BANCO CENTRAL DE LA REPUBLICA ARGENTINA

COMUNICACION " A " 2575 I 21/08/97

A LAS ENTIDADES FINANCIERAS:

Ref.: Circular
CAMCO 1 - 90
Cámaras Electrónicas de Compensación. Homologación técnica

Nos dirigimos a Uds. para comunicarles las condiciones de homologación técnica que las Cámaras Electrónicas de Compensación deben reunir para el inicio de sus actividades, de acuerdo con los términos de la Sección 5 "Requisitos de homologación técnica" de la Comunicación "A" 2557.

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Alejandro L. Saravia
Subgerente General
de Informática y Organización

Hector O. Biondo
Subgerente General
de Operaciones

ANEXO

- INDICE -

I - Capacidad de Operación

1. Disponibilidad del Sistema

Debido a la naturaleza del ciclo de procesamiento de medios de pagos, es imprescindible que cada Cámara Electrónica cumpla diariamente con los horarios de corte de procesos definidos en los documentos de Modelo y Diseño Conceptual de cada producto.

Sus sistemas deberán estar disponibles en forma adecuada para que sus entidades adheridas puedan intercambiar la totalidad de sus transacciones dentro de las ventanas de operación definidas.

Una Cámara Electrónica debe ser capaz de procesar todas las transacciones dentro de la ventana de operación diaria en un 99% de los días del año. Asimismo el 1% restante deberá procesarse con una demora de no más de dos horas respecto a la ventana de operación diaria.

El Sistema de Compensación Electrónica de Medios de Pago de Bajo Valor necesita ser altamente confiable y disponible, por lo que resulta conveniente que la Plataforma de Ejecución de la Cámara Electrónica sea tolerante a fallas, de manera tal de asegurar que problemas eléctricos, roturas de discos, fallas de hardware o errores de usuarios, no afecten al Sistema.

El sistema debe asegurar una alta disponibilidad y confiabilidad. Por tal motivo, debe contemplarse en el diseño de cada estrato de su arquitectura la incorporación de la redundancia suficiente.

2. Ajuste del sistema a los estándares definidos para la red del B.C.R.A. (STAF)

Dado que la liquidación final de la operatoria se realiza sobre el Sistema MEP del B.C.R.A., debe ajustarse la conectividad del sistema a los estándares en uso. Los mismos cubren:

- Protocolo de red
- Seguridad (acceso y encripción)
- Servicios (transacciones, transferencia de archivos y correo)
- Ventanas de tiempo

Para el estado actual de la red STAF rige lo especificado en el reglamento de uso, operación y contrato de adhesión.

Para el futuro esquema transaccional regirán las siguientes especificaciones técnico funcionales:

- Protocolo de red: TCP/IP
- Seguridad (acceso y encripción): encripción de IP, sistema de gestión de control de acceso por claves y adhesión a proyecto KERBEROS para la validación de los recursos a ser usados por las aplicaciones
- Servicios:
  .Transacciones según estándares ISO8583, UNEDIFACT, NACHA y propia del B.C.R.A.

.Transferencia de archivos con protocolo a determinar
.Integración de mensajería de correos electrónicos bajo norma X.400

- Ventanas de tiempo: las definidas por las aplicaciones y procedimientos de operación del futuro esquema

3. Ajuste del sistema al estándar de comunicación fijado para el esquema de interconexión entre cámaras electrónicas

- Protocolo de red
- Seguridad (acceso y encripción)
- Servicios (transacciones, transferencia de archivos y correo)
- Ventanas de tiempo

4. Capacidad de resguardos (Cintas/Cartriges)

- Velocidades de transferencia de dispositivos adecuadas para la toma de resguardos en la ventana de proceso
- Procedimiento para la toma de resguardos de sistema operativo y aplicativos
- Estructura organizativa para el mantenimiento de los resguardos

5. Capacidad de proceso

- Capacidad de procesamiento suficiente para cumplir con la rutina de sistemas en la ventana de tiempo operativa
- Capacidad de reserva en tiempo de CPU no consumido, capacidad libre en discos, memoria (no usada), etc. no menor del 30%, para el caso de sobreexigencias puntuales
- Sistema de control de uso del sistema para determinar el nivel de utilización de los parámetros vitales, que permita como mínimo:
  . Adelantarse a problemas potenciales de falta de capacidad o detección anticipada de "cuellos de botella"
  . Adquirir los datos de entrada al planeamiento de capacidad
- Procedimiento para el seguimiento de las estadísticas de uso
- Estructura organizativa para la toma de decisiones en el planeamiento de capacidad

6. Manejo de volumen crítico de transacciones

- Capacidad para procesar el máximo número de operaciones
- Sistema de monitoreo y control de transacciones

7. Provisión de energía

- La instalación debe estar dimensionada para no menos de un 100% de sobrecarga instantánea (surge)
- UPS que asegure funcionamiento continuo de las partes del sistema definidas como críticas, en forma ininterrumpida sobre la ventana de recuperación en instalación alternativa co-

mo mínimo. La capacidad de recuperación de UPS debe ser acorde con las ventanas de tiempo definidas

- Sistema de monitoreo de equipos e instalación eléctrica:
  . Energía eléctrica alternativa (UPS y Generadores):
    -funcionamiento continuo de las partes del sistema definidas como críticas
    -capacidad suficiente para mantener en operación ininterrumpida frente a fallas de alimentación principal
    -sistema para el monitoreo de equipos de energía alternativos
- Estructura organizativa y procedimientos de mantenimiento y operación

8. Comunicación con Sitio Alternativo de Procesamiento (SAP)

Diseño de red que permita operar con cambios mínimos en los sistemas en caso de fallas.

9. Capacidad de administración y monitoreo centralizado del sistema

- Política para el manejo y ajuste de capacidades
- Integración del control del sitio alternativo de procesamiento
- Procedimientos y estructura organizativa para la administración de la red
- Herramientas de administración de la red
- Procedimientos para el seguimiento del uso de la red

10. Servicios de mantenimiento de equipos y sistemas

- Contratos de mantenimiento y política de manejo de problemas
- Sistema de registro de fallas
- Control de reparaciones y seguimiento de problemas

11. Capacidad de carga de datos en forma alternativa

- Procedimientos alternativos de carga en caso de fallas en los subsistemas de ingreso de datos
- Procedimientos alternativos de comunicaciones para el caso de fallas en el medio de acceso principal

II. Condiciones de Seguridad

Las Cámaras Electrónicas deberán garantizar la seguridad del sistema a fin de proteger la información, evitando su uso y divulgación no autorizada, su modificación, daño o perdida.

1. Comunicaciones

Se requiere que la información transmitida a través de los enlaces que interconectan las distintas Cámaras Electrónicas entre si y estas con sus entidades financieras clientes, sean encriptados. Para ello deben considerarse tres aspectos:

- Intercambio de claves de encripción
- Mecanismo de encripción de los datos
- Autenticación de la información.

Se deberá utilizar el sistema de encripción de clave pública RSA (Rivest, Shamir y Aldeman). El tamaño de las claves públicas deberá ser de no menos de 1024 bits. Las mismas deberán ser actualizadas con una frecuencia de una vez por año.

La tecnología de autenticación que usa RSA debe soportar el estándar MD5 para la firma electrónica. Este mecanismo define como se agrega una firma electrónica a un mensaje o archivo encriptado. La adición de esta información a un archivo habilita que la fuente pueda ser autenticada y asegura que el contenido no haya sido modificado desde el momento en que el usuario autenticado lo envió.

La encripción de los datos mismos (los archivos de transacciones) será el estándar DES de múltiples capas. Estos mecanismos soportan claves de tamaño variable y tienen una velocidad de procesamiento adecuada para la encripción de los archivos de lotes de transacciones.

Por razones de seguridad y facilidad de administración, la Cámara Electrónica mantendrá la responsabilidad de administrar las claves para sus entidades financieras clientes. Cada participante podrá definir si la encripción la realizara por software o hardware en su Centro de transmisión.

2. Lógica

En las aplicaciones de una Cámara Electrónica deberán existir mecanismos para evitar accesos y modificaciones de transacciones no autorizados, doble procesamiento y pérdida de operaciones, garantizando el cumplimiento de la confidencialidad, disponibilidad e integridad de los datos.

La seguridad del sistema a nivel de arquitectura de computación deberá incluir como mínimo:

- Manejo de facilidades estándar de seguridad, tales como caducidad de contraseñas, time-out de terminales, etc.
- Control del acceso lógico a las aplicaciones, permitiendo que

todos los usuarios autorizados, y solo ellos, puedan acceder a los recursos apropiados
- Autenticación de la fuente de todas las transacciones
- Rastreo de auditoría del uso de aplicaciones y/o utilitarios del sistema y un mecanismo de recuperación ("rollback")
- Control de duplicación de transacciones, archivos y/o procesos
- Seguridad lógica a nivel de sistemas operativos
- Seguridad lógica para otros componentes de la arquitectura de sistemas tales como el Sistema de Gestión de Base de Datos y el Monitor de Transacciones en línea
- El ambiente de producción de la Cámara Electrónica deberá estar separado de los ambientes de desarrollo y de cualquier otro ambiente de producción que pudiera existir en el mismo sistema

3. Física

Los centros de procesamiento electrónico de datos (principal y alternativo), deberán contar con un esquema completo de seguridad física. Esto incluye como mínimo:

- Seguridad en general del edificio
- Control de acceso al ámbito de sistemas
- Sistema de detección, aviso y extinción, tales como detectores de humo/calor, extintores, alarmas, etc.
- Contratos de mantenimiento de hardware y software

III. Plan de contingencias

Ante la ocurrencia de un evento que imposibilite el procesamiento de la Cámara Electrónica, esta deberá restablecer el servicio desde su lugar habitual o su sitio de operación alternativo (hot-site), debiendo completar el ciclo de procesamiento con una demora de no más de dos horas respecto a la ventana de operación diaria.

El sitio de operación alternativo deberá estar ubicado a una distancia razonable del centro principal, tal que adicionalmente se cubran contingencias de tipo natural y tumultos.

La instalación de back-up deberá estar lo suficientemente alejada como para utilizar otra fuente de alimentación eléctrica (despacho de cargas distinto), provisión de comunicaciones desde un centro de servicio diferente y estar libre de cualquier desastre natural que pudiera afectar al centro de procesamiento principal.

Cada Cámara Electrónica deberá tener planes formales y aprobados de contingencia para asegurar el servicio continuo de procesamiento de datos los que, como mínimo, deberán contemplar:

- Testeos en forma completa, por lo menos, dos veces por año
- Todas las aplicaciones críticas
- Todos los equipos mainframes, minicomputadores, redes y
- computadores personales que intervengan en la operación habitual
- Designación y comunicación de las responsabilidades del personal para la atención de la contingencia
- Recuperación automática de los datos y aplicaciones en el equipo alternativo
- Recuperación y direccionamiento de los vínculos de teleproce-samiento y/o comunicaciones
- Disponer, en el centro alternativo, de todos los insumos necesarios para la producción

IV. Otros

1. Propiedad de los programas fuentes

Si el servicio de procesamiento electrónico de datos fuera realizado por un proveedor externo, deberá aclararse expresamente en el contrato que regula la relación entre el proveedor y la Cámara Electrónica, como continuará esta normalmente con sus procesos si eventualmente el proveedor dejara de operar en el mercado o de prestar sus servicios.

2. Resguardos de datos

Se deberá realizar el resguardo de los datos procesados diariamente por las Cámaras Electrónicas como sigue:

- Obtención de dos copias de la información procesada
- Almacenamiento en lugares seguros, ignífugos y físicamente separados a una distancia razonable
- Testeos y recuperos periódicos en forma aleatoria para asegurar la calidad del contenido de los resguardos

3. Auditoría de Sistemas

Deberán contar con una auditoría de sistemas la cual cumplirá un programa continuo de trabajos basado en un análisis de riesgos, con el objeto de analizar, detectar y avisar los peligros que conlleva el funcionamiento de la Cámara Electrónica.

4. Comités de Crisis

Deberán contar con dos equipos permanentes con capacidad resolutiva que tendrán a su cargo el manejo de la situación de crisis vinculada con: a) dificultades de los miembros para liquidar sus saldos y b) inconvenientes técnicos en el procesamiento de la información.

5. Normas y procedimientos

Formalizarán su funcionamiento mediante manuales y/o normas y procedimientos que deberán contener como mínimo:

- Manual de funciones y responsabilidades
- Metodología para el desarrollo y mantenimiento de aplicaciones, incluyendo prueba e implantación de sistemas y participación del usuario
- Documentación de los sistemas
- Normas y procedimientos para la puesta en marcha de programas en producción
- Procedimiento para requerimientos de usuarios
- Normativa de operaciones de los procesos
- Documentación de los procesos/sistemas
- Normas y procedimientos sobre resguardos de datos

- Documentación de la red de telecomunicaciones
- Normas y procedimientos sobre seguridad física
- Normas y procedimientos sobre administración, seguimiento y control de la seguridad lógica
- Procedimientos de recuperación operativa y operación critica ante contingencias