CEF ANÁLISIS

INFORME CEF MACROFINANCIERO

Nº 19 / DICIEMBRE 2018

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

ECONOMÍA INTERNACIONAL
UN RESULTADO MEJOR A LO ESPERADO DE LA CUMBRE DEL G20

ACTIVIDAD ECONÓMICA
IPOM DE DICIEMBRE, "PAÑOS FRÍOS" AL PESIMISMO REINANTE.

BANCA
TIPO DE CAMBIO E INFLACIÓN: DOS PALANCAS CRÍTICAS DEL RIESGO PARA LA BANCA.

PENSIONES
ESTADÍSTICAS DEL MERCADO LABORAL DEL SISTEMA DE PENSIONES VS ESTADÍSTICAS DEL INE.

TEMA DE ANÁLISIS
CIBERSEGURIDAD Y CÓMO ENFRENTARLA

NUEVA NORMATIVA FINANCIERA

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

UN RESULTADO MEJOR A LO ESPERADO DE LA CUMBRE G20

Se esperaba poco de la reunión de los líderes mundiales en Buenos Aires el último fin de semana de noviembre. Esto porque desde la llegada de Trump al gobierno de Estados Unidos, las cumbres de este nivel suelen no generar buenas noticias. Por esa razón es que los resultados, especialmente la reunión del presidente norteamericano con su par chino, Xi Jinping, fueron recibidos con beneplácito por los mercados, y no tanto porque se pudiera decir que los problemas se han resuelto, sino porque se hizo menos evidente que se fueran a agravar en el corto plazo.

Las dos buenas noticias que resultaron de esta Cumbre fueron que se logró firmar una declaración conjunta, y que al menos en forma momentánea, bajaron las tensiones de la Guerra Comercial entre China y Estados Unidos, ya que éste último país aceptó postergar por 90 días el anuncio de un alza adicional de aranceles que se iniciaría el 1° de Enero.

En relación a la declaración conjunta, es más que nada un conjunto de buenas intenciones, pero al menos es un punto de partida en común. En el documento los líderes del bloque afirmaron que el comercio y la inversión internacionales son importantes motores del crecimiento, la innovación, la creación de empleo y el desarrollo, junto con destacar la contribución del sistema comercial multilateral para lograr este objetivo. Reconocieron, sin embargo, que los mecanismos vigentes aún no han cumplido su función y enfatizaron la necesidad de una reforma de la Organización Mundial del Comercio (OMC), con el fin de mejorar su desempeño.

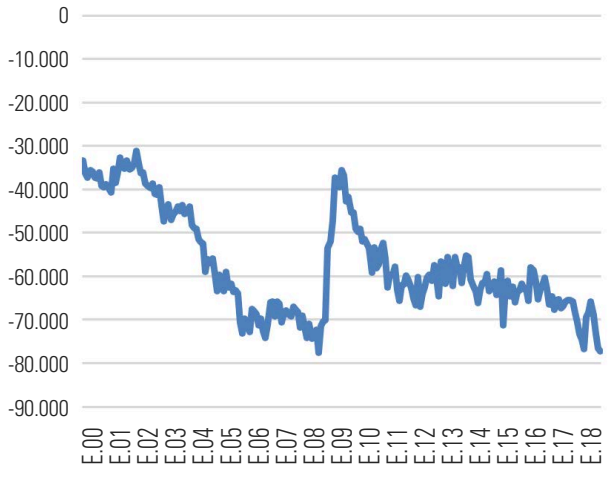
En relación con el cambio climático, la declaración conjunta afirma que este es un compromiso irreversible, ya que refleja la responsabilidad de cada país. El documento también apoya las actividades de cooperación con los países en desarrollo, particularmente los más vulnerables a este fenómeno climático. Sin embargo, señala también que "Estados Unidos reitera su decisión de retirarse del Acuerdo de París".

Por último, los líderes del G20 acordaron que la revolución tecnológica es un desafío relacionado con el trabajo, que no puede ser inseparable de la educación continua. También coincidieron en promover la igualdad de género, considerándola una tarea primordial, no solo como una realidad de justicia social y desarrollo.

Respecto a la baja de las tensiones en la Guerra Comercial entre Estados Unidos y China, lo más relevante parece ser el compromiso de este último país para avanzar en la apertura comercial, lo que si finalmente se hiciera efectivo, significaría que Trump, a través de un medio inapropiado como es una guerra de aranceles, habría logrado un resultado exitoso. Sin embargo, nada asegura aún ese desenlace, por lo que seguiremos en compás de espera en este tema. En lo concreto, el presidente chino se comprometió a reducir algunas barreras comerciales y de inversión y proteger mejor los derechos de propiedad intelectual, aunque sin establecer un compromiso de medidas específicas y pormenorizadas.

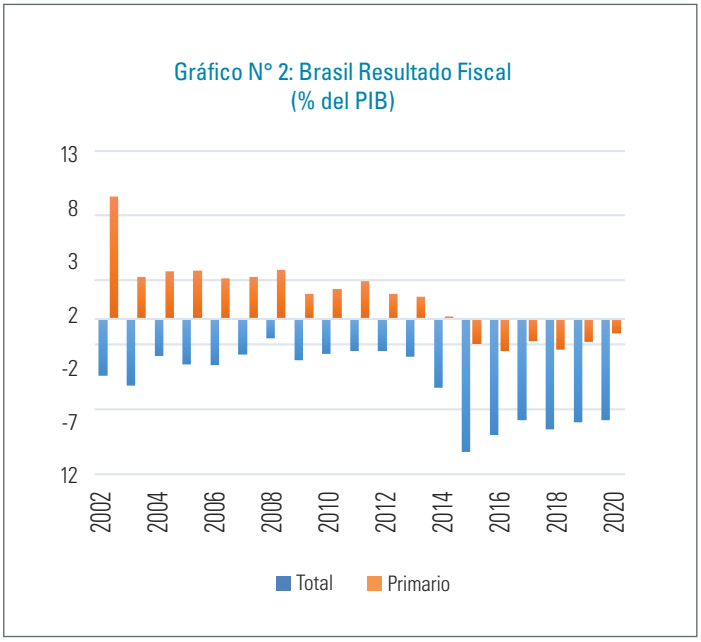
Es interesante constatar que a pesar del alza arancelaria por parte del gobierno americano, la balanza de bienes y servicios de ese país ha continuado deteriorándose (Gráfico N° 1), lo que se explica por la política fiscal expansiva y la apreciación del dólar. Es evidente que el mix de políticas que se está siguiendo no parece consistente con el objetivo de reducir el desequilibrio externo.

Gráfico N° 1: USA Balanza de Bienes y Servicios (US$ millones)



Fuente: U.S. Bureau of Economic Analysis

En nuestro continente lo más relevante, sin duda, es el cambio de mando en Brasil el 1° de Enero. Jair Bolsonaro sigue siendo una gran incógnita, pero ha formado un equipo económico que plantea como modelo de reformas a seguir el del gobierno militar chileno. Eso podría ser una muy buena noticia, si el gabinete no contara también con un componente nacionalista (el gobierno militar chileno también lo tuvo), y si además no tuviera un Congreso con mayoría opositora. El escenario se ve difícil, pero al menos existe una chance de que Brasil inicie un proceso de reformas que lo hagan viable fiscalmente, condición que hoy está lejos de cumplir. El Gráfico N° 2 muestra el déficit fiscal de ese país, que en parte muy importante se explica por el pago de intereses de la deuda (el costo de muchos años de exceso de gasto público). Para 2018 el FMI estima un déficit fiscal total de 8% del PIB (dentro de los más elevados del mundo) y un déficit primario (antes del pago de intereses) de un 1,8% del PIB. El pago de intereses de la deuda pública, por ende, representa más de un 6% del PIB. Aliviar esta situación pasa por generar una trayectoria sostenible del gasto público, de manera de lograr reducir las tasas de interés de la deuda pública, la cual alcanza a un 88% del PIB en términos brutos y a un 56% neto.



Fuente: IMF

En lo económico y fiscal, el plan del nombrado Ministro de Hacienda y Economía, Pablo Guedes, incluye un amplio plan de privatizaciones, una reforma de pensiones, que introduciría un sistema de capitalización individual, una reforma administrativa que reduce el tamaño del Estado (el gasto público representa un 38% del PIB), una simplificación tributaria y un proceso de apertura comercial, que termine con la política de sustitución de importaciones. La tarea es titánica, pero de resultar exitosa, abre la posibilidad de que Brasil pueda salir de la crisis terminal en la que lleva varios años. Lo que parece más complejo es lograr el apoyo del Congreso, que requiere la construcción de alianzas para aprobar las reformas anunciadas.

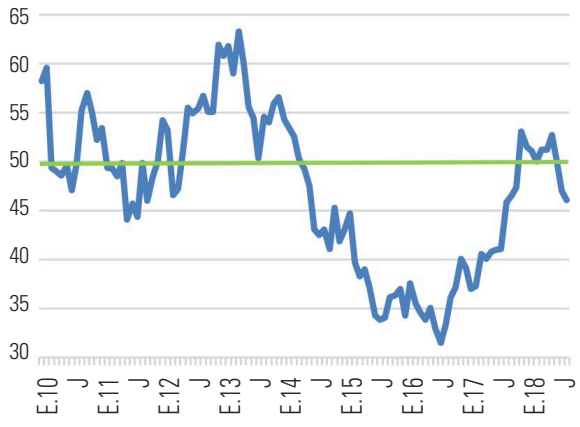
ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

IPOM DE DICIEMBRE, "PAÑOS FRÍOS" AL PESIMISMO REINANTE

El último Informe de Política Monetaria del Banco Central mantiene una perspectiva positiva para el crecimiento de la economía, aunque finalmente la tasa de expansión del PIB del año que termina se estima en un 4%, el límite inferior del rango proyectado en el IPoM de septiembre. Planteamos en esa oportunidad que dicho rango tenía un sesgo relativamente optimista, aunque el resultado es bastante mejor al que se esperaba hace un año atrás, con un contexto externo menos positivo, y bastante más incierto.

Este IPoM se da a conocer en medio de un contexto confuso en términos de la evaluación del desempeño de nuestra economía. A pesar de que las cifras muestran en forma indesmentible una recuperación de la actividad, liderada por la inversión, pareciera cundir el pesimismo, con un deterioro de los índices de confianza y expectativas. Este comportamiento de las expectativas se puede ver en el Indice de Percepción de la Economía (IPEC) de Adimark, que se muestra en el gráfico a continuación.

Gráfico N° 3: Índice IPEC Adimark



Fuente: Adimark

En informes anteriores mencionábamos que no había justificaciones claras para el excesivo optimismo que se había generado luego del cambio de gobierno, y en la misma forma tampoco hoy existen justificaciones para el ánimo negativo, que además tiene a retroalimentarse.

Por lo anterior, es positivo que en su último IPoM el Banco Central haya puesto paños fríos a este discurso medio depresivo sobre la economía, señalando que estamos en un proceso de recuperación, reflejados en signos muy positivos sobre el comportamiento de la inversión, y que en 2019 el país volvería a crecer probablemente a un ritmo superior al de la economía mundial. También parece positivo que este informe intente poner más claridad sobre las cifras de empleo del INE, algo peores a lo esperado en relación al dinamismo de la actividad. De acuerdo a lo que muestran otras fuentes de información, el mercado laboral sí estaría respondiendo al fuerte repunte de la inversión, y quedarían por resolver algunos problemas metodológicos de los datos del INE, lo que parece bastante urgente. La encuesta de empleo no sólo es clave para determinar el curso de la política monetaria, sino también para la implementación de la política social.

Sigue siendo preocupante, no obstante, que esta discusión sobre la coyuntura, con los habituales altos y bajos del IMACEC, deje de lado un tema bastante más relevante, y sobre el cual el rol de los políticos y de los técnicos es clave; el crecimiento potencial, referido a las perspectivas de desarrollo de mediano plazo, que son las que finalmente importan en el bienestar de la población. Las estimaciones de mediano plazo que hace el Banco Central son bastante claras en mostrar el desafío pendiente, a través de estimaciones de crecimiento del PIB que van de más a menos entre 2018 y 2020. Estas pasan de un 4% para el año que termina a un 3,75% en 2019 y a un 3,25% en 2020, cifra similar a las estimaciones de crecimiento potencial. Algo similar ocurre con las proyecciones de la demanda interna, que crecería un 4,7% este año, un 3,8% el siguiente y un 3,3% en 2020. En definitiva, el gobierno cumpliría la meta de duplicar el crecimiento del gobierno anterior, pero eso no significa que estemos prontos a cruzar el umbral del desarrollo.

El tema de fondo, que está poco presente en la discusión política y comunicacional, es el crecimiento de tendencia, muy relacionado con la productividad del capital y del trabajo. Es bastante evidente que en esa materia tenemos un problema que lleva ya casi dos décadas, y que sólo fue atenuado durante 2004 y 2012 años por el boom de los commodities. Recordemos que esta discusión ya se tenía con fuerza durante el gobierno de Ricardo Lagos, con varias agendas de productividad, que claramente han sido insuficientes para resolver el problema. Incluso el ex Ministro de Hacienda de Bachelet, Rodrigo Valdés, hablaba del problema estructural de nuestro sector exportador. Este desafío de productividad no fue parte de la agenda del gobierno anterior, sino por el contrario, se implementó un set de reformas que dañaron la inversión, desincentivaron el empleo formal, afectaron la certeza jurídica y aumentaron el grado de captura del Estado por parte de los funcionarios públicos. Si el objetivo es que recuperemos cifras de crecimiento de 4% o más hacia adelante, corregir las reformas del período 2014-2017, junto con avanzar en otros importantes temas pendientes, es una condición absolutamente necesaria.

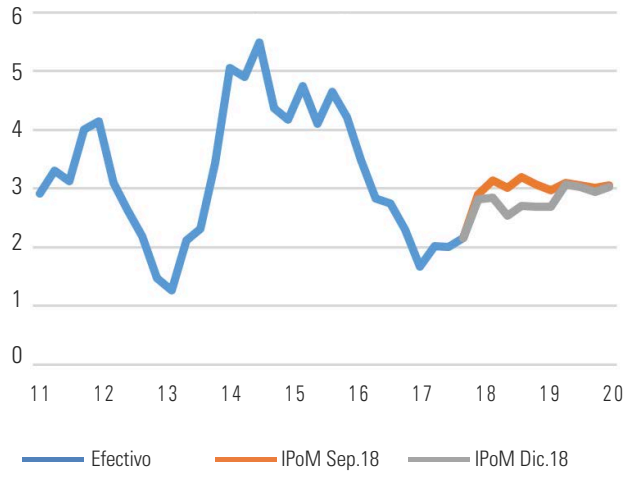
El actual gobierno está haciendo esfuerzos serios en esa materia, y si bien es cierto que sería deseable una mayor prioridad a estos temas de carácter más estructural, muy poco se puede hacer sin el concurso del poder legislativo. Llama a veces la atención que los mismos que muestran su preocupación por cifras de crecimiento y de empleo por debajo de lo que nos gustaría, muestren luego un claro rechazo a la sola discusión de iniciativas muy necesarias, muchas de las cuales están claramente identificadas en el "Acuerdo para el Desarrollo Integral", recientemente dado a conocer por el grupo de expertos que fue convocado por el gobierno. Tenemos bastante claro el diagnóstico, las políticas necesarias para solucionar los problemas, y ahora lo que falta es la voluntad política para llevarlas a cabo.

TIPO DE CAMBIO E INFLACIÓN: DOS PALANCAS CRÍTICAS DEL RIESGO PARA LA BANCA.

Luego de décadas en que las turbulencias internacionales podían tener efectos devastadores en los mercados locales -principalmente a través del tipo de cambio, alzas en las tasas de interés e inflación-, es una gran noticia observar que estos temas, debido a las buenas políticas públicas implementadas y al manejo cuidadoso de los agentes privados, pasan a segundo plano dentro del debate local (aunque siempre sin perder su importancia y centralidad).

Nos hemos acostumbrado –en buena hora- a un alto nivel en la discusión de políticas ligadas al sector financiero. Nos parece normal contar con informes de la calidad del IPoM o del Informe de Estabilidad Financiera (extremadamente completos y complejos), pero no son la norma en el resto del mundo. Estos informes permiten ver y analizar las fortalezas y debilidades del sistema financiero local y la banca.

Gráfico N° 4: Inflación efectiva y proyectada por el Banco Central (IPOM)

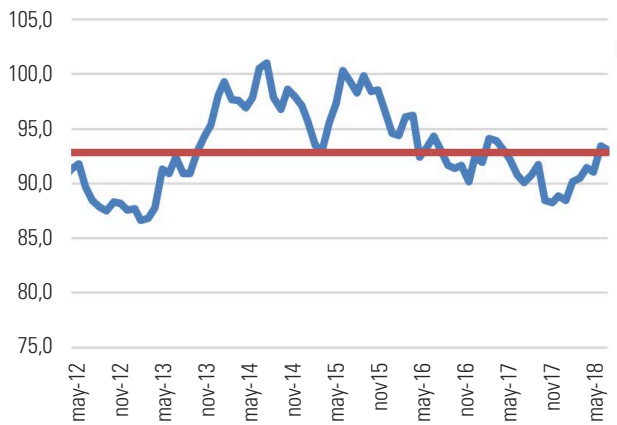


Fuente: Banco Central

Respecto de la inflación proyectada, el IPoM menciona que permanece dentro del rango meta (gráfico N° 4) y que realizará los ajustes necesarios a la política monetaria para ello. Es interesante destacar la credibilidad de esta meta, observada en el diferencial entre las tasas de créditos en UF vs créditos en pesos, como destaca el mismo informe.

Respecto del tipo de cambio, el informe indica que se encuentra al centro del nivel proyectado si se utiliza el tipo de cambio real (es decir, no parece estar ni sobre ni por debajo de su valor promedio de los últimos 10 años, lo que hace difícil predecir en qué dirección se moverá en el futuro).

Gráfico N° 5: Índice de Tipo de Cambio Real -TCR (1986=100)

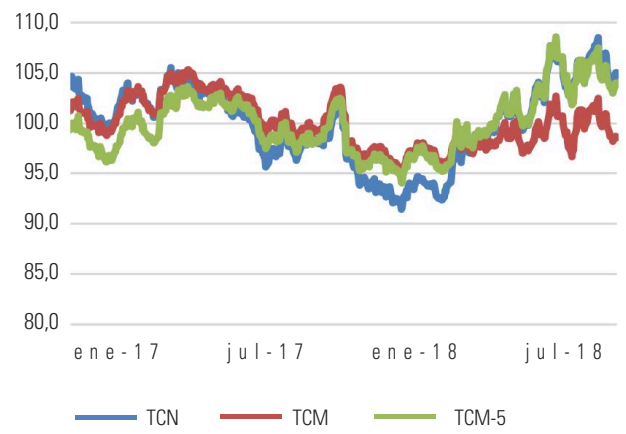


Fuente: Banco Central.

El riesgo implícito es que el aumento en el tipo de cambio se traduzca en mayor inflación (fruto del aumento del precio de los bienes importados –pass through como le llaman los economistas-), y que las empresas no puedan ajustar dichas variaciones.

Sin embargo, lo que no mencionan dichos informes en un escenario de alta volatilidad del tipo de cambio (gráfico N° 6), y aumento en la incertidumbre política global, es igualmente informativo: no existe mención alguna de temor a descalces bancarios. Tampoco hay mención a riesgos de quiebras masivas en empresas orientadas al comercio exterior, aun cuando la economía local está altamente pesificada (a diferencia de economías como Argentina que trabajan en gran medida con el dólar).

Gráfico N° 6: Indice Tipo de Cambio Nominal (%)



Fuente: Banco Central.

Pareciera que el tipo de cambio flexible obliga a las empresas a convivir con dicha volatilidad y a la banca a evaluar los riesgos de descalce, ofreciendo productos de cobertura cuando corresponde. Todo ello ayuda a la profundidad del mercado financiero y entrega una flexibilidad para adaptarse a cambios en las condiciones internacionales, entregando un pilar a la fortaleza macroeconómica del país.

Tenemos un mercado financiero muy desarrollado para el tamaño de la economía, y mantenerlo es fundamental para el país. Aunque parezca irrelevante para el público general, tiene efectos reales: por ejemplo, Chile es de los pocos países que tienen créditos hipotecarios a 30 años –en gran medida fruto de esta estabilidad-. De manera similar, basta preguntar en el resto de Latinoamérica cómo y a qué precio se financian empresas medianas. Finalmente, la fortaleza del mercado financiero también es importante para evitar el efecto de los ciclos y las crisis económicas, que cuando son simultáneas con crisis financieras, multiplican el efecto real de la crisis y disminuyen la velocidad de recuperación (con los consiguientes costos para toda la población, especialmente la más vulnerable).

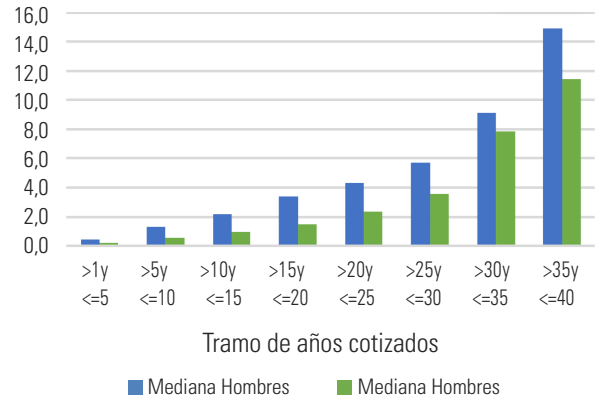
ESTADÍSTICAS DEL MERCADO LABORAL DEL SISTEMA DE PENSIONES VS ESTADÍSTICAS DEL INE.

El último IPoM remeció el escenario al indicar que la recuperación económica ha tenido más fuerza en el empleo que lo que indican los datos del INE. Este es un tema que venía siendo discutido ampliamente entre economistas y que hemos abordado en números anteriores.

Una de las fuentes administrativas utilizadas por el Banco Central corresponde a los datos del sistema de pensiones. La Superintendencia publica constantemente información de sus afiliados, montos cotizados y número de cotizantes; y utiliza esta información para hacer un seguimiento de las condiciones del empleo en Chile.

El empleo es fundamental para las pensiones. Como hemos visto, las lagunas previsionales –periodos sin pago de cotizaciones- son la principal causa de las bajas pensiones actuales (ver gráfico N° 7). Por ejemplo, un año sin cotizaciones al inicio de la vida laboral, si bien representa sólo un 2,5% de la vida laboral, puede afectar en hasta un 3,9% las pensiones[1]. Cabe mencionar que el mismo año sin cotizaciones a los 65 años -el final de la vida laboral-, cuando se asume una estructura de sueldos similar al promedio actual que se obtiene de la CASEN, representa aproximadamente un 1,1% de la pensión. Por ello la participación, y especialmente la participación temprana en el mercado laboral es tan relevante; pero no cualquier participación, sino que idealmente empleos formales con pago de leyes sociales (pensiones, seguro de salud y otros componentes de las seguridad social). Esto último justifica la obligatoriedad de las cotizaciones y la responsabilidad del empleador de realizar su pago.

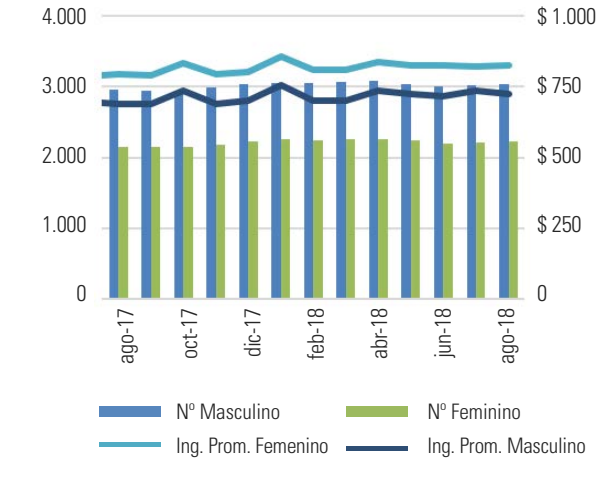
Gráfico N° 7: Pensión Autofinanciada en U.F. por sexo y tramo de años cotizados



Fuente: Superintendencia de Pensiones

Atendida esta obligatoriedad de cotizar del sistema laboral chileno para trabajadores dependientes –y prontamente independientes vía global complementario-, las estadísticas que provee la Superintendencia son un buen indicador de cambios en el empleo formal (gráfico N° 8).

Gráfico N° 8: Número e Ingreso Promedio de Cotizantes Dependientes (miles de $)

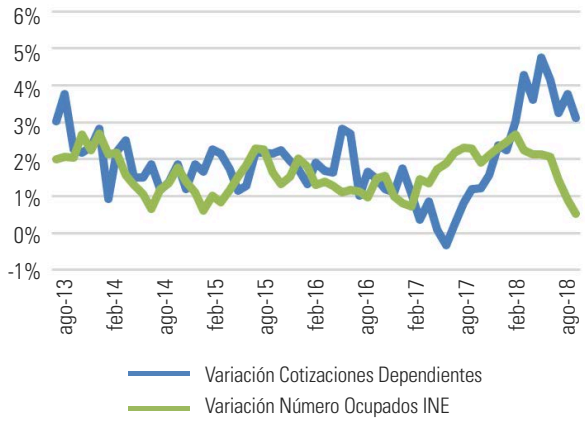


Fuente: Superintendencia de Pensiones

[1] Base de cálculo utiliza 40 años de empleo (sin lagunas laborales), 10% de cotizaciones y 4% de interés real.

Si comparamos estas cifras con las cifras de empleo del INE (gráfico N°9), notamos que la aceleración en la velocidad de crecimiento de cotizantes se desacopla de los datos del empleo durante los últimos dos años, donde en el último tiempo el INE muestra cifras muy bajas de recuperación del empleo respecto de las cifras administrativas del sistema de pensiones (y anteriormente muy altas en tiempos de desaceleración).

Gráfico N° 9: Variación Cotizantes Dependientes vs % Variación Ocupados INE



Fuente: Superintendencia de Pensiones e INE

En resumen, la información estadística del sistema de pensiones muestra una recuperación del mercado laboral que tiene más fuerza que la que muestran los datos del el INE (consistente con el informe del IPoM), y esto es una buena noticia para las futuras pensiones de los trabajadores que participan actualmente en la fuerza laboral.

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

CIBERSEGURIDAD Y CÓMO ENFRENTARLA

Hace cinco meses publicamos nuestro primer reporte sobre Ciberseguridad. Hoy el tema se ha vuelto cada vez más recurrente y diversos artículos la abordan desde múltiples perspectivas. Este informe revisa algunos conceptos básicos y presenta los últimos avances y discusiones, incluido un breve resumen del capítulo del Informe de Estabilidad Financiera y las conclusiones del reciente encuentro "CIBERSEGURIDAD: ¿CÓMO ENFRENTAMOS EL DESAFÍO?" organizado por el CEF-ESE.

Las noticias de los últimos meses han vuelto a poner en el centro de la noticia la Ciberseguridad. Ello ha logrado que las empresas comiencen a tomar conciencia de la situación, pero la ignorancia al respecto persiste. Este informe se enfoca en las sugerencias respecto de cómo combatir un ataque en la empresa basados en la experiencia de Equifax, víctima del mayor robo de información privada en EE.UU., que afectó a más de 143 millones de personas.

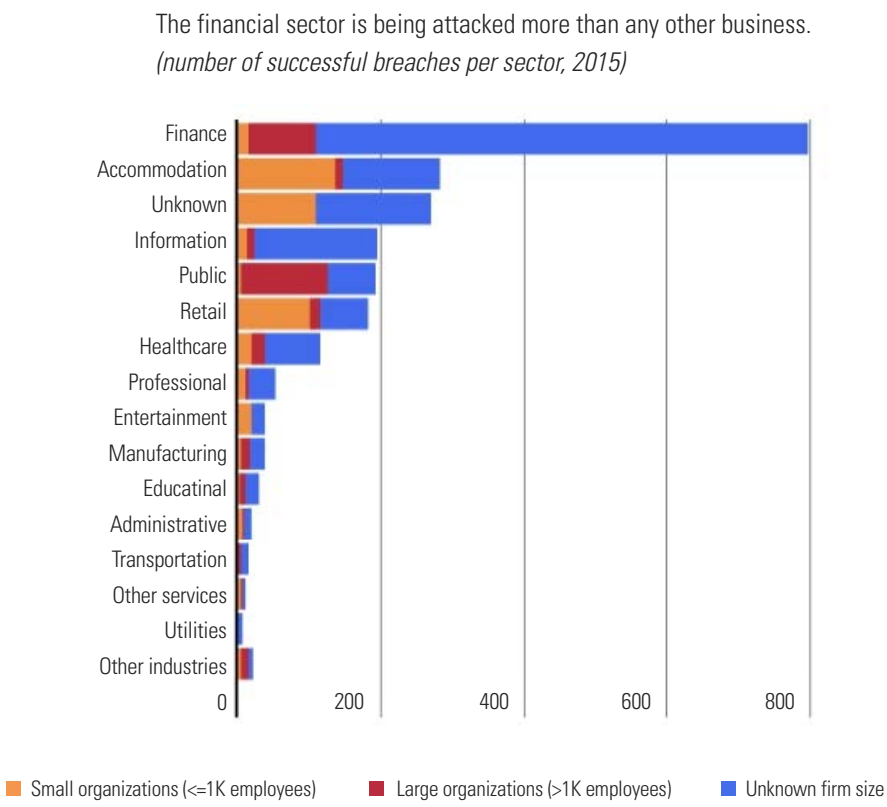
Conociendo los ciberataques

Los ciberataques son ataques a los sistemas de información de empresas e instituciones que alteran códigos de programación o la data con que ellos se nutren. Al afectar su lógica de funcionamiento, generan efectos disruptivos en los servicios u obtienen acceso a información privada que mantienen las empresas e instituciones.

Dentro de las instituciones que "atacan" y desarrollan software para atacar sistemas, se mencionan grupos criminales, corporaciones, activistas e incluso "lobos solitarios" con agendas personales. Sin embargo, los principales actores son estados, donde existe una guerra soterrada entre naciones para la cual, a diferencia de las guerras tradicionales, aún no existen códigos ni normas mínimas de convivencia (no hay información precisa sobre el rol de China, Rusia y Corea del Norte, entre otros; ni del de contraataques de EE.UU. y otros países occidentales).

Las víctimas más comunes de ciberataques incluyen servicios básicos (energía, agua potable y similares), el sector financiero, medios de comunicación, servicios de salud y otros objetivos estratégicos. Entre los sectores productivos víctimas de ataques, al año 2015 la mayor incidencia se relacionaba con servicios financieros (Figura N° 1, FMI). Sin embargo, los últimos ataques han ampliado la base y en la actualidad, si bien las cifras no son precisas, se estima que las industrias de la salud y servicios básicos son las víctimas más frecuentes.

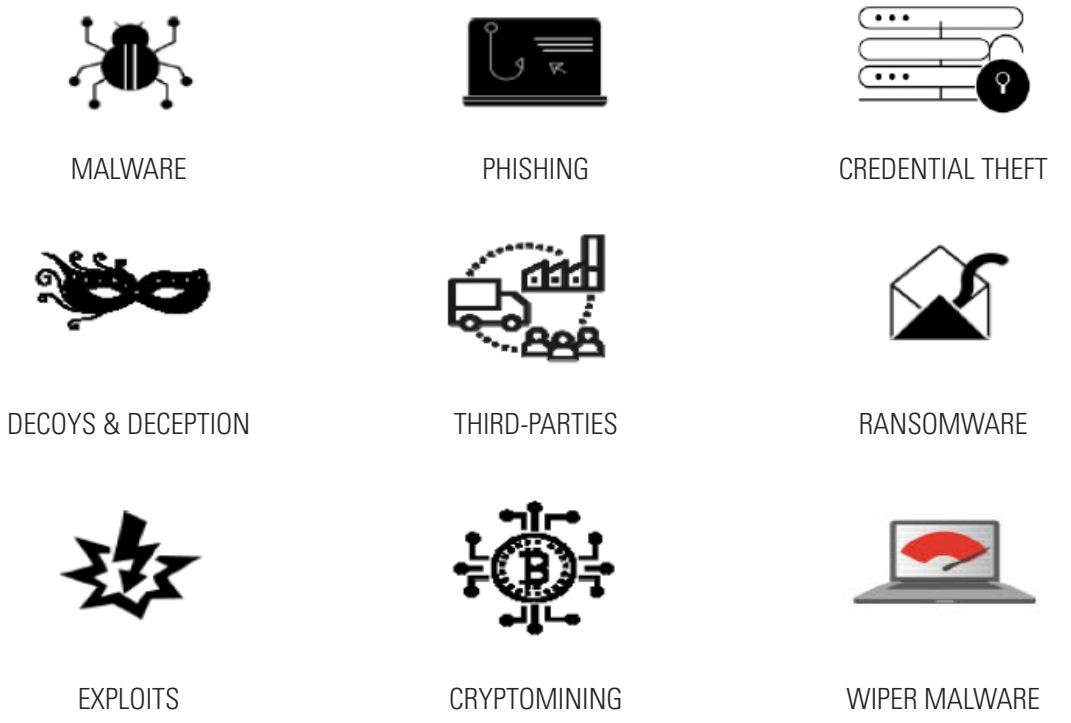
Figura N° 1 Finance industry under cyber attack



Fuente: Verizon; and IMF staff calculations

El objetivo de un ataque informático puede ser desestabilizar sistemas, robar información, cometer fraude, acceder a información privada del competidor, o simplemente "mostrar que es capaz" de acceder –relacionado a demostraciones de poder o amenazas encubiertas-; entre muchos otros objetivos. Es así como los ciberataques se pueden clasificar según los efectos buscados: disrupción del servicio (usualmente ataques DoS o "Denial of Service"), fraude, causar daño eliminando archivos e información de la víctima, o la filtración de información privada. Esta distinción es importante, porque un ataque que suspende el servicio puede ser realizado sin modificar el sistema atacado y por lo tanto, si bien es dañino, no es lo mismo que uno que ingresa al sistema informático de la víctima filtrando, borrando o modificando información.

Figura N° 2: Herramientas y tácticas para ciberataques



Fuente: Presentación EndGame Andrea Little (ESE Business School, 24/10/2018)

Un tipo especial de ataque que ha ganado presencia últimamente son los ataques DoS (Denial of Service). Estos suelen ser el fruto de la acción de "bots" o programas que corren procesos automáticamente y lo que hacen es ralentizar o suspender el servicio de la víctima. Las herramientas más comunes para realizar ataques cibernéticos son Malwares de distinta naturaleza y Spoofing (Figura N° 2). A continuación hacemos una breve descripción de estos conceptos.

Denial of Service

Consiste básicamente en afectar la capacidad de respuesta de un servicio haciendo que opere de manera más lenta o eventualmente colapse, mediante ingresos o consultas coordinadas a los servidores que proveen el servicio. La consulta coordinada normalmente es gatillada por otros virus "bots". Este tipo de ataque no "ingresa" a los sistemas para "modificar" su operación.

Una analogía que ayuda a entender este tipo de ataque, es pensar en los servicios online, por ejemplo de su banco, como si fueran una carretera. Están diseñados para atender un número de clientes –autos- "normal". A veces muchos clientes entran simultáneamente a una misma hora, y así como las carreteras deben estar diseñadas para las horas pico, los sistemas informáticos se diseñan para responder a esta demanda. Ahora bien, imagine que todos los habitantes de una ciudad deciden salir a la misma hora por la misma carretera. Probablemente se armará una fila muy larga y eventualmente un taco que no avanza pues la carretera no está diseñada para este evento –ni tampoco es bueno que lo esté, pues significaría tener veinte pistas cuando en tiempos normales se requiere máximo una-. Algo similar sucede con los servidores cuando reciben muchas consultas al mismo tiempo, no dan abasto y colapsa el servicio. Lo importante de este caso es que la seguridad del sistema no se vio afectada y el cliente puede estar tranquilo. Sin embargo, que la seguridad del sistema no esté afectada, no implica que la suspensión o ralentización del sistema sea inocuo. En el extremo, si la torre de control de un aeropuerto es atacada y no es capaz de responder a tiempo, es extremadamente grave. Si un banco no es capaz de realizar una compra de dólares en el momento que lo solicita el cliente y el tipo de cambio sube en el intertanto, también puede ser muy grave.

La pregunta que se debe hacer la potencial víctima es cuál es la consecuencia de la suspensión del servicio. La solución –o mecanismo de prevención-, dada las características de este tipo de ataque, dependerá de la industria. Es probable que atendido los costos para la mayoría de los servicios, sea óptimo no preocuparse mayormente de este problema.

Spoofing

Este tipo de ataque sucede cuando un tercero intenta suplantar la página o dirección de la empresa o institución a la que quiere acceder la víctima. Este ataque es muy difícil de prevenir por parte de las instituciones, pues la información es obtenida directamente desde el cliente.

Un ejemplo común es el "phishing". Consiste en el envío de un email que se supone proviene de una institución conocida por el cliente, que redirige –a través de un link en el mismo mail- a una página que simula la de dicha institución (por ejemplo, de un Banco). Cuando el cliente "pincha" el link del mail falso, se abre una página falsa –idéntica a la real- donde el cliente debe ingresar sus datos y contraseñas. Luego estas contraseñas son utilizadas por el delincuente para cometer fraudes ingresando a la cuenta del cliente por las vías regulares.

Las instituciones pueden protegerse de este tipo de ataque mediante sistemas redundantes, de manera que para hacer una transacción, no baste la contraseña sino que sea necesario algún elemento adicional (como tarjetas de coordenadas, generadores de números aleatorios, preguntas de seguridad adicional, etc.). Sin embargo, el mejor cuidado es la educación del cliente, quien debe ser cuidadoso al ingresar su información personal.

Malware

El malware se refiere en forma genérica a los distintos tipos de virus que "infectan" los sistemas ingresando y modificando los códigos con que ellos operan. Este tipo de ataque es el más complejo y su prevención, a diferencia de los anteriores donde la responsabilidad es compartida con clientes, es cien por ciento responsabilidad de la empresa víctima del ataque.

Existen virus de diversa naturaleza; virus comunes que simplemente destruyen información al ingresar a los sistemas, virus troyanos que atacan las medidas de seguridad de los sistemas permitiendo el acceso de otros malware o abriendo "backdoors" (puertas de entrada no detectadas por los sistemas para permitir futuros ataques), ransomware que bloquean el sistema infectado y exigen pagar un rescate para acceder nuevamente –normalmente mediante criptomonedas-, adware que muestran publicidad no deseada personalizada gracias al acceso de información privada del sistema que infecta y spywares, que obtienen y comparten información guardada en el sistema atacado. Es importante destacar que estos virus al infectar sistemas, buscan esconderse para no ser detectados y pueden permanecer latentes o con niveles de actividad muy bajos durante mucho tiempo.

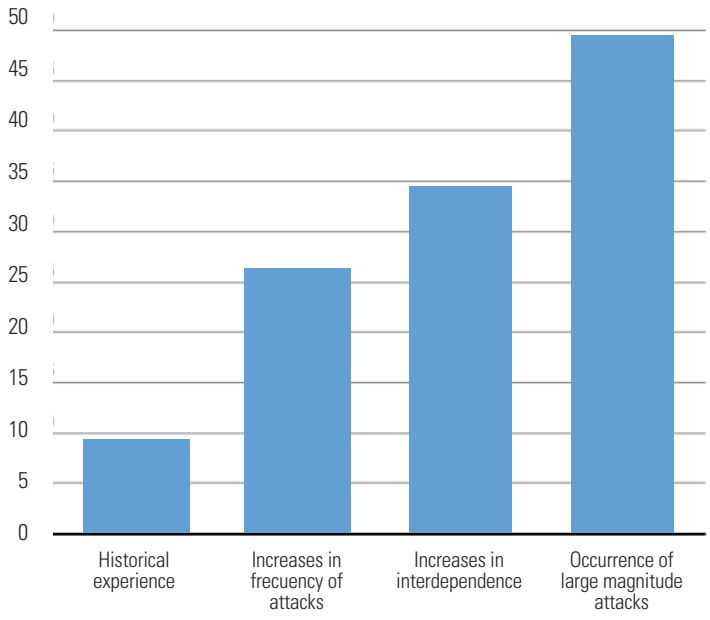
Los ataques informáticos más complejos utilizan más de un medio simultáneamente. Ejemplos de estos ataques más sofisticados incluyen "malwares" que infectan cientos de computadores y permanecen latentes hasta una fecha y hora determinada, en la cual coordinan el ingreso remoto y simultáneo de millones de solicitudes a un mismo sistema –generando un Denial of Service- o disminuyendo las medidas de seguridad. Fruto de este primer ataque los sistemas quedan más vulnerables, lo que es aprovechado para un intento de hackeo o un segundo ataque con el objeto de cometer un fraude o derechamente una suspensión de servicio más compleja.

El costo de los ciberataques para una Empresa

Las consecuencias para diversas industrias de un ataque informático no son evidentes ni mucho menos fáciles de medir e identificar. Los costos evidentes son los costos directos del fraude y de la suspensión del servicio según el tipo de ataque, que pueden llegar a representar desde 9% hasta 45% del ingreso neto en el caso de los servicios financieros según proyecciones del FMI.

Figura N° 3: Potencial impact on back profits

Financial institutions worlwide face potential losses from cyber-attacks ranging from 9% of net income based on experience so far up to half of profits in the worst-case scenario.
(percent of net income)



Fuente: IMF Staff estimates

Sin embrago, los costos indirectos pueden ser más importantes. Dentro de los costos indirectos se deben considerar:

- Demandas de clientes (por vulneración de su privacidad cuando el resultado es el robo de información privada confidencial, o por daños cuando el resultado es la suspensión del servicio). Firmas de abogados –al menos en EEUU- han visto en ellas una oportunidad de negocio multimillonaria con demandas colectivas que superan los 200 millones en compensaciones (tabla Nº1), lo que permite prever que seguirán aumentando[2].
- Costos de prevención y actualización de sistemas para evitar ataques.
- Daños reputacionales cuando los ataques son exitosos (e incluso a veces cuando no lo son, pero dejan en evidencia vulnerabilidades o rompen la sensación de seguridad del cliente).
- Efectos sistémicos o "contagio" hacia otras empresas de la industria de la empresa que es víctima del ataque.

Tabla N°1: Acciones colectivas destacadas desde 2013 hasta 2016 en EEUU por problemas de ciberseguridad (cifras en US$)

Empresa	Fecha	Tipo Data	Resultado Acción Colectiva
Home Depot	08/2016	Data tarjeta	Hasta $13 MM acciones colectivas; hasta $6.5 MM por 18 meses servicio monitoreo crédito; cambio prácticas seguridad
Target	05/2016	Data tarjeta	Hasta $20.25 MM acciones colectivas; $19.10 MM a MasterCard, Hasta $67 MM a Visa
Sony	04/2016	Login e info personal	Hasta $2 MM pérdidas potenciales; hasta $2.5 MM robo identidad; 2 años servicio monitoreo crédito
St. Joseph Health System	02/2016	Data salud	$7.5 MM pago directo; hasta $3 MM acciones colectivas; un año servicio monitoreo crédito; cambio prácticas seguridad
Target	11/2015	Data tarjeta	Hasta $10 MM claims; cambio prácticas seguridad
LinkedIn	09/2015	Login	Hasta $1.25 MM claims; cambio prácticas seguridad
Adobe	08/2015	Login y data tarjeta	Cambio prácticas seguridad y auditoría
Sony Gaming Networks	05/2015	Data tarjeta e info personal	Hasta $1 MM robo identidad; beneficios adicionales (juegos gratis, suscripciones, crédito virtual, pagos menores)
AvMed	02/2014	Info personal	Hasta $3 MM; cambio prácticas seguridad
Purchasing Power	10/2013	Info personal	Hasta $225 M acciones colectivas; hasta 1 año servicio monitoreo crédito; cambio prácticas seguridad
CBR Systems	07/2013	Data salud	Hasta $500,000 claims; $2 MM robo identidad; 2 años servicio monitoreo crédito; cambios prácticas seguridad
Michaels Stores	04/2013	Data tarjeta	$800,000 class claims; 2 años servicio monitoreo crédito; cambios prácticas seguridad

Fuente: Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy (By Alexander H. Southwell, Eric Vandevelde, Ryan Bergsieker and Jeana Bisnar Maute, February 3, 2017. Columbia Law School)

[2] Consideramos es un riesgo potencial si en Chile de desarrolla esta industria legal (especialmente para empresas que manejan datos personales).

Ciberseguridad y estabilidad financiera

En su Informe de Estabilidad Financiera, el Banco Central destaca el riesgo sistémico de potenciales ataques a gran escala al sistema financiero. La creciente sofisticación, mayores niveles de tecnología y la interconexión de las entidades financieras aumentan el riesgo de los ataques más allá del evidente riesgo operacional para la empresa que es víctima del ataque.

Se identifican cinco casos donde existen amenazas a la estabilidad financiera. Primero, si la disrupción en el servicio de una institución se propaga al resto debido a las interconexiones del sistema financiero. Segundo, si se interrumpe el normal flujo de pagos, afectando a las demás instituciones a través del sistema de pagos de alto valor (SPAV). Tercero, si se pierde información crítica para el sistema financiero (incluyendo información de clientes). Cuarto, si se debilita la situación patrimonial de una institución financiera como consecuencia de un robo de sus recursos. Quinto, si la confianza de los agentes en la seguridad del sistema financiero afecta –por ejemplo inhibiendo las transacciones- la actividad financiera.

Fruto de esto, se trabaja –con apoyo del FMI- en el diseño e implementación de un protocolo de contingencia para problemas de riesgos operacionales causados por disrupciones a la ciberseguridad. Al mismo tiempo, se resaltan las acciones del poder Ejecutivo que anunció un proyecto de ley de Ciberseguridad Financiera, como parte de una estrategia general del Gobierno. Este pondría exigencias proporcionales al potencial impacto de la entidad financiera sobre el sistema; obligación de reportar continuamente a las autoridades sobre gestión e incidentes específicos; y elaboración de evaluaciones de riesgo, planes de contingencia, capacitación en ciberseguridad y realización de pruebas, entre otros temas.

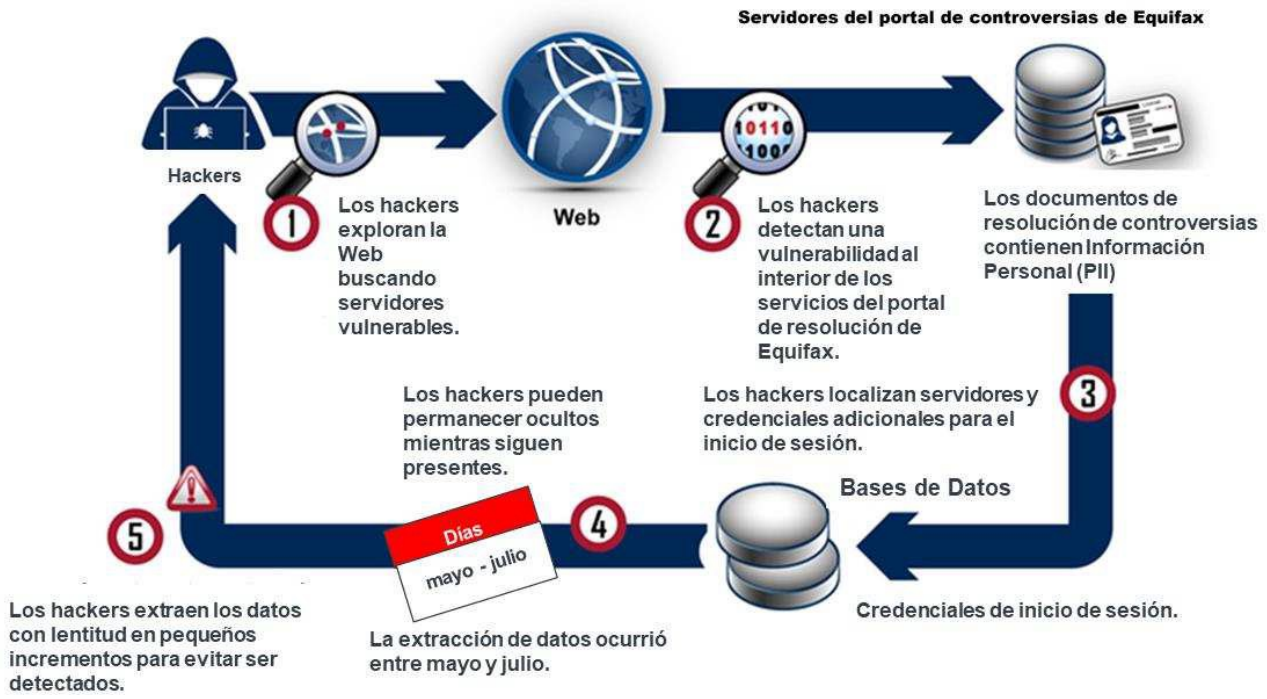
Por último, el Banco Central además de resaltar su interés y preocupación justificada por su mandato legal de supervisar el buen funcionamiento de los sistemas de pago, solicita a las distintas entidades financieras del sector privado que revisen de manera permanente si los riesgos de ciberseguridad a los que están expuestos están bien administrados. Ello tanto por su deber con los clientes, como por los riesgos de contagio en un modelo altamente interconectado y por el efecto de mermas en confianza para el sistema.

Cómo opera un ataque informático: el caso de Equifax

Equifax representa un buen ejemplo para entender cómo pueden operar los ataques informáticos y sus consecuencias. Adicionalmente existe un gran nivel de información pues uno de los requisitos que le exigió la justicia norteamericana para enmendar sus acciones –y negligencia-, fue contar y educar al respecto.

El ingreso al sistema de Equifax se logró a través de un sistema secundario –el sistema de resolución- donde hackers encontraron una vulnerabilidad (un servidor con los certificados vencidos). A partir de este primer ingreso pudieron obtener información privada y credenciales, lo que les permitió acceder a sistemas primarios. En este periodo implantaron una serie de programas que lentamente fueron extrayendo información de datos –entre mayo y junio- para evitar ser detectados.

Figura N° 4:



Fuente: GAO, según información dada por Equifax

El resultado de este hackeo fue crítico para una empresa cuyo negocio principal es el manejo de información. Se filtró información privada, comprometiendo potencialmente a más de 143 millones de consumidores de EE.UU. Al día siguiente de hacerse pública la información la acción de la empresa cayó un 14%, acumulando una caída de 35% en seis sesiones.

Recomendaciones para prevenir un ataque informático

Tal vez la primera recomendación, es asumir que el ataque no se puede prevenir 100%. Sólo es posible disminuir su probabilidad de ocurrencia y minimizar sus consecuencias negativas. Las empresas deben tener un plan.

Las recomendaciones más prácticas tienen cuatro aristas principales: la primera es "humana", la segunda es de tecnología, la tercera de sistemas y procesos; y la cuarta de incentivos y responsabilidades.

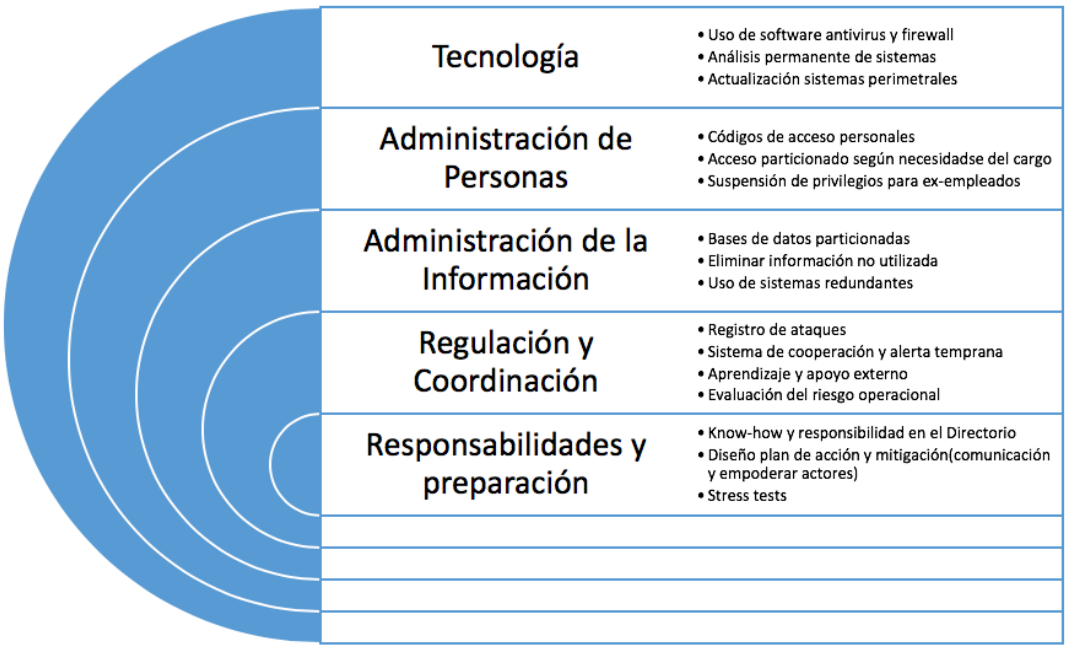
Respecto de la arista humana, la empresa debe preguntarse quién tiene acceso a qué información (probablemente el área comercial no requiera acceso al número de la tarjeta de crédito del cliente que sí requiere el área de cobranza). La recomendación es controlar las claves de acceso de los trabajadores y particionar la información a la que cada uno de ellos puede acceder. También se debe tener especial cuidado con las claves de acceso de ex empleados en cuanto dejan las empresas. Finalmente, es importante capacitar en el uso de las tecnologías y en medidas de precaución para minimizar la probabilidad de ataques (acceso a páginas restringidas, mails sospechosos, archivos ".exe", etcétera).

Respecto de la arista tecnológica, como el caso de Equifax demuestra, el sistema es tan débil como su eslabón más débil. Se deben revisar los certificados de seguridad de TODOS los sistemas con acceso a la red (por poco importante que parezcan) y mantener los antivirus, firewall y otros software preventivos actualizados permanentemente. También es fundamental hacer una evaluación de riesgos tecnológico –y esta evaluación debe ser constante, pues la tecnología es extremadamente dinámica. Al respecto, los expertos sugieren evaluar los sistemas partiendo de la premisa que la empresa ya es víctima –no que podría serlo- y por lo tanto, debe buscar activamente señales de malwares y virus instalados en sus sistemas (recordando que estos están diseñados para ser invisibles, mantenerse latentes durante algún periodo y engañar a los programas que los identifican). También es importante renovar los sistemas informáticos –pues van quedando obsoletos y sistemas seguros hace cinco años probablemente ya no lo sean- e idealmente incorporar nuevos métodos y tecnologías con mayores grados de seguridad en su operación (como podría ser el uso de blockchain y biometrics).

Para la arista del manejo de información, aquellas empresas que mantienen información privada o reservada de clientes –por ejemplo financieras y de salud-, deben particionar la información y guardarla en bases independientes (el objetivo es que cada base sea inútil por sí misma). Por ejemplo, si un hacker accede a la base de RUT, sólo tendrá una lista de números; si accede a la de nombres, sólo una lista de nombres; y si lo hace a la de tarjetas de crédito, sólo tendrá un listado de números... la única forma que pueda utilizar la información, es si es capaz de juntar el nombre, con el RUT y el número de tarjeta, pero para ello debe acceder al menos a tres o cuatro bases de datos simultáneamente y esto, además de multiplicar cuatro el esfuerzo, probablemente gatille señales de alerta temprana luego del primer hackeo que permitan reaccionar.

También se recomienda definir protocolos para eliminar información por obsolescencia, antigüedad o no uso. En tiempos del Big Data, en que la información es uno de los principales activos de las empresas y el costo de almacenaje es muy bajo, esta recomendación encuentra alta resistencia. Sin embargo, preguntarse cuál sería el costo de una filtración de los datos que mantiene la empresa, debe ser un aspecto clave a la hora de decidir qué información mantener. La premisa es que nada teme quien nada esconde/guarda.

Figura N° 5: Aspectos Claves en la Prevención de Ciberataques



En otra arista de la prevención, se resalta la necesidad de trabajos de inteligencia y coordinación a nivel de industrias, e incluso internacionalmente (los ataques suelen ser secuenciales y por lo tanto, la alerta temprana de una primera víctima puede ayudar a preparar a posibles nuevas víctimas). Al respecto, atendido los incentivos a callar cuando existen ataques –pues los daños reputacionales pueden ser relevantes- la regulación o autoregulación debe obligar a que los ataques sean reportados ("lo que no se mide, no se puede mejorar"), aunque es razonable que el reporte sea sin publicidad y reservado al momento del ataque.

Otra línea de acción muy recomendada especialmente para empresas financieras, es la medición del riesgo. Corresponde a las empresas comenzar evaluar –a veces con metodologías estadísticas tales como el "Value at Risk"[4], el riesgo operacional implícito en un ciberataque.

Para que estos cambios sean reales, la experiencia muestra que no pueden ser políticas "bottom up". Es fundamental establecer obligaciones y responsabilidades al más alto nivel. Se sugiere por lo tanto incorporar know-how –incluso a nivel del directorio- para que esta dimensión del riesgo sea evaluada y exista accountability en la alta dirección.

Finalmente, es fundamental trabajar con el público general y los clientes para limitar los daños reputacionales. Aunque no lo parezca, la reacción óptima a veces puede ser la interrupción del servicio y el cliente debe saber que la suspensión, en estos casos extremos, trabaja en su propio beneficio. Es fundamental la transparencia y que el cliente y el público conozcan la situación y sus posibles consecuencias de primera fuente.

[4] Bouveret 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment". IMF WP143

Selección proyectos de Ley mundo financiero y económico con movimientos en el mes de noviembre (incluido diciembre hasta 06/11)

		Fecha	Proyecto	Boletín *
SENADO	Votados	27-11-18	Se aprobó en general y en particular el proyecto de acuerdo, en segundo trámite constitucional, que aprueba el Acuerdo para Modificar el Tratado de Libre Comercio entre el Gobierno de la República de Chile y el Gobierno de Canadá.	11605-10
		27-11-18	Aprueba el Acuerdo de Asociación Económica Integral entre el Gobierno de la República de Chile y el Gobierno de la República de Indonesia	11748-10
		13-11-18	Aprueba en particular el proyecto de ley, en primer trámite constitucional, que modifica la ley N° 19.220, que regula el establecimiento de bolsas de productos agropecuarios.	9233-01
		07-11-18	Aprueba en general proyecto, en segundo trámite constitucional, que crea el Consejo Fiscal Autónomo. Fija como plazo para presentar indicaciones el 29/11.	11777-05
	Informados Comisión de Hacienda	28-11-18	Crea una sociedad anónima del Estado denominada `Intermediación Financiera S. A. Segundo informe de comisión en Segundo trámite constitucional.	11554-05
		28-11-18	Aprueba Convención para Evitar la Doble Imposición entre estados de la Alianza del Pacífico (Chile, Colombia, Mexico y Perú). Primer informe de comisión en Segundo trámite constitucional.	11871-10
	Vistos Comisión Hacienda	05-12-18	Proyecto de ley que modifica las normas para la incorporación de los trabajadores independientes a los regímenes de protección social.	12002-13
		28-11-18	Proyecto de ley que modifica la ley N° 20.743, respecto del mes de concesión del aporte familiar permanente.	11977-05
C. DIPUTADOS	Votados	29-11-18	Aprueba proyecto que perfecciona textos legales para promover la inversión. Aprobado y despachado al Senado.	11747-03
		28-11-18	Proyecto de Presupuestos del Sector Público 2019. Informe de la Comisión Mixta. Despachado el proyecto.	12130-05
		22-11-18	Aprueba proyecto que incorpora el contrato de teleoperadores. Segundo trámite Constitucional. Aprobado en general. El proyecto vuelve a la Comisión de Trabajo y Seguridad Social.	8263-13
		20-11-18	Aprueba proyecto que modifica el código del Trabajo en materia de trabajo a distancia. Primer Trámite Constitucional. Despachado el proyecto al Senado.	12008-13
		08-11-18	Aprueba protocolo adiciona al acuerdo de complementación económica con Mercosur. Primer trámite constitucional. Despachado el proyecto al Senado.	11730-10
		06-11-18	Aprueba proyecto que modifica el Código del Trabajo en materia de contrato de trabajo por obra o faena (confiriendo el derecho a feriado anual y una indemnización equivalente a dos y medio días de remuneración por cada mes trabajado si el contrato hubiere estado vigente por un mes o más). Modificaciones del Senado. Despachado el proyecto.	7691-13
	Informados Comisión de Hacienda	05-12-18	Proyecto que modifica la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma y otros textos legales que indica.	8466-07
	Vistos Comisión Hacienda	28-11-18	Proyecto de ley, iniciado en mensaje, que "Moderniza la Legislación Tributaria"	12043-05

** Más información ingresando el número de boletín a wwww.bcn.cl; www.congreso.cl o www.camara.cl según corresponda.*
*** Se informa sólo el último movimiento de cada proyecto.*

NUEVA NORMATIVA FINANCIERA

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

Del 1/11 al 6/12

	Normativas en trámite (últimos 3 meses)			Normativas emitidas		
	Nombre	Resumen	Sujeto	Circular	Resumen	Sujeto
SBIF	Información de personas relacionadas	Nuevos archivos del Manual de Sistema de Información para el control de límites de crédito	Bancos	Carta circular N°5	Aclara uso de los códigos de actividad económica para efectos de la información enviada mediante el archivo D03	Bancos
	Modificación a Capítulo III.B.2.1 del Compendio de Normas Financieras del Banco Central de Chile.	Modificaciones en las normas de gestión y medición de la posición de liquidez	Bancos	Circular 3642	Recopilación Actualizada de Normas. Capítulo 20-9. Complemeta instrucciones sobre Ciberseguridad y Gestión de la Continuidad de Negocio	Bancos
	Incidentes de Ciberseguridad	Los bancos informarán todos los incidentes en materia de Ciberseguridad ocurridos en el mes en curso, incluida la información actualizada de incidentes reportados en el periodo anterior, que aún no hayan sido corregidos. Se entenderá por incidente de ciberseguridad todo evento que ponga en riesgo o afecte negativamente los activos de información de la institución presentes en el ciberespacio.	Bancos	Circular 3641	Modifica plazo para respuesta de requerimientos sobre reclamos de 20 a 10 días hábiles bancarios	Bancos
				Circular 6	Complementa y corrige instrucciones en normas generales para empresas emisoras de tarjetas de pago	Emisores de tarjetas de pago
				Circular 171	Modifica plazo para respuesta de requerimientos sobre reclamos de 20 a 10 días hábiles bancarios	Cooperativas de ahorro y crédito
CMF	Modifica inscripción de facturas	Proyecto Normativo que regula la inscripción de facturas y títulos representativos de facturas en el Registro de Productos.	Todos	OFC 1071	Informa vector de tasas de descuento para valorización de pasivos de seguros	Seguros
	Modifica Circular 2110	Modifica instrucciones respecto de comunicación de prórroga del plazo de liquidación de siniestros y de información estadística agregada de liquidación de siniestros.	Todos	Circular 2239	Modifica circular N°1835, instrucciones relativas a forma y contenido informqación de inversiones y sistema de evaluación de riesgo mercado cartera inversiones.	
				OFC 1064	Comunica tasa de interés de actualización - Diciembre 2018	Seguros
				OFC 1066	Informa vector de tasas de descuento para valorización de pasivos de seguros, correspondientes a octubre de 2018	Seguros
				OFC 1065	Comunica nuevo valor Unidad de Seguro Reajustable para noviembre de 2018.	Seguros
				OFC 1064	Comunica tasa de interés de actualización - Noviembre 2018	Seguros
				OFC 1063	Informa tasa de descuento de valorización de pasivos de seguros correspondientes a septiembre de 2018	Seguros
				OFC 1062	Informa vector de tasas de descuento para valorización de pasivos de seguros, correspondientes a septiembre de 2018	Seguros

NUEVA NORMATIVA FINANCIERA

ESE BUSINESS SCHOOL
Universidad de los Andes
CEF - Centro Estudios Financieros

Del 1/10 al 6/11

	Normativas en trámite (últimos 3 meses)			Normativas emitidas		
	Nombre	Resumen	Sujeto	Circular	Resumen	Sujeto
SP	NT329	Régimen de Inversión de los Fondos de Pensiones: Permite Lanzamiento de Opciones Call Cubiertas	AFPs	Cicular 2061	Determina tabla de reajustes e intereses penales a aplicar por las AFP para diciembre de 2018. Aplicable a cotizaciones en que no corresponde utilizar recargo beneficio AFP	AFP
				Circular 2060	Determina tabla de reajustes e intereses penales a aplicar por las AFP para diciembre de 2018. Aplicable a cotizaciones en cobranza judicial y que corresponde utilizar recargo beneficio AFP	AFP
				Cicular 2059	Parámetrso para el cálculo de límites de inversión de los fondos de pensiones y fondos de cesantía: deroga circular 2043 de 13 julio 2018.	AFP y AFC
				Circular 2058	Determina tabla de reajustes e intereses penales a aplicar por la AFC para noviembre de 2018	AFC
				Cicular 2057	Determina tabla de reajustes e intereses penales a aplicar por las AFP para noviembre de 2018. Aplicable a cotizaciones en que no corresponde utilizar recargo beneficio AFP	AFP
				Circular 2056	Determina tabla de reajustes e intereses penales a aplicar por las AFP para noviembre de 2018. Aplicable a cotizaciones en cobranza judicial y que corresponde utilizar recargo beneficio AFP	AFP
				Circular 2055	Información sobre rentabilidad de la cuota del Fondo de Cesantía, de acuerdo a lo establecido en el N° 2 del capítulo I, de la letra D, del Título I, Libro V del Compendio de Normas del Seguro de Cesantía. Mayo 2018 - Agosto 2018	AFC
				Circular 2054	Información sobre rentabilidad de la cuota del Fondo de Pensiones, de acuerdo a lo establecido en las letras A y B del Título IX del Libro I del Compendio de Normas del Sistema de Pensiones.	AFP
				Circular 2053	Información sobre rentabilidad de la cuota del Fondo de Cesantía, de acuerdo a lo establecido en el N° 2 del capítulo I, de la letra D, del Título I, Libro V del Compendio de Normas del Seguro de Cesantía. Enero 2018 - Abril 2018	AFC

PUBLICACIÓN CENTRO DE ESTUDIOS FINANCIEROS
ESE BUSINESS SCHOOL
UNIVERSDAD DE LOS ANDES

DIRECTORA EJECUTIVA
María Cecilia Cifuentes, Magíster en Economía, Pontificia Universidad Católica de Chile
mceciliacifuentes.ese@uandes.cl

INVESTIGADOR ASOCIADO
Juan Gabriel Fernández, Ph.D. en Economía en la Universidad de Boston
jgfernandez.ese@uandes.cl

CENTRO DE ESTUDIOS FINANCIEROS
El Centro de Estudios Financieros del ESE Business School de la Universidad de los Andes tiene como objetivo de profundizar la comprensión del mercado financiero, promover las buenas prácticas en su funcionamiento e influir, a través de la investigación y otras actividades, en las políticas públicas relacionadas.

DISCLAIMER
La información aquí contenida se expone a título meramente informativo y no constituye una recomendación de inversión, oferta, valoración de carteras o patrimonios, ni asesoría financiera o legal. Dicha información tampoco es un reflejo de posiciones (propias o de terceros) en firme de los intervinientes en el Mercado Financiero Chileno.

El objetivo es informar, hacer propuestas de buenas prácticas o políticas públicas y generar discusión sobre el funcionamiento del mercado financiero local y la economía en general. Este informe está basado en información pública y modelos o proyecciones propias que utilizan dicha información como insumo, y por lo tanto está sujeto a error.

Los análisis y opiniones aquí presentadas, son de responsabilidad exclusiva de sus autores y no representan la opinión de la Universidad.

Sus autores no serán responsables de ninguna pérdida financiera, ni decisión tomada sobre la base de la información contenida en este Informativo mensual.