"Modifica la ley General de Bancos y la ley N°19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores, en el sentido de exigir medidas de resguardo para los clientes de bancos e instituciones financieras que sufran ataques informáticos

Boletín N°12055-03

Considerando:

1.- La incorporación de las tecnologías de la información en la forma de generar, procesar y administrar sus activos de información es una realidad extendida en los bancos e instituciones financieras. *"En este ámbito la Ciberseguridad, concepto que comprende al conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta, es fundamental para evitar los efectos adversos de sus riesgos y amenazas inherentes sobre la seguridad de la información y la continuidad del negocio".*[1]

2.- Actualmente, la ciberseguridad de los bancos e instituciones financieras en Chile se encuentra pobremente regulada. A falta de normas legales que regulen la materia, solamente hay normas de nivel infra legal que, por lo demás, adolecen de una implementación que asegure su efectividad. En este sentido se puede citar la recopilación actualizada de normas Capítulo 20-8 de la Superintendencia de Bancos e Instituciones Financieras (SBIF)[2], la cual sólo establece una obligación de informar los incidentes vinculados a la ciberseguridad. Sin embargo, no existen sanciones por la omisión de la información íntegra y oportuna. El único incentivo del Banco o institución financiera para implementar una adecuada gestión de incidentes relativos a la ciberseguridad radica en el hecho de que esto es considerado en la evaluación de gestión y solvencia que haga la SBIF de las entidades bancarias, lo cual puede terminar influyendo en su calificación de riesgo operacional[3].

---

1 Circular 3.633 del 24 de enero de 2018 de la Superintendencia de Bancos e instituciones financieras

2 http://www.sbif.cl/sbifweb3/internet/archivos/norma_10696_1.pdf

3https://www.eldinamo.cl/nacional/2018/06/04/vulneracion-de-seguridad-del-banco-de-chile-no-habra-multas-ni-indemnizaciones-tras-caida-de-sistemas/

3.-El ciberataque del 24 de mayo de 2018 al Banco de Chile dejó en evidencia la falta de regulación en la materia y la debilidad de nuestras instituciones. En aquella ocasión el Banco de Chile fue víctima de un ciberataque que obligó a la suspensión de más de 9 mil sucursales a nivel nacional. Finalmente, la entidad reconoció la pérdida de 10 millones de dólares. Aunque existen informaciones que señalan que el banco podría haber sido defraudado en un monto cercano a los 100 millones de dólares, dando a conocer un monto mucho menor que correspondería sólo a lo recuperado[4]. El Banco atacado habría demorado 3 días en controlar la emergencia

Por otra parte, hasta la fecha de presentación de este proyecto de ley, no hay certezas acerca de un eventual robo de información de los clientes del Banco[5].

4.- La insuficiente regulación de los ciberataques a bancos e instituciones financieras ha tenido como consecuencia una pobre implementación de esta. En efecto, el Superintendente de Bancos e Instituciones Financieras reconoció que, respecto de esta clase de incidentes, "Lo que podemos hacer es dar recomendaciones y monitorear lo que está ocurriendo, pero no tenemos protocolos como los que hay en países como Singapur, donde la obligación de las instituciones es estar operando antes de cuatro horas de ocurrido el hecho"[6]. Asimismo, señaló que para esta clase de incidentes tampoco se prevén sanciones para los Bancos[7]

5.- La situación descrita en las consideraciones precedentes dan cuenta del riesgo en que se encuentra un sector de la mayor relevancia para el país, como lo es el sector financiero. En razón de lo expuesto, este proyecto de ley viene a elevar a rango legal el deber de los bancos de implementar sistemas de ciberseguridad así como el establecimiento de deberes de información ante un ciberataque. Lo anterior encuentra fundamento en el hecho de que, a causa de la fé pública comprometida en una actividad como la bancaria, la vulneración de la ciberseguridad de un Banco

4 https://www.biobiochile.cl/noticias/economia/negocios-y-empresas/2018/06/10/defraudacion-tras-ataque-informatico-al-banco-de-chile-podria-ser-aun-mayor.shtml

5 https://www.eldinamo.cl/nacional/2018/06/14/hackeo-al-banco-de-chile-expertos-develan-desproteccion-a-datos-de-clientes/

6 Publimetro 7 Junio 2018. Página 14. Sección: "Emprende"

7 https://www.eldinamo.cl/nacional/2018/06/14/hackeo-al-banco-de-chile-expertos-develan-desproteccion-a-datos-de-clientes/

es, sin duda, una información relevante a la cual deben tener acceso oportuno la autoridad sectorial, los clientes del Banco afectado y el público en general.

Por otra parte, este proyecto también viene a proteger a los clientes del banco o instituciones financieras ya que establece el deber legal de informar a aquellos respecto de la ocurrencia algún incidente de ciberseguridad que pueda razonablemente afectar sus datos personales.

6.- **Las leyes afectadas por este proyecto de ley** son el DFL Nº 3 de 2016 que fija el texto refundido, coordinado y sistematizado de la Ley General de Bancos, y la ley 19.496 que establece normas sobre protección de derechos de los consumidores. Respecto del primer cuerpo legal, este proyecto agrega 2 artículos nuevos (los artículos 49 bis y 49 ter), y respecto del segundo cuerpo legal agrega un artículo nuevo (el artículo 17 M).

7.- **La idea matriz** de este proyecto de ley es establecer medidas que resguarden eficazmente el interés público y los derechos de los clientes de los bancos e instituciones financieras ante un ciberataque.

Por tanto, en razón de las consideraciones precedentes, los diputados firmantes venimos en presentar el siguiente:

PROYECTO DE LEY

Artículo primero: Agréguense los siguientes nuevos artículos al DFL Nº 3 de 1997 que fija el texto refundido, coordinado y sistematizado de la Ley General de Bancos

1.- Artículo 49 bis: Cada banco e institución financiera deberá implementar el sistema de ciberseguridad más seguro posible según la mejor tecnología disponible. Asimismo, deberá actualizar su sistema de ciberseguridad en la medida que la mejor tecnología evolucione.

Ante la ocurrencia de un incidente de ciberseguridad le corresponderá al Banco acreditar la existencia y el debido funcionamiento de las medidas de seguridad.

2.- Artículo 49 ter: Los bancos e instituciones financieras deberán informar al Superintendente de Bancos e Instituciones financieras de cualquier ciberataque o intento de ciberataque dentro de una hora luego de que como tome conocimiento de este.

Los Bancos e instituciones financieras que sufran la interrupción de sus actividades a causa de algún incidente de ciberseguridad deberán restablecer sus actividades en un plazo máximo de cuatro horas luego de ocurrido el incidente.

Sin perjuicio de lo dispuesto en los incisos precedentes, el Banco o institución financiera afectado deberá publicar en un periódico de circulación nacional, dentro de 3 días corridos desde el incidente la siguiente información: día del incidente que afectó la ciberseguridad, la naturaleza del incidente sufrido, el número potencial de clientes afectados y el daño al patrimonio del banco.

Artículo segundo: Agréguese a la ley 19.496 que establece normas sobre protección de derechos de los consumidores el siguiente nuevo artículo 17 letra M:

1.- Artículo 17 M: Dentro del plazo de 24 horas luego de haber tomado conocimiento de haber sido víctima de algún incidente de ciberseguridad, las instituciones a que se refiere el inciso primero del artículo 17 B de esta ley, deberán informar a sus clientes respecto de cualquier vulneración a la ciberseguridad de la cual pueda razonablemente resultar la destrucción, filtración, pérdida o alteración de los datos personales o la comunicación o acceso no autorizados a dichos datos. La omisión del deber de información a los clientes, o la entrega de información que induzca al error al cliente, constituirá una infracción a las normas de esta ley y será sancionada con la multa que establece el artículo 17 letra K, sin perjuicio de las indemnizaciones que pueda determinar el juez competente de acuerdo a esta ley.

La información que los bancos deben entregar a sus respectivos clientes que razonablemente puedan encontrarse en algunas de las situaciones previstas en el inciso anterior, deberá ser informada por escrito al deudor, al último correo electrónico registrado por el deudor con el banco o en su defecto, al último domicilio registrado por el deudor con el proveedor.

ALEJANDRO BERNALES MALDONADO
Diputado de la República
Partido Liberal de Chile
Distrito 26
(Autor principal)

VLADO MIROSEVIC VERDUGO
Diputado de la República
Partido Liberal de Chile
Distrito 1