

INFORME SINTETICO DE AUDITORIA

Código del Proyecto: 4.24.00.00

Nombre del Proyecto: *Auditoría general del hardware y la
seguridad en el Banco de la Ciudad de Buenos Aires.*

AÑO 2000

Subproyecto: *Comunicaciones e intercambio de datos
con el GCBA.*

Buenos Aires, 17/4/2002

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

Av. Corrientes 640 piso 5º Capital Federal

Presidente

Dr. Vicente Mario Brusca

Auditores Generales:

Dr. Jorge Argüello

Dr. Nicolás Corradini

Dra. Noemí Fernández Cotonat

Dr. Daniel Rodríguez

Dra. Gabriela Serra

Dr. José María Pazos



CODIGO DEL PROYECTO: 4.24.00.00

NOMBRE DEL PROYECTO: Auditoría general del hardware y la seguridad en el Banco de la Ciudad de Buenos Aires.

SUBPROYECTO: Comunicaciones, intercambio de datos con el GCBA e interfaces internas.

PERÍODO BAJO EXAMEN: Enero a Septiembre de 2001

FECHA DE PRESENTACIÓN DEL INFORME:

EQUIPO DESIGNADO:

Director de Proyecto: Dr. Ricardo Martín

Supervisor : Dra. Claudia Sencio

Auditores : Ing. José Recasens, Héctor Zancada,
Ing. Rodolfo Bella, Oscar Ciarlotti y
Lic. Francisco Camean Ariza

OBJETIVO: Auditoría de sistemas informáticos que permita evaluar la seguridad de las comunicaciones y los métodos de intercambio de información con el GCBA.

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047

I. OBJETO DE LA AUDITORIA

Revisión de la organización, administración y seguridad de las comunicaciones de datos de la red digital del BCBA, y el intercambio de información entre el Gobierno de la Ciudad de Buenos Aires (GCBA) y el Banco de la Ciudad de Buenos Aires (BCBA).

II. ALCANCE

El examen fue realizado de conformidad con el siguiente marco normativo:

- Normas de auditoría externa de la AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES (A.G.C.B.A), aprobadas por la Ley N° 325 y las Normas Básicas de Auditoría Externa aprobadas por el Colegio de Auditores de la Ciudad de Buenos Aires según Resolución N° 161/00 –AGCBA.
- Normas emitidas por el Banco Central de la República Argentina (BCRA) estableciendo los requisitos operativos mínimos del Área de Sistemas de Información de las Entidades Financieras.
- Restantes normas detalladas en Anexo I.

El trabajo de auditoría relacionado con este Subproyecto fue desarrollado, conjuntamente con el de las restantes etapas del Proyecto, en el período comprendido entre el 1° de enero y el 30 de septiembre de 2001. Los resultados de las pruebas ejecutadas fueron notificados y confirmados con la Gerencia de Sistemas a la fecha de elaboración del presente informe. En el anexo II se detallan los procedimientos aplicados.

Para evaluar la red, los equipos de comunicaciones, racks, cableado, encriptadores y medidas de seguridad fueron seleccionadas las siguientes áreas:

- Centro de Cómputos (DPD), sito en Esmeralda 664.
- Gerencia de Sistemas, ubicada en Sarmiento 630.
- Sucursales N° 35 (La Lucila), N° 22 (Once), N° 14 (Barracas) , N° 12 (Centro) , N° 52 (R.S Peña 541) y N° 45 (25 de Mayo y Sarmiento), seleccionadas al azar.

III. LIMITACIONES AL ALCANCE

No se ha tenido acceso a la siguiente información y/o documentación:

CORRIENTES 640, PISO 5° - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047

- Normas de procedimiento estipulando los mecanismos a seguir para el intercambio de información entre el BCBA y el GCBA. La mencionada normativa fue solicitada en forma verbal durante el relevamiento practicado y mediante nota sin número elevada por el equipo de trabajo a la Gerencia General con fecha 03/07/01.

Los mencionados elementos fueron suministrados junto con el descargo presentado por la Sindicatura del Banco, de fecha 12/03/02. Las Normas de Procedimiento acompañadas fueron dictadas en el mes de diciembre de 2001, esto es, tres meses después de la finalización de las tareas de campo de este proyecto de auditoría, razón por la cual ameritan un detallado análisis en el seguimiento que sobre este trabajo se diponga.

IV. ACLARACIONES PREVIAS

En Anexo III se expone el diagrama general de la red de comunicaciones vigente y en Anexo IV un esquema detallado; adicionalmente se destacan los siguientes aspectos que surgen del relevamiento realizado:

- El BCBA dispone de un anillo de fibra óptica¹ que vincula el Centro de Cómputos (DPD), la Casa Matriz y el Área de Desarrollo y Mantenimiento de los Sistemas, ubicado en Sarmiento 630, áreas que constituyen los tres nodos principales. Las Sucursales se conectan con este anillo a través del vínculo digital provisto por la firma IMPSAT S.A., proveedor externo que tiene también a su cargo el encriptado entre nodos.
- Los nodos principales se encuentran enlazados² mediante fibra óptica de alta velocidad (2 Megabits por segundo); el anillo proporciona caminos alternativos en caso de caída de alguno de los vínculos. Por otra parte, la comunicación de los nodos principales con las sucursales se efectúa con enlaces de menor velocidad (128/256 kb por segundo).
- La red de comunicaciones se encuentra dividida en dos subredes en forma lógica, estableciendo los siguientes vínculos:
 - Cajeros automáticos (ATM) con el DPD y la red LINK, utilizando el protocolo X25 con frame relay.
 - Las Sucursales con el DPD, los tres nodos principales entre sí, y las comunicaciones con entes externos (BCRA, tarjeta de crédito VISA y otros).
- El acceso lógico a la red está administrado a través de la plataforma Windows NT, concentrando los permisos en un equipo residente en el DPD.

¹ Cable compuesto por material de vidrio o transparente que permite la transmisión de un rayo de luz o rayo láser. Se utiliza para la transmisión de información a grandes velocidades y distancias.

² Conexión física (cable directo o medio compartido) entre dos nodos o dispositivos de red.

- El acceso a Internet³ es provisto por la firma Vía Network S.A. a través de líneas telefónicas; adicionalmente provee asiento en el Sitio Web y el servicio "Housing", que consiste en el mantenimiento de un servidor Web del banco en oficinas del proveedor (ISP, Internet Service Provider).
- El vínculo entre los equipos "Stratus Continuum" se encuentra duplicado, a través de fibra óptica y radio enlace. Por otra parte, el vínculo entre la Sucursal N° 22 (Once) y el DPD (Esmeralda 664) dispone de una conexión redundante vía radio enlace y tiene una velocidad de 2 Mb.
- Los cajeros automáticos "neutrales" (que funcionan fuera de las sucursales) poseen una conexión redundante en prevención de la caída del vínculo principal.
- Cada sucursal dispone de un servidor Windows NT Server que administra la comunicación local, y de un vínculo redundante punto a punto como solución alternativa a la caída del principal, provisto por IMPSAT.
- La red externa del BCBA permite conectarse con las siguientes entidades: ARGENCARD, LINK, BCRA, VERAZ, AFIP, CABAL, DATANET y VISA.

V. OBSERVACIONES

1. Seguridad Física:

- 1.1. La estructura de las instalaciones es inadecuada, de acuerdo a estándares internacionales establecidos por normas ISO / IEC 11.801, agrupadas en la norma UTP, categoría 5.
- 1.2. La instalación del cableado de datos y los dispositivos de comunicaciones es insegura.

2. Seguridad Lógica:

- 2.1. Algunos SWITCHES no se encuentran protegidos con claves de acceso (password).

Con posterioridad a la finalización de las tareas de campo, y de acuerdo a lo informado por la entidad en su descargo de fecha 12/03/02, esta auditoría pudo verificar que el presente aspecto ha sido subsanado.

³ La mayor red de comunicaciones del mundo, que utiliza el conjunto de protocolos de TCP/IP (que consiste en un conjunto de servicios de red que proporcionan comunicación entre dispositivos de una red heterogénea).

2.2. Los Servicios de Red carecen de protección lógica.

2.3. Carencia de un antivirus corporativo.

3. Monitoreo de la red.

3.1. El monitoreo de la red es insuficiente, atento que el mismo no detecta tráfico excesivo ni intentos de forzar la obtención de passwords.

3.2. Tal como fuera manifestado en el punto 2.4. del capítulo Observaciones del Informe del Subproyecto "Aspectos generales vinculados con la organización, el equipamiento, la red de comunicaciones, la seguridad lógica y la tecnología informática", la entidad no dispone de software que permita efectuar un control integral de la red de comunicaciones con funciones de inventario de dispositivos conectados, administración de licencias, instalación centralizada y otros del tipo Unicenter, Tivoli o similar.

3.3. El software de monitoreo de vínculos instalado en el Centro de Cómputos, en oportunidad de la visita de esta Auditoría (16/05/01), se hallaba fuera de servicio.

4. Diseño.

Adicionalmente a las observaciones incluidas en el informe del Subproyecto: "Aspectos generales vinculados con la organización, el equipamiento, la red de comunicaciones, la seguridad lógica y la tecnología informática" sobre la existencia de números de IP⁴ públicos, falta de segmentación⁵ y utilización de Windows 98 en equipos conectados a la red, se hallaron los siguientes aspectos relativos al diseño actual:

4.1. Las computadoras personales (PC) ajenas al banco pueden conectarse a la red interna visualizando la misma y operando sin ser identificadas como equipos extraños.

⁴ Dirección utilizada para identificar en forma lógica a equipos en un ambiente de comunicaciones.

⁵ Proceso de dividir una red en varios segmentos, a los efectos de facilitar su administración, la detección de fallos, el aislamiento de sus partes, etc.



4.2. Riesgos de acceso indebido a la red a través de usuarios conectados a Internet por Dial-Up.⁶

Al día de la fecha la Gerencia de Area de Sistemas se encuentra gestionando un vínculo corporativo a Internet, ante el próximo vencimiento del contrato con el actual proveedor, Via Network.

4.3. Las impresoras departamentales pueden ser accedidas a través del servicio Web de la red interna del banco sin ninguna restricción.

5. Servicio brindado por proveedores externos.

5.1. El BCBA no administra la seguridad de sus vínculos encriptados, toda vez que la encriptación de los datos que viajan a través de la red de IMPSAT es realizada por dicho proveedor externo.

5.2. Existencia de vínculos sin encriptación.

5.3. Ausencia de contrato con la firma IMPSAT.

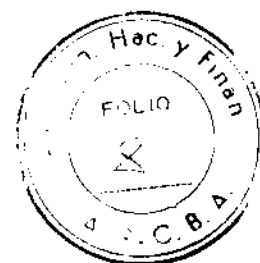
5.4. Fallas en el funcionamiento de la línea de contingencia.

6. Intercambio de información con el GCBA.

De acuerdo a lo señalado en el informe sobre el Subproyecto consignado en el primer párrafo del punto 4. precedente, la metodología utilizada para el intercambio de información con el GCBA resulta antigua e ineficiente; adicionalmente, presenta deficiencias como las que se señalan:

6.1. La entidad no puso a disposición de esta Auditoría las normas de procedimiento estableciendo el circuito a seguir para el intercambio de información sobre sueldos y pago a proveedores, a pesar de haber sido solicitadas en diversas oportunidades. La circunstancia planteada, volcada en el acápite de Limitaciones al Alcance, limita la opinión, para el presente proyecto, sobre la suficiencia y el adecuado cumplimiento de la normativa vigente.

⁶ Dial Up, o marcador automático es una comunicación que se establece utilizando la red telefónica para la transmisión de datos bajo demanda.



6.2. Sueldos.

- a) El GCBA, algunas de sus reparticiones y organismos descentralizados y/o autónomos remiten información por medio de disquetes sin encriptación y sin protección física ni lógica a la Gerencia de Relaciones con el GCBA y Organismos Públicos.
- b) Algunos organismos pertenecientes al Sector Público de la Ciudad de Buenos Aires (entre los cuales se incluye la A.G.C.B.A) no tramitan el pago de los sueldos a su personal a través de la Gerencia de Relaciones con el Gobierno de la Ciudad, sino a través de determinadas Sucursales. .
- c) La información es enviada desde la Gerencia de Relaciones con el GCBA al DPD -después de practicar un control de totales- en disquetes sin protección lógica.

6.3. Pago a Proveedores.

- a) La Gerencia de Relaciones con el GCBA dispone de un equipo perteneciente al GCBA con un módem habilitado para recibir información sobre pagos provenientes de la Tesorería.
- b) La Gerencia de Relaciones con el GCBA valida el total de los listados recibidos de las reparticiones con la información recibida por soporte magnético. El mencionado proceso no resulta suficiente para asegurar la veracidad de la información, toda vez que no detecta errores en las liquidaciones a favor de los proveedores que podrían ser compensadas, dada la debilidad planteada en el apartado precedente.
- c) No existe un proceso automatizado para la transferencia de la información de la Tesorería del GCBA al Banco. El empleo de herramientas del tipo Lotus Notes o similar permite, además de incorporar esta funcionalidad, configurar el encriptado y la transmisión compacta de la información.
- d) No se utiliza la red interna del banco para la transmisión de datos desde la Gerencia de Relaciones con el GCBA al DPD del banco.

6.4. Préstamos con retención de haberes

También en este circuito el intercambio de información con las dependencias se instrumenta a través de diskettes sin protección lógica.

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047



VI. RECOMENDACIONES.

1. Seguridad física

1.1 Prever la resolución de este aspecto en las nuevas oficinas asignadas a la Gerencia, separando el cableado de datos del eléctrico.

1.2

- a. Evaluar la alternativa de tender el cableado por piso ducto o cable canal. Respecto de las cajas de conexión, se considera conveniente que las mismas se encuentren amuradas y cumplan con los estándares de categoría 5 (CAT-5).
- b. Amurar los rack y colocar cerraduras en las puertas delantera y trasera.
- c. Idem 1.1.
- d. Reorganizar el cableado de los ATM y colocar cerraduras para imposibilitar el acceso a personas ajenas.
- e. Evaluar la posibilidad que todos los equipos de comunicaciones se encuentren alojados en racks, dotando a los mismos de adecuadas medidas de seguridad.
- f. Considerar la alternativa de alojar en un mismo rack y en una ubicación segura, el equipo de comunicaciones y el servidor NT.

2. Seguridad Lógica:

2.2

- a. Eliminar el usuario anónimo y utilizar los usuarios del NT PRINDPD para el ingreso al puerto 21 (FTP).
- b. Cerrar todos los puertos de los equipos que no sean indispensables para el funcionamiento del sistema.

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047



- c. Considerar la conveniencia de impartir instrucciones internas tendientes a que los usuarios de los equipos se abstengan de compartir sus discos y utilicen el correo electrónico como herramienta de comunicación.

2.3 Agilizar la implementación de un antivirus corporativo para evitar los efectos descriptos.

3. Monitoreo de red.

3.1 Instalar e implementar un control efectivo, por medio de un software de generación de alarmas, que posibilite la detección de tráfico excesivo en la red e intento de obtención de password .

3.2 Evaluar la alternativa de incorporar un software de administración y mantenimiento de red que permita obtener un inventario en línea de los equipos conectados a la red.

3.3 Prever que el software de monitoreo de red se encuentre encendido en forma permanente, en un lugar visible y genere una alarma sonora ante la caída de un vínculo.

4. Diseño.

4.1 Identificar el equipamiento por medio de un nombre y otras características específicas del mismo. Adicionalmente, se recomienda evaluar la posibilidad de generar un aviso cada vez que se conecte a la red un equipo ajeno al banco.

4.2 Evaluar la alternativa de negar el acceso a la red interna del banco a los equipos que accedan a Internet vía Dial Up, con el fin de evitar los efectos descriptos.

4.3 Implementar claves de acceso a todas la impresoras departamentales.

5. Servicio brindado por proveedores externos.

5.1. La Dependencia "Seguridad en Tecnologías de Información" debiera establecer un mecanismo que garantice la confidencialidad de las operaciones transmitidas a través de IMPSAT, incluso respecto de éste proveedor.

5.2. Agilizar la incorporación, a todos los vínculos de comunicaciones del banco, equipos de encriptación, de manera tal de dotar a los datos que se transmiten de la confidencialidad y seguridad exigida por el marco normativo vigente.

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047

- 5.3. Rever el vínculo establecido con el proveedor, procurando acordar un mecanismo de sanción por problemas o fallas en los servicios.
- 5.4. Revisar el correcto funcionamiento de la línea contingente, asegurando la automaticidad del proceso ante la caída del vínculo principal.

6. Intercambio de información con el GCBA

6.2. Sueldos

- a. Eliminar el uso de disquetes y utilizar el sistema de encriptación de llave pública / privada para el resguardo de la información que migre de la red interna del banco en medios magnéticos u ópticos.
- b. Canalizar por una misma Dependencia toda la información vinculada con el GCBA y el BCBA, dotando de un control centralizado a las transacciones realizadas con ese Sector.
- c. Utilizar la red del banco para la transmisión de la información.

6.3. Pago a proveedores

a) y b)

La información entre la Tesorería del GCBA y el BCBA debe ser transmitida en forma segura, utilizando técnicas de encriptación. Adicionalmente, dicha medida debe aplicarse a la información intercambiada por dial up.

c)

Evaluar la alternativa de incorporar herramientas del tipo Lotus Notes o similar, a los fines de obtener los beneficios consignados.

d)

Idem 6.2.c)

6.4. Préstamos con Retención de Haberes

Idem 6.3. a).

VII. CONCLUSIÓN

Como resultado de las pruebas realizadas han surgido algunos aspectos que afectan la seguridad física y lógica, la continuidad y calidad del servicio y la eficiencia en los procesos. Los mencionados aspectos (tratados en el Capítulo VI del precedente) pueden sintetizarse en:

- Inadecuado tendido de cables e inseguridad en las instalaciones de algunos equipos de comunicación.
- Ausencia de claves de acceso en algunos Switches, servicios de red sin protección lógica y falta de un antivirus corporativo.
- Monitoreo de red discontinuo e insuficiente y ausencia de un software que permita efectuar un control integral de los dispositivos conectados.
- Debilidades en el diseño de la red, entre las cuales adquiere relevancia el riesgo de acceso indebido de usuarios conectados a Internet por Dial-Up.
- Aspectos vinculados con el servicio brindado por proveedores externos, que impactan en la continuidad del servicio y que ponen en riesgo la confidencialidad de la información del banco.
- Procedimientos antiguos e ineficientes para el intercambio de información con el GCBA.

La adopción de medidas conducentes a subsanar estos aspectos, algunas de ellas en vías de implementación, se traducirá en mejoras en la seguridad de las instalaciones, de los equipos y de la información, dotando de mayor eficiencia al proceso de transferencia interna de esta última y a su intercambio con organismos y dependencias del GCBA.

ANEXO I

MARCO NORMATIVO

- Comunicación "A" 2659 del 23/1/98 del Banco Central de la República Argentina, sus complementarias y modificatorias: "A" 3149, "A" 3198 y "B" 6776.
- Comunicación "A" 2985 del 14/9/99 del Banco Central de la República Argentina.
- Normas y recomendaciones de seguridad establecidas por la DGEySI.
- Manual de Seguridad de Redes de la Subsecretaría de la Gestión Pública dependiente de la Jefatura de Gabinete de Ministros , utilizado en el ámbito de la Administración Pública Nacional.
- Manual de Auditoría Informática de la Sindicatura General de la Nación, SIGEN.
- Guía de Aproximación a la Seguridad de los Sistemas de Información (MAGERIT versión 1.0) del Ministerio de Administraciones Públicas de España.
- Manual de apoyo al curso "Seguridad Informática en Nuevas Instalaciones", dictado del 24/7/2000 al 28/7/2000 en la Escuela de Ciencias Informáticas (ECI) de la Facultad de Ciencias Exactas y Naturales de la UBA por el Dr. Manuel Medina de la Universidad Politécnica de Cataluña, Barcelona.
- DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria. (Evaluation Criteria).
- Ley 25326 de protección de los datos personales según texto publicado en el BO del 2/11/2000.
- Informe de la Asociación de Usuarios de Servicios Bancarios (AUSBANC)

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047

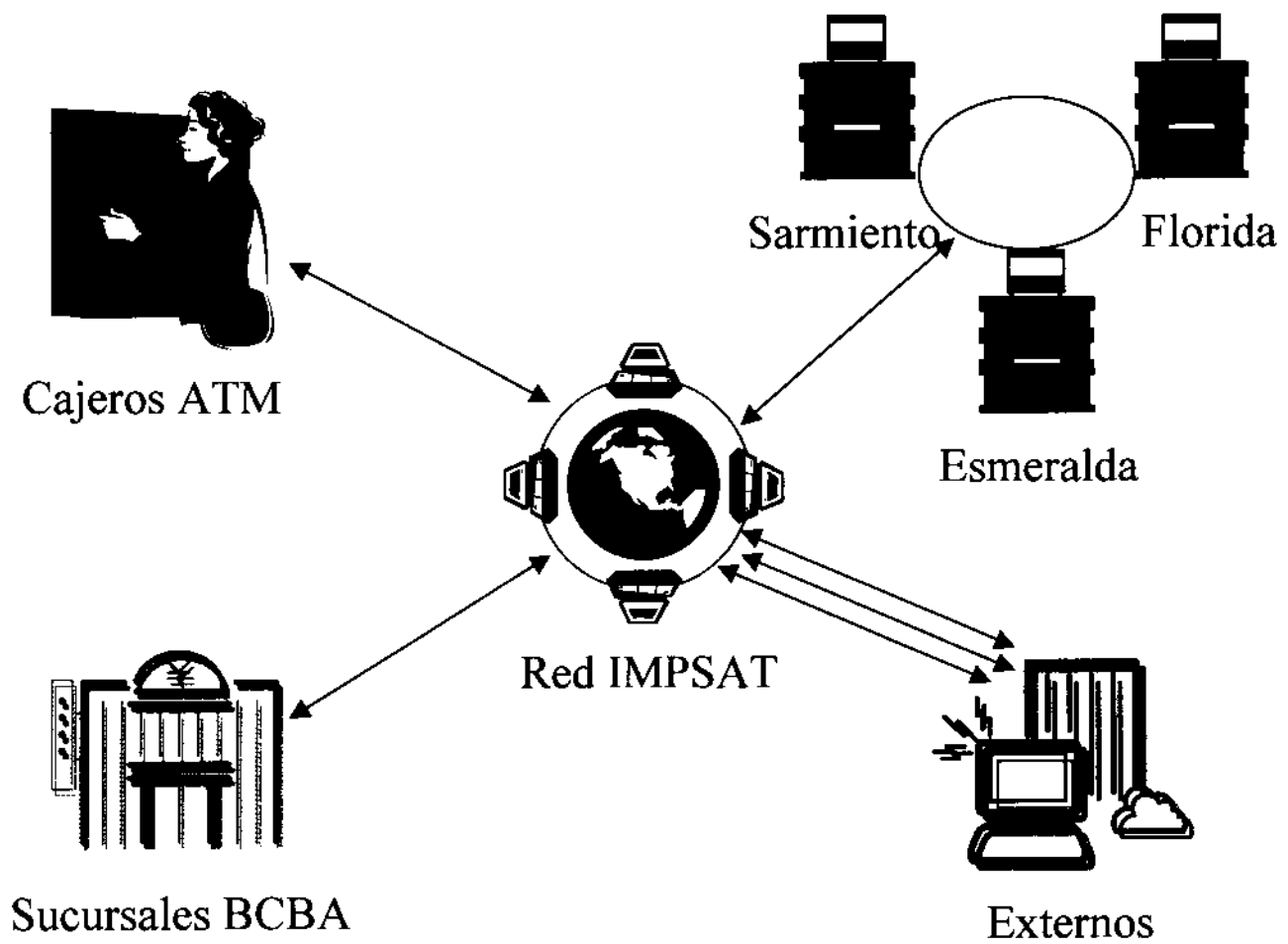
ANEXO II

PROCEDIMIENTOS DE AUDITORÍA APLICADOS

- Entrevistas con el personal jerárquico y operativo de las áreas involucradas de las Gerencias de Área Sistemas y de Seguridad en Tecnologías de Información.
- Relevamiento de las instalaciones del Centro de Cómputos (DPD) , la Gerencia de Sistemas y 4 Sucursales seleccionadas al azar (N° 35 – La Lucila, N° 22-Once, N° 14 –Barracas, N° 12 (Centro), N° 52 (R.S.Peña 541) y N° 45 (25 de Mayo y Sarmiento), seleccionadas al azar.
- Lectura y análisis de informes de Auditoría de Sistemas, elaborado por la Gerencia de Auditoría Interna.
- Obtención y análisis de Organigramas, Manuales Operativos, Normas de Procedimiento y Planes de Contingencia.
- Verificación del cumplimiento de normas internas y externas y confrontación con estándares que surgen de las normas nacionales e internacionales.
- Inspección ocular tendiente a cotejar la existencia de encriptadores en el DPD y las Sucursales.
- Revisión de los contratos formalizados con los proveedores Impsat (comunicación) y Via Networks (Servicio Internet) relacionados con la Gerencia de Área de Sistemas.
- Entrevistas con personal responsable de las áreas de soporte técnico, comunicaciones, mesa de ayuda y responsables de las sucursales.
- Revisión de los racks de comunicaciones y los equipos instalados en las sucursales N° 35 (La Lucila), N° 22 (Once), N° 14 (Barracas) y N° 12 (Centro)
- Ejecución de software de reconocimiento de redes, análisis de tráfico, auditoría de passwords, control de puertos sobre servidores y control de seguridad de switches y routers⁷.
- Realización de entrevistas con responsables de la Gerencia de Relaciones con el GCBA, relevando el procedimiento utilizado para el intercambio.
- Análisis de seguridad del sitio Web por medio de software de análisis y seguridad.

⁷ Dispositivos que realizan funciones de puente o de encaminador en la transmisión de datos, en forma individual o simultánea, pudiendo actuar como puente para algunos protocolos y encaminador para otros.

ANEXO III
ESQUEMA GLOBAL DE LA RED DE COMUNICACIONES

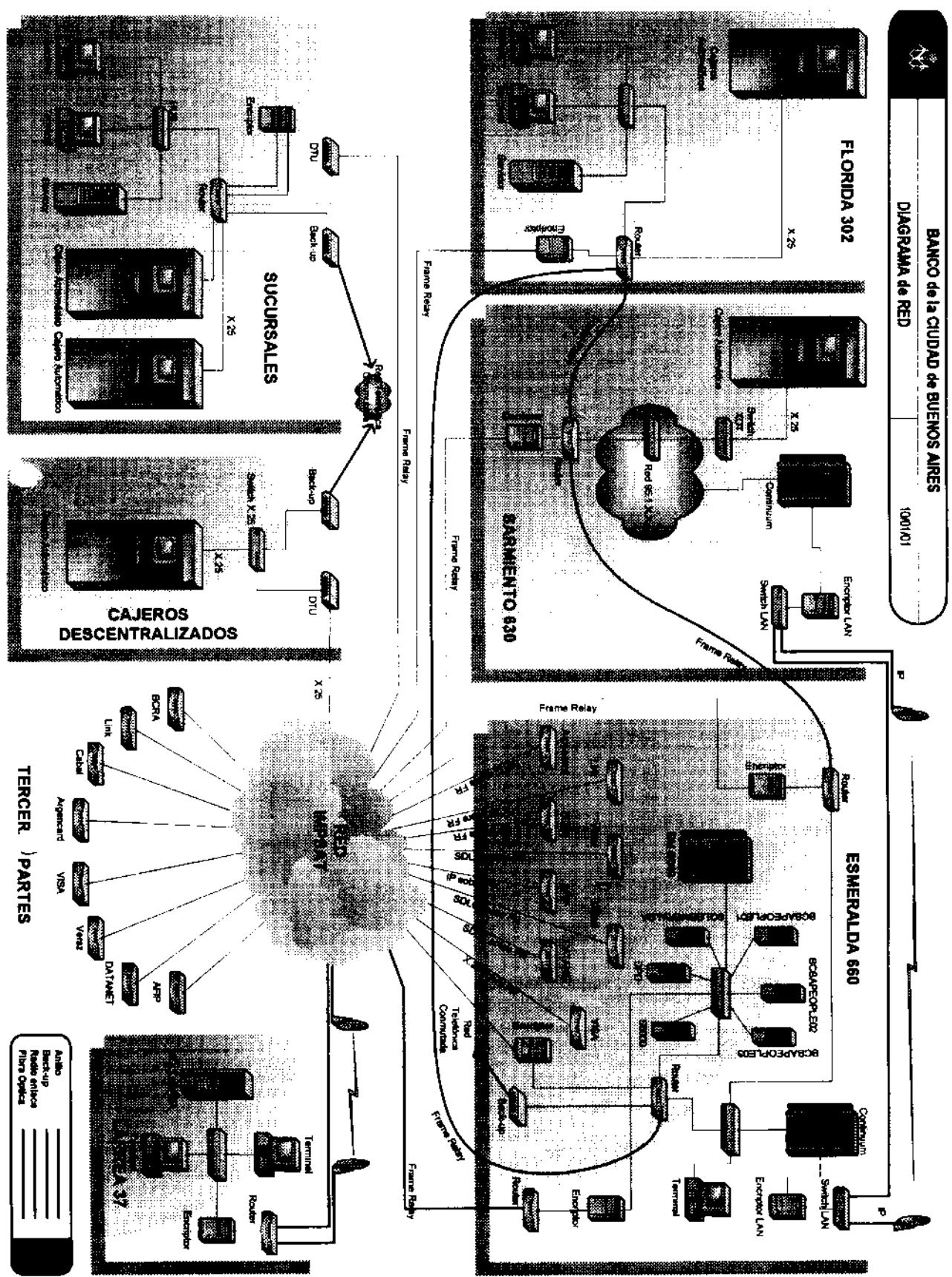


CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047



ANEXO IV
ESQUEMA DETALLADO DE LA RED DE COMUNICACIONES

CORRIENTES 640, PISO 5º - C1043AAT, CIUDAD DE BUENOS AIRES
TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047



CORRIENTES 640, PISO 5° - C1043AAT, CIUDAD DE BUENOS AIRES
 TEL. 4321-3700 / 4323-3388/6967/1796 – FAX 425-5047

ANEXO V
TIEMPOS DE CORTE DE SERVICIO POR CAÍDAS EN LOS VÍNCULOS (*)

Dependencia	Fecha y hora caída	Fecha y hora restitución	Tiempo fuera de servicio (**)	Tiempo máximo según Pliego (**)	Exceso (**)
Procuración Gral. Del GCBA	22/2/2001 11:30	23/2/2001 15:30	1,680	130	1,550
Sucursal 39	17/2/2001 12:30	19/2/2001 11:32	2,822		2,692
Sucursal 31	1/3/2001 19:20	8:04	764		634
Sucursal 31	21/3/2001 19:19	22/3/01 8:19	780		650
Sucursal 37	24/3/2001	No informado	1,092		962
Corporación rematadores	18/4/2001 9:09	19/4/2001 14:32	1,763		1,633
Argencard	31/5/2001 7:40	5/6/2001	7,200 (***)		7,070
Datanet-eds	31/5/2001 7:40	1/6/2001 11:00	980		850
Pab 19	Total mensual Mayo 2001		3,945		3,815
Sucursal 31	15/5/2001 4:57	16/5/2001 10:27	1,770		1,640
Sucursal 29	Total mensual Mayo 2001		790		660
Sucursal 58	Total mensual Mayo 2001		1,433		1,303
Argencard	Total mensual Junio 2001		6,930		6,800
Sucursal 19	Total mensual Junio 2001		238		108

(*) Fuente: Información producida por la Gerencia de Área de Sistemas con fecha 23/08/01.
 (**) En cantidad de minutos.
 (***) El proveedor no restableció el servicio durante 5 días.

