunidades en las diferentes organizaciones. El valor de la información es cada vez mayor y el mundo se ha venido dando cuenta de la importancia que tiene como activo.

No obstante, la digitalización de los datos ha traído consigo amplios desafíos en materia de seguridad. La infraestructura sobre la que se soportan los datos y las funcionalidades tecnológicas traen consigo amenazas frente a la posibilidad de robos o vulneraciones sobre la información.

Entendiendo el valor que representan actualmente los datos almacenados digitalmente, los delincuentes han venido desarrollando modalidades de fraude como el *Ransomware*, que consiste en “secuestrar” la información de una persona u organización para luego pedir un rescate para “liberarla”. En los últimos días, el ataque de un software malicioso denominado *Wanna Cry* ha puesto en alerta a instituciones públicas y privadas de todo el mundo al ver la potencialidad de masificación y daño que tiene un ataque informático de este tipo.

Estas situaciones deben propiciar un aprendizaje frente a la necesidad de concientizar a todas las personas y organizaciones frente a los esquemas y mecanismos de seguridad de la información y de capacidad de respuesta a estos incidentes con el objetivo de mitigar al máximo la afectación que pueda materializarse.

Colombia
Principales Indicadores Macroeconómicos*

	2014	2015					2016					2017	
	Total	T1	T2	T3	T4	**Total**	T1	T2	T3	T4	**Total***	T1	**Total Proy.**
PIB Nominal (COP Billones)	**757,0**	192,5	197,1	202,4	207,1	**799,3**	209,3	214,0	216,2	223,1	**862,7**	224,5	**916,2**
PIB Nominal (USD Billones)	**316,4**	74,7	76,2	64,8	65,8	**253,8**	66,9	71,5	73,9	74,1	**286,6**	76,3	290,7
PIB Real (COP Billones)	**515,5**	131,1	132,0	133,6	134,5	**531,3**	134,6	135,2	135,3	136,6	**541,6**	136,2	**551,3**
Crecimiento Real													
PIB Real (% Var. interanual)	**4,6**	2,8	3,0	3,2	3,3	**3,1**	2,6	2,4	1,2	1,6	**2,0**	1,1	**1,8**
Precios													
Inflación (IPC, % Var. interanual)	**3,7**	4,6	4,4	5,4	6,8	**6,8**	8,0	8,6	7,3	5,7	**5,7**	4,7	**4,6**
Inflación básica (% Var. interanual)	**2,8**	3,9	4,5	5,3	5,9	**5,9**	6,6	6,8	6,7	6,0	**6,0**	5,6	**...**
Tipo de cambio (COP/USD fin de periodo)	**2392**	2576	2585	3122	3149	**3149**	3129	2995	2924	3010	**3010**	2941	**3152**
Tipo de cambio (Var. % interanual)	**24,2**	31,1	37,4	53,9	31,6	**31,6**	**21,5**	**15,8**	**-6,3**	**-4,4**	**-4,4**	**-6,0**	**4,7**
Sector Externo (% del PIB)													
Cuenta corriente	**-6,1**	-7,1	-5,5	-8,0	-6,1	**-7,4**	-5,1	-3,8	-4,8	-3,4	**-4,4**	...	**-3,6**
Cuenta corriente (USD Billones)	**-19,5**	-6,8	-5,3	-7,6	-6,1	**-18,9**	-3,6	-2,8	-3,6	-2,6	**-12,5**	...	**-13,9**
Balanza comercial	**-3,6**	-6,3	-4,6	-8,3	-7,5	**-7,3**	-5,4	-3,9	-4,7	-4,2	**-4,6**	...	**-3,1**
Exportaciones F.O.B.	**20,2**	15,9	15,8	17,3	15,8	**17,9**	12,9	14,0	14,0	14,9	**14,2**	...	**10,2**
Importaciones F.O.B.	**23,9**	22,1	20,4	25,6	23,3	**25,1**	18,3	17,9	18,7	19,1	**18,8**	...	**13,3**
Renta de los factores	**-3,9**	-2,4	-2,5	-2,0	-0,8	**-2,2**	-1,6	-1,8	-1,9	-1,4	**-1,7**	...	**-1,8**
Transferencias corrientes	**1,4**	1,5	1,5	2,3	2,2	**2,1**	1,9	1,9	1,8	2,2	**2,0**	...	**1,6**
Inversión extranjera directa	**5,1**	4,4	5,3	3,4	3,3	**4,6**	6,7	5,0	2,9	4,1	**4,7**	...	**4,4**
Sector Público (acumulado, % del PIB)													
Bal. primario del Gobierno Central	**-0,2**	0,0	0,8	1,0	-0,5	**-0,5**	0,2	...	...	...	**...**	...	**...**
Bal. del Gobierno Central	**-2,4**	-0,4	-0,2	-1,0	-3,0	**-3,0**	-0,9	-1,1	-2,7	...	**-3,9**	...	**-3,3**
Bal. estructural del Gobierno Central	**-2,3**	...	...	...	...	**-2,2**	...	...	...	...	**-2,1**	...	**-2,0**
Bal. primario del SPNF	**0,7**	0,6	1,8	1,8	-0,6	**-0,6**	1,0	2,1	1,8	...	**0,9**	...	**0,5**
Bal. del SPNF	**-1,4**	0,2	0,7	-0,4	-3,4	**-3,4**	0,2	0,5	-0,6	...	**-2,6**	...	**-2,3**
Indicadores de Deuda (% del PIB)													
Deuda externa bruta	**26,8**	36,5	37,1	37,5	37,9	**37,9**	40,4	41,2	41,1	42,5	**42,5**	...	**...**
Pública	**15,8**	21,8	22,2	22,4	22,7	**22,7**	24,2	24,8	24,8	25,2	**25,2**	...	**...**
Privada	**11,0**	14,7	14,9	15,1	15,2	**15,2**	16,2	16,3	16,3	17,2	**17,2**	...	**...**
Deuda bruta del Gobierno Central	**40,5**	39,8	40,5	45,3	45,1	**45,1**	43,6	44,4	45,1	...	**...**	...	**...**

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*

	mar-17 (a)	feb-17	mar-16 (b)	Variación real anual entre (a) y (b)
Activo	**558.799**	**553.737**	**518.375**	**3,0%**
Disponible	37.441	37.013	36.387	-1,7%
Inversiones y operaciones con derivados	100.553	99.309	103.541	-7,2%
Cartera de crédito	398.438	396.435	358.628	6,1%
Consumo	108.097	107.320	95.242	8,4%
Comercial	228.561	227.623	208.479	4,7%
Vivienda	50.636	50.418	44.573	8,5%
Microcrédito	11.145	11.074	10.333	3,0%
Provisiones	19.782	19.558	16.140	17,1%
Consumo	7.323	7.279	5.870	19,2%
Comercial	10.070	9.867	8.211	17,1%
Vivienda	1.584	1.602	1.329	13,8%
Microcrédito	792	797	719	5,3%
Pasivo	**487.470**	**480.341**	**449.222**	**3,7%**
Instrumentos financieros a costo amortizado	423.342	420.424	384.624	5,1%
Cuentas de ahorro	154.348	157.802	159.008	-7,3%
CDT	144.525	141.571	107.456	28,5%
Cuentas Corrientes	48.970	49.511	48.519	-3,6%
Otros pasivos	2.718	2.604	2.835	-8,4%
Patrimonio	**71.330**	**73.396**	**69.153**	**-1,5%**
Ganancia / Pérdida del ejercicio (Acumulada)	**1.978**	**1.342**	**2.652**	**-28,7%**
Ingresos financieros de cartera	11.070	7.413	9.451	11,9%
Gastos por intereses	5.079	3.302	3.605	34,6%
Margen neto de Intereses	6.544	4.339	5.805	7,7%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**3,87**	**3,70**	**3,13**	**0,74**
Consumo	5,36	5,25	4,81	0,55
Comercial	3,30	3,11	2,40	0,90
Vivienda	2,44	2,40	2,05	0,39
Microcrédito	7,61	7,69	7,01	0,60
Cubrimiento**	**128,2**	**133,4**	**143,7**	**15,42**
Consumo	126,4	129,2	128,0	-1,67
Comercial	133,4	139,5	163,8	-30,39
Vivienda	128,4	132,6	145,6	-17,21
Microcrédito	93,3	93,6	99,2	-5,82
ROA	1,67%	1,46%	2,06%	-0,4
ROE	13,65%	11,49%	16,24%	-2,6
Solvencia	15,83%	15,11%	15,21%	0,6

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