

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA



COMUNICACIÓN "A" 4192

18/08/2004

A LAS ENTIDADES CAMBIARIAS:

Ref.: Circular
CONAU 1 - 670

Requisitos Operativos Mínimos de Tecnología y
Sistemas de Información para las Casas y
Agencias de Cambio.

Nos dirigimos a Uds. para comunicarles que se han establecido los Requisitos Operativos Mínimos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio, los que deberán ser cumplimentados dentro de los 90 días corridos de emitida la presente Comunicación.

Cabe aclarar que los incumplimientos a estas disposiciones serán considerados falta grave a los fines de la aplicación del Art. 41 de la Ley de Entidades Financieras.

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Ricardo O. Maero
Gerente de Régimen
Informativo

Rubén Marasca
Subgerente General de
Análisis y Auditoría

ANEXO



B.C.R.A.	Requisitos Operativos Mínimos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio
----------	---

-INDICE-

Sección A. Introducción

Sección B. Controles Generales de Tecnología

- B.1. Administración y control de los recursos de tecnología y sistemas de información
- B.2. Proveedores de servicios informáticos
- B.3. Documentación
- B.4. Seguridad física, resguardos de la información y continuidad del procesamiento
- B.5. Seguridad lógica y de acceso a los datos
- B.6. Telecomunicaciones y redes
- B.7. Servicios a través de internet

Sección C. Controles a los Sistemas de Información

- C.1. Cumplimiento de requisitos normativos
- C.2. Integridad y validez de la información
- C.3. Administración y registración de las operaciones
- C.4. Sistemas de información que generan los regímenes informativos requeridos por el Banco Central de la República Argentina
- C.5. Sistema aplicativo de contabilidad
- C.6. Sistema de transferencias electrónicas de fondos

Versión:1ª.	COMUNICACIÓN "A" 4192	Vigencia: 18/08/2004	Página 1
-------------	-----------------------	-------------------------	----------



Seccin A – Introduccin

Las casas y agencias de cambio debern establecer, de acuerdo con el volumen y complejidad de su estructura, procesos y operaciones, una estrategia de control para la proteccin de sus activos informticos, asegurando la disponibilidad, integridad y confidencialidad de su informacin, optimizando la eficiencia en la administracin de los datos, considerando las amenazas y las vulnerabilidades asociadas a cada entorno tecnolgico, su impacto en el negocio, los requerimientos y los estndares vigentes.

Las presentes disposiciones pretenden establecer un marco metodolgico que promueva el desarrollo e implementacin de adecuados procesos de control para las funciones de tecnologa y sistemas de informacin de las casas y agencias de cambio y facilite la puesta en prctica de medidas que aseguren la salvaguarda de los recursos informticos y reduzcan los riesgos asociados.

El criterio bsico a utilizar deber contemplar los siguientes pilares:

- Identificacin y administracin de los riesgos inherentes al procesamiento informtico, de acuerdo con los objetivos del negocio y las necesidades de informacin,
- Implementacin de controles que aseguren la validez y la confiabilidad de los datos procesados,
- Definicin y establecimiento de procedimientos de seguridad y mecanismos de control de acceso lgico que garanticen la proteccin de los activos informticos,
- Sana administracin de los recursos y sistemas de informacin y
- Registracin y control de las actividades realizadas.

El esquema de referencia metodolgico que se indica en las secciones siguientes no es excluyente de aquellos mecanismos adicionales que las casas y agencias de cambio consideren que debern formar parte de la estrategia de administracin y control de sus recursos de informacin.



B.C.R.A.	Requisitos Operativos Mínicos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio
----------	---

Sección B - Controles Generales de Tecnología

1 – Administración y control de los recursos de tecnología y sistemas de información

El personal propio de tecnología y sistemas de información de las Casas y Agencias de Cambio deberá depender funcionalmente de un nivel tal que permita garantizar su independencia de las áreas usuarias. Cuando las funciones relacionadas con la administración de los servicios informáticos se encuentren tercerizadas, se deberán implementar adecuados controles y/o contar con recursos humanos técnicamente capacitados, ya sea a través de personal bajo relación de dependencia o de terceros que no estén vinculados con los proveedores, para ejercer un control objetivo y eficiente sobre las actividades que se desarrollan externamente.

Asimismo, deberán delimitarse las funciones de desarrollo y mantenimiento de sistemas aplicativos, operación y procesamiento de datos, administración de la seguridad informática, soporte técnico y tecnología, de manera que se garantice un adecuado control por oposición de intereses.

2 – Proveedores de servicios informáticos

Las casas y agencias de cambio que tercericen total o parcialmente actividades relacionadas con la tecnología informática y sistemas de información, deberán suscribir contratos formales con los proveedores externos, identificando los riesgos y definiendo las condiciones de los servicios brindados.

Los contratos deberán contener como mínimo: el alcance de las tareas, acuerdos, términos y compromisos de disponibilidad y confidencialidad, los niveles mínimos de prestación de los servicios, la participación de subcontratistas, el derecho a realizar auditorías por parte de las casas ó agencias de cambio en las instalaciones del proveedor, los mecanismos de resolución de problemas, la duración del contrato y cláusulas de finalización, la asignación de roles y responsabilidades y el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo y por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad del procesamiento.

Además, los contratos deberán establecer claramente el acceso irrestricto y sin limitaciones para la Superintendencia de Entidades Financieras y Cambiarias a los datos, programas fuentes, toda la documentación técnica relacionada (diseño de archivos, diagramas técnicos, detalles de procesos, otros) y a la realización de auditorías periódicas en las instalaciones del proveedor, a fin de verificar el cumplimiento de todos los aspectos contemplados en las circulares vigentes.

Versión:1ª.	COMUNICACIÓN "A" 4192	Vigencia: 18/08/2004	Página 2
-------------	-----------------------	-------------------------	----------



En los casos en que el procesamiento se realice en dependencias de terceros y con el objeto de delimitar lógica y/o físicamente el entorno en el cual se realizan las actividades de la entidad, deberá existir una adecuada separación entre los ambientes de procesamiento propios, de los proveedores externos y de otros posibles clientes de éstos. Las condiciones regulatorias serán las exigidas para las actividades realizadas en la entidad y no podrán tercerizarse servicios con proveedores que a su vez tengan contratada la función de auditoría interna y/o externa.

La gerencia superior de las casas y agencias de cambio será la responsable primaria del control de las actividades que hayan sido delegadas mediante un contrato de tercerización, debiendo considerar en todo momento que se delegan actividades pero nunca la responsabilidad de la entidad sobre éstas.

3 - Documentación

De acuerdo con la estructura y complejidad de sus funciones informáticas, las casas y agencias de cambio deberán contar con políticas, normas, estándares, procedimientos y/o prácticas para los aspectos relacionados con la planificación, seguridad, operación y control de los sistemas de información y su tecnología asociada.

También deberán contar con documentación técnica y manuales de usuarios de los sistemas aplicativos, del equipamiento informático y su software de base, diagramas topológicos de las redes de telecomunicaciones y toda aquella documentación relacionada con los recursos de información.

4 - Seguridad física, resguardos de la información y continuidad del procesamiento

Según la naturaleza y magnitud de sus características tecnológicas, las casas y agencias de cambio deberán implementar apropiadas medidas de seguridad física y control ambiental en sus instalaciones, para reducir los riesgos relacionados con accesos no autorizados, daños y amenazas ambientales sobre el equipamiento informático, las facilidades de telecomunicaciones y el almacenamiento de los soportes de información.

Deberán contar con resguardos de los archivos de datos y programas ("backups") previniéndose, como mínimo, la generación de dos copias y manteniendo una de ellas en un sitio de almacenamiento externo. La modalidad, frecuencia, localización y períodos de retención de los respaldos (diarios, semanales, mensuales, otros) deberán garantizar su disponibilidad y recuperación ante cualquier inconveniente que se presente con el procesamiento y mantenerse en condiciones de ser procesados por el término de 10 años.

A los fines de no interrumpir las actividades normales y procesos críticos del negocio y conforme con una adecuada evaluación de los riesgos, las casas y agencias de cambio deberán desarrollar un plan de contingencias o documento equivalente, probado en forma parcial periódicamente y en forma integral como mínimo anualmente. El mencionado plan deberá establecer con claridad y precisión los cursos de acción a seguir, los tiempos a cumplir, la definición de responsabilidades, el equipamiento alternativo, los archivos, las telecomunicaciones, los proveedores de servicios de tecnología y sistemas de información y todos aquellos recursos necesarios para lograr la continuidad del procesamiento.



5 – Seguridad lógica y de acceso a los datos

Considerando los potenciales niveles de riesgo identificados, las casas y agencias de cambio deberán clasificar los recursos tecnológicos y sistemas de información según su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados por los mismos. Los niveles de accesibilidad deberán diseñarse considerando qué usuarios o grupos de usuarios tendrán derecho de acceso y con qué privilegios accederán a los datos, funciones y servicios informáticos.

Se deberán implementar métodos para el control del acceso lógico a los sistemas y servicios de información, los que dependerán de la sensibilidad y el valor de los datos a proteger, debiéndose considerar como mínimo: el cambio obligatorio de las contraseñas de acceso en el primer inicio de sesión, 8 (ocho) caracteres de longitud para las claves, el registro histórico de las últimas 12 (doce) contraseñas utilizadas, el intervalo de caducidad automática de las mismas a los 30 (treinta) días, el bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso fallidos, la desconexión automática de la sesión del usuario en la aplicación y en la red por tiempo de inactividad a los 15 (quince) minutos, la no utilización de usuarios genéricos y la implementación de técnicas de encriptación con adecuados algoritmos para el archivo de las contraseñas.

Además, se considerarán sanas prácticas de seguridad: la modificación de las claves maestras y de las cuentas especiales "por defecto", el control de la composición de las contraseñas (por ejemplo: caracteres alfabéticos, numéricos, especiales, mayúsculas y minúsculas), limitaciones para accesos concurrentes, la identificación única (ID's) de usuarios, definición de opciones y menús para acceder a las funciones de los sistemas de información y la dinámica en la actualización de los derechos de acceso, revocando los usuarios que se desvincularan de la entidad y modificando los perfiles de aquellos que cambien de función.

Deberán implementarse adecuadas restricciones para la utilización de programas utilitarios sensitivos, editores y compiladores, propios de los sistemas operativos de las distintas plataformas y herramientas de operación. Asimismo, deberán desarrollarse mecanismos formales para la asignación y la utilización de usuarios especiales con capacidades de administración, que puedan ser usados en caso de emergencia o interrupción de las actividades. Los usuarios definidos con estas características deberán contar con adecuadas medidas de resguardo y acceso restringido, registrando su utilización y realizando controles posteriores sobre los reportes de eventos, analizando la concordancia entre las tareas realizadas y el motivo por el cual se los solicitó.

A fin de minimizar el riesgo de actualizaciones accidentales en el entorno productivo, el ingreso de programas no probados, evitar accesos no autorizados a los datos y garantizar la correspondencia entre los programas "fuentes" y los programas "ejecutables", las casas y agencias de cambio deberán definir un adecuado esquema de separación entre sus ambientes informáticos de procesamiento (desarrollo, prueba y producción) asegurando que los analistas y programadores de sistemas no tengan acceso al entorno productivo, ni los operadores accedan al ambiente ni a las herramientas utilizadas para el desarrollo y el mantenimiento de los sistemas de aplicación.



B.C.R.A.

Requisitos Operativos Mínicos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio

También se deberán implementar reportes de seguridad que registren las actividades de los usuarios, los intentos fallidos de acceso y bloqueos de cuentas, la utilización de usuarios con accesos especiales y el uso de utilitarios sensitivos. Se deberá proteger la integridad de la información registrada en dichos reportes, resguardándose adecuadamente y manteniéndose en archivo por un término no menor a 10 años, utilizando para ello soportes de almacenamiento no reutilizables.

6 - Telecomunicaciones y redes

Las casas y agencias de cambio deberán establecer mecanismos de protección para los datos que se transmiten por las redes de telecomunicaciones, mediante técnicas de encriptación por "hardware" y/o "software" que garanticen el intercambio de información con total seguridad, implementando técnicas y procesos de autenticación, confidencialidad e integridad de la información para prevenir su pérdida, modificación o uso inadecuado.

7 – Servicios a través de internet

Se deberán implementar dispositivos de control entre las redes públicas y la red privada de la entidad que brinden adecuados mecanismos de protección y garanticen la no-intromisión, la detección de intrusos y la prevención contra software malicioso.

En los casos en que se ofrezcan servicios transaccionales a través de internet, deberá existir un adecuado esquema de seguridad entre los sistemas de la entidad y las aplicaciones con los servicios propios de la red. Se deberán utilizar protocolos seguros e implementar mecanismos para identificar a los clientes y garantizar la integridad de las transacciones.



Sección C – Controles a los Sistemas de Información

1- Cumplimiento de requisitos normativos

Las casas y agencias de cambio deberán considerar para el desarrollo de los sistemas aplicativos que se utilizarán para procesar su información comercial y de gestión, la implementación de apropiados controles según los requerimientos legales y regulatorios vigentes establecidos por el Banco Central de la República Argentina.

2 - Integridad y validez de la información

Los sistemas informáticos se deberán tener controles automatizados que permitan minimizar errores en la entrada, procesamiento y consolidación de datos, en la ejecución de los procesos de actualización de archivos y bases de datos y en la salida de la información.

Los datos que se registren en los sistemas aplicativos deberán ser sometidos a controles programados que aseguren la integridad, validez y confiabilidad de la información procesada, incluyendo: dígitos verificadores, validaciones de códigos, tipo y tamaño de campos, rangos de valores, signos, referencias cruzadas, registraciones fecha-valor, correlatividad de las operaciones, plazos, cierres, reaperturas de períodos y otros.

Los parámetros que limiten el ingreso de datos en los mencionados sistemas deberán tener adecuados niveles de acceso para su actualización, y restricciones en cuanto a la posibilidad de ser modificados a través de funciones específicas.

Asimismo, estos sistemas deberán contemplar controles programados que limiten la modificación y la eliminación de datos básicos y pactados de las operaciones concretadas, movimientos y saldos.

El sistema aplicativo utilizado para el procesamiento de las operaciones de compra y venta de moneda extranjera, deberá contar con procesos de validación para consultar la información de personas físicas y jurídicas con “medidas precautorias” exigidas por el B.C.R.A. Además, deberá contar con adecuados mecanismos de control sobre los montos máximos establecidos para operar en cambios.

El sistema aplicativo de clientes deberá poseer adecuados controles de integridad y validez, considerando su identificación única y los datos obligatorios de acuerdo con las normas vigentes.

Todos los sistemas aplicativos deberán generar registros de auditoría conteniendo las actividades de los usuarios, las tareas realizadas, las funciones monetarias y no monetarias utilizadas, e identificar quién ingresó y autorizó cada transacción, los cuales deberán ser revisados regularmente por los responsables del control interno. Se deberá proteger la integridad de la información registrada en dichos reportes, la que deberá ser resguardada adecuadamente y permanecer en condiciones de ser recuperada, manteniéndose disponible por un término no menor a 10 años, utilizando para ello soportes de almacenamiento no reutilizables.



3 – Administración y registración de las operaciones

Las casas y agencias de cambio deberán registrar y procesar sus operaciones en los sistemas aplicativos correspondientes, no pudiendo administrar ninguna operación en forma manual, en hojas de cálculo, herramientas de escritorio, u otro software utilitario.

Para el caso de nuevos servicios o productos, las entidades contarán con un período máximo de 90 días corridos a partir de la primera operación para administrar, registrar y procesar la información en los sistemas aplicativos correspondientes.

4 – Sistemas de información que generan los regímenes informativos requeridos por el Banco Central de la República Argentina

Las casas y agencias de cambio deberán contar con sistemas aplicativos o procesos automatizados para la generación de los regímenes informativos requeridos por el Banco Central de la República Argentina, evitando el reingreso o intercambio no automatizado de datos entre distintos sistemas, sin requerir del ingreso de datos significativos en forma manual y no debiéndose efectuar ajustes a la información generada previamente en forma automática.

Cuando se deba ingresar información manual por no residir ésta en los archivos o bases de datos de la entidad, se deberá realizar a través de programas específicos, en archivos independientes, con un adecuado esquema de seguridad, controles de integridad y validez y sin la posibilidad de modificar la información generada en forma automatizada.

5 - Sistema aplicativo de contabilidad

Deberá existir una adecuada integración entre los sistemas aplicativos que procesan la información de la entidad y el sistema aplicativo de contabilidad, registrando automáticamente en cada cuenta contable, en forma correcta y oportuna, todos los movimientos producto de las operaciones efectuadas.

El sistema de contabilidad deberá tener controles necesarios para impedir el ingreso de asientos desbalanceados, dar de baja y modificar asientos procesados, eliminar cuentas que tengan o hayan tenido saldos o movimientos durante el ejercicio, dar de alta cuentas con saldo, modificar saldos de cuentas en forma directa y otras registraciones de similares características.

El período máximo para el ingreso de asientos fecha-valor será de 5 días para el personal que debe ingresar movimientos contables normalmente. Superado dicho plazo, dentro del mes abierto y hasta un máximo de 40 días corridos, sólo se podrán ingresar transacciones fecha valor con la autorización de la máxima autoridad contable de la casa o agencia de cambio, expresada con su firma y sello en los comprobantes correspondientes, y la utilización de su clave de acceso personal, o en su defecto con la intervención bajo idénticas características de un funcionario designado por el directorio o autoridad equivalente.



B.C.R.A.	Requisitos Operativos Mínicos de Tecnología y Sistemas de Información para las Casas y Agencias de Cambio
----------	---

Se deberán emitir listados con los movimientos fecha-valor procesados, los cuales deberán mantenerse en archivo por un término no menor a 10 años, utilizando para ello soportes de almacenamiento no reutilizables. Cuando no exista este tipo de movimientos, en el listado deberá figurar una leyenda que indique esta situación.

6 - Sistema de transferencias electrónicas de fondos

Los sistemas que se utilicen para procesar las transferencias electrónicas de fondos deberán cumplir con los requisitos mínimos de controles internos establecidos en la presente Comunicación, referidos a la seguridad física, a la seguridad lógica de acceso a los datos, y al cumplimiento de requisitos normativos.

Con el fin de poder asegurar un adecuado control por oposición de intereses, no deberán existir usuarios con atributos simultáneos de ingreso, verificación y/o envío de operaciones, debiéndose designar responsables individuales para cada una de las funciones mencionadas. Asimismo, deberán implementarse mecanismos que aseguren la confidencialidad, resguardo, registro y control de la utilización de las claves maestras de los sistemas de transferencias.

Los listados que reflejen la actividad diaria de los mensajes enviados y recibidos, pendientes, rechazados, y otros, deberán ser controlados y mantenidos en archivo durante 10 años, utilizando para ello soportes de almacenamiento no reutilizables.

Versión:1ª.	COMUNICACIÓN "A" 4192	Vigencia: 18/08/2004	Página 8
-------------	-----------------------	-------------------------	----------