ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Semana Económica 2019

Edición 1202

El rol de las juntas directivas en la gestión de los riesgos cibernéticos

16 de septiembre de 2019

• Los ciberataques son una amenaza para todo el sistema financiero. La naturaleza cambiante y el crecimiento del riesgo cibernético para las instituciones financieras exige enfrentar efectivamente los desafíos desde el mayor nivel y de forma estratégica.

• Las juntas directivas tienen una función de gobierno vital, que determina el comportamiento general de la empresa y establece el apetito de riesgo de la organización. En ciberseguridad, las juntas deben ejercer de manera efectiva la supervisión, favoreciendo y fortaleciendo el diálogo entre los gerentes de seguridad de la información y prevención del fraude, de forma tal que se cumplan los objetivos estratégicos de la organización.

• A pesar de que las juntas han adquirido mayor conciencia del ciberriesgo en años recientes, hace falta trabajar en un conjunto de principios sobre cómo responder y desarrollar ciberresiliencia en sus organizaciones. En este sentido, las recomendaciones propuestas por el Foro Económico Mundial sirven de guía para los miembros de la junta.

• Es fundamental que el sistema financiero colombiano logre consensos sobre los principios bajo los cuales se deben diseñar estrategias ajustadas a las necesidades de ciberresiliencia del país.

Director:

Santiago Castro Gómez

ASOBANCARIA:

Santiago Castro Gómez
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Germán Montoya Moreno
Director Económico

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

Edición 1202

El rol de las juntas directivas en la gestión de los riesgos cibernéticos

Editor

Germán Montoya Moreno
Director Económico

Participaron en esta edición:

Jaime Rincón Arteaga
Andrés Quijano Díaz
María Camila Barrera Neira
Santiago Castiblanco Hernández

Los ciberataques son una amenaza para todo el sistema financiero. La naturaleza cambiante y el crecimiento del riesgo cibernético para las instituciones financieras se debe a varios factores: tecnologías emergentes, interconexiones entre instituciones financieras y entre terceros, esfuerzos de los ciberdelincuentes por encontrar nuevos métodos para atacar y comprometer los sistemas de tecnología de la información y las comunicaciones (TI) y el atractivo que tienen las entidades financieras para los ciberdelincuentes que buscan ganancias financieras ilícitas.

Actualmente, la resiliencia cibernética y la gestión del riesgo cibernético son desafíos críticos para la mayoría de las organizaciones. A pesar de esto, la alta dirección reconoce cada vez más las profundas implicaciones que estos riesgos tienen para la reputación y existencia de la empresa, por lo que la responsabilidad de administrarlos se encuentra a nivel de junta directiva.

Esta edición de la Semana Económica analiza algunos de los principios y herramientas que el Foro Económico Mundial propone a las juntas directivas para lograr una adecuada resiliencia cibernética. Así mismo, expone algunos ejemplos de organizaciones que tuvieron un impacto significativo en su reputación y negocio como consecuencia de incidentes de seguridad relacionados con la violación de sus datos.

El reto de ciberresiliencia

Para enfrentar efectivamente los desafíos cibernéticos, no basta con implementar mecanismos de ciberseguridad, se requiere de un pensamiento estratégico general por parte de los directivos. Es decir, la resiliencia cibernética debe ser tratada como una cuestión de cultura [1]. Dicha resiliencia requiere que los agentes en los niveles más altos de una empresa, organización o gobierno, reconozcan la importancia de evitar y mitigar los riesgos de manera proactiva. Si bien es responsabilidad de todos cooperar para garantizar una mayor resiliencia cibernética, la estrategia debe estar determinada desde el más alto nivel.

La protección es importante, pero las organizaciones también deben garantizar la operación y continuidad de sus sistemas para aprovechar las oportunidades que brinda

[1] *World Economic Forum, Partnering for Cyber Resilience*, 2012, http://www3.weforum.org/docs/WEF_IT_

la digitalización. Si bien hay muchas definiciones sobre ciberseguridad, hay una diferencia entre la ciberseguridad y el pensamiento más estratégico de resiliencia[2]. Además, como la vulnerabilidad en un área puede comprometer a toda la red, la resiliencia requiere un enfoque centrado en los sistemas.

En los próximos años, miles de millones de nuevos dispositivos se conectarán a internet, así como a redes corporativas y gubernamentales. Estos dispositivos en red traen consigo la amenaza de nuevos riesgos para la empresa y, lo que es más importante, para los sistemas en red que afectan a millones de clientes.

El rol de las juntas directivas

La naturaleza sistemática de estas amenazas requiere un conjunto diferente de respuestas de los responsables políticos y juntas directivas. Ya no es suficiente abordar la seguridad de la red con un enfoque de prueba y error o de baja supervisión, como ha sido el caso de muchas organizaciones. En lugar de implementar soluciones posteriores a los problemas, las juntas y los líderes deben desarrollar rápidamente capacidades conocidas para proporcionar una base de referencia sólida para superar los desafíos futuros.

Las juntas directivas tienen una función de gobierno vital, que determina el comportamiento general de la empresa y establece el apetito de riesgo de la organización. En ciberseguridad, las juntas deben ejercer de manera efectiva la supervisión favoreciendo y fortaleciendo el dialogo entre los gerentes de seguridad de la información y prevención del fraude de forma tal que se cumplan los objetivos estratégicos de la organización.

Principios de la junta para lograr resiliencia cibernética

Algunos principios o recomendaciones que contribuyen a mejorar la toma de decisiones estratégicas de la junta directiva y administrar de manera efectiva los recursos de seguridad dentro de sus organizaciones se resumen en 10 principios básicos[3]:

Principio 1. Responsabilidad por la ciberresiliencia. La junta en su totalidad asume la responsabilidad última de supervisar el riesgo cibernético y la resiliencia. La junta puede delegar la actividad de supervisión primaria a un comité existente (por ejemplo, un comité de riesgo) o a un nuevo comité (por ejemplo, un comité de resiliencia cibernética).

Principio 2. Seguimiento y monitoreo. Los miembros de la junta deben recibir orientación sobre resiliencia cibernética y conocer periódicamente las amenazas y tendencias recientes, con el asesoramiento y la asistencia de expertos externos independientes que estén disponibles según lo solicitado.

Principio 3. Oficial responsable. La junta debe asegurarse que un funcionario corporativo sea responsable de informar sobre la capacidad de la organización para gestionar la resiliencia cibernética y el progreso en la implementación de los objetivos. Además debe garantizar que este oficial tenga acceso regular, autoridad suficiente, dominio del tema, experiencia y recursos para cumplir con estas obligaciones.

Principio 4. Integración de la ciberresiliencia. La junta debe garantizar que la administración integre la resiliencia cibernética y la evaluación del riesgo cibernético en la estrategia comercial de la organización y en la gestión de riesgos en toda la empresa, así como en la asignación de recursos y presupuestos.

Principio 5. Apetito de riesgo. La junta debe definir y cuantificar anualmente la tolerancia al riesgo empresarial en relación con la resiliencia cibernética y debe garantizar que esto sea coherente con la estrategia corporativa y el apetito por el riesgo.

Principio 6. Evaluación de riesgos e informes. La junta debe empoderar a la gerencia para realizar una evaluación cuantificada y comprensible del riesgo, amenazas y eventos como un elemento permanente de la agenda durante las reuniones.

Principio 7. Planes de resiliencia. La junta debe garantizar que la gerencia apoye al oficial responsable de la ciberresiliencia para la creación, implementación, prueba y mejora continua de planes de gestión de riesgo cibernético, adecuadamente armonizados a todo el negocio. El oficial a cargo debe monitorear el desempeño e informar regularmente a la junta.

Principio 8. Comunidad. La junta debe alentar a la gerencia a colaborar con otras partes interesadas, según

[2] *Harvard University page on cybersecurity,* https://cyber.harvard.edu/cybersecurity/Main_Page.
[3] *Dobrygowski, Daniel, "Cyber resilience: everything you (really) need to know",* Forum Blog, 8 July 2016, https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know .

sea relevante y apropiado, con el fin de garantizar la resiliencia cibernética sistémica.

Principio 9 Revisión. La junta debe garantizar que se lleve a cabo anualmente una revisión formal e independiente de la resiliencia cibernética de la organización.

Principio 10 Efectividad. La junta debe revisar periódicamente su propio desempeño en la implementación de estos principios o buscar consejo independiente para la mejora continua.

Papel de la Junta Directiva en la gestión del ciberriesgo

De acuerdo con el Foro Económico Mundial[4], el papel que deberían tener las juntas directivas en la gestión del riesgo cibernético, las acciones para su debida gestión y los componentes que estas deben tener en cuenta de la evaluación del ciberriesgo, revelan alguna características que bien vale la pena señalar. En efecto, la evaluación del riesgo cibernético contribuye al programa de seguridad cibernética de la organización al proporcionar lo requerido para priorizar las acciones. Particularmente las juntas directivas deben entender y evaluar:

1. El nivel de tolerancia al riesgo cibernético / apetito de riesgo.

   La junta debe alinear el nivel general de tolerancia al riesgo con el equipo ejecutivo, definiendo las necesidades de sostenibilidad a largo plazo del accionista que representa. Esta discusión debe tomar en cuenta eventos estratégicos futuros, las expectativas del mercado, así como la posición competitiva de la organización. La junta debe tener en cuenta la capacidad de la organización para absorber riesgos materializados y equilibrar el valor de riesgo tolerado y el potencial de negocio. Este riesgo aceptado de hacer negocios incluye todos los diferentes tipos de riesgo: los tradicionales, como el riesgo de crédito, y los nuevos tipos de riesgo, como el riesgo cibernético.

2. Identificación del riesgo cibernético antes de las acciones de gestión.

.

   La identificación del riesgo cibernético de una organización debe tener en cuenta consideraciones jurídicas, operacionales, financieras, de reputación y estratégicas. Normalmente, estas consideraciones comprenden una agregación significativa de los riesgos cibernéticos a lo largo de las dos dimensiones de probabilidad e impacto, con cada dimensión ubicada entre niveles altos y bajos. Así pues, cualquier riesgo concreto puede representarse como un punto en una matriz tradicional de 3x3 (Cuadro 1).

Cuadro 1. Matriz probabilidad e impacto para la medición de riesgos cibernéticos

Probabilidad	Impacto		
	Bajo	Medio	Alto
Baja	Muy bajo	Bajo	Medio
Media	Bajo	Medio	Alto
Alta	Medio	Alto	Muy alto

Fuente: Instituto Nacional de Ciberseguridad[5].

Acciones para la gestión de riesgos

Después de revisar los riesgos cibernéticos presentados y alinear su probabilidad e impacto, la junta debe evaluar las acciones para gestionarlos.

Los posibles tipos de acciones de gestión incluyen:

Acciones de mitigación: los riesgos pueden mitigarse mediante controles o capacidades técnicas, administrativas, físicas y organizativas. Ejemplos de ello son los controles de riesgos dirigidos a las personas y a la cultura, como la formación de los empleados, o campañas de sensibilización.

Controles de riesgos organizativos/procedimentales, como disposiciones contractuales, políticas, gobernanza, legislación e intercambio de información entre industrias, o ayuda mutua y respuestas coordinadas (esta categoría incluye controles de riesgos administrativos).

Existen estándares que sirven como marco de referencia para la evaluación y gestión de riesgos cibernéticos. La mayoría de estos abordan necesidades específicas de los funcionarios y ejecutivos encargados de la ciberseguridad

[4] Advancing Cyber Resilience Principles and Tools for Boards, 2017.
[5] Consultado en: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo.

en la organización. No obstante, muchos de estos contienen conceptos técnicos que dificultan una discusión estratégica y fluida con la junta directiva.

Algunos de los estándares y marcos de referencia utilizados por las organizaciones son: (i) la serie de normas ISO / IEC 27000; (ii) el Control *Objectives for Information and Related Technologies* (COBIT) de ISACA; (iii) NIST *Special Publication* (SP) 800 Series; (iv) el *Federal Information Processing Standards* (FIPS) de NIST; (v) *OCTAVE Allegro* y (vi) *Payment Card Industry Security Standards Council* (PCISSC)

Cada uno de estos estándares usa diferentes taxonomías y metodologías para su área particular de aplicación. Aunque todos comparten elementos técnicos y enfoques comunes, el Foro Económico Mundial elaboró, dada la dificultad de algunos de los conceptos técnicos, un marco de referencia para identificar y evaluar el riesgo cibernético, el cual permite adaptar las estrategias al nivel de la junta directiva (Gráfico 1).

Este marco de referencia sirve como insumo para que la junta directiva pueda tener discusiones más estructuradas sobre el impacto del riesgo cibernético en su organización. Así mismo, la junta directiva podrá evaluar la pertinencia de los reportes que realiza el área de ciberseguridad.

Los estándares mencionados anteriormente definen el riesgo cibernético como la combinación de probabilidad de un incidente dentro de los sistemas de información y el impacto de este en los activos de la entidad[6]. En este sentido, los riesgos cibernéticos son un problema comercial con aspectos técnicos, esto teniendo en consideración que los riesgos cibernéticos pueden afectar y verse afectados por todas las áreas de la organización e incluso por otras partes de la cadena de valor (proveedores y terceros).

Como se observa en el Cuadro 2, el impacto de un incidente cibernético resulta de la pérdida de una o múltiples cualidades de un activo, ya sea una pérdida de

confidencialidad, integridad, disponibilidad o responsabilidad. Por otra parte, la combinación de vulnerabilidades y amenazas identificadas indica la probabilidad del incidente cibernético. En caso tal de que

Gráfico 1. Marco de evaluación de riesgos cibernéticos de las Juntas Directivas.

Fuente: Foro Económico Mundial

[6] *World Economic Forum. (2017). Advancing Cyber Resilience Principles and Tools for Boards.*

no sea factible realizar una cuantificación del incidente, la organización debe hacer una evaluación cualitativa utilizando una escala "baja / media / alta" para priorizar el riesgo.

Componentes de la evaluación del riesgo cibernético por parte de la junta directiva

Paso 1: activos. La junta debe tener una perspectiva sobre el inventario de los activos más importantes de la organización. Este inventario incluye sistemas de *hardware* y *software* redes, e infraestructura para operar sus sistemas, así como la información, personas y recursos externos. Para una evaluación a nivel de junta, los activos deben ser agregados en categorías.

Paso 2: pérdidas de los activos y su impacto. En el siguiente paso, se debe evaluar el impacto potencial de un incidente. Por lo tanto, cada activo priorizado identificado previamente debe ser evaluado bajo estas dimensiones (Cuadro 3):

Para cada celda de la matriz, el impacto de la pérdida está determinado. Se recomienda tomar todos los costos asociados: (i) costo directamente asociado con el incidente (por ejemplo, pérdida financiera debido a datos de transacciones manipulados o pérdida en ventas); (ii) costo indirectamente asociado con el incidente (por ejemplo, un daño a la reputación de la organización), y (iii) costo de investigar el incidente (por ejemplo, costo externo de asesores)

Luego de que las pérdidas potenciales y el impacto son determinados, la probabilidad de un incidente debe ser evaluada con el fin obtener el valor esperado del riesgo.

Paso 3: vulnerabilidades. La combinación del nivel de amenaza y vulnerabilidades indica la probabilidad de que un incidente se materialice. Las vulnerabilidades pueden clasificarse dentro de las siguientes categorías: (i) personas y cultura; (ii) procesos y organización y (iii) tecnología e infraestructura.

Mientras que para la última categoría hay herramientas de prueba automatizadas que se ejecutan continuamente por

Cuadro 2. Ejemplos de riesgos

Riesgo	Impacto		Probabilidad		Resultado
	Activo en riesgo	Pérdida de	Vulnerabilidad	Amenaza	
Pérdida de integridad y confiabilidad de datos financieros	Información financiera o sistemas. Ej. Ordenes de transferencia	Integridad y confiabilidad	Procesos: no se modifican los controles (duales) lo que permite a los empleados manipular sistemas o datos financieros	Fraude interno	Pérdida de fraude financiero directo menos recuperaciones de seguros. Costo directo de investigación del incidente (recursos internos y externos) Riesgo reputacional, impacto en ventas, cuota de mercado y precio de la acción. Sanciones y multas.
Pérdida de confidencialidad de los datos de los clientes	Datos de los clientes, reputación.	Confidencialidad	Personas: se contacta a un empleado que no está capacitado y no es consciente cuando envía los datos del cliente por correo electrónico	Ataques de phishing de una organización criminal	Costo directo de investigación del incidente (recursos internos y externos) Riesgo regulatorio, impacto en las ventas, costo de renovación de pólizas de seguros y precio de la acción. Sanciones y multas del supervisor.

Fuente: Foro Económico Mundial

Cuadro 3. Dimensiones para la evaluación de los activos priorizados.

Tipo de activos	Confidencialidad	Pérdida de Integridad y confianza	Pérdida de Disponibilidad	Pérdida de Confidencialidad
	Datos de clientes			
	Datos financieros			
	IP			
	Producción y control de sistemas			

Fuente: Foro Económico Mundial

equipos operativos, las dos primeras categorías deber ser estudiadas de forma distinta.

Algunas preguntas típicas que deben plantearse en torno a estas categorías incluyen: ¿cuál es el nivel de conciencia y capacitación de nuestros empleados?; ¿están seguros nuestros empleados de qué es seguro y qué no? y, ¿qué tan fácil sería tener acceso a información, modificar datos o hacer que no estén disponibles?

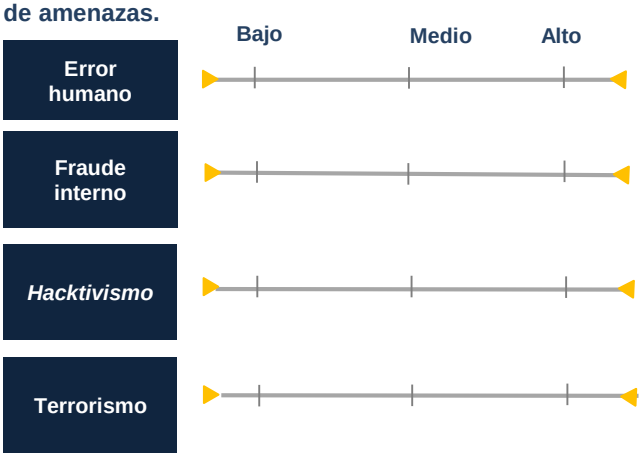
La junta debe ser consciente de que el patrón de riesgo de una empresa puede cambiar de repente y necesita ser actualizado continuamente por la administración, basado en cambios como la introducción de nuevas tecnologías, que pueden aumentar las oportunidades de ataque por parte de nuevos agentes de amenaza.

Debido a su importancia, los riesgos cibernéticos deberían ser parte de la agenda estándar de las reuniones de la junta. Así mismo, la gerencia debe reportar cambios en los patrones de riesgo, las medidas de mitigación correspondientes y la exposición al riesgo residual.

Paso 4: amenazas. Como se mencionó anteriormente, la probabilidad de un incidente resulta de una combinación de amenazas y vulnerabilidades que pueden ser explotadas. En general, las juntas directivas tienen un alto nivel de conciencia y comprensión de la relevancia de amenazas generales y cibernéticas a sus negocios.

La junta debe considerar las amenazas en el contexto de los negocios actuales y futuros y determinar su relevancia para la organización en una escala de bajo a alto. Cada grado en la escala asigna la probabilidad de que se realice un ataque contra la organización *(hacktivismo*, error humano, terrorismo, entre otros). Este análisis debe tener en cuenta la experiencia y recursos conocidos disponibles por los agentes de amenaza (ráfico 2).

Gráfico 2. Escala para la probabilidad de ocurrencia de amenazas.



Fuente: Foro Económico Mundial.

A nivel operativo, el área de seguridad de la organización debe contar con un servicio de inteligencia de amenazas cibernéticas que pueda identificar los agentes de amenaza que podrían llegar a impactar a la entidad. Este servicio puede ser contratado con un tercero o con recursos propios de la empresa.

Una vez se han evaluado las amenazas y vulnerabilidades, la junta directiva debe combinar los cuatro elementos del marco de referencia de riesgo cibernético y preguntarse:

1. ¿Cuáles son los activos más importantes identificados en el paso 1?
2. ¿Cuáles serían las pérdidas potenciales de estos activos si sufren el mayor nivel de impacto?
3. ¿Qué combinación de vulnerabilidades y amenazas

podría derivar en una pérdida y,
4. ¿Qué tan probable es que se de esa combinación?

A partir de este análisis, la junta directiva podrá determinar el nivel de impacto y probabilidad de los riesgos cibernéticos y ubicarlos con mayor precisión (Cuadro 1).

Casos de organizaciones con incidentes de ciberseguridad

En los últimos años se han presentado varios casos en los que se puede evidenciar cómo las malas decisiones de las juntas directivas han causado daños económicos a la organización y a sus accionistas.

El 30 de noviembre del 2018 se dio a conocer una de las brechas de seguridad más icónicas de los últimos años cuando la cadena hotelera de lujo, Marriott, declaró que una base de datos de reservas había sido comprometida por un tercero desconocido. Ello significó dejar expuestos los datos de más de 339 millones de clientes alrededor del mundo, como nombres, correos, direcciones, teléfonos, números de pasaporte e incluso información financiera[7].

Después de varias investigaciones, la cadena confirmó que se había encontrado un troyano que permitió el acceso remoto a los sistemas de la base de datos y que los cibercriminales habían estado en sus sistemas desde julio del 2014.

Lo curioso en este caso es que la compañía conoció la brecha de seguridad en septiembre, pero no fue sino hasta finales de noviembre que lo hicieron público. Esta decisión no solo puso en riesgo durante varios meses a los clientes cuya información fue robada, sino también fue una de las causas por las que hoy la compañía fue multada por más de 100 millones de libras esterlinas por la Oficina del Comisionado de Información del Reino Unido, que consideró que existió una brecha de información y una violación a la Regulación General de Protección de Datos (GDPR, por sus siglas en inglés), dados los 7 millones de ciudadanos del Reino Unido cuya información fue comprometida[8].

Otro ejemplo del impacto que pueden llegar a tener los incidentes cibernéticos, es el conocido caso de robo de datos a Equifax en el 2017. Equifax, buró de crédito, sufrió un incidente cibernético en el cual la información personalmente identificable (PII, por sus siglas en inglés) de alrededor de 147 millones de clientes de Estados Unidos fue robada, siendo considerada unas de las peores violaciones de datos de la historia, teniendo en cuenta la naturaleza de la información que fue asaltada[9]. El ataque, perpetuado por *hackers* que explotaron una falla en el *software* de código abierto que usó el buró, conllevó a demandas colectivas, al retiro del *Chief Information Officer* (CIO) Dave Webb, *Chief Security Officer* (CSO) Susan Mauldin y al CEO Richard Smith[10] y una multa de la Comisión Federal de Comercio (FTC) de Estados Unidos de 700 millones de dólares[11].

Teniendo en cuenta lo anterior, se evidencia que en el alcance de los ataques cibernéticos no solo se ve la adquisición ilegal de datos cruciales de los clientes por parte de delincuentes, sino en los riesgos reputacionales, multas de supervisores y, en este caso, cambios organizacionales dentro de la compañía.

Así mismo, en 2019 la agencia calificadora de riesgo Moody's bajó la perspectiva de Equifax de estable a negativa (debido al incidente de ciberseguridad mencionado anteriormente). Por primera vez, este tipo de incidentes fue considerado como el principal factor que ha motivado cambios en la perspectiva[12].

De igual manera, la agencia anunció que desarrollará *ratings* para evaluar el riesgo que tienen las

[7] *O'Flaherty, K. (11 de marzo de 2019). Forbes. Obtenido de Marriott CEO Reveals New Details About Mega Breach: https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#13b5ba66155c*
[8] *formation Commissioner's* Office. (9 de julio de 2019). *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach.* Obtenido de https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
[9] BBC (2019). *Equifax top ay up to $700m to settle data breach*. Obtenido de https://www.bbc.com/news/technology-49070596
[10] PrWeek (Septimebre 20, 2017). Timeline of a crisis. How Equifax responded to one of the worst hacks in history. Obtenido de https://www.prweek.com/article/1445241/timeline-crisis-equifax-responded-one-worst-hacks-history
[11] Forbes (Julio 22, 2019). *Equifax just got fined up to $700 Million For That Massive 2017 Hack*. Obtenido de https://www.forbes.com/sites/thomasbrewster/2019/07/22/equifax-just-got-fined-up-to-700-million-for-that-massive-2017-hack/#7f5f21e83e96
[12] CNBC (Mayo 22, 2019). *Equifax just became the first company to have its Outlook downgraded for a cyber attack*. Obtenido de https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html

compañías de sufrir un impacto significativo a raíz de un ciberataque[13].

De acuerdo con lo anterior, es primordial que las juntas directivas incluyan en sus planes de negocio aspectos como la integración de ciberresiliencia en la organización, la implementación, desarrollo y constante mejora de planes de resiliencia. No solo por el bienestar de la compañía en términos reputacionales de supervisores, sino por el creciente interés del mercado en percibir y calificar qué compañías cuentan con suficiente protección a sus sistemas y a los datos de sus clientes. En un estudio realizado por la consultora PricewaterhouseCoopers se señala que los inversionistas consideran los ataques cibernéticos como la principal amenaza a las compañías, por encima de la incertidumbre geopolítica, el populismo y proteccionismo[14].

Otro ejemplo para considerar es la brecha de seguridad que presentó uno de los bancos con más emisiones de tarjetas de crédito en Estados Unidos, Capital One, quien descubrió que en marzo de 2019 un tercero se había robado información de tarjetahabientes de Estados Unidos y Canadá, información a la que se accedió por medio de un *firewall* mal configurado. La información expuesta incluye aproximadamente 140.000 números de seguro social y 80.000 números de cuentas. La demás información filtrada corresponde a nombres, direcciones, fechas de nacimiento, puntajes de crédito e información transaccional.

Ahora bien, como ha señalado el Foro Económico Mundial, a pesar de que las juntas han adquirido mayor conciencia del ciberriesgo en años recientes, hace falta trabajar en un conjunto de principios sobre cómo responder y desarrollar ciberresiliencia en sus organizaciones. En este sentido, las recomendaciones propuestas por el Foro Económico Mundial sirven de guía para los miembros de la Junta.

Consideraciones finales

Organismos multilaterales como el Foro Económico Mundial han realizado esfuerzos por sensibilizar a la alta dirección de las organizaciones para tomar decisiones asertivas y estratégicas en ciberseguridad. En la medida que existan nuevas metodologías para cuantificar el riesgo cibernético y sea percibido por parte de los inversionistas y actores del mercado, la importancia de este tema para los miembros de la junta será mayor.

En este sentido, el sistema financiero colombiano debe definir los principios bajo los cuales se deben diseñar estrategias ajustadas a las necesidades de ciberresiliencia del país.

Finalmente, vale la pena destacar que el éxito y eficiencia de este tipo de estrategias no solo depende de los planes o adecuaciones a la estructura organizacional de las entidades, sino de una cultura que involucre a todos los actores relevantes como colaboradores y proveedores.

[13] CNBC (Noviembre 12, 2018). *Moody's is going to start building the risk of a business-ending hack into its credit ratings*. Obtenido de https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html
[14] PwC (2018)*Transparency in the digital age: companies should talk about their cyber security*. Obtenido de https://www.pwc.co.uk/cyber-security/pdf/transparency-in-the-digital-age.pdf

Colombia
Principales indicadores macroeconómicos

	2015	2016	2017					2018					2019*		
	Total	Total	T1	T2	T3	T4	Total	T1	T2	T3	T4	Total	T1	T2	Total
Producto Interno Bruto**															
PIB Nominal (COP Billones)	**804,7**	**863,8**	217,5	218,7	233,7	250,3	**920,2**	231,2	234,3	248,8	264,3	**978,5**	246,2	251,7	**1044,1**
PIB Nominal (USD Billones)	**255,5**	**287,0**	74,0	72,0	79,6	83,9	**308,4**	83,1	79,9	83,7	81,3	**301,1**	77,6	78,5	**328,0**
PIB Real (COP Billones)	**804,7**	**821,5**	193,9	201,9	209,4	227,4	**832,6**	197,8	207,8	214,9	233,5	**854,0**	203,8	214,0	**881,3**
PIB Real (% Var. interanual)	**3,0**	**2,1**	1,4	1,3	1,5	1,2	**1,4**	2,0	2,9	2,6	2,7	**2,6**	3,1	3,0	**3,2**
Precios															
Inflación (IPC, % Var. interanual)	**6,8**	**5,7**	4,7	4,0	4,0	4,1	**4,1**	3,1	3,2	3,2	3,2	**3,2**	3,2	3,4	**3,4**
Inflación sin alimentos (% Var. interanual)	**5,2**	**5,1**	5,1	5,1	4,7	5,0	**5,0**	4,1	3,8	3,7	3,5	**3,5**	3,3	3,2	**3,2**
Tipo de cambio (COP/USD fin de periodo)	**3149**	**3010**	2941	3038	2937	2984	**2984**	2780	2931	2972	3250	**3250**	3175	3206	**3183**
Tipo de cambio (Var. % interanual)	**31,6**	**-4,4**	-6,0	1,5	0,4	-0,9	**-0,9**	-5,5	-3,5	1,2	8,9	**8,9**	14,2	9,4	**-2,1**
Sector Externo (% del PIB)															
Cuenta corriente	**-6,3**	**-4,2**	-4,7	-3,3	-3,5	-1,9	**-3,3**	-3,4	-3,8	-3,6	-4,4	**-3,7**	-4,6	…	**-4,2**
Cuenta corriente (USD Billones)	**-18,6**	**-12,0**	-3,5	-2,5	-2,8	-1,6	**-10,3**	-2,8	-3,1	-3,1	-3,7	**-12,7**	-3,6	…	**-13,7**
Balanza comercial	**-6,2**	**-4,5**	-3,4	-3,3	-2,9	-1,3	**-2,7**	-1,9	-2,7	-2,7	-3,7	**-2,7**	-3,5	…	**-1,7**
Exportaciones F.O.B.	**15,7**	**14,8**	15,0	15,3	15,6	15,8	**15,4**	15,7	16,5	16,3	16,6	**15,9**	16,3	…	**14,4**
Importaciones F.O.B.	**21,9**	**19,3**	18,4	18,6	18,5	17,2	**18,2**	17,6	19,2	19,0	20,3	**18,6**	19,8	…	**16,5**
Renta de los factores	**-2,0**	**-1,8**	-3,1	-2,2	-2,7	-2,7	**-2,7**	-3,6	-3,3	-3,2	-3,4	**-3,3**	-3,3	…	**-3,2**
Transferencias corrientes	**1,9**	**2,1**	1,9	2,2	2,1	2,2	**2,1**	2,0	2,2	2,3	2,7	**2,3**	2,2	…	**2,2**
Inversión extranjera directa (pasivo)	**4,0**	**4,9**	3,4	3,4	6,4	4,5	**4,4**	2,4	4,5	3,2	3,2	**3,3**	4,3	…	**12,0**
Sector Público (acumulado, % del PIB)															
Bal. primario del Gobierno Central	**-0,5**	**-1,1**	-0,7	0,2	0,6	-0,8	**-0,8**	-0,3	-1,1	-1,9	-0,3	**-0,3**	-0,6	…	**-2,0**
Bal. del Gobierno Central	**-3,0**	**-4,0**	-1,2	-1,2	-2,0	-3,6	**-3,6**	-0,6	-1,5	-3,0	-3,1	**-3,1**	0,0	…	**-2,4**
Bal. estructural del Gobierno Central	**-2,2**	**-2,2**	…	…	…	…	**-1,9**	…	…	…	…	**-1,9**	…	…	**-1,5**
Bal. primario del SPNF	**-0,6**	**0,9**	-0,1	1,2	2,0	0,5	**0,5**	0,5	0,8	0,7	0,2	**0,2**	1,0	…	**-2,2**
Bal. del SPNF	**-3,4**	**-2,4**	-0,5	-0,3	-0,8	-2,7	**-2,7**	0,0	-0,5	-1,8	-2,9	**-2,9**	0,4	…	**1,0**
Indicadores de Deuda (% del PIB)															
Deuda externa bruta	**38,2**	**42,5**	38,5	38,5	39,9	40,0	**40,0**	38,1	38,1	38,4	39,7	**39,7**	41,1	…	**…**
Pública	**22,6**	**25,1**	22,9	22,4	23,2	23,1	**23,1**	22,1	21,8	21,8	21,9	**21,9**	22,7	…	**…**
Privada	**15,6**	**17,4**	15,6	16,0	16,7	16,9	**16,9**	16,1	16,3	16,5	17,7	**17,7**	18,5	…	**…**
Deuda bruta del Gobierno Central	**40,8**	**42,5**	43,6	44,1	45,6	46,6	**43,1**	43,7	46,1	48,0	49,8	**49,8**	47,6	…	**…**

* Proyecciones. ** PIB Real: Datos originales. - DANE, base 2015.
Fuente: PIB y Crecimiento Real – DANE, proyecciones Asobancaria. Sector Externo – Banco de la República, proyecciones MHCP y Asobancaria. Sector Público – MHCP. Indicadores de deuda – Banco de la República, Departamento Nacional de Planeación y MHCP.

Colombia
Estados financieros del sistema bancario*

	jun-19 (a)	may-19	jun-18 (b)	Variación real anual entre (a) y (b)
Activo	**657.077**	**654.793**	**588.500**	**8,0%**
Disponible	47.636	46.530	34.865	32,1%
Inversiones y operaciones con derivados	125.385	126.210	107.181	13,1%
Cartera de crédito	460.578	459.177	429.009	3,8%
Consumo	134.394	133.150	119.555	8,7%
Comercial	249.711	250.094	239.223	0,9%
Vivienda	64.172	63.623	58.218	6,6%
Microcrédito	12.302	12.310	12.013	-1,0%
Provisiones	28.114	28.382	26.211	3,7%
Consumo	10.213	10.152	9.558	3,3%
Comercial	14.728	15.099	13.778	3,4%
Vivienda	2.292	2.261	2.026	9,4%
Microcrédito	880	871	850	0,1%
Pasivo	**571.736**	**571.324**	**512.255**	**7,9%**
Instrumentos financieros a costo amortizado	492.118	488.597	446.110	6,7%
Cuentas de ahorro	182.107	180.653	165.228	6,6%
CDT	161.084	160.509	153.502	1,5%
Cuentas Corrientes	53.593	53.196	49.745	4,2%
Otros pasivos	9.280	9.364	3.387	164,9%
Patrimonio	**85.341**	**83.469**	**76.245**	**8,2%**
Ganancia / Pérdida del ejercicio (Acumulada)	**4.970**	**4.512**	**4.269**	**12,6%**
Ingresos financieros de cartera	22.754	18.915	21.792	1,0%
Gastos por intereses	6.860	6.661	7.917	-16,2%
Margen neto de Intereses	15.472	12.875	14.516	3,0%
Indicadores				**Variación (a) - (b)**
Indicador de calidad de cartera	**4,65**	**4,78**	**4,89**	**-0,24**
Consumo	5,22	5,24	5,85	-0,63
Comercial	4,56	4,81	4,69	-0,12
Vivienda	3,27	3,26	3,13	0,15
Microcrédito	7,32	7,16	7,78	-0,47
Cubrimiento	**131,3**	**129,2**	**125,0**	**-6,25**
Consumo	145,5	145,6	136,6	8,86
Comercial	129,3	125,4	122,9	6,40
Vivienda	109,1	109,1	111,3	-2,19
Microcrédito	97,8	98,8	90,9	6,94
ROA	1,67%	1,66%	1,46%	0,2
ROE	13,22%	13,47%	11,51%	1,7
Solvencia	15,06%	15,07%	15,76%	-0,7

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

Edición 1202

Colombia

Principales indicadores de inclusión financiera

	2015	2016	2017					2018		2019
	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2
Profundización financiera - Cartera/PIB (%) EC	**49,9**	**50,2**	**50,1**	49,8	49,8	49,4	50,1	**50,1**	49,9	50,1
Efectivo/M2 (%)	**12,53**	**12,59**	**12,18**	12,40	12,07	12,27	13,09	**13,09**	12,76	12,84
Cobertura										
Municipios con al menos una oficina o un corresponsal bancario (%)	**99,9**	**99,7**	**100**	99,9	100	99,9	99,2	**99,2**	…	…
Municipios con al menos una oficina (%)	**75,3**	**73,9**	**73,9**	74,0	74,1	74,2	74,4	**74,4**	74,5	74,4
Municipios con al menos un corresponsal bancario (%)	**99,6**	**99,5**	**100**	99,9	100	98,2	98,3	**98,3**	…	…
Acceso										
Productos personas										
Indicador de bancarización (%) SF*	**76,30**	**77,30**	**80,10**	80,10	80,8	81,3	81,4	81,4	82,3	…
Indicador de bancarización (%) EC**	**75,40**	**76,40**	**79,20**	79,00	79,70	80,4	80,5	80,5	81,3	…
Adultos con: (en millones)										
Cuentas de ahorro EC	**23,01**	**23,53**	**25,16**	25,00	25,3	25,6	25,75	25,75	25,79	
Cuenta corriente EC	**1,75**	**1,72**	**1,73**	1,74	1,81	1,8	1,89	1,89	1,95	
Cuentas CAES EC	**2,81**	**2,83**	**2,97**	3,00	3,02	3,02	3,02	3,02	3,03	
Cuentas CATS EC	**0,10**	**0,10**	**0,10**	0,10	0,10	0,10	0,71	0,71	2,10	
Otros productos de ahorro EC	**0,58**	**0,77**	**0,78**	0,78	0,81	0,82	0,81	0,81	0,83	
Crédito de consumo EC	**8,28**	**8,74**	**9,17**	7,23	7,37	7,47	7,65	7,65	7,82	
Tarjeta de crédito EC	**8,94**	**9,58**	**10,27**	9,55	9,83	9,98	10,05	10,05	10,19	
Microcrédito EC	**3,50**	**3,56**	**3,68**	3,41	3,50	3,49	3,51	3,51	3,49	
Crédito de vivienda EC	**1,31**	**1,39**	**1,43**	1,34	1,37	1,38	1,40	1,40	1,41	
Crédito comercial EC	**-**	**1,23**	**1,02**	0,65	0,67	0,66	…	…	…	
Al menos un producto EC	**24,66**	**25,40**	**27,1**	26,8	27,2	27,5	27,64	27,64	28,03	
Uso										
Productos personas										
Adultos con: (en porcentaje)										
Algún producto activo SF	**64,5**	**66,3**	**68,6**	67,1	68,0	68,4	68,5	68,5	69,2	
Algún producto activo EC	**63,5**	**65,1**	**66,9**	65,7	66,6	67,1	67,2	67,2	67,8	
Cuentas de ahorro activas EC	**71,7**	**72,0**	**71,8**	67,7	68,4	68,4	68,3	68,3	68,9	
Cuentas corrientes activas EC	**86,3**	**84,5**	**83,7**	84,4	85,0	85,1	85,5	85,5	85,8	
Cuentas CAES activas EC	**87,3**	**87,5**	**89,5**	89,7	89,8	89,8	89,7	89,7	89,8	
Cuentas CATS activas EC	**96,5**	**96,5**	**96,5**	96.5	95,2	96,5	67,7	67,7	58,2	
Otros pdtos. de ahorro activos EC	**53,1**	**66,6**	**62,7**	62,0	62,5	62,1	61,2	61,2	61,3	
Créditos de consumo activos EC	**82,4**	**82,0**	**83,5**	82,0	81,5	81,8	82,2	82,2	81,7	
Tarjetas de crédito activas EC	**92,0**	**92,3**	**90,1**	88,9	88,9	88,7	88,7	88,7	88,3	
Microcrédito activos EC	**70,8**	**66,2**	**71,1**	71,2	70,4	69,4	68,9	68,9	68,9	

Edición 1202

Colombia

Principales indicadores de inclusión financiera

	2015	2016	2017					2018		2019
	Total	Total	Total	T1	T2	T3	T4	Total	T1	T2
Créditos de vivienda activos EC	**79,1**	**79,3**	**78,9**	78,2	77,7	77,8	77,8	77,8	77,8	…
Créditos comerciales activos EC	**-**	**85,3**	**84,7**	59,2	58,7	57,6	…	…	…	…
Acceso										
Productos empresas										
Empresas con: (en miles)										
Al menos un producto EC	**726,8**	**751,0**	**775,2**	944,3	947,8	946,6	946,5	946,5	940,7	…
Cuenta de ahorro EC	**475,5**	**500,8**	**522,7**	649,7	647,7	648,9	…	…	…	…
Cuenta corriente EC	**420,4**	**420,9**	**430,7**	488,9	505,2	502,4	…	…	…	…
Otros productos de ahorro EC	**11,26**	**15,24**	**14,12**	14,4	14,1	14,0	…	…	…	…
Crédito comercial EC	**223,2**	**242,5**	**243,6**	265,3	272,2	276,5	…	…	…	…
Crédito de consumo EC	**96,65**	**98,72**	**102,5**	104,4	106,7	105,3	…	…	…	…
Tarjeta de crédito EC	**77,02**	**79,96**	**94,35**	102,1	104,4	105,1	…	…	…	…
Al menos un producto EC	**726,7**	**751,0**	**775,1**	944,3	947,8	946,6	…	…	…	…
Uso										
Productos empresas										
Empresas con: (en porcentaje)										
Algún producto activo EC	**75,2**	**74,7**	**73,3**	71,6	71,9	71,6	...	...	…	…
Algún producto activo SF	**75,2**	**74,7**	**73,3**	71,7	71,9	71,6	71,6	71,6	70,0	…
Cuentas de ahorro activas EC	**49,1**	**49,1**	**47,2**	48,1	47,7	48,2	…	…	…	…
Otros pdtos. de ahorro activos EC	**45,3**	**57,5**	**51,2**	50,8	49,5	49,5	…	…	…	…
Cuentas corrientes activas EC	**90,5**	**89,1**	**88,5**	88,5	88,2	88,6				
Microcréditos activos EC	**60,8**	**63,2**	**62,0**	58,5	58,5	57,2				
Créditos de consumo activos EC	**84,8**	**84,9**	**85,1**	83,7	83,4	83,7	…	…	…	…
Tarjetas de crédito activas EC	**85,6**	**88,6**	**89,4**	90,6	89,8	90,0				
Créditos comerciales activos EC	**89,2**	**91,3**	**90,8**	91,0	91,1	91,4	…	…	…	…
Operaciones (semestral)										
Total operaciones (millones)	**4.333**	**4.926**	**5.462**	-	2.926	-	3.406	**6.332**	-	3.953
No monetarias (Participación)	**44,7**	**48,0**	**50,3**	-	52,5	-	55,6	**54,2**	-	57,8
Monetarias (Participación)	**55,3**	**52,0**	**49,7**	-	47,4	-	44,3	**45,8**	-	42,1
No monetarias (Crecimiento anual)	**33,3**	**22,22**	**16,01**	-	18,66	-	30,9	**25,1**	-	48,7
Monetarias (Crecimiento anual)	**6,09**	**6,79**	**6,14**	-	6,30	-	7,0	**6,7**	-	20,0
Tarjetas										
Crédito vigentes (millones)	**13,75**	**14,93**	**14,89**	14,91	15,03	15,17	15,28	**15,28**	15,38	15,47
Débito vigentes (millones)	**22,51**	**25,17**	**27,52**	28,17	28,68	29,26	29,57	**29,57**	31,17	31,39
Ticket promedio compra crédito ($miles)	**215,9**	**205,8**	**201,8**	194,1	196,1	183,1	194,4	**194,4**	191,8	193,3
Ticket promedio compra débito ($miles)	**137,4**	**138,3**	**133,4**	121,2	123,2	120,3	131,4	**131,4**	116,8	116,4

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