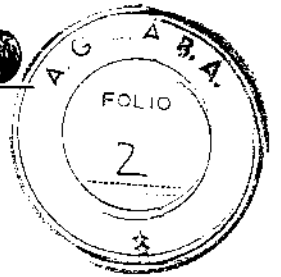




INFORME FINAL DE AUDITORIA

PROYECTO N°4.24.00.00
AUDITORIA GENERAL DEL HARDWARE
Y LA SEGURIDAD EN EL BANCO DE
LA CIUDAD DE BUENOS AIRES
AUDITORIA LEGAL Y
FINANCIERA
PERIODO 2001

Buenos Aires, Octubre de 2001



AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

PRESIDENTE

Dr. Vicente Mario Brusca

AUDITORES GENERALES

Lic. Daniel Rodríguez

Dra. Gabriela Serra

Dr. Jorge Argüello

Dr. Nicolás Corradini

Dra. Noemí Fernández Cotonat

Dr. José María Pazos

Av. Corrientes 640 piso 5º Capital Federal

CODIGO DEL PROYECTO: 4.24.00.00

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

SUBPROYECTO: Aspectos generales vinculados con la organización, el equipamiento, la red de comunicaciones, la seguridad lógica y la tecnología informática.

PERÍODO BAJO EXAMEN: enero a julio de 2001.

FECHA DE PRESENTACIÓN DEL INFORME: 9/10/2001

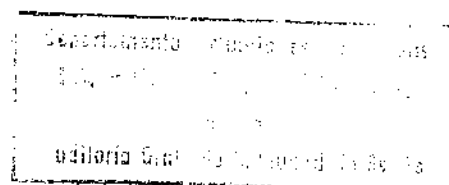
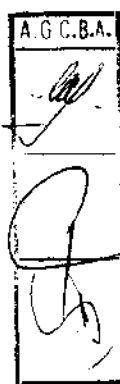
EQUIPO DESIGNADO:

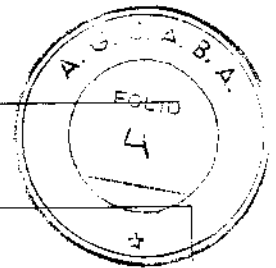
Director de Proyecto: Dr. Ricardo Martín

Supervisor : Dra. Claudia Sencio

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

OBJETIVO: Auditoria de sistemas que permita opinar acerca de la calidad del servicio, su seguridad y resguardo.





**Informe Final de Auditoría
Proyecto N° 4.24.00.00**

DESTINATARIO

**Señora
Presidenta de la Legislatura
De la Ciudad Autónoma de Buenos Aires
Lic. María Cecilia Felgueras**

En uso de las facultades conferidas por el artículo 135 de la Constitución de la Ciudad Autónoma de Buenos Aires y por la Ley 70, artículos 131, 132 y 136, la Auditoría General de la Ciudad de Buenos Aires procedió a efectuar un examen en el ámbito del Banco de la Ciudad de Buenos Aires con el objeto que se detalla en el apartado 1

I. OBJETO DE LA AUDITORIA

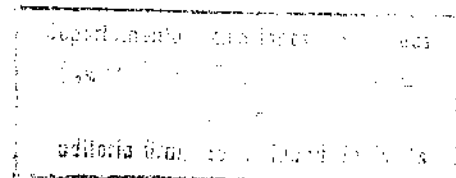
Revisión de los niveles de riesgo e identificación de situaciones y aspectos que impliquen debilidad en el sistema de control, en los equipos y la red de comunicaciones que soportan los aplicativos centrales del Banco y sus respectivos sistemas operativos, evaluando aspectos relacionados con las prestaciones, la seguridad física (acceso al Centro de Cómputos, Plan de evacuación y de Contingencias) y la seguridad lógica (perfiles de usuarios, utilización de passwords, registros de Logs y manuales operativos) respecto de las siguientes plataformas:

- IBM 390
- Stratus
- Windows NT

II. ALCANCE

El examen fue realizado en el período comprendido entre el 1° de enero y el 31 de julio de 2001 de conformidad con el siguiente marco normativo:

- Normas de auditoría externa de la AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES, 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.

Para evaluar la seguridad física, 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) y N° 12 (Centro).

En esta primera etapa la tarea se circunscribió a relevar y evaluar la organización y los aspectos generales de las áreas auditadas. No se incluyen observaciones específicas referidas a la red de comunicaciones, el nivel de servicios y tiempo de respuesta de los cajeros, las interfases con los sistemas contables y la seguridad del hardware y los ambientes operativos, aspectos que serán analizados en detalle en informes posteriores.

La tarea realizada no incluyó procedimientos sobre los aplicativos que corren en la Plataforma IBM 390, no obstante lo cual se señalan, con relación a los mismos, algunas debilidades halladas durante el relevamiento inicial de la estructura de procesamiento de la entidad.

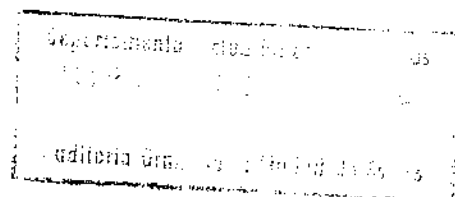
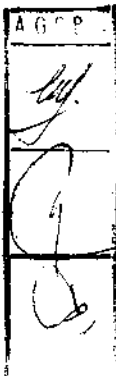
III. ACLARACIONES PREVIAS:

1. Organización

El Área de Sistemas y Tecnología Informática depende funcionalmente de un Gerente Coordinador, quien reporta en forma directa al Gerente General. Al 31/12/00 su dotación ascendía a 174 empleados, incluyendo personal efectivo, contratados y pasantes, participando en un 6.6% del total de los recursos humanos del banco. Al 30/6/01 su dotación tuvo un incremento del 13.8% respecto del cierre del último ejercicio económico finalizado el 31/12/00, dando lugar a un crecimiento de la participación del personal del Área de Sistemas en la dotación total, que llegó así al 7.3%.

La seguridad informática está a cargo de un área específica denominada Seguridad en Tecnología de la Información independiente de la Gerencia de Sistemas, que reporta en forma directa al Directorio; el esquema descrito responde al requisito de independencia exigido por la Com. "A" 2659 del Banco Central y sus modificatorias.

Dependen de la Gerencia de Sistemas las siguientes áreas:



- La Subgerencia de Aplicativos Centrales, que se encarga de los sistemas empleados para el procesamiento de los Plazos Fijos, Caja de Ahorros y Cuentas Corrientes, entre otros.
- La Subgerencia de Microsistemas, que tiene a su cargo los sistemas que operan sobre computadoras personales (PC), servicios de Internet y e-bussines.
- La Subgerencia de Tecnología, que tiene entre sus funciones el Soporte Técnico, Operaciones y Comunicaciones.
- La Coordinación de Planeamiento y Control de Gestión, que se encarga del seguimiento de los proyectos y la organización de la documentación.
- La Supervisión de Investigación, que tiene entre sus funciones principales la de evaluar la incorporación de nuevas tecnologías.

2. Estructura económica

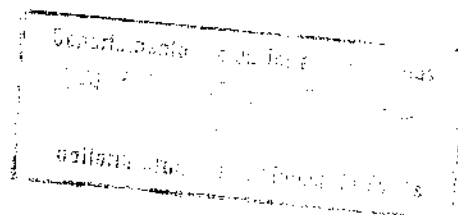
Durante el ejercicio económico finalizado el 31/12/00 la Gerencia de Sistemas generó gastos por \$ miles 15.559 (Anexo III): \$ miles 3.874 fueron imputados a amortizaciones de maquinarias, equipos y gastos de organización y \$ miles 11.685 a erogaciones que motivaron aplicaciones de fondos.

Los gastos imputados a la Gerencia de Área de Sistemas representan el 10.7% del total de los gastos administrativos del banco.

En ese mismo ejercicio el banco llevó a cabo adquisiciones de maquinarias y equipos de computación por \$ miles 2.605, y de activos relacionados a la Gerencia de Sistemas - imputados al rubro Gastos de Organización y Desarrollo- por \$ miles 2.356, guarismos que, en forma conjunta representan el 32.7 % de los saldos contabilizados en los mencionados rubros.

Para el ejercicio económico N° 125 iniciado el 1/1/01 han sido presupuestadas inversiones en tecnología informática y equipamiento de sucursales y dependencias por \$ miles 9.080, de los cuales \$ miles 5.114 tienen como finalidad la adquisición de máquinas y equipos de computación, y \$ miles 3.965, están destinados a la compra de activos correspondientes al rubro Gastos de Organización y Desarrollo; el mencionado importe representa el 40% del total de las inversiones presupuestadas para el ejercicio.

Las cifras provisionales que arrojan los estados contables del primer semestre del 2001 muestran inversiones que alcanzan a \$ miles 1.228,9 en maquinarias y equipos de computación y \$ miles 903 en activos imputados al rubro Gastos de Organización y



Desarrollo, guarismos que muestran una ejecución del orden del 24.0% y el 22.8% del presupuesto anual de ambos rubros.

3. Aspectos técnicos.

A continuación se realiza una síntesis del esquema de informatización y las comunicaciones del banco.

3.1. Centro de Procesamiento y otras Áreas informáticas (Anexo IV)

Coexisten 4 Plataformas vinculadas a través de la red

- AS 400: la entidad cuenta con 7 equipos IBM AS 400 sobre los cuales se corren algunas aplicaciones, como ser la liquidación de sueldos, las operaciones de Pignoraticio y el soporte de la Administración de Personal con el sistema Algoliq, interconectados mediante servidores centrales a la plataforma IBM 390
- Windows NT: da servicios en línea a las 44 Sucursales y a los Centros Recaudadores, soportando al Sistema Mosaic que posee una interfase gráfica. La aplicación de sucursales ha sido renovada en el año 1999 con la instalación del sistema Mosaic, y se le están haciendo continuas mejoras.

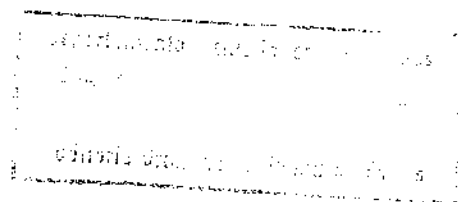
Dentro de la Plataforma NT algunos sistemas están implementándose o en vías de implementación, entre ellos el módulo Contabilidad, de People Soft; Oma Plus, que atiende la operativa de Títulos y Valores y Mesa de Dinero; Recupero de Créditos, y el software de oficinas como Word, Excel y otro tipo de programas utilitarios de uso corriente.

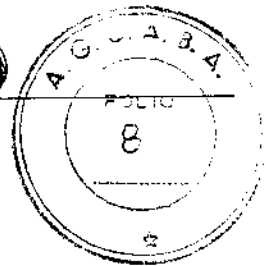
La información se transfiere entre esta red y el equipo /390 mediante interfases Batch, es decir que las transacciones ingresan al equipo principal en lotes y en forma diferida, no de a una y en el momento en que se procesan. Esto implica que hay un desfasaje de tiempo desde el momento en que se captura la operación hasta que se consolida la información y se procesa en dicha plataforma central.

- IBM 390: dentro de esta Plataforma se procesan, clasificadas por rubro, las siguientes aplicaciones:

Cartera Activa:

- ✓ Créditos Comerciales.
- ✓ Préstamos Personales.
- ✓ Gestión.





- ✓ Cuentas Corrientes.
- ✓ Pignoraticio y Ventas.
- ✓ Exterior y Cambio.

Cartera Pasiva:

- ✓ Caja de Ahorros
- ✓ Judiciales
- ✓ Plazo Fijo
- ✓ Cuentas Corrientes.

Recaudaciones:

- ✓ Recaudación de Servicios
- ✓ Tarjetas de Crédito.

Contable:

- ✓ Interfases People Soft
- ✓ Bienes de Uso
- ✓ Suministros.

Servicios:

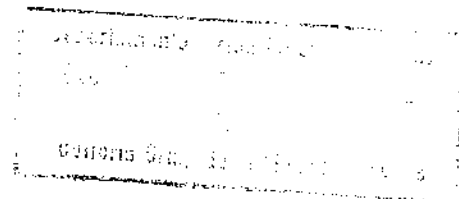
- ✓ Acreditación de Comercios.
- ✓ Acreditación de Sueldos.
- ✓ Banca Telefónica.
- ✓ Cobranzas Automáticas.
- ✓ Datanet
- ✓ Jubilaciones
- ✓ Administración de Tarjetas Moderban.

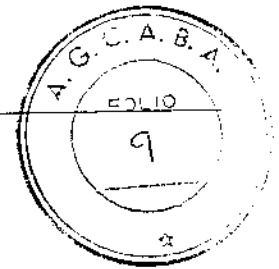
B.C.R.A.:

- ✓ Régimen Informativo.
- ✓ Clasificación de Deudores.
- ✓ Prevención del Lavado de Dinero.

Operación:

- ✓ Compensación Electrónica.





- ✓ Interfases entre Sistemas.
- ✓ Movimiento Interdependencias.

Clientes

- ✓ Nexos.

- Stratus Continuum: da servicios en línea a las 44 Sucursales, a los cajeros automáticos del banco (ATM) pertenecientes a la red Moderban, a la interconexión con Link y, a través de esta última, con Banelco y con redes del exterior.

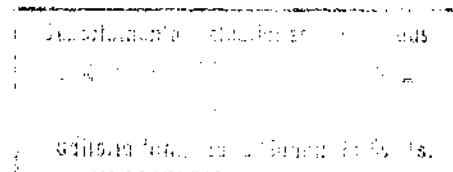
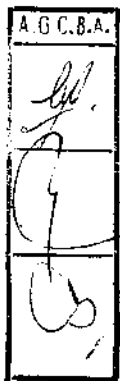
Este equipo posee características de procesamiento continuo, operando con dos unidades similares que poseen sus elementos duplicados, replicando automáticamente la información. Las referidas unidades (ubicadas físicamente en edificios diferentes distantes en aproximadamente 600 metros) funcionan entre sí como respaldo de información en sede externa, con lo cual la entidad obtiene un backup continuo recíproco. No obstante, la información activa que se almacena en esta plataforma es la correspondiente al día, que todas las noches se transfiere mediante procesos en lote al mainframe IBM 390, donde se almacena el universo total de datos.

El Stratus funciona con un sistema operativo propio y soporta la operatoria on line de Cajas de Ahorro y Cuentas Corrientes, entre otras, ejecutándola a través de un aplicativo denominado "ON2".

3.2. Red de Comunicaciones

En Anexo V se describe el diagrama global vigente; adicionalmente se destacan los siguientes aspectos, que surgen del relevamiento practicado:

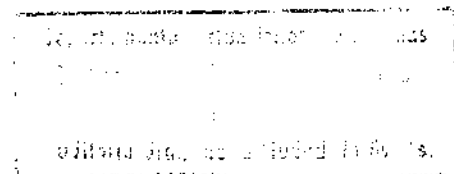
- La red de comunicación digital es provista por un proveedor externo, cuya denominación es IMPSAT S.A.. Dicho proveedor también tiene a su cargo el encriptado entre nodos, utilizando a tal fin software y hardware con dispositivos específicos.
- El BCBA dispone de un anillo de fibra óptica que vincula el Centro de Cómputos (DPD), la Casa Matriz y el Área de Desarrollo y Mantenimiento de los Sistemas, sito en Sarmiento 630, áreas que constituyen los tres nodos principales. Las Sucursales se conectan con este anillo a través del vínculo digital provisto por IMPSAT.
- Los nodos principales se encuentran enlazados mediante fibra óptica de alta velocidad (2 Megabits); el anillo proporciona caminos alternativos en caso de caída de alguno de los vínculos.



- El Banco cuenta con una red de Cajeros Automáticos (ATM) que, a febrero de 2001, ascendía a 102 unidades.

- El monitoreo de los cajeros automáticos (ATM) es llamado usualmente "non Stop" o "7X24", lo cual equivale a decir que es efectuado los siete días de la semana, 24 horas por día; el mantenimiento técnico de estos cajeros es provisto por la empresa Diebold.
El software detecta fallas de cajeros en forma automática, permitiendo el conocimiento inmediato del problema para instar a su rápida solución, y es operado por personal del BCBA.
- Para el conocimiento de los problemas relativos a las terminales de las sucursales, se dispone de una mesa de ayuda (help desk), la cual concentra los pedidos utilizando un software especial y los deriva a las áreas de Soporte Técnico (si el problema es de hardware o comunicación) o Seguridad en Tecnología Informática (si la falla está relacionada con la seguridad lógica).
- El servicio de acceso a Internet es desarrollado por el proveedor Vía Network, quien lo brinda a través de líneas telefónicas; adicionalmente, provee asiento en el Sitio Web.
- El correo electrónico se desarrolla a través de un servicio interno que es atendido por Soporte Técnico, y que interactúa con el provisto por Vía Network.

A G C B A.
<i>[Signature]</i>
<i>[Signature]</i>



Para una clara exposición de los aspectos que merecieron observaciones, los mismos fueron clasificados en cuatro grupos, de acuerdo a los siguientes contenidos:

1. Aspectos generales relacionados con el equipamiento y los aplicativos.
2. Cuestiones generales relativas a la Red de Comunicaciones.
3. Aspectos generales relacionados con la Seguridad Lógica y en Tecnología Informática.
4. Intercambio de la información con el G.C.B.A.

1) Aspectos generales relacionados con el equipamiento y los aplicativos.

1.1. Carencia de un sistema que integre a la totalidad de los aplicativos comerciales.

El software en uso no integra la información producida por los diferentes aplicativos comerciales: en algunos casos se hace necesario acudir a un elevado número de interfaces para consolidar la información, y en otros es necesario desarrollar procesos manuales para la obtención de datos requeridos por usuarios internos y/o externos (BCRA y auditores externos, entre otros).

La situación comentada genera demoras a los usuarios internos y externos, que en muchos casos deben recurrir a soluciones de emergencia para atender las demandas operativas, generando riesgos de errores en la información elaborada.

1.2. Diversidad de plataformas.

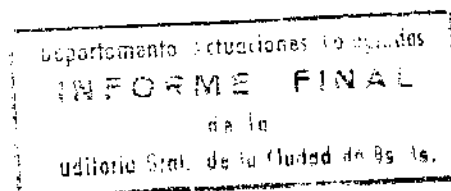
El esquema descrito en el apartado 3.1. de las Aclaraciones Previas ocasiona mayores costos de mantenimiento, por pago de licencias, de operación, administración y soporte técnico, entre otros.

1.3. Incremento de costos y del riesgo derivados de la utilización de varios equipos AS 400 geográficamente dispersos.

La utilización de 7 unidades IBM AS 400 y la disímil ubicación física de las mismas da origen a mayores costos de operación y mantenimiento e incrementa los riesgos de acceso físico indebido, obstaculizando las tareas de control sobre los mismos.

1.4. Antigüedad de los aplicativos que corren sobre la Plataforma IBM 390.

Algunos aplicativos utilizados en el BCBA, como por ejemplo Créditos, Cuentas Corrientes y Préstamos Personales, presentan características de escasa



flexibilidad, evidenciando un importante retraso tecnológico que se traduce, entre otros efectos, en mayores costos de mantenimiento.

Adicionalmente, el software que se emplea ha sido desarrollado para operatorias en lotes, de uso frecuente en décadas anteriores, no contemplando la utilización de Bases de Datos, que mejora la organización, almacenamiento y explotación de la información.

1.5. Escasa parametrización del software utilizado en la Plataforma IBM 390.

El software utilizado carece de las facilidades de parametrización propias de los sistemas modernos, lo cual implica que para mantenerlo o efectuarle modificaciones, o para incorporar nuevas funciones, se debe requerir necesariamente la participación de personal técnico entrenado para modificar el código fuente.

Esta situación incrementa los costos y ocasiona demoras en la implementación de modificaciones, lo cual hace más lenta la reacción a las crecientes demandas del negocio bancario.

Con relación a las observaciones plasmadas en los apartados 1.1. a 1.5. precedentes cabe señalar que el Banco está llevando a cabo un proceso de selección de nuevos sistemas aplicativos centrales, considerando como tales los correspondientes a clientes, operaciones activas y pasivas, la interconexión con Contabilidad y demás aplicativos departamentales, con la finalidad de dar respuesta a los planes de negocios del Banco.

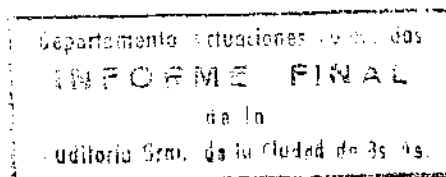
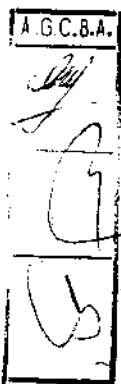
Durante el año 2000 se llevaron a cabo a este respecto las siguientes instancias:

- Se creó una comisión de técnicos de las Áreas Administración de Operaciones y Sistemas y Tecnología.
- Se establecieron pautas de trabajo y cronograma de tareas.
- Se definieron alcances, conceptos funcionales y conectividad entre plataformas.

Los prerequisites establecidos para la selección fueron los siguientes:

- Sistema integrado con criterio de Cliente Único.
- Motor de Base de Datos Relacional.
- Sistema en funcionamiento en alguna entidad financiera de plaza.
- Costo razonable (no superior a \$ 10 millones).
- Funcionamiento Transaccional, On Line – Real Time, lo cual equivale a que la operación se capture y a partir de ese momento no pase por más manos, que esté conectado en línea y en tiempo real en el momento en que la operación se ejecuta, quedando registrada sin interfases o procesos batch.
- Independencia de la plataforma de hardware (criterio de funcionalidad).

La metodología de selección fue establecida en las siguientes instancias:



- Entrevistas y demostraciones con Proveedores y Bancos Usuarios.
- Análisis y definición de la matriz de evaluación.
- Análisis de experiencias de costos y dificultades.
- Estimación de costos indicativos del proyecto.
- Profundización del Módulo Operaciones Activas.
- Análisis de nuevas alternativas en el mercado, en proceso de argentinización, denominado "Servidor Financiero Getronics".

En el descargo producido con fecha 26/10/01 la entidad informa que el personal técnico asignado se encuentra confeccionando los pliegos mediante los cuales se realizará un concurso por invitación para la adquisición de un software integral, modalidad que fue autorizada mediante Resolución de Directorio N° 465, de fecha 13/09/01.

- 1.6. Ausencia de un Plan de mediano y largo alcance con indicación de las actividades a desarrollar en cada etapa, presupuesto estimado, sectores involucrados, objetivos, plazos y recursos.

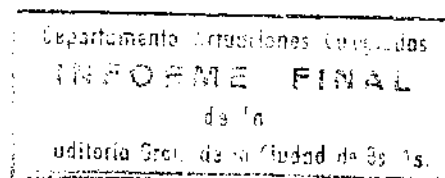
La documentación relevada no contempla la planificación realizada sobre algunos aspectos clave, entre los que adquieren relevancia los siguientes:

- Duración del plan.
- Cantidad de etapas y periodos de sus desarrollos.
- Actividades previstas en cada etapa, revisiones planificadas y periodicidad de las mismas.
- Insumos necesarios, recursos presupuestados y sectores involucrados en los distintos procesos.
- Fecha de finalización estimativa.

En una reunión mantenida con el máximo nivel de la Gerencia de Sistemas se ha informado a esta Auditoría sobre la existencia de un plan de sistemas a mediano y largo plazo que contiene los elementos precisados, pero el mencionado documento no fue suministrado atento que, conforme a las manifestaciones vertidas, se encuentra pendiente de aprobación por parte del Directorio.

La entidad en su descargo informa que la resolución de este aspecto se encuentra estrechamente ligada a la concreción de la contratación del software integral aludida en el último párrafo del punto 1.5.

- 1.7. Carencia del servicio "Home Banking"



La entidad carece del servicio del título, indispensable a la hora de realizar la oferta y prestación de servicios a través de Internet. La situación descrita genera una apreciable desventaja competitiva frente al resto del sistema.

Cabe señalar que en la reunión consignada en el punto anterior, la entidad ha informado que para el primer trimestre del 2002 tiene prevista la incorporación de este servicio, que será desarrollado a través de la Red Link.

- 1.8. Algunos aplicativos operan fuera del entorno de seguridad provisto por los Sistemas Operativos de los equipos principales.

A título de ejemplo podemos mencionar el Sistema de Transferencias entre Sucursales, que funciona sobre Computadoras Personales (PC) situadas en la Sucursal, fuera de los equipos principales.

La entidad ha implementado algunas medidas tendientes a la salvaguarda de la información almacenada en los mencionados equipos, entre las cuales adquiere relevancia el encriptado de los archivos.

No obstante lo expuesto, la situación planteada constituye una debilidad en la seguridad del aplicativo, toda vez que el entorno de las PC ofrece un resguardo sustancialmente inferior al provisto por los Sistemas Operativos de los equipos principales, generando mayores riesgos de eventuales alteraciones o modificaciones de la información existente, o del ingreso de operaciones ficticias.

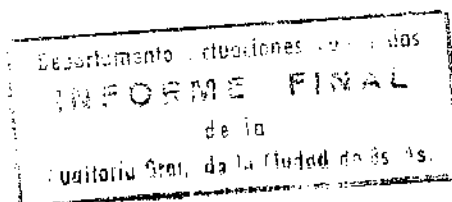
La entidad en su descargo señala que las aplicaciones serán reemplazadas una vez instalado el sistema central a contratar, aludido en el último párrafo del punto 1.5.

2) Cuestiones generales relativas a la red de comunicaciones.

- 2.1. Falta de segmentación.

La red interna del Banco no se encuentra segmentada, con lo cual se incrementan las posibilidades de eventuales accesos no autorizados, dada la exposición del diseño a un universo de usuarios excesivo. Asimismo, la situación comentada deteriora la performance de la red, ocasionando mayores demoras en su utilización.

- 2.2. Números de IP públicos.



Los IP (direcciones utilizadas para identificar en forma lógica a los equipos en un ambiente de comunicaciones) son públicos, lo cual obstaculiza sensiblemente la salida a Internet a través de la red principal, ante la superposición de las direcciones internas y externas.

Dicha salida se realiza a través de módems y líneas telefónicas instaladas para cada uno de los usuarios habilitados (aproximadamente 150).

2.3. Ausencia de herramientas de Monitoreo de Red orientadas a la seguridad.

El banco no dispone de herramientas que permitan detectar intentos de accesos no autorizados (hackeos), y conocer el origen de la acción. Adicionalmente se advierte la carencia de dispositivos con capacidad de filtrado de servicios, entre los que se pueden citar el FTP (transferencia de archivos) y Telnet (habilitación de terminales remotas), entre otros.

2.4. Carencia de un software que permita efectuar un monitoreo integral de la red.

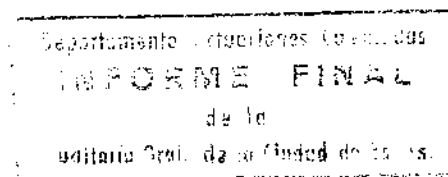
La entidad no cuenta con un software que permita efectuar un monitoreo integral de la red, que incluya funciones tales como realizar un inventario del equipamiento conectado, asistencia remota con acceso a la terminal del usuario incorporado, instalación centralizada de software, administración de licencias, y otras, del tipo "Unicenter", "Tívoli" o similar.

La situación descripta limita la eficiencia del soporte de red y del monitoreo de su seguridad, como así también reduce la posibilidad de resguardar los dispositivos conectados.

3) Aspectos generales relacionados con la Seguridad Lógica y la Tecnología Informática.

3.1. Falta de seguridad lógica en los datos publicados en la página Web de la entidad.

El sitio Web del Banco tiene el servicio para su acceso remoto habilitado sin password con clave anónima, o sea que es de acceso público, lo cual implica que cualquier usuario con los conocimientos necesarios y acceso a Internet puede modificar o borrar la información publicada sin restricción.



Esta situación también posibilita la eliminación de las páginas Web total o parcialmente, lo que podría generar la suspensión del servicio hasta que se recupere la información desde su respaldo.

Con posterioridad a la finalización del presente informe, la entidad ha regularizado la observación planteada.

3.2. Faltan evidencias de algunos controles de seguridad practicados sobre las plataformas Stratus Continuum, IBM 390 y Windows NT.

A título de ejemplo se advierte la ausencia de evidencias sobre la ejecución de controles sobre la configuración de arranque de máquina y las actividades efectuadas bajo permisos especiales, entre otros.

3.3. Puestos de trabajo con acceso libre a la red.

Existen equipos de usuarios finales conectados a la red que utilizan Windows 98.

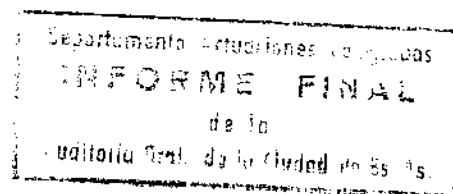
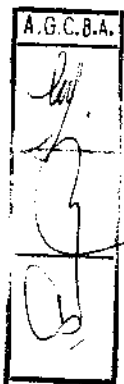
El mencionado software posibilita el acceso a la red sin los límites desarrollados por el entorno operativo, circunstancia que los hace poco recomendables por la escasa seguridad que ofrecen.

4. Intercambio de la información con el Gobierno de la Ciudad de Buenos Aires.

La metodología utilizada para el intercambio de información con el GCBA resulta antigua y poco eficiente, ya que presenta deficiencias como las que se señalan:

- En la transmisión de datos relacionados con la liquidación de haberes se utilizan diskettes, los cuales se intercambian sin protección física ni lógica, y sin aplicar encriptación a la información que contienen.
La situación descrita facilita la alteración de la información y su contenido, como así también el posible acceso a la misma de personal no autorizado.
- El intercambio no se encuentra automatizado, circunstancia que genera, además de los riesgos descritos en el apartado anterior, el insumo de tiempos y recursos humanos adicionales para la obtención y control de la información a transferir.

No obstante se señala que la información para pagos de sueldos recibida por la entidad desde Recursos Humanos del GCBA comenzó a ser encriptada en calidad de prueba piloto, a raíz de la observación plasmada en el Informe de la A.G.C.B.A Nro 28, del 14/11/2000. Adicionalmente, el Gerente de Sistemas informó a esta



auditoría que la entidad está en proceso de adquisición de un software (PGP) tendiente al encriptado de la información, aspecto que no fue verificado en el transcurso de la presente revisión.

VI. RECOMENDACIONES.

Capítulo 1)

Puntos 1.1, 1.2., 1.4. y 1.5.

Establecer un cronograma para la urgente implementación del Plan de Sistemas, contemplando la resolución de las debilidades planteadas.

Punto 1.3.

Evaluar la posibilidad de concentrar el procesamiento en uno o dos equipos ubicados en no más de dos locaciones.

Punto 1.6.

Agilizar la aprobación y la implementación del Plan de Sistemas.

Punto 1.7.

Incluir en la Planificación realizada la incorporación del servicio "Home Banking", especificando el período en el cual se dará comienzo a la mencionada prestación.

Punto 1.8.

Incorporar las aplicaciones que funcionan en la periferia de los Sistemas Operativos centrales al ambiente controlado por los mismos.

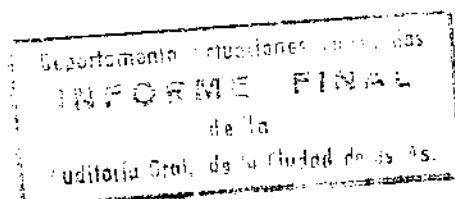
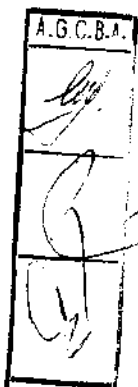
Capítulo 2)

Puntos 2.1. a 2.4.

Revisar en forma integral el diseño de la red de comunicaciones, analizando la resolución de los aspectos observados en forma conjunta. Adicionalmente, corresponderá evaluar la incorporación de firewalls o dispositivos similares, de números de IP privados (como los correspondientes a la clase A 10), y agilizar la implementación del software para la administración y el monitoreo integral de la red.

Capítulo 3)

Punto 3.2.



Desarrollar rutinas escritas con la revisión a practicar en forma diaria sobre la función de arranque de las máquinas y sobre las actividades desarrolladas con permisos especiales. Adicionalmente, y con relación a estas últimas, correspondería producir en todos los casos la documentación que respalde el motivo de su utilización, y un detalle de las acciones realizadas en cada caso.

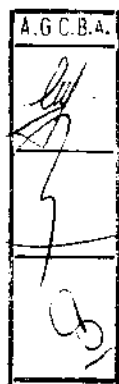
Punto 3.3.

Eliminar la utilización del sistema operativo Windows 98 para los puestos de trabajo.

Capítulo 4)

Adoptar medidas tendientes a subsanar las debilidades planteadas, entre las cuales resultarían de utilidad:

- Evaluar la automatización para el traspaso y recepción de la información.
- Incorporación de técnicas de encriptación para los archivos intercambiados.
- Utilización de correo electrónico con ruteo pre-programado para el traspaso de la información, incorporando herramientas del tipo Lotus-Notes o similar.



Departamento Asesorías Legales
INFORME FINAL
de la
Auditoría Gen. de la Ciudad de Bs. As.

VII. CONCLUSIÓN

En la actualidad coexisten cuatro plataformas en la red informática del banco: AS 400, Windows NT, IBM 390 y Continuum.

Las principales desventajas de la arquitectura informática actual pueden sintetizarse básicamente en:

- Diversidad de Plataformas.
- Antigüedad del software, que se traduce en un importante retraso tecnológico de los Aplicativos Centrales.
- Bajo nivel de parametrización, lo cual implica que para mantenerlo o para incorporarle nuevas funcionalidades, se debe requerir necesariamente la participación de personal técnico entrenado para modificar el código.
- Falta de integración de los aplicativos.
- Redundancia y limitaciones en el modelo de datos.
- Altos costos recurrentes.

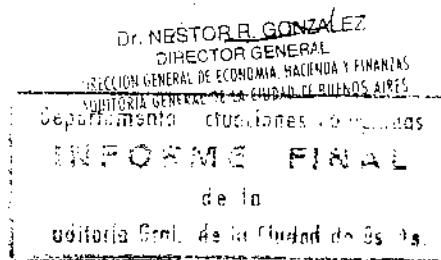
Estas debilidades traen aparejados los siguientes efectos:

- Gran esfuerzo para la obtención de información confiable y elevados costos de mantenimiento.
- Plazos prolongados en la atención de requerimientos de usuarios internos, generando impaciencia por información.
- Insatisfacción del usuario, debiendo recurrir a soluciones de emergencia para atender las demandas operativas sin permitir una adecuada planificación.
- Retraso respecto de la competencia de los Bancos que han resuelto su plan de sistemas.
- Reacción más lenta a la demanda del negocio bancario.
- Demora en la actualización tecnológica de los recursos humanos de la organización.

El Banco ha iniciado en el año 2000 gestiones tendientes a la adquisición de un nuevo sistema aplicativo central, que reemplazaría al vigente. El proceso de selección se inició con la creación de una comisión de técnicos de las Áreas Administración de Operaciones y Sistemas y Tecnología para la selección de un sistema integrado de cliente único.

Si bien en los últimos años se han producido importantes avances en los sistemas de información y en la seguridad informática del banco, aún subsisten importantes debilidades que deberían resolverse a la mayor brevedad posible.

El establecimiento de un cronograma para el plan de sistemas, con la máxima celeridad en su desarrollo, redundará en una rápida solución de los problemas informáticos a los que la entidad se encuentra expuesta, fortaleciéndola en su competitividad ante las crecientes demandas del mercado.

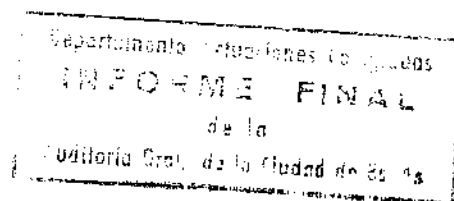
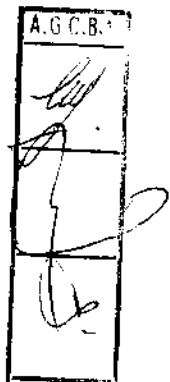


ANEXOS:**ANEXO I: MARCO NORMATIVO APLICABLE****ANEXO II: PROCEDIMIENTOS DE AUDITORÍA APLICADOS****ANEXO III: GERENCIA DE SISTEMAS – GASTOS IMPUTADOS AL 31/12/00****ANEXO IV: CIRCUITOS DE DATOS DEL BANCO CIUDAD****ANEXO V: ESQUEMA DE RED DEL BANCO CIUDAD**

Departamento de Auditoría General
INFORME FINAL
de la
Auditoría General de la Ciudad de Bogotá

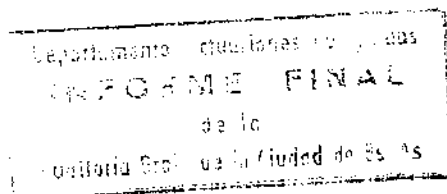
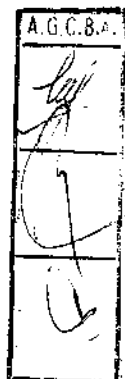
ANEXO I MARCO NORMATIVO APLICABLE

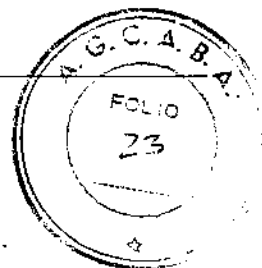
- Comunicación "A" 2659 del 23/1/98 del Banco Central de la República Argentina, sus complementarias y modificatorias: "A" 3149, "A" 3198 y "B" 6776.
- Comunicación "A" 2985 del 14/9/99 del Banco Central de la República Argentina.
- Normas y recomendaciones de seguridad establecidas por la DGEySI.
- 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.
- Ley de Entidades Financieras N° 21.526.
- Informe de la Asociación de Usuarios de Servicios Bancarios (AUSBANC)



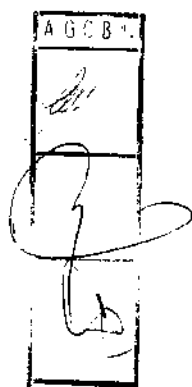
ANEXO II PROCEDIMIENTOS DE AUDITORÍA APLICADOS

- Entrevistas con el personal jerárquico y operativo de las áreas involucradas de las Gerencias de Área Sistemas, de Seguridad en Tecnologías de Información.
- Visita a 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 y Sucursal Centro), aplicándose los siguientes procedimientos:
 - Verificación de las medidas de seguridad física generales.
 - Revisión de la ejecución de los respaldos de información en función de la política de Back up en los Ambientes 390, Stratus y NT.
 - Cotejo del monitoreo efectuado sobre los cajeros automáticos.
 - Verificación del cumplimiento de las normas de seguridad relativas a grabación y resguardo de cintas de monitoreo de cajeros en las cuatro sucursales inspeccionadas.
- Visita a la totalidad de los cajeros de la red Moderban y revisión del servicio que prestan.
- Revisión del procedimiento de otorgamiento de claves para los ambientes 390, Stratus y Windows NT.
- Lectura y análisis de los siguientes informes:
 - Auditoría del Sistema de Liquidación de Haberes Centralizado y Descentralizado, realizado por la DGE y SI en el año 1995.
 - Informes de auditores externos, internos e inspectores del BCRA relacionados con las áreas auditadas, las observaciones halladas y su posterior seguimiento.
- 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 consignadas en Anexo I.
- Ejecución de software de testeo para determinar la configuración de la red accesible desde dos puestos de trabajo instalados en Sarmiento 640 y Esmeralda 660.





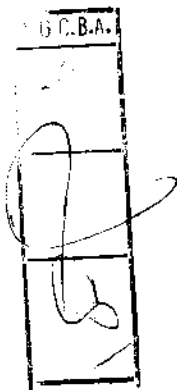
- Verificación de la seguridad del acceso al sitio Web del BCBA.
- Verificación de la existencia de encriptadores en el DPD y las Sucursales.



Departamento Inspecciones y Vigilancia
INFORME FINAL
 de la
 Auditoría General de la Ciudad de Buenos Aires

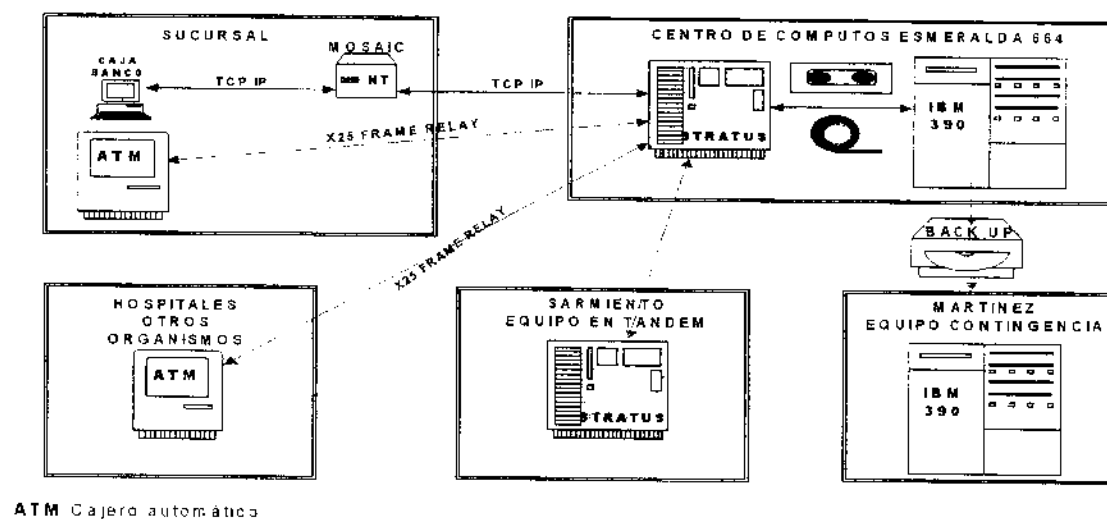
ANEXO III
GERENCIA DE ÁREA DE SISTEMAS
GASTOS IMPUTADOS AL 31/12/00
En miles de \$

	<i>Gcia. de Sistemas</i>	<i>Total Banco</i>	<i>Participación</i>
Remuneraciones	5,384	71,389	7.5%
Cargas sociales sobre Remuneraciones	675	9,438	7.1%
Indemnizaciones y Gratificaciones	55	866	6.3%
Gastos de Representación y Movilidad	8	1,790	0.5%
Servicios al Personal	433	8,635	5.0%
Servicios de Seguridad	29	3,599	0.8%
Honorarios	25	2,372	1.0%
Seguros	19	704	2.8%
Alquileres	1,807	3,285	55.0%
Papelería y útiles	31	924	3.3%
Electricidad y comunicaciones	44	4,203	1.1%
Propaganda y publicidad	0	8,512	0.0%
Impuestos : Gravámenes y Contribución municipal	7	2,366	0.3%
Total Gastos de Mantenim., Conservación y Rep.	2,708	5,319	50.9%
Total Depreciaciones Maquinas, eq. e instalaciones	1,390	6,730	20.7%
Amortización Gastos de Org. Y Desarrollo	2,484	2,484	100.0%
Otros	460	12,862	3.6%
Total	15,559	145,478	10.7%
Amortizaciones	3,874		
Gastos	11,685		
	15,559		



Departamento Asesorías Técnicas
INFORME FINAL
de la
Auditoría General de la Ciudad de Bogotá

ANEXO IV

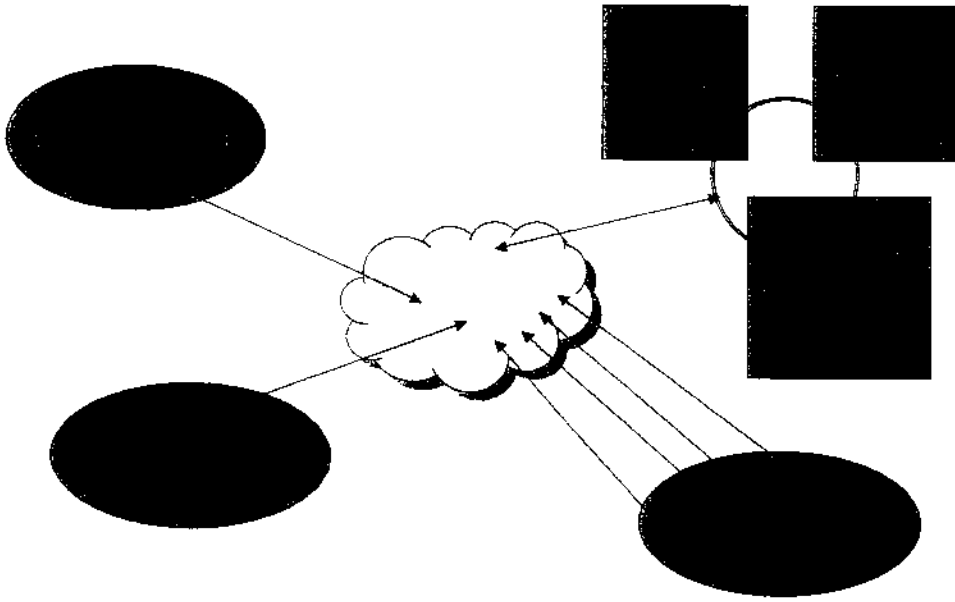
CIRCUITOS DE DATOS
BANCO CIUDAD

A.G.C.B.A.

Departamento de Situaciones Contingencias
INFORME FINAL
de la
Auditoría General de la Ciudad de Bs. As.

ANEXO V

Esquema de Red Banco



AGCBA.
<i>[Signature]</i>
<i>[Signature]</i>
<i>[Signature]</i>

Departamento de Ingresos de la Ciudad de los Rios
INFORME FINAL
 de la
 Auditoria General de la Ciudad de los Rios