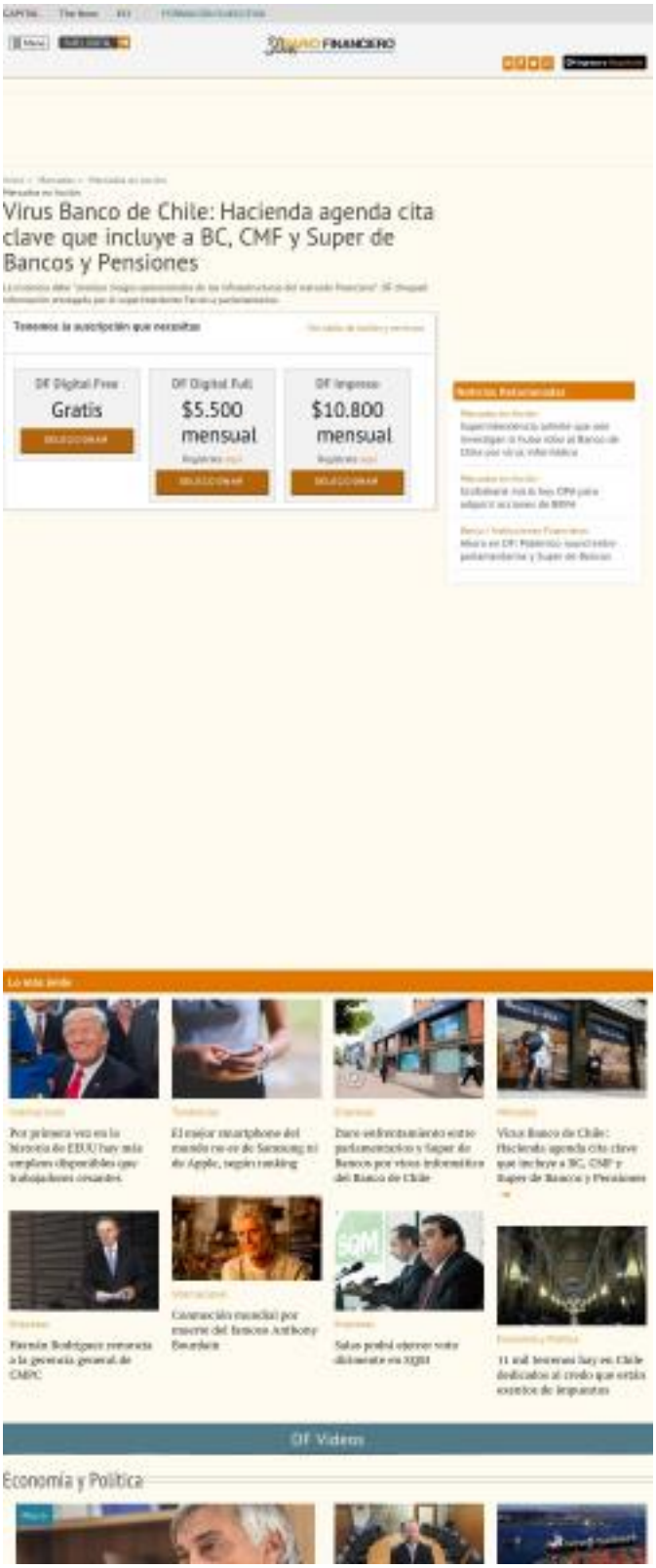
LITORALPRESS

Fecha: 08-06-2018 **Visitas:** 68.694 **Favorabilidad:** No Definida
Fuente: Diario Financiero **VPE:** 230.125
Título: **Virus Banco de Chile: Hacienda agenda cita clave que incluye a BC, CMF y Super de Bancos y Pensiones**

Link: https://www.df.cl/noticias/mercados/mercados-en-accion/virus-banco-de-chile-hacienda-agenda-cita-clave-que-incluye-a-bc-cmf-y/2018-06-07/204324.html



La instancia debe “analizar riesgos operacionales de las infraestructuras del mercado financiero”. DF chequeó información entregada por el superintendente Farren a parlamentarios. El ataque internacional que sufrió Banco de Chile producto de un virus informático el pasado 24 de mayo, y que aún no es superado por completo por parte de la entidad financiera, según confirmó el superintendente de Bancos, Mario Farren, en la comisión de Economía del Senado, sigue generando reacciones entre las autoridades.Desde Teatinos 120 comentaron que, “en el marco del monitoreo constante que ha estado realizando el Ministerio de Hacienda, desde el primer momento, a la situación que afectó al Banco de Chile, esta cartera reactivó y citó para el martes 12 de junio al grupo de Trabajo de Continuidad Operacional, creado en diciembre de 2016 en el marco del Comité de Estabilidad Financiera”.Este grupo es liderado por Hacienda y reúne a equipos técnicos y de supervisión de los organismos regulatorios del país. Estarán presentes en el encuentro de este martes, según confirmó Hacienda, el Banco Central, la Comisión para el Mercado Financiero, la Superintendencia de Bancos e Instituciones Financieras y la Superintendencia de Pensiones.Esta instancia tiene como mandato “analizar los riesgos operacionales de las infraestructuras del mercado financiero y sus participantes -entre los que se cuentan los bancos-, y proponer cambios legales y regulatorios para mitigar estos riesgos y sus efectos sobre el sistema financiero”.De acuerdo a lo expresado por la cartera liderada por Felipe Larraín, el grupo informará los resultados al Consejo de Estabilidad Financiera.Más dudasLa intervención del superintendente de Bancos, Mario Farren, en el Senado para explicar el ataque del virus internacional que sufrió la compañía ligada al grupo Luksic y Citibank fue comentada no sólo por los parlamentarios, sino que también al interior de gobierno.El regulador habría dejado más interrogantes sobre lo que está sucediendo en la firma que respuestas, de acuerdo a los que estuvieron presentes en el encuentro.La cita de Farren con los senadores no fue bien evaluada. Varios miembros del Ejecutivo reconocen en privado que “no tuvo una preparación adecuada” para enfrentar las preguntas de los legisladores.Cuando se le preguntó si los efectos del virus informático que atacó al banco ya están superados por la firma, el regulador manifestó que aún es “materia de investigación”.Otro aspecto abordado por la autoridad es el eventual robo de fondos propios de Banco de Chile que aún no está claro, pues “son materias de revisión que se está conduciendo en este momento”, sostuvo Farren.Quien ha tomado cartas en el asunto respecto a ciberseguridad en el sistema financiero es el Banco Central. El ente emisor dijo que desde hace tiempo está “trabajando en la revisión y fortalecimiento de sus medidas de seguridad, con la finalidad de prevenir y mitigar los efectos de eventuales ciberataques contra sus sistemas y procesos, teniendo especialmente presente para ello los diversos incidentes ocurridos en esta materia a nivel internacional”.De esa forma, dispuso “destinar mayores recursos humanos y tecnológicos para estar mejor preparado frente a los crecientes riesgos a que está expuesto el sistema financiero en este ámbito”.Bancos en México y Canadá sufrieron ataques el último mesDos de los mayores bancos de Canadá y otros tres en México fueron afectados en las últimas semanas por ciberataques que derivaron en millonarias transferencias fraudulentas y una investigación parlamentaria. En el país latinoamericano, Banxico deberá informar al Congreso sobre intervenciones maliciosas que sufrió el Sistema de Pagos Electrónicos Interbancarios (SPEI). En el episodio, que se extendió desde el 27 de abril hasta mediados de mayo, se registraron transacciones fraudulentas por más de US$ 15,3 millones y entre las entidades afectadas estuvieron la filial de Citi, Citibanamex; Banorte y Banejército. "Se abrieron cuentas falsas. Se metieron en estos bancos, en sus sistemas de conexión al SPEI, y de los bancos sacaron recursos de la institución financiera", reconoció el presidente de la Asociación de Bancos de México (AMB), Marcos Martínez, en una entrevista televisiva. Agregó que "fue una operación bien orquestada". Por su parte, el gobernador de Banxico, Alejandro Díaz de León, informó que el evento afectó a "diversos participantes en la cadena de pagos electrónicos", pero aseguró que las personas no fueron víctimas. Agregó que "es un ataque de importancia y del que, por lo menos en el sistema de pagos, no teníamos antecedentes". Golpe en Canadá Días después, los canadienses Bank of Montreal y Canadian Imperial Bank of Commerce (CIBC) reportaron ataques: hackers aseguraban tener acceso a cuentas de unos 90 mil clientes y amenazaban publicar los datos si no se les pagaba. Ambas instituciones contactaron a las autoridades y a los clientes potencialmente afectados para aconsejar que monitorearan sus cuentas y cambiaran sus contraseñas, pero, hasta ayer, no se reportaban transacciones sospechosas. Las mayores entidades financieras del país han colaborado con el banco central para mejorar los

sistemas de defensa ante los ciberataques. Los ciberataques han ido en aumento en el mundo. El año pasado, la empresa estadounidense de monitoreo de crédito Equifax sufrió la mayor brecha de la historia: se robaron datos de datos de más de 145 millones de personas, incluyendo nombres, fechas de nacimiento, números de seguridad social, direcciones y datos de tarjetas de crédito.¿Onemi o superintendencia de la ciberseguridad?Los coletazos del ciberataque que aún siguen afectando al banco ligado al grupo Luksic dejan en claro la necesidad de continuar avanzando en la tramitación del proyecto de Ley de Ciberseguridad y en consolidar una institucionalidad que se haga cargo, al menos, de desempeñar aquellas funciones definidas como esenciales en la Política Nacional de Ciberseguridad (PNCS) trazada al 2022.La gestión técnica de incidentes que se generen en la Red de Conectividad del Estado está a cargo de los CSIRT (concepto europeo de Equipos de Respuesta a Incidentes de Seguridad Informática), aunque algunos expertos no están seguros si alguna vez estos equipos han operado durante una vulneración.A este diagnóstico se suma la falta de coordinación de los actores y de una única entidad a cargo, señala Cristian Ocaña, presidente de la recién creada Alianza Chilena de Ciberseguridad, que entre sus objetivos, buscará articular canales de comunicación entre privados y gobierno. "Debería haber un organismo único que coordine a todos esos coordinadores que están dando vuelta, como una Onemi de la ciberseguridad a nivel de Estado, que ante un desastre se le comunique todo", grafica.El docente de la **Universidad** de **Santiago**, Felipe Sánchez, aconseja que la organización de los CSIRT sea sectorial para que "esté todo interconectado, donde se pueda transmitir información, por ejemplo del software que se utilizó para el ataque, en forma expedita y que no estén sufriendo incidentes similares cada uno de estos actores", afirma."Hay una mayor concientización de las empresas y ya no es tan difícil batallar con el argumento respecto de las inversiones que hay que hacer en ciberseguridad", repara el gerente general de Makros, Marcelo Díaz.Una figura más empoderada que una Onemi de la ciberseguridad es la que propone el senador PPD Felipe Harboe, quien plantea la figura de una entidad con las facultades de una superintendencia. "Lo que se va a requerir es la coordinación respecto de diferentes sectores, pero a su vez el mejoramiento de los estándares del mundo privado, y para eso la posibilidad de una superintendencia que tenga facultades normativas a través de reglamentos a veces es bien adecuado", explica.Harboe remarca que su propuesta de Agencia de Protección de Datos apunta hacia allá, con atribuciones que le permitirán hacer auditorías para determinar causas.DF Check"Personal del banco se trasladó hasta el Banco Central y con información cargada en un pendrive. Desde el sistema operativo del Central se realizaron los pagos de alto valor y no se afectó la cadena de pago"El Banco Central aclaró que dispone de sistemas de contingencia que "están a disposición de cualquier institución bancaria que lo solicite". Además, estos cuentan con altos estándares de seguridad y, si bien están dentro del Central, "los bancos que requieran utilizarlas para conectarse al Sistema de Pago de Alto Valor lo hacen como si estuvieran conectándose desde sus propias instalaciones. Por razones de seguridad, estos sistemas no permiten el acceso a internet ni tampoco el uso de pendrives ni algún otro tipo de conexión"."¿Por qué no nos constituimos inmediatamente? Íbamos a ser un estorbo. Nos parecía que no tenía un valor constituirnos en ese minuto".La Ley de Bancos en lo referente a fiscalización establece en los artículos 12 y 13 que el regulador en su mandato de velar por el cumplimiento de la normativa, "podrá examinar sin restricción alguna y por los medios que estime del caso" a los fiscalizados. Como también, "impartirles instrucciones y adoptar las medidas tendientes a corregir las deficiencias que observare y, en general, las que estime necesarias en resguardo de los depositantes u otros acreedores y del interés público". Todo ello, cuando lo "estime conveniente"."Tenemos que desarrollar dentro de la Sbif la capacidad técnica y tecnológica de poder nosotros también entender la dimensión y magnitud de esto".De acuerdo a la memoria 2017 de la Superintendencia de Bancos, la entidad viene trabajando desde 2016 en temas de ciberseguridad a través de la realización de conferencias sobre el asunto, en la participación de mesas de trabajo con autoridades público-privadas y en regulaciones. Entre 2014 a la fecha, el regulador bancario ha hecho cinco cambios normativos en lo que respecta a riesgos operacionales, incluyendo la seguridad de la información y ciberseguridad.