BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" 2659	23/01/98

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular RUNOR 1 - 260. CONAU 1 - 243. Requisitos operativos mínimos del área de sistemas de información de las entidades financieras

Nos dirigimos a Uds. a los efectos de comunicarles que esta Institución adoptó la siguiente resolución:

1. Aprobar, con vigencia desde el 1.7.98, los "Requisitos operativos mínimos del área de sistemas de información (SI)" que figuran en anexo a la presente comunicación.

2. Establecer que, en relación con lo dispuesto en el punto precedente, los auditores externos deberán emitir un informe especial al 31.3.98 y al 30.6.98 sobre el grado de avance en el cumplimiento de las disposiciones a que se refiere dicho punto.

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

Alfredo A. Besio
Gerente de Normas para
Entidades Financieras

Ruben A. Escobar
Gerente de Auditoria
Externa de Sistemas

ANEXO

Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de las áreas de sistemas de información, los cuales involucran al Directorio, Consejo de Administración o autoridad equivalente, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos:

- Eficacia: La información y los procesos relacionados deben ser relevantes y pertinentes para el desarrollo de la actividad. Deben presentarse en forma correcta, coherente, completa y que pueda ser utilizada en forma oportuna.

- Eficiencia: El proceso de la información debe realizarse mediante una optima utilización de los recursos.

- Confidencialidad: La información critica o sensible debe ser protegida a fin de evitar su uso no autorizado.

- Integridad: Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.

- Disponibilidad: Los recursos y la información deben estar disponibles en tiempo y forma, cuando sea requerida.

- Cumplimiento: Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades financieras.

- Confiabilidad: Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la entidad, en la presentación de informes financieros a los usuarios internos y en su entrega al Banco Central de la República Argentina y demás organismos reguladores.

Todos estos aspectos deben ser aplicados a cada uno de los recursos intervinientes en los procesos de tecnología informática, tales como: datos, sistemas de aplicación, tecnología, instalaciones y personas.

Los puntos que se detallan a continuación enumeran una serie de requisitos mínimos que las entidades financieras y las cámaras de compensación de fondos deberán cumplir, los que serán sometidos a supervisión por parte de la Superintendencia de Entidades Financieras y Cambiarias.

(La denominación "entidad" comprende tanto a las entidades financieras como a las cámaras de compensación de fondos).

1. Organización y control del área de sistemas de información.

1.1. Dentro de la estructura organizacional, el área de Sistemas de Información debe depender funcionalmente de un nivel tal que permita garantizar su independencia de las áreas usuarias.

1.2. El área debe presentar una clara delimitación de las tareas entre desarrollo y mantenimiento de sistemas, operaciones, soporte técnico y supervisión, de manera que garantice una adecuada segregación de funciones y no impida un control por oposición de intereses. Asimismo, deberá mantener una separación de funciones entre desarrollo y mantenimiento de sistemas y administración de bases de datos.

En las entidades con hasta 10 sucursales la función de soporte técnico podrá depender funcionalmente del sector de operaciones.

1.3. Debe existir un Plan de Sistemas formal que permita una supervisión continua y directa de las tareas que realizan los distintos sectores y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un periodo de 1 año.

Asimismo, debe existir un plan estratégico de sistemas, que contenga los proyectos principales y los cronogramas de su implementación, para un periodo de por lo menos 3 años.

1.4. El control gerencial del área debe ser formal, manteniéndose en archivo -durante 2 años- los documentos escritos en los que los sectores informan a sus supervisores las distintas actividades realizadas, con el objeto de permitir un adecuado control del cumplimiento de las políticas, objetivos y planeamientos definidos por la gerencia.

1.5. En las entidades con mas de 10 sucursales deberá existir un Comité de Sistemas para el tratamiento institucional de políticas, objetivos y planeamiento del área de Sistemas de Información en el cual deben intervenir los máximos niveles directivos y/o gerenciales de las áreas que disponga la entidad, formalizando el contenido de las reuniones mediante actas, las que se deberán mantener archivadas durante un periodo de por lo menos 2 años.

2. Normativa y procedimientos de operación de sistemas, programación y tecnología.

2.1. Deben existir políticas generales, una clara definición de las misiones y funciones de todos los puestos de trabajo (responsabilidad, dependencia, funciones que supervisa, etc.), estándares y procedimientos escritos que sean la base de la planificación, el control y la evaluación gerencial del área.

2.2. Deben existir manuales con estándares de metodología para el diseño, desarrollo y mantenimiento de los sistemas aplicativos. Su aplicación regirá para todos los nuevos sistemas y para las modificaciones cuyos desarrollos sean posteriores a la fecha de la presente comunicación.

2.3. Debe existir documentación de: los sistemas aplicativos; la operación de los procesos informáticos; los procesos de recuperación de datos y archivos; los procesos de copias y resguardo de datos; la seguridad física y lógica; la administración de la red de telecomunicaciones; los procedimientos para la puesta en marcha de programas en producción; el tratamiento de los requerimientos de usuarios; los manuales de usuario; los procedimientos de transferencias de fondos, etc.

2.4. Debe existir documentación detallada sobre el equipamiento informático, que incluya diagramas y distribución física de las instalaciones, inventario de "hardware" y "software" de base, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.

Esta información comprende tanto al centro de procesamiento de datos principal como de los secundarios, redes departamentales, sucursales, transferencias de fondos y al centro alternativo para contingencias.

3. Control de operaciones computarizadas o procesos.

3.1. Debe existir una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberá incluir como mínimo el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos de registración de los hechos y problemas, los procedimientos sobre cancelaciones y reprocesos en cada una de las actividades, las relaciones con otras áreas y los mecanismos de distribución de la información.

3.2. Deben existir procedimientos de control para garantizar la efectivización correcta de cambios cuando corresponda, tales como: cambios de programas en bibliotecas de producción, archivos, definiciones de diccionarios de datos, ordenes de corrida de programas, etc.

3.3. En los casos en que existan distintos centros de procesamiento, debe haber un responsable por el control centralizado de las operaciones y procesos que se realicen en ellos.

4. Proveedores externos.

4.1. Deben existir contratos formalmente establecidos con los proveedores externos de "software", procesamiento y/o servicios, en los cuales se contemplen aspectos tales como el procedimiento por el cual la entidad, ante cualquier situación que pudiera sufrir el proveedor por la cual dejara de operar o de prestar sus servicios en el mercado, pueda obtener los datos, programas fuentes, manuales y documentación técnica, a los efectos de poder asegurar la continuidad en el procesamiento.

Además, en los contratos debe establecerse claramente que la Superintendencia de Entidades Financieras y Cambiarias tendrá acceso irrestricto a los datos y a toda documentación técnica relacionada (diseño de archivos, tipo de organización, etc.).

4.2. La entidad debe contar con recursos humanos técnicamente capacitados para ejercer un control eficiente sobre las tareas que desarrolla el proveedor externo, ya sea a través de agentes bajo relación de dependencia o que no estén vinculados con los proveedores externos.

5. Integridad y validez de la información procesada.

Los sistemas de información computarizados deben tener incorporados en su programación validaciones y controles mínimos para asegurar la integridad y validez de la información que procesan (referidos a: fechas, número de cuentas, número de clientes, tasas de interés, plazos, importes, etc.)

6. Implantación de la seguridad lógica.

6.1. Dentro de la estructura de la entidad debe existir una función para la administración y control de la seguridad de acceso a los datos que garantice su independencia del área de Sistemas de Información.

En las entidades con hasta 10 sucursales esta función podrá ser desempeñada por el máximo responsable del área de sistemas.

6.2. Debe existir una política formal de seguridad informática, en la que se detallen como mínimo los siguientes aspectos: nivel de confidencialidad de los datos, procedimiento de otorgamiento de claves de usuarios para el ingreso a los sistemas, estándares fijados para el acceso y autenticación de usuarios, cursos de acción a seguir en caso de inicio de sumarios a empleados o desvinculación de estos o de terceros de la entidad.

6.3. Respecto al acceso y autenticación de los usuarios se deben fijar, como mínimo, los siguientes valores: 4 caracteres de longitud para las "passwords", la no repetición de las últimas 5 palabras claves, etc. Asimismo, se deben establecer, como topes máximos, los siguientes recaudos: desactivar la terminal luego de 3 intentos de accesos fallidos, desconexión por inactividad de la terminal a los 30 minutos, intervalo de caducidad automática de las claves a los 30 días, etc.

6.4. El sistema de seguridad debe mantener los archivos de claves o "passwords" encriptadas, generar reportes de auditoria sobre intentos de violaciones, el uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales, los que deberán mantenerse en archivo durante 3 años, utilizando para ello soportes de almacenamiento no reutilizables (papel, CD, disco óptico u otras tecnologías de esa característica).

El administrador de la seguridad lógica es el responsable primario del control y seguimiento diario y formal de estos archivos y reportes.

6.5. Debe restringirse el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, dejando documentado cuando ello ocurra.

6.6. El esquema de seguridad debe incluir una apropiada separación de los ambientes de desarrollo y mantenimiento de sistemas y operaciones (producción), no permitiendo el ingreso de analistas y programadores al entorno productivo, ni de operadores al ambiente o a las herramientas de desarrollo.

6.7. La puesta en producción de los programas debe ser realizada por personal que no tenga relación con el área de desarrollo y mantenimiento de sistemas, mediante un procedimiento que garantice la correspondencia entre los programas "fuentes" y "ejecutables".

7. Continuidad del procesamiento de datos.

7.1. Deben existir procedimientos de resguardo de datos ("backups"), conteniendo una planificación detallada con la cantidad, frecuencia, lugares apropiados de almacenamiento tanto internos como externos, inventarios detallados, responsable y forma de la administración de los medios magnéticos. Estos procedimientos deben prever, como mínimo, la generación de 2 copias de resguardo, manteniendo el almacenamiento de una de ellas en un edificio ubicado a una distancia razonable del centro de procesamiento.

7.2. Los periodos de retención de los resguardos de datos y programas (diarios, semanales, mensuales, "software" que los administra, etc.) deben asegurar su recuperación ante cualquier inconveniente de procesamiento que se presente.

Asimismo, los respaldos de información contable (datos filiatorios, saldos al inicio del mes, movimientos, etc.) deben mantenerse disponibles, por duplicado y en condiciones de ser procesados, durante 10 años.

7.3. Se deben realizar pruebas formales y debidamente documentadas de recuperación y de integridad de los resguardos de datos ("backups")

7.4. Se debe contar con un plan de contingencias/ emergencias, probado en forma integral como mínimo anualmente, que establezca con claridad y precisión los cursos de acción a seguir, los tiempos, las responsabilidades, los archivos, las telecomunicaciones y todos aquellos recursos necesarios para lograr la continuidad del procesamiento, ante una situación que afecte el normal desarrollo de las tareas de producción.

7.5. Se debe disponer de equipamiento alternativo (propio o por convenios formales con terceros) para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales. Deberá estar localizado en un edificio ubicado a una distancia razonable del centro de procesamiento.

7.6. Las instalaciones deben tener una apropiada seguridad física y ambiental, con adecuados controles de acceso. Se debe permitir el acceso al área de procesamiento solo a personal autorizado y en ella no debe haber material combustible innecesario. Deben instalarse controles de detección automática de humo/ calor y elementos para la extinción de incendios.

Los listados y documentación de datos, programas y sistemas deben estar resguardados con adecuadas medidas de seguridad, como así también debe existir un procedimiento para determinar su destrucción o desecho, una vez cumplido su periodo de retención.

8. Teleprocesamiento y telecomunicaciones.

8.1. Se deben establecer mecanismos de protección de los datos que se transmiten por la red de telecomunicaciones, mediante técnicas adecuadas de encripción por "hardware" y/o "software".

8.2. Se debe contar, dentro de las redes de telecomunicaciones, con un "software" debidamente administrado, a fin de proveer una adecuada seguridad para los accesos a las redes, los cambios a su sistema operativo y el monitoreo de la actividad que se desarrolla en ellas.

9. Sistemas aplicativos.

9.1. Las operaciones activas y pasivas deben registrarse, administrarse y procesarse en los sistemas aplicativos correspondientes, no pudiendo registrarse/ administrarse ninguna operación en forma manual, en planillas de cálculo o con otros "software" utilitarios.

Para el caso de nuevos servicios o productos, la entidad contara con un periodo máximo de 90 días corridos, a partir de la primera operación, para registrar/ administrar estas operaciones en los sistemas aplicativos correspondientes. En estos casos deberán contar con la autorización formal del comité de sistemas de la entidad y su comunicación al área de auditoria interna.

9.2. Por cada sistema aplicativo, se debe mantener actualizada la documentación técnica que contenga, como mínimo: objetivos, alcances, diagrama del sistema, registro de modificaciones, lenguaje de programación, propiedad de los programas fuentes, problemas o limitaciones conocidas, descripción del "hardware" y "software" utilizados, su interrelación con las

redes de telecomunicaciones, descripción de las pantallas que permiten la modificación directa de datos de producción (cambio de parámetros, formulas, tasas, datos, etc.).

9.3. En los archivos de las aplicaciones correspondientes a operaciones pasivas, deben figurar individualmente los datos filiatorios (apellido y nombre, CUIT/ CUIL/ CDI, en este último caso, cuando corresponda, número de documento, etc.) de todos los titulares de cada una de las cuentas.

9.4. Todos los sistemas aplicativos deben emitir diariamente un listado ordenado por sucursal y cuenta, con los movimientos "fecha-valor" procesados, los que deberán ser mantenidos en archivo durante 3 años, a los efectos de su posterior revisión por los responsables del control. Cuando no exista este tipo de movimientos, en el listado deberá figurar una leyenda que indique esta situación.

9.5. Deben contar con un sistema de información de gestión para ser utilizado por las máximas autoridades en la toma de decisiones, que obtenga e integre en forma totalmente automatizada los datos que residen en los archivos o bases de datos de sus aplicaciones.

9.6. El sistema de contabilidad debe tener controles necesarios para impedir el ingreso de asientos diarios desbalanceados, dar de baja cuentas que tengan o hayan tenido saldos durante el ejercicio, dar de alta cuentas con saldo sin la contrapartida correspondiente, modificar saldos de cuentas sin movimientos y otras registraciones de esta naturaleza.

9.7. El periodo máximo para el ingreso de asientos "fecha- valor" en el sistema de contabilidad es de 5 días para el personal que debe ingresar movimientos contables normalmente. Superado dicho plazo y dentro del mes abierto (aproximadamente 40 días corridos para las entidades que no tienen filiales en el exterior y 60 días corridos para aquellas que las tengan), se deberán ingresar transacciones solo con autorización de la máxima autoridad contable de la entidad, expresada con su firma y sello en los comprobantes correspondientes y la utilización de su clave de acceso personal ("password"), o en su defecto con autorización de un funcionario designado por el gerente general, de acuerdo con lo que dispongan las normas aprobadas por el directorio o autoridad equivalente de la entidad. En estos casos, deben ser notificadas las auditorias internas y externas.

9.8. El periodo máximo para el ingreso de movimientos "fecha-valor" en los sistemas aplicativos es de 5 días.

9.9. Las entidades deben contar con sistemas automatizados de generación de información al Banco Central de la República Argentina, evitando el reingreso o intercambio no automatizado de datos entre distintos ambientes.

En los casos en que se deba producir ingreso manual de información, por no residir esta en sus archivos, ello debe ser realizado a través de programas específicos, en un entorno de seguridad apropiado, en archivos independientes, sin posibilidad de modificar la información ya generada en forma automatizada.

La Superintendencia de Entidades Financieras y Cambiarias verificara especialmente que la información correspondiente a la clasificación de la cartera de consumo se debe generar en forma automatizada y no debe existir la posibilidad de modificarla para mejorarla, sin perjuicio de la aplicación en el futuro de esa restricción a otras informaciones.

9.10. Se debe contar con un archivo con "clave de cliente único" de manera que permita establecer correctamente la totalidad de las operaciones pasivas y activas de cada cliente en la entidad.

9.11. Se debe establecer un procedimiento de control centralizado que permita verificar periódicamente la efectivización, por parte de las sucursales, del cierre de cuenta de los firmantes de cuentas corrientes inhabilitados por el Banco Central de la República Argentina.

9.12. La información al Banco Central de la República Argentina de los cheques rechazados y sus firmantes debe generarse automáticamente por el mismo sistema aplicativo que administra las cuentas corrientes o por un subsistema que tome automáticamente los datos generados por este sistema. En los casos en que el cheque no haya sido firmado por todos sus titulares, los que no firmaron deberán ser eliminados en un proceso posterior.

10. Sistema de transferencias de fondos (SWIFT, MEP, otros) y cámaras compensadoras electrónicas.

10.1. Los sistemas que se utilicen para la transferencia de fondos deben cumplir con los requisitos mínimos de controles internos establecidos en los puntos anteriores, en lo que se refiere a la seguridad física y lógica y operación de los equipos.

10.2. No deben existir usuarios con atributos simultáneos de ingreso, verificación y/o envío de mensajes, a fin de poder asegurar un adecuado control por oposición de intereses. Se deberán designar responsables individuales por cada uno de los atributos mencionados.

10.3. Los listados que reflejen la actividad diaria deberán ser controlados y mantenidos en archivo durante 10 años, a efectos de su posterior revisión por los responsables del control y en virtud de las normas contables legales.

11. Cajeros automáticos, banca telefónica y "home banking".

11.1. Los cajeros automáticos ("ATM's") que conformen una red administrada por una entidad y/o por terceros, deben funcionar en un esquema de proceso en tiempo real y conexión directa ("on - line") con el computador que administra la red y la base de datos que opera.

11.2. En caso de interrupción del vinculo, entre un cajero automático y el computador que lo administra, el cajero deberá quedar fuera de servicio para todo tipo de transacciones monetarias hasta la normalización del proceso.

11.3. La apertura de los cajeros automáticos debe ser realizada por dos personas, dejando constancia escrita en un acta de su Participación y resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, etc.

11.4. En las transacciones cursadas por cajeros automáticos que impliquen movimientos de fondos, se deberá emitir el comprobante correspondiente o, como mínimo, se deberá dar la opción al usuario para que se imprima o no el mismo.

11.5. Los cajeros automáticos, en todos los casos, deberán imprimir, en tiempo real, un listado o cinta de auditoria, en la que quede reflejada toda su actividad (consultas, transacciones, mensajes del "software" y censores, etc.) con detalle de fecha, hora e identificación del cajero automático.

11.6. Se debe generar un archivo en soporte magnético, con todas las transacciones y mensajes del sistema, para uso de los responsables del control y auditoria. Este archivo debe reunir todas las condiciones de seguridad e integridad con el fin de garantizar su confiabilidad y mantenerse disponible durante 5 años.

11.7. Se deberán fijar medidas para establecer apropiadamente la "clave de identificación del cliente" ("PIN") y el mantenimiento de su confidencialidad, debiendo estar encriptados en todos los lugares en que se aloje o transmita y restringir su acceso con apropiados y justificados niveles de seguridad.

Asimismo los programas, archivos y medios magnéticos que contengan formulas, algoritmos y datos utilizados para calcular el "PIN" deben estar sujetos a las mismas condiciones de seguridad.

11.8. El procedimiento de embozado de tarjeta y generación de "PIN" debe contemplar una adecuada separación de funciones a fin de no concentrar en un mismo sector o funcionario ambas actividades.

11.9. Los procesos de generación e impresión de los "PIN" deben asegurar que estos no aparezcan impresos en forma visible y/o asociados al número de cliente, ni se puedan visualizar por pantalla, a fin de garantizar su confidencialidad.

11.10. Los "PIN" y las tarjetas no deben ser entregados en forma conjunta, sino formar parte de procedimientos separados.

11.11. Los sistemas que requieran "PIN" para ser utilizados, deben restringir el acceso del cliente después de, como máximo, tres intentos fallidos.

11.12. La entidad debe proveer al cliente de un número de transacción por cada operación cursada.

11.13. Los sistemas de banca telefónica que realicen operaciones de movimientos de fondos, no pueden funcionar basándose en que el cliente tenga que comunicar su "PIN" a un interlocutor humano.