



BANCO CENTRAL DE CHILE

CARTA CIRCULAR

Bancos N° 617
Soc. Administradoras Ley N° 20.345 N° 9

ANT.: Capítulos III.H., III.H.4, numeral 31, y III.H.4.1, Título XI numeral 14, del Compendio de Normas Financieras, que contienen normas referidas al Sistema LBTR.

MAT.: Indica recomendaciones de continuidad operativa y de seguridad para el acceso a la Red Privada del Banco Central de Chile (RPBC), atendida su condición como elemento crítico del Sistema LBTR.

Santiago, 27 de junio de 2019

Señor Gerente:

Me permito comunicarle que, de conformidad con lo dispuesto en el numeral 31 del Capítulo III.H.4 “Sistema de Liquidación Bruta en Tiempo Real del Banco Central de Chile (Sistema LBTR)” del Compendio de Normas Financieras, se ha resuelto presentar un conjunto de recomendaciones y mejores prácticas a nivel técnico y operativo, tendientes resguardar las capacidades de conexión y comunicación requeridas a los Participantes del Sistema LBTR, específicamente en lo relacionado con la disponibilidad que a estos se requiere, en cuanto a su acceso a la red de comunicaciones privadas del Banco Central de Chile (RPBC), de conformidad con el Título II del Reglamento Operativo del Sistema LBTR contenido en Capítulo III.H.4.1 del Compendio citado.

Lo indicado, previéndose además que la RPBC constituye un sistema o elemento crítico del Sistema LBTR, de acuerdo con la normativa aplicable a dicho sistema de pagos de alto valor y sus Procedimientos de Continuidad Operacional vigentes, por configurar un medio de comunicación autorizado por el Banco Central de Chile (BCCh), que permite a los participantes acceder a un servicio de consultas y operación del Sistema LBTR, y al Sistema SOMA para uso de la Facilidad de Liquidez Intradía (FLI) y de la Facilidad de Liquidez Intradía con Línea de Crédito con Garantía Prendaria (FLI con LCGP), vinculadas con la liquidación de operaciones en el Sistema LBTR.

Por lo anterior, a fin de contribuir a prevenir, mitigar y resolver la eventual ocurrencia de riesgos de pérdida de integridad, confidencialidad y/o disponibilidad de los servicios que el BCCh entrega a través de esa red; se recomienda que los participantes del Sistema LBTR, cumplan al menos con las siguientes recomendaciones de continuidad operativa y de seguridad, en carácter de mejores prácticas:



BANCO CENTRAL DE CHILE

1. Contar con dos enlaces de comunicación con empresas distintas entre cada centro de procesamiento de datos del participante y el proveedor de servicios que el BCCh tenga contratado.
2. Contar con un Firewall, de manera de limitar el tráfico solo al requerido para operar el servicio entre las estaciones cliente y los servicios finales publicados en la RPBC. El Firewall debiese contar con una adecuada configuración de seguridad, tomando como referencia estándares técnicos y buenas prácticas de la industria (custodia y monitoreo de cuentas privilegiadas, monitoreo de cambios de reglas, procesos de parchado, plantillas de hardening, etc.).
3. Contar con procesos frecuentes de actualización y parchado de los equipos y las estaciones que se conecten a la RPBC, ya sea en carácter de infraestructura principal o de respaldo, siguiendo las recomendaciones formuladas por los proveedores.
4. Contar con componentes de antimalware con tecnologías de protección avanzada, en los equipos y las estaciones que se conecten a RPBC.
5. Contar con una adecuada configuración de seguridad (*hardening*), según las recomendaciones formuladas por los proveedores y la industria (Ej. las que publica el NIST), en las estaciones que se conectan a RPBC.
6. Contar con equipos exclusivos (no compartidos) para operar en la RPBC.
7. Contar con conexión a la RPBC desde más de una estación, para disponer de alternativas en caso que una falle.
8. Contar con elementos y/o configuraciones de seguridad que protejan el tráfico entre el proveedor de acceso y las estaciones conectadas a la RPBC (por ejemplo, encriptar tráfico entre estaciones participantes o utilización de segmentos de red exclusivos, entre otros).
9. Contar con soluciones de protección avanzada sobre las estaciones que se conectan a la RPBC (por ejemplo, Multifactor de Autenticación, Sistemas de Prevención de Intrusos y Firewall de Host, entre otros).
10. Contar con un sitio o lugar de contingencia en caso de no poder acceder a las instalaciones físicas dispuestas para la conexión a la RPBC.
11. Contar con controles que limiten la cantidad de equipos que se conecten a la RPBC a solo aquellos definidos por cada participante.

Mediante las recomendaciones y mejores prácticas identificadas, se persigue que los participantes del Sistema LBTR puedan mantener niveles de ciberseguridad y continuidad operativa adecuados, respecto de sus propios equipos y sistemas destinados a acceder a la RPBC, velando, de este modo, por la mitigación oportuna y razonable de eventuales riesgos de pérdida de integridad, confidencialidad y/o disponibilidad de cualquiera de los servicios que el BCCh entrega a través de dicha red. Asimismo, estas recomendaciones y el propósito antedicho se extienden a la utilización de la RPBC respecto del Sistema SOMA, en lo referido al uso de las facilidades de liquidez vinculadas con el Sistema LBTR.



BANCO CENTRAL DE CHILE

La incorporación de este conjunto de recomendaciones de continuidad operativa y de seguridad para los participantes del Sistema LBTR al utilizar la RPBC, en la condición de mejores prácticas identificadas en la actualidad, en carácter de criterios mínimos que se sugiere observar al acceder y hacer uso de esta red, podrá ser objeto de revisión y actualización, a fin de prevenir, mitigar y resolver eventuales efectos adversos que puedan incidir en la seguridad, confiabilidad, resiliencia y/o eficiencia de la RPBC; incluyendo, en su caso, la eventual imposición de estándares obligatorios en esta materia, de conformidad con la normativa del Sistema LBTR.

Asimismo, cabe considerar que las recomendaciones formuladas no alteran las obligaciones a que están sujetos los participantes del Sistema LBTR, en lo referido a la mantención, a su cargo y en adecuado funcionamiento, de los equipos y sistemas necesarios para conectarse y comunicarse con el Sistema LBTR, cumpliendo con los requisitos que su Reglamento Operativo contemple en esta materia, incluyendo lo referido a las capacidades de respaldo y recuperación con que deben contar en caso de contingencia; y el deber de dar cumplimiento a las demás exigencias que en materia de continuidad operativa y seguridad, les sean impuestas por el respectivo organismo supervisor.

Saluda atentamente a usted,

A handwritten signature in blue ink, consisting of several fluid, overlapping strokes.

ALEJANDRO ZURBUCHEN SILVA
Gerente General