INFORME DEL CONSEJO DEL BANCO CENTRAL DE CHILE SOBRE SUSTRACCION DE INFORMACION RESERVADA

Y

NORMAS Y PROCEDIMIENTOS DE RESGUARDO APLICABLES EN ESTA MATERIA

INDICE

ANEXOS

I.- Presentación

Este es un Informe del Consejo del Banco Central de Chile a la Comisión de Hacienda del Senado para dar cuenta de diversos antecedentes relacionados con la sustracción de información reservada que se detectó el 30 de enero pasado y que ha tenido una extensa cobertura en los medios durante las recientes semanas. El Informe está dividido en tres secciones, además de esta breve presentación, e incluye cuatro anexos a los cuales se hace referencia en el texto de las secciones.

II.- Antecedentes sobre la sustracción de información reservada

- El miércoles 29 de enero el Presidente don Carlos Massad detectó irregularidades en su correo electrónico, lo cual lo hizo alertar a la Gerencia de Informática.

- En rápida investigación, el día jueves 30 se detecta que una persona distinta del Presidente estaba utilizando su cuenta de correo electrónico para enviar mensajes a su cuenta personal, para luego reenviarlos a terceros fuera del Banco Central.

- Se constata que esta persona es la Srta. Pamela Andrada, segunda secretaria de don Carlos Massad. El Presidente encarga al Gerente General hacerse cargo del tema, con expresas instrucciones de adoptar las medidas correspondientes.

- En la investigación interna practicada, se interroga a la Srta. Andrada y ella reconoce su actuación, proporcionando diversos antecedentes. El mismo día jueves se le notifica que se pone fin a su contrato de trabajo, por incumplimiento grave de diversas disposiciones normativas y del propio contrato.

- Con las pruebas que hasta ese momento se habían reunido, el Gerente General evaluó, junto con la Fiscalía del Banco, que correspondía a la Institución presentar a los Tribunales querella por los delitos relacionados con la divulgación de información de carácter reservado. Se comunicó lo anterior al Sr. Presidente, quien fue de opinión de interponer querella con la máxima urgencia. La querella quedó presentada el sábado 1° de febrero en la mañana y fue ratificada el

lunes 3 de febrero a primera hora. Ese mismo día se informó a la Superintendencia de Valores y Seguros para los efectos legales correspondientes, ya que la información reservada se entregaba a Enzo Bertinelli, quien desempeñaba el cargo de Gerente General de Inverlink Corredores de Bolsa S.A., empresa fiscalizada por esa Superintendencia.

- El Banco emitió un comunicado en la mañana del mismo día 3 de febrero, y posteriormente, conforme a lo acordado por los Consejeros, en la tarde tuvo lugar una conferencia de prensa donde el Gerente General y el Fiscal respondieron diversas preguntas sobre el tema.

- El Consejo, en su sesión ordinaria celebrada el miércoles 5 de febrero, tomó conocimiento formalmente de todos los antecedentes reunidos respecto de la sustracción de información reservada que afectó al Banco, del estado del proceso penal iniciado al efecto, y encargó al Gerente General que proponga las medidas destinadas a complementar las normas y procedimientos que rigen en materia de información.

- En este aspecto, cabe destacar que en un lapso inferior a 48 horas el Banco comprobó y evaluó la gravedad de los hechos que lo afectaron, adoptó las acciones que legalmente le correspondían y puso los antecedentes a disposición de los Tribunales, únicos organismos competentes para investigar delitos y aplicar sanciones.

- Los Tribunales son los encargados de determinar el hecho punible y sus partícipes, sin perjuicio de la actuación activa que le corresponde al Banco Central en su carácter de querellante en esta causa. En este contexto, el Banco ha colaborado estrechamente con los tribunales y la policía de investigaciones y ha continuado aportando nuevos antecedentes al Juez que sustancia el proceso. El Presidente prestó declaración voluntaria apenas iniciada la investigación y así también lo han hecho, en carácter de testigos, varios funcionarios del Banco.

- El Banco no puede proporcionar antecedentes específicos sobre los hechos materia de la querella presentada al Tribunal y demás antecedentes del proceso, por cuanto con ello se pondría en serio riesgo el éxito de la investigación judicial amparada por el secreto de sumario.

- El Consejo, en una nueva sesión ordinaria, celebrada el día lunes 10 de febrero, evaluó lo acontecido hasta esa fecha y luego, en sesión extraordinaria del jueves 13 de febrero acordó solicitar la designación de un Ministro en Visita para que se avoque exclusivamente a la sustanciación de este proceso, por considerar que la actuación de los Tribunales de Justicia constituye la mejor garantía de transparencia frente a la situación ocurrida. En la misma sesión se acordó también informar a la Comisión de Hacienda del Senado acerca de los acontecimientos ocurridos y de las medidas adoptadas.

- La querella del Banco Central de Chile se interpuso en contra de la ex funcionaria Pamela Andrada Díaz; de Enzo Bertinelli, Gerente General y representante legal de Inverlink Corredores de Bolsa S.A., empresa que integra el conglomerado económico del mismo nombre; y en contra de todos aquellos que resulten responsables, en carácter de autores, cómplices o encubridores.

- Según se indica en la querella, Pamela Andrada transmitió información reservada del Banco Central de Chile al correo electrónico de Bertinelli y, para ello, previamente accedía al computador del Presidente del Banco en los momentos en que éste no se encontraba en su oficina. En otras ocasiones accedía al computador del Presidente y transmitía información de la naturaleza indicada al ubicado en su puesto de trabajo y desde allí la divulgaba a Enzo Bertinelli.

- La querella se fundamenta en la trasgresión de las normas del artículo 247 bis del Código Penal, relativo al uso indebido de información reservada por parte del empleado público; artículo 248 bis del Código Penal, sobre cohecho, en el caso de Pamela Andrada; y del artículo 250 del Código Penal, sobre soborno, en el caso de Enzo Bertinelli. Además, la querella se basa en los artículos 2° y 4° de la ley 19.223, que tipifica figuras penales relativas a la informática.

- Con fecha 14 de febrero de 2003, el Tribunal resolvió, con el mérito de los antecedentes reunidos, someter a proceso a Pamela Andrada como autora de los delitos de cohecho previsto en el artículo 248 bis del Código Penal y de infracción al artículo 4° de la ley 19.223, antes citada, y a Enzo Bertinelli como autor de los delitos de soborno de que

trata el artículo 250 del Código Penal e infracción del artículo 2° de la ley 19.223, sobre figuras penales relativas a la informática.

- Por resolución de fecha 18 de febrero de 2003, el Pleno de la Iltma. Corte de Apelaciones de Santiago acogió la petición planteada por el Banco Central de Chile y acordó designar Ministro en Visita Extraordinaria para que sustancie este proceso.

- La investigación judicial, una vez establecidos los delitos antedichos y la participación que en ellos correspondió a los procesados Andrada y Bertinelli, se ha centrado fundamentalmente, en el uso que pudo haberse dado a esta información reservada en el interior del conglomerado Inverlink, dada la posición relevante que ocupaba en éste el procesado Bertinelli, materia en la cual el Instituto Emisor ha continuado colaborando con la investigación judicial para lograr el total esclarecimiento de los hechos delictuales de que fue objeto.

- Con fecha 18 de febrero de 2003 se hizo parte en la causa en carácter de querellante, el Consejo de Defensa del Estado; y, con fecha 21 de febrero de 2003, la Superintendencia de Valores y Seguros interpuso querella basada en la contravención de las normas aplicables a la información privilegiada, a que se refiere el artículo 60 de la Ley de Mercado de Valores.

III.- Normas y procedimientos del Banco Central en el tratamiento de la seguridad de la información

Introducción

La seguridad de la información en el Banco Central forma parte de una política de seguridad institucional que abarca variadas áreas de gran importancia y con interrelaciones entre ellas. El Banco, por ejemplo, mantiene y administra un elevado volumen de reservas internacionales, lo cual requiere una sofisticada política de seguridad que abarca aspectos físicos y ambientales, de sistemas de comunicación internacionales y domésticos, de personal altamente calificado, de riesgos financieros y políticos, de sistemas contables en línea, de dobles controles internos y externos, u otros. Asimismo, las funciones de tesorería necesitan sus propios procedimientos específicos de seguridad en la administración de

las bóvedas, emisión, distribución, conteo y destrucción de circulante, manejo de valores físicos y/o desmaterializados, entre otros. Igualmente, la mesa de dinero, con sus operaciones diarias de compras, ventas, licitaciones y rescates de muy diversos instrumentos financieros, tiene un subsistema específico de seguridad que incluye grabaciones, estrictas normas de licitaciones, operaciones electrónicas en tiempo real, transparencia total, auditorías especializadas, sistemas de comunicación con la banca a prueba de interferencias, planes de contingencia, entre otros. En fin, podrían mencionarse varias otras actividades donde la seguridad es un aspecto de la máxima relevancia y de preocupación permanente para el Consejo y la Administración.

En el caso de la seguridad en el uso de la información, se distinguen básicamente las normas según criterios de Confidencialidad (asegurar que la información sea accesible solo por usuarios autorizados) e Integridad (salvaguardar la exactitud y totalidad de la información). Al igual que en la mayoría de las instituciones modernas, la información que maneja el Banco Central de Chile es cuantiosa, compleja y, en términos generales, puede mantenerse en forma impresa y/o almacenada electrónicamente. Asimismo, la información puede ser trasmitida usando medios electrónicos, físicos y/o verbales.

Adicionalmente, el Consejo se ha preocupado desde hace tiempo por adoptar estilos de trabajo y publicación de informaciones que aumenten la transparencia y reduzcan la probabilidad de filtraciones. Por ejemplo, la cifra de IMACEC se publicaba 6 días después de estar disponible; hoy se publica sólo pocas horas después. Las licitaciones de papeles del Banco Central se realizan ahora electrónicamente, y el precio de cierre se conoce minutos después de cerrada la licitación, comparado con 4 horas o más de demora en el pasado. El comunicado con la decisión adoptada en las Reuniones de Política Monetaria se publica minutos después del término de la reunión, la que concluye normalmente luego del cierre del mercado.

Se han eliminado todas las restricciones cambiarias, de movimientos de capitales y de comercio exterior, de modo que las operaciones no tienen demora. El tipo de cambio flota libremente, y las operaciones excepcionales de intervención se publican con anterioridad en tiempo y montos máximos.

El Informe de Política Monetaria contiene el análisis y los supuestos y riesgos que considera el Consejo en relación con la marcha de la economía. Finalmente los principales discursos o intervenciones de las altas autoridades del Banco Central se publican simultáneamente en nuestra página web, para que todo el mercado cuente con la misma información.

En el contexto mencionado, la presente sección describe, en términos globales y resumidos, las normas, reglamentos, procedimientos y prácticas de trabajo en el Banco Central relativas a la seguridad en el uso de la información.

Normas legales y reglamentarias.

a) Todo funcionario del Banco tiene la obligación de saber que la información que se almacena o circula en el Banco Central de Chile es de carácter reservado, mientras el Consejo no disponga lo contrario, y que se expone a drásticas sanciones si hace uso no autorizado de cualquier información. Esto se puede constatar al menos en los siguientes textos de documentos conocidos por todos los empleados y que están permanentemente accesibles en las páginas de la INTRANET del Banco:

   i) Ley Orgánica Constitucional del BCCH
      - Titulo V Artículo 66. Sobre reserva de antecedentes relativos a las operaciones que el banco efectúe
      - Titulo VIII Artículo 86. Sobre obligaciones de conservar durante un plazo mínimo de 5 años sus libros, formularios, correspondencia, documentos y papeletas

   ii) Contrato individual de trabajo
      Se establece, como obligación esencial, mantener absoluta reserva de las situaciones o negocios que se relacionen con el Banco y que el funcionario llegare a conocer en el desempeño de su cargo. Existe, además, una modificación al texto del contrato, que data desde 1999, donde se incorpora esta obligación de reserva, la que se mantiene incluso una vez que el funcionario haya dejado de pertenecer al Banco.

   iii) Reglamento del Personal

Establecido por el Consejo conforme al artículo 18, N°3 de la Ley Orgánica Constitucional que rige al Banco y que regula las relaciones de los funcionarios con la Institución. Dicho reglamento contiene normas sobre obligaciones, prohibiciones y conflictos de intereses, semejantes a las que se establecen en el Título III de la Ley de Bases Generales de la Administración del Estado. (Ver Anexo A)

iv) Circulares Internas
- N°294. Sobre reserva con la información que debe mantener el personal del Banco y directrices sobre comunicaciones.
- N° 298 y 335 Sobre Uso de Correo Electrónico.
(reproducidas también en Anexo A)

b) El Banco dispone de un Compendio de Normas Administrativas Internas, que se revisa y perfecciona periódicamente (a lo menos una vez al año), el cual contiene, entre otras, disposiciones detalladas sobre la forma en que los funcionarios deben tratar la información de la cual son responsables (Ver, especialmente, Capítulo IV: "Normas sobre Funciones Informáticas", el cual se reproduce en el Anexo B de este informe)

c) Asimismo, el Banco Central dispone de un conjunto de normas generales de diseño y flujogramación de procedimientos, las que incluyen, entre otros, instrucciones sobre la estructura, preparación, aprobación y derogación de procedimientos. La estructura de estos procedimientos considera una introducción con el contenido y marco reglamentario, definiciones sobre términos y nomenclaturas utilizadas y una descripción detallada de las actividades, responsabilidades y mecanismos de control interno. La actualización de procedimientos es anual, efectuada por encargados en cada unidad formalmente designados, aprobada por los gerentes respectivos e informada a las unidades involucradas y a Contraloría interna.

En la actualidad existen 164 Procedimientos Administrativos formalmente establecidos y publicados en la INTRANET del Banco.

d) En el Banco existe una Contraloría interna, establecida en la Ley Orgánica Constitucional y dependiente del Consejo, que lleva a cabo auditorías periódicas a todas las unidades de la organización, incluyendo materias de carácter informático y de cumplimiento de normas.

   El Consejo aprueba anualmente el plan de trabajo de la Contraloría y ésta le presenta informes trimestrales sobre sus auditorías, las cuales abarcan un importante número de áreas cada año. Las recomendaciones de la Contraloría son evaluadas por la administración y se toman acciones, cada vez que corresponde.

e) Asimismo, el Banco solicita periódicamente evaluaciones externas de diversos aspectos de sus sistemas de información, incluyendo la seguridad, los cuales son puestos a disposición del Consejo y de la Administración superior.

f) Finalmente, existen las revisiones anuales de los auditores externos, realizadas conforme a lo establecido en el Artículo 76° de la LOC, las que en todos los casos abarcan materias referidas a sistemas de información.

Políticas y prácticas de trabajo

a) Los diversos informes de uso interno, minutas, proyectos de acuerdo, informes estadísticos, u otros, son distribuidos a destinatarios predeterminados, según lo haya definido la instancia pertinente (generalmente es el Gerente responsable del documento o bien el propio Consejo). En este sentido, el grupo destinatario de cada informe o documento interno se define descentralizadamente en las diversas unidades y queda establecido en los "procedimientos administrativos", en instrucciones de la respectiva unidad y/o en "listas de distribución" impresas en los propios informes. No hay, en consecuencia, un solo reglamento centralizado que defina el tratamiento de toda la cuantiosa y diversa información interna.

b) Asimismo, sólo pueden acceder a la información que se almacena electrónicamente en carpetas compartidas o áreas comunes, aquellos funcionarios que han sido expresamente autorizados, para efectuar determinadas labores con los documentos, lo cual se decide

en las instancias gerenciales responsables de la información. A manera de ejemplo, existe actualmente una "carpeta" destinada a almacenar todos los documentos y minutas que se ponen en tabla para las sesiones de los consejos informales ("pre-Consejos"). A dicha carpeta sólo tienen acceso, a través de sus cuentas individuales, los miembros del Consejo y un reducido número de altos ejecutivos del Banco. Una descripción de estas prácticas de trabajo se adjunta en el Anexo C.

c) Como se ha dicho, no ha sido práctica del Banco adoptar una política centralizada destinada a definir qué información es más "altamente sensible" (no obstante que toda la información tiene el carácter de "reservada"). Sin embargo, a nivel de cada gerente se han establecido prácticas de especial prudencia en el envío de información altamente sensible. Esta especial prudencia se puede manifestar, en la práctica, en el uso de sobres "reservados", "personal" y/o "confidencial", la cuidadosa conformación del grupo de personas destinatarias, el envío de e-mails con restricciones de impresión y/o reenvío, el establecimiento de horarios especiales para difundir la información, u otros.

d) El correo electrónico ha adquirido un uso cada vez más generalizado en las comunicaciones internas y externas del Banco. Esta circunstancia, al igual que en muchas empresas, ha modificado significativamente los hábitos de trabajo en cuanto a las funciones de las secretarias en la manipulación de los flujos de información desde y hacia sus respectivos jefes.

Sistemas de información computacionales

En el área más específica de la seguridad de los sistemas de información computacionales, sus variados aspectos tienen en cada caso, normas, procedimientos y herramientas que los regulan y administran.

a) Para el caso de las instalaciones centrales, tanto del Área ampliada de Operaciones, como de la Sala de Operaciones, al interior de dicha Área, se cuenta con cámaras de vigilancia y control de accesos a través de tarjetas de identificación. El acceso a los equipos

centrales, ubicados en la Sala de Operaciones, es controlado por los operadores de sala y personal autorizado.

b) En materia de respaldos, éstos se encuentran automatizados de acuerdo a políticas predefinidas y su almacenamiento se realiza en edificios distintos.

c) La red de comunicaciones está organizada distinguiendo la comunicación interna de las comunicaciones externas. Para el caso de las comunicaciones externas, a través de Internet, red Banco Central con la banca y otras conexiones para sistemas de información específicos, se utilizan equipos de control llamados firewalls, con distintos niveles de seguridad programables, los que permiten filtrar y controlar los accesos. Asimismo, los servidores que manejan las comunicaciones del Banco con terceros, cuentan con un sistema de detección de intrusos, procedimientos de seguridad de las máquinas y con la aplicación de actualizaciones periódicas de resguardos del sistema operativo. La comunicación interna también está regulada por sistemas de seguridad compatibles. En el caso del correo electrónico, además, se filtra el correo no deseado.

d) Para toda la instalación del Banco se cuenta con diversas herramientas de control de accesos no deseados, antivirus y administración de códigos de usuario y passwords para los diferentes recursos asignados a niveles personales y compartidos.

e) En cuanto a la seguridad en el acceso a los sistemas de información y a los datos de las bases de datos corporativas, se trabaja con cuentas de red de cada usuario, con perfiles de acceso predefinidos por los responsables de la información. Los sistemas de información a los cuales tienen acceso usuarios externos están sometidos a todos los controles de acceso propios de las comunicaciones externas, como asimismo de los controles relativos a sistemas de información.

f) En el funcionamiento de los sistemas computacionales se utilizan controles y monitoreos de empresas externas especialistas en seguridad de plataformas y equipamiento computacional. Asimismo, se contratan auditorías especiales que verifican la correcta mantención de los niveles de seguridad exigidos, incluyendo la aplicación de tests de sensibilidades de riesgos.

IV.- Medidas y acciones para complementar las actuales normas y procedimientos sobre seguridad de la información.

Los acontecimientos conocidos relativos al robo de información del Banco Central hacen necesario adoptar acciones destinadas a complementar las políticas de seguridad vigentes, a la luz de la reciente experiencia.

Sin perjuicio de las medidas ya adoptadas, especialmente en cuanto a instrucciones precisas a los usuarios, que incluye el control más expedito de los mails enviados desde el Banco a terceros, el Consejo ha instruido al Gerente General para que antes del próximo 28 de marzo presente los proyectos de acuerdo, reglamentos y procedimientos que permitan poner en práctica medidas de rápida aplicación en las siguientes áreas:

a) Reglamento centralizado para manipulación de determinadas informaciones.

Sin abandonar las normas vigentes para toda la información "reservada", parece conveniente consolidar y centralizar en un documento aquellas disposiciones y procedimientos específicos relativos a la manipulación de un subconjunto de información que se puede calificar como **"altamente sensible" (IAS)**

Para estos efectos, se elaborará un capítulo del Compendio de Normas Administrativas Internas que contenga un reglamento especial para el tratamiento de la **IAS**. Deberán incorporarse a dicho capítulo tanto los procedimientos que actualmente se encuentran dispersos, como aquellos nuevos que se hagan necesarios a la luz de una "jerarquización" de la información.

El reglamento deberá contener, a lo menos:

- Un listado de la **IAS** (ejemplos: anticipos del IMACEC, balanza comercial u otros datos económicos, opciones de política monetaria, versiones preliminares del IPOM, cupos de licitación de papeles, minutas de medidas económicas importantes, mails con "anticipos y opiniones" relevantes, u otros)

- Un listado de los responsables de la elaboración, distribución y archivo de la **IAS.**

- Los grupos de distribución, cuando corresponda.

- Los únicos medios y formas autorizados para distribuir la **IAS** (impresa o electrónicamente), en cada caso:

  Ejemplos: i) forma de distribuir el "anticipo" del IMACEC: se enviará un mail a los miembros del grupo de distribución, avisándoles que pueden ver las nuevas cifras en un determinado "sitio"; la entrada a ese "sitio" será posible sólo con una clave especial que solo conoce el destinatario; ii) forma de distribuir la minuta previa a la RPM: impresa, en sobre "reservado", no antes de 24 horas del inicio de la RPM; iii) forma de enviar un e-mail que contenga "opiniones" o comentarios con **IAS:** quien envía o reenvía deberá hacerlo con expresa mención en su encabezamiento y con una opción que garantice que solo lo pueda abrir el titular de la cuenta.

- Las obligaciones y responsabilidades del destinatario de la **IAS.**

- Políticas de respaldos.

- Establecimiento de controles periódicos de eventuales filtraciones.

b) Responsabilidad del titular en su cuenta de correo e información de tráfico

No obstante que la cuenta de correo electrónico es individual e intransferible, aquellos miembros del Consejo, gerentes u otras jefaturas que, por razones justificadas, otorguen acceso a su cuenta de correo electrónico a terceras personas (secretarias, asesores, u otros funcionarios) deberán comunicarlo a la Gerencia de Informática, con copia a la Contraloría, al menos una vez cada semestre.

El titular que otorgue ese acceso será responsable del uso del correo electrónico por parte de los terceros autorizados, y para estos efectos quedará a su expedita e inmediata disposición la información del tráfico de e-mails desde y hacia su cuenta, así como del tráfico de las cuentas de aquellos a quienes le tenga autorizado el acceso.

c) Adaptación de softwares.

La Gerencia de Informática procederá a la adaptación, cuando sea necesario, de los softwares para que los usuarios puedan asegurarse que no habrá filtraciones de la **IAS** que reciban electrónicamente. Ver ejemplos de algunas opciones en Anexo D.

d) Auditorías semestrales.

La Contraloría interna establecerá como política permanente e incorporará en sus planes anuales de trabajo una auditoría obligatoria semestral a todas las unidades del Banco en relación al cumplimiento de las normas relativas al tratamiento de la **IAS**. Esta auditoría debe incluir explícitamente a todas las unidades y funcionarios que reciban, envíen o almacenen **IAS**.

e) Entrenamiento y capacitación

La Gerencia de Informática deberá poner a disposición de todos los funcionarios que reciban, envíen o almacenen **IAS**, permanentemente, sesiones de entrenamiento en el uso de herramientas computacionales para evitar riesgos de filtraciones en la manipulación de **IAS**. Esta disponibilidad de entrenamiento deberá ser adecuadamente publicitada entre los usuarios al menos una vez cada semestre.

f) Difusión de las normas de seguridad informática.

Finalmente, la Gerencia de Informática deberá adoptar la política de reiterar, al menos una vez al mes, en las pantallas de todos los computadores, las normas básicas de seguridad informática (ejemplo, “avisos” tales como: archive su correo **IAS** en carpetas personales; recuerde que su cuenta de correo es vulnerable; ¿cambió su password en el último mes? ; etc)