AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

AGCBA

INFORME FINAL DE AUDITORIA

PROYECTO Nº 4.24.00.00

Auditoria General del hardware y la seguridad en el Banco de la Ciudad de Buenos Aires.

SUBPROYECTO: Seguridad lógica y física y procesamiento de las interfases con el Sistema de Contabilidad.

Buenos Aires, Marzo de 2003

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

SUBPROYECTO: Seguridad lógica y física y procesamiento de las Interfases con el Sistema de Contabilidad.

PERÍODO BAJO EXAMEN: Mayo 2001 a febrero 2002.

FECHA DE PRESENTACIÓN DEL INFORME:

EQUIPO DESIGNADO:

Director de Proyecto: *Lic. Martín, Ricardo*

Supervisor : *Dra. Sencio, Claudia*

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

OBJETIVO: Examinar la calidad del servicio informático, su seguridad y resguardo, para los entornos operativos que soportan las aplicaciones centrales.

A.G.C.B.A.

Informe Final de Auditoría
Proyecto Nº 4.24.00.00

DESTINATARIO

Sra. Presidenta
Legislatura de la Ciudad
Autónoma de Buenos Aires
Lic. María Cecilia Felgueras

En uso de las facultades conferidas por la Constitución de la Ciudad Autónoma de Buenos Aires de acuerdo al artículo 135, la ley número 325 del 18 de febrero de 2000 dictada por la Honorable Legislatura de la Ciudad Autónoma de Buenos Aires en su artículo número 6 y, supletoriamente, la ley 24.156 (AGN) la Auditoría General de la Ciudad procedió a efectuar un examen en el ámbito de las Gerencias de Sistemas y la Gerencia de Relaciones con el GCBA y Organismos Públicos del Banco de la Ciudad de Buenos Aires.

OBJETO DE LA AUDITORIA

Evaluar la organización del área informática que atiende los sistemas centrales en sus aspectos generales, la seguridad lógica y física y el procesamiento de las interfases de los aplicativos al sistema contable, con relación a las siguientes plataformas y la red de comunicaciones que las vincula:

- IBM 390
- Stratus
- Windows NT

ALCANCE

El trabajo de auditoría relacionado con este Subproyecto fue desarrollado, conjuntamente con el de las restantes etapas del Proyecto, en el período comprendido entre enero de 2001 y mayo de 2002, 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 Nº 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.

A.G.C.B.A.

FINAL

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 Centro, N° 35 (La Lucila), N° 22 (Once), N° 14 (Barracas).

ACLARACIONES PREVIAS:

En el Centro de Procesamiento y otras áreas informáticas 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 desfase de tiempo desde el momento en que se captura la operación hasta que se la consolida y 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.

FOLIO

FINAL

- ✓ 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.

A.G.C.B.A.

FINAL

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".

La Red de Comunicaciones presenta las siguientes características:

- Es provista por un proveedor externo, cuya denominación es IMPSAT S.A., quien 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.

- La comunicación de los nodos principales con las sucursales se efectúa con enlaces de menor velocidad (128/ 256 kb).

- 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 y 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.

- 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 Via Network.

La información contable se procesa a través del sistema denominado "PeopleSoft", que es una aplicación que corre bajo ambiente Windows NT, consistente en 4 módulos: activo fijo, presupuestos, contabilidad y cuentas a pagar. PeopleSoft Contabilidad General permite definir un plan contable que refleje el modo en que el usuario atiende sus negocios, hacer un seguimiento de productos, proyectos, cartera de valores, normas, dotaciones, servicios o cualquier dato que refleje la naturaleza de sus operaciones.

El módulo contable se alimenta de información proveniente de otros sistemas como cuentas corrientes, caja de ahorros y plazos fijos, llevándose a cabo la concentración a través del denominado "Módulo Integrador Contable (MIC)" que genera dos tipos de registros: de transacciones y de asientos contables automáticos.

En la actualidad el banco se encuentra en la fase de ajustes post implementación. Según los análisis previos, la instalación del sistema contable PeopleSoft eliminará las limitaciones y restricciones del viejo sistema, generando puestos de trabajo online con la contabilidad.

OBSERVACIONES:

1. Aspectos Generales

Adicionalmente a lo observado 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 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, se detectaron las siguientes debilidades:

1.1. Ausencia de políticas generales del área de Sistemas.

La falta de políticas en esta materia denota apartamientos a la Com. "A" 3198 del BCRA, que exige en el punto 3.1. la formalización de políticas generales tendientes a orientar sobre los lineamientos del hardware a utilizar, los estándares de desarrollo de software, comunicaciones, programación, procedimientos, operaciones y otros en las que debería apoyarse el planeamiento.

Cabe señalar que el aspecto tratado en este apartado fue también objetado por la Gerencia de Auditoría Interna, en el Informe N° 79/125.

1.2. El organigrama de la Gerencia de Sistemas no responde a su esquema funcional.

Existen cargos en la estructura del área de Sistemas no cubiertos a la fecha de la revisión. A título de ejemplo, se destacan el Subgerente de Microsistemas, el Subgerente de Tecnología, el Supervisor de Investigación, la Supervisión de e-business e Internet.

La situación comentada reviste apartamientos al esquema funcional vigente, que debería adaptarse o reformularse en función de las necesidades operativas del área.

1.3. Insuficiente información elaborada por la Mesa de Ayuda, dependiente de la Gerencia de Sistemas.

Los documentos elaborados por esa dependencia no brindan información cualitativa sobre los problemas más usuales que afectan a los usuarios, toda vez que sólo contienen datos estadísticos relativos a las tareas que se realizan, según su naturaleza.

La ausencia de información completa puede eventualmente afectar las decisiones que se adopten para la mejora de los servicios y la celeridad en la resolución de los problemas detectados, entre otros beneficios.

1.4. Inexistencia de manuales con estándares de metodología para el diseño, desarrollo y mantenimiento de los sistemas aplicativos.

La debilidad planteada dificulta el planeamiento, el control y la ejecución de las tareas de desarrollo, puesta en marcha y adecuaciones de los sistemas, a la vez que vulnera las disposiciones del punto 3.2. de la Com. "A" 3198, que exigen contar con este elemento.

Cabe señalar que este aspecto mereció observaciones de la Gerencia de Auditoría Interna, en el Informe N° 79/125 del 21/ 06/01.

1.5. La documentación relacionada con los sistemas de información no se encuentra debidamente actualizada.

De acuerdo a las manifestaciones vertidas por funcionarios de la Gerencia de Sistemas, el contenido de sus Manuales se encuentra desactualizado, situación que genera una mayor dependencia de los especialistas que trabajan en el mantenimiento de los aplicativos.

Adicionalmente, no existen facilidades para acceder, actualizar y compartir las normas y manuales relacionados con los Sistemas, las estructuras de datos y los diseños entre las diferentes áreas, entre otros.

Cabe señalar que la información sobre los Sistemas de información y Procesos se encuentra impresa, lo que dificulta su actualización y consulta por parte de los diferentes sectores que la utilizan.

1.6. El personal del área "Coordinación de Procesamiento de Datos" no dispone, en todos los casos relevados, de procedimientos dictados con relación a los siguientes temas:

- Control de calidad a los procesos informáticos para asegurar la correcta ejecución de los aplicativos.
- Cancelación de programas y pasos a seguir para su resolución, en los casos que no se requiera la intervención del analista.

La ausencia de normas o instructivos da lugar a vacíos sobre los circuitos administrativos a seguir en las áreas involucradas, los niveles de control y los responsables de su realización, afectando la uniformidad de los procesos, a la vez que puede ocasionar demoras u omisiones en el desarrollo de las tareas y sus respectivos controles.

Cabe señalar que con posterioridad a la finalización de las tareas de campo fueron elaborados instructivos de trabajo sobre el primero de estos aspectos; no obstante los mismos no se encuentran formalmente implementados, por no haber sido homologados.

A.G.C.B.A.

1.7. Observaciones relacionadas con la contratación del servicio de comunicaciones.

Adicionalmente al aspecto señalado en el punto 5.3. del Informe del Subproyecto "Comunicaciones, intercambio de datos con el GCBA e interfases Internas", sobre la ausencia de contrato con el proveedor del servicio (IMPSAT) y de cláusulas contemplando la aplicación de penalidades por demoras o daños ocasionados ante caídas en el vínculo o deficiencias en el servicio, se advierte la ausencia del siguiente requisito:

- Facultad de acceso irrestricto a los datos y a la documentación técnica relacionada por parte de la Superintendencia de Entidades Financieras, condición indispensable para dar cumplimiento a la Comunicación "A" 2659, vigente a la fecha de firma del contrato.

1.8. Duplicidad de imputaciones para ingresar manualmente algunas operaciones pasivas al sistema.

La información sobre operaciones pasivas rechazadas se vuelca en planillas de cálculo, para su posterior ingreso al sistema mediante la utilización de técnicas de graboverificación.

Dicho esquema da lugar al insumo de tiempo y recursos adicionales para el doble ingreso de las transacciones, que podría evitarse si la dependencia de origen registrara estas novedades directamente en el sistema, eliminándose así la instancia posterior.

2. Seguridad Física

2.1. Dificultades en el acceso al Generador de energía eléctrica que alimenta al Centro de Cómputos (DPD) del Banco.

El generador de energía eléctrica se encuentra físicamente ubicado en el edificio de la Dirección General de Rentas; por lo que el acceso al mismo requiere la autorización del personal de seguridad de dicha Dirección. El esquema descrito puede ocasionar demoras para el acceso en situaciones de emergencia que requieran la puesta en marcha del generador en forma manual, especialmente durante los feriados o fines de semana.

Cabe señalar que se ha instalado un dispositivo de arranque automático para amortiguar el impacto de esa debilidad, no obstante, una falla de este dispositivo o la falta de combustible motivada por un corte prolongado en el suministro hacen indispensable el acceso del personal del banco para accionar el generador en forma manual.

2.2. No se cumplieron las prácticas relacionadas con el Plan de evacuación en los últimos tres años.

En los últimos tres años no se han efectuado, en el Centro de Cómputos de Esmeralda 664 (DPD), las prácticas al Plan de evacuación previstas en el punto 7.2. de la Com. "A" 3198. Conforme a esa normativa, las pruebas deben realizarse con periodicidad anual.

2.3. Existencia de elementos inflamables en el Centro de Cómputos.

Fueron detectados elementos inflamables en el espacio físico asignado al DPD, tales como algunos muebles de madera, depósito de papel, archivos de documentación y otros. Esto incrementa los riesgos de posibles siniestros, generando incumplimientos al punto 7.3. de la Com. "A" 3198, que establece que en el área de procesamiento no debe haber material combustible innecesario.

2.4. Ausencia de detectores de humo

Faltan detectores de humo en el sector donde está ubicado el equipo Stratus Continuum en el piso 4° de Sarmiento 664, situación que incumple las disposiciones contenidas en el punto 7.3. de la Comunicación "A" 3198 sobre seguridad física y ambiental.

2.5. Los planes de contingencia para los equipos de Sucursales son incompletos.

El contrato celebrado con el proveedor ISC-Bunker Ramo Argentina S.A. incluye cláusulas estableciendo que, en caso de desperfecto en los servidores de Sucursales o Centros de Recaudación que impidan la atención al público, el proveedor se hace cargo de su resolución en un lapso promedio de 2 horas. Asimismo se acuerda que el servicio brindado por el proveedor excluye la recuperación de datos y la carga de parámetros de la sucursal, tareas que la entidad mantiene a su cargo.

No obstante, las mencionadas previsiones sólo contemplan aspectos parciales y no cumplimentan en su totalidad los requisitos aludidos en el punto 7.4. de la Com. "A" 2659 y 7.1. de la Com. "A" 3198.

Cabe señalar que en el descargo de fecha 30/10/02, la entidad señala que el contrato mencionado en el primer párrafo culminó con posterioridad a la finalización de las tareas de campo, no habiendo sido renovado. Adicionalmente, informa que el servicio es en la actualidad prestado con recursos internos del banco, por lo que resulta pasible de un seguimiento futuro.

2.6. Ausencia de evidencias que acrediten la realización de pruebas de funcionamiento de los planes de contingencia sobre equipos Stratus, equipos en redes, servidores de las sucursales y equipos conectados a la Plataforma Windows NT del DPD.

La situación descripta incrementa el riesgo de imprevistos en la puesta en marcha del servicio alternativo en caso de resultar necesaria su ejecución, a la vez que genera apartamientos de las disposiciones contenidas en el punto 7.1. de la Com. "A" 3198, que exigen la realización de pruebas formales y documentadas de recuperación y de integridad de los backups.

A.G.C.B.A.

En su descargo de fecha 30/10/02 la entidad informa que, con posterioridad a la finalización de las tareas de campo, se han realizado pruebas de contingencia sobre la plataforma Stratus, por lo que la debilidad planteada resulta pasible de seguimientos futuros.

2.7. El Procedimiento para el registro de backups en IBM 390 y Stratus es manual.

A la fecha del relevamiento el procedimiento utilizado para la registración y seguimiento de las cintas se realizaba en forma manual, lo cual incrementaba la probabilidad de errores y lo tornaba ineficiente.

Cabe señalar que con posterioridad a la finalización de las tareas de campo este aspecto ha sido subsanado, habiéndose implementado un sistema de registración automatizado.

2.8. Ausencia de evidencias sobre el cumplimiento de los aspectos normados para el resguardo y destrucción de listados y documentos.

La Com. "A" 3198 establece, en el apartado 7.3. que los listados y documentación de datos, como así también los 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 período de retención, establecido en 10 años.

No obstante, de las entrevistas mantenidas se desprenden las siguientes debilidades:

- No existen evidencias sobre la ejecución de tareas tendientes a la clasificación de la documentación en forma previa a su eliminación o desecho.
- La papelería es donada a instituciones de bien público, sin depurar en forma previa los listados que contienen información confidencial de los clientes.

El esquema utilizado induce a riesgos de incumplimiento de las disposiciones emanadas de la Ley 21.526 y su modificatoria 24.144, que prohíbe a las entidades revelar las operaciones pasivas que realicen, salvo excepciones expresamente establecidas (jueces en causas judiciales, organismos recaudadores y BCRA, entre otras).

3. Seguridad lógica

3.1. El BCBA no supervisa la seguridad de algunos servicios brindados por proveedores externos.

Algunos servicios, entre los que se encuentran el sitio Web, el correo electrónico, el home banking y el servicio de información telefónica, son brindados por proveedores externos, quienes tienen a su cargo la administración de su seguridad.

No obstante no haberse hallado situaciones que impacten la seguridad de esos servicios, a excepción de la plasmada en el punto siguiente, el esquema utilizado hace necesaria la supervisión a cargo de la entidad.

La debilidad descripta resulta asimilable a la observada en el Informe del Subproyecto "Comunicaciones e intercambio de datos con el GCBA" respecto del encriptado de los vínculos de la red de comunicaciones e implica riesgos de accesos indebidos de personal no autorizado.

Si bien en el descargo de fecha 30/10/02 el banco indica la regularización posterior de este aspecto, no brinda precisiones ni acompaña la documentación respaldatoria pertinente, por lo que resulta pasible de un seguimiento futuro.

3.2. El sistema de Banca Telefónica posibilita el acceso indebido a la información de los depositantes.

El servicio de banca telefónica brindado por el Banco Ciudad, a través del número 4325-3271, permite llevar a cabo determinadas operaciones, como ser la obtención de saldos de cuentas de depósito, apertura de nuevas cuentas, pedido de chequeras, pedido de boletas de depósito, consultas sobre tarjetas de crédito y estado de préstamos personales, entre otras.

Cuando un cliente del banco se incorpora a este servicio, el sistema no confirma adecuadamente su identidad, lo que hace posible que otra persona, con sólo conocer el número de documento o CUIL de un cliente, obtenga acceso a información sujeta al secreto bancario. Ello permite realizar las siguientes operaciones a personas no autorizadas:

- Obtención de saldos en cuentas de depósitos de ahorristas que nunca utilizaron el servicio.
- Creación de una clave de acceso (password), que inhabilitaría al verdadero titular de las cuentas a utilizar posteriormente ese servicio.
- Restantes detalladas en el primer párrafo.

El acceso no autorizado a los saldos de las cuentas de depósito vulnera las disposiciones consignadas en la Ley de Entidades Financieras sobre el secreto de las operaciones pasivas de las entidades financieras.

3.3. Inseguridad ante el ingreso de las claves PIN en operaciones de cajeros ventanilla.

Los dispositivos para el ingreso de las claves PIN en los cajeros ventanilla no presentan condiciones adecuadas de seguridad, dado que por su ubicación pueden ser visualizados por otros usuarios. Adicionalmente, las cámaras instaladas pueden registrar la clave al momento de su ingreso, restando confidencialidad al proceso.

Este aspecto fue observado por la Gerencia de Auditoría Interna en el Informe N° 53/125, del 28/06/01.

3.4. Inseguridad de las nuevas claves de acceso otorgadas para todos los entornos.

Las claves otorgadas por primera vez a los usuarios son conocidas por el responsable de seguridad hasta tanto el usuario efectúa el primer inicio de sesión. Sobre el particular se advierte que no se dispone de plazos máximos para su sustitución o reemplazo, situación que resta confidencialidad a las claves durante un lapso de tiempo indeterminado.

Adicionalmente, y con relación a las claves asignadas por rehabilitación, son informadas telefónicamente a través de la Mesa de Ayuda. Si bien el usuario está obligado a su modificación en el primer acceso, tampoco en este caso existen plazos máximos para proceder en tal sentido, restando confidencialidad y aumentando las posibilidades de accesos indebidos.

Por último, y con relación a la rehabilitación, no se dispone de procedimientos tendientes a confirmar la identidad del usuario que efectuó la modificación de la clave de acceso, lo que conlleva a riesgos que el cambio sea realizado por otro usuario, sin que la situación sea detectada en forma oportuna.

3.5. Debilidades en la comunicación de la desvinculación de los agentes, que impactan en los controles sobre la administración de las claves.

El área de personal no comunica en forma oportuna a Seguridad en Tecnología de la Información la desvinculación transitoria o permanente de los agentes, para que este último proceda a la baja de sus respectivas claves. Adicionalmente, no se restringe el acceso a los usuarios del BCBA en horarios que difieran de sus respectivas jornadas laborales.

Las tareas mencionadas son necesarias para el adecuado cumplimiento de las disposiciones contenidas en el punto 6.2. de la Com. "A" 3198.

Cabe señalar que este aspecto se encuentra alcanzado por el comentario del último párrafo del punto 3.1. precedente.

3.6. No se aplica de manera completa la política de administración centralizada de usuarios y sus permisos de acceso en el entorno Windows NT.

Se detectaron algunos usuarios que inician su sesión con permisos no definidos centralmente por Seguridad en Tecnología de la Información.

Si bien los casos hallados fueron aislados, la situación planteada denota apartamientos a las políticas internas que, no obstante su falta de formalidad, constituyen prácticas habituales en la materia.

También en este caso resulta de aplicación lo comentado en el último párrafo del punto 3.1. precedente.

3.7. Falta de planes de capacitación sobre aspectos vinculados a la seguridad para usuarios finales.

Los Planes de Seguridad suministrados por Seguridad en Tecnologías de Información no contemplan acciones a desarrollar para la capacitación de los usuarios finales, situación que puede repercutir, en términos desfavorables, en la seguridad de la información.

3.8. Debilidades en los controles ejecutados sobre la captura de datos, durante el proceso de graboverificación de la información.

El área de captura de datos, a cargo del sector "Coordinación de Procesamiento de Datos" de la Gerencia de Sistemas, no deja documentado en forma fehaciente qué persona realizó la grabación o verificación de los lotes.
Si bien lleva registro de quién lo hace en cada caso, el graboverificador no firma como constancia de haber realizado efectivamente la tarea.

Adicionalmente se advierte que la verificación es realizada, en ciertos casos, por el mismo operador que graba la información, lo cual induce a errores de interpretación del material que se digitaliza.

Con relación a este aspecto, la entidad formula el descargo mencionado en el punto 3.1. precedente, resultando aplicables los comentarios vertidos a ese respecto.

4. Aspectos relacionados con la red de cajeros automáticos

Durante el relevamiento de la red se detectaron las siguientes situaciones derivadas del vínculo establecido con las redes Link y Maestro, que impactan en términos desfavorables en la imagen del banco frente a sus clientes:

4.1. Debilidades en las compras realizadas a través de Maestro.

Se ha detectado una operación de compra que no fue aprobada por Maestro; no obstante el importe fue debitado de la caja de ahorros del cliente.

La situación planteada dio lugar a numerosos y lentos trámites para el recupero de los fondos del cliente, quien adicionalmente resultó perjudicado por la imposibilidad de concretar oportunamente la compra.

Conforme a la información recibida, la debilidad tuvo su origen en la caída del vínculo al momento de la transacción, demandando un exhaustivo seguimiento de la misma con el administrador del servicio.

A.G.C.B.A.

4.2. Problemas derivados de pagos de tarjetas de crédito a través de los cajeros de la red Moderban.

Los cajeros automáticos de la red Moderban no informan las tarjetas de crédito que se pueden abonar por su intermedio.

Adicionalmente los cajeros aceptan pagos de tarjetas que no poseen convenios de cobranza (Diners). En estos casos el cajero admite la operación sin emisión del comprobante; no obstante, no alerta al usuario sobre la no realización del pago respectivo.

4.3. Debilidades en la información proporcionada por los cajeros sobre transferencias entre cuentas de un mismo cliente.

En las pruebas realizadas sobre el funcionamiento de la red se practicó una transferencia entre cuentas vinculadas de un mismo cliente. En esa oportunidad la operación fue informada como cancelada a través del monitor del cajero automático, no obstante el movimiento fue realizado y registrado en las cuentas afectadas, sin emisión del comprobante.

5. Transferencias entre dependencias

Adicionalmente a la observación plasmada en el Informe del Subproyecto Titulado "Aspectos generales vinculados con la organización, el equipamiento, la red de comunicaciones, la seguridad lógica y la tecnología informática" (Informe N° 109 de la página web www.agcba.gov.ar) sobre la operabilidad de algunos aplicativos fuera del entorno de seguridad provisto por los Sistemas Operativos de los equipos principales, merecen destacarse los siguientes aspectos:

5.1. Existen transferencias entre sucursales que no se ingresan a través de los aplicativos centrales, lo cual denota falta de automaticidad en la carga integral de datos. La situación descripta conlleva al insumo de tiempos y recursos adicionales para el registro de algunas transacciones, acrecentando los riesgos de errores en la información.

5.2. Las transacciones que no se procesan automáticamente se ingresan al sistema mediante el empleo de diskettes, no utilizándose el correo electrónico con técnicas de encriptación , que brinda mayor rapidez y seguridad a la transmisión.

Con posterioridad a la finalización de las tareas de campo, la entidad llevó a cabo la optimización del "Sistema TRIN" para la remisión de operaciones de transferencias internas entre dependencias.

A la fecha de elevación del presente informe el proceso no ha concluido, por lo que la opinión acerca de la resolución de los aspectos planteados se emitirá en ocasión de un seguimiento posterior.

6. Interfases con el sistema contable (People Soft)

6.1. Los procedimientos escritos por el Area de Desarrollo de Sistemas, para la realización de tareas de control de producción de las interfases, no han sido formalmente implementados.

No se encuentran homologados los procedimientos de control definidos en el párrafo anterior, ejecutados por la Coordinación de Procesamiento de Datos, debilidad que conlleva a los efectos señalados en el punto 1.6. precedente.

6.2. Ejecución de numerosos procesos manuales para corregir rechazos en las imputaciones ingresadas en los sistemas.

Se produce una importante cantidad de rechazos de los asientos ingresados que deben ser corregidos manualmente, lo cual induce a riesgos de errores u omisiones en la información, generando ineficiencias en el aprovechamiento de los recursos de la organización.

En su descargo la entidad informa que en la actualidad los reportes tendientes a verificar la consistencia entre los subsistemas y la contabilidad se encuentran automatizados. Dichos procesos, denominados "Balanceo Operativo Contable" (BOC), han sido implementados con posterioridad a la finalización de las tareas de campo, sobre los sistemas de caja, saldos inmovilizados y caja de ahorros, hallándose en desarrollo el proceso sobre el sistema de cuentas corrientes.

RECOMENDACIONES

1. Aspectos Generales:

1.1. Implementar formalmente políticos generales de sistemas, de modo de dar cumplimiento a las previsiones contenidas en la normativa vigente.

1.2. Adaptar el esquema funcional al organigrama vigente, o en su defecto, modificar este último en función de las necesidades operativas, atendiendo la adecuada segregación de funciones.

1.3. Analizar la posible incorporación a los informes de indicadores que alerten sobre los principales problemas que afectan al cliente interno. Adicionalmente, procedería evaluar la conveniencia de realizar encuestas periódicas formales de satisfacción a los usuarios.

1.4. Incorporar a las normas los estándares de metodología exigidos por las normas.

1.5. Mantener actualizada la documentación de los sistemas, evaluando la posible utilización de soportes digitales o herramientas que faciliten su actualización periódica. Adicionalmente se recomienda posibilitar el acceso a los manuales y las normas a través de la red de comunicaciones.

1.6. Homologar las normas e instruir formalmente al personal sobre el circuito a seguir para la ejecución de los procesos y sus respectivos controles.

1.7. Instrumentar o reforzar procedimientos de control sobre el cumplimiento de la normativa en los contratos actuales y en aquellos que se celebren en el futuro.

1.8. Evaluar la posibilidad que el ingreso al sistema lo realice la dependencia responsable, de modo de evitar las ineficiencias descriptas.

2. Seguridad Física

2.1. Coordinar con la DGR la adopción de medidas que permitan el rápido acceso al generador de energía eléctrica para el personal del banco.

2.2. Cumplimentar las prácticas previstas en la normativa.

2.3. Implementar acciones tendientes a la eliminación de los materiales combustibles innecesarios.

2.4. Incorporar detectores de humo en el Site del equipo Stratus.

2.5. Confeccionar un plan de contingencia para el ambiente Windows NT de Sucursales.

2.6. Efectuar pruebas de los planes de contingencia sobre el Stratus, equipos en redes, servidores de las Sucursales y equipos conectados a la Plataforma Windows NT del DPD, al menos una vez al año, documentando formalmente sus resultados.

2.8. Dictar instructivos imponiendo la obligatoria clasificación de la documentación en forma previa a su eliminación, donación o desecho.

3. Seguridad lógica

3.1. La Dependencia "Seguridad en Tecnologías de Información" debería establecer mecanismos que garanticen la confidencialidad de las comunicaciones, incluso respecto del proveedor del servicio.

3.2. Evaluar la incorporación de mecanismos que impidan el acceso indebido a la información de los depositantes.

3.3. Evaluar la adopción de medidas de seguridad tendientes a subsanar la debilidad descripta, por ejemplo, la utilización de dispositivos (cajas acrílicas u otros) que impidan la visualización de claves por parte de terceros, la incorporación de alertas a los usuarios, u otras que se consideren apropiadas.

3.4.

- Minimizar el período de vigencia de la clave provisoria.
- Adoptar recaudos tendientes a verificar la identidad del usuario antes de la habilitación o rehabilitación de las claves.

3.5. Prever la implementación de circuitos informativos con la Gerencia de Área de Desarrollo Humano y Capacitación que permitan conocer las ausencias temporales de los agentes. Adicionalmente, corresponderá evaluar la adopción de recaudos tendientes a la baja temporal de las claves de los agentes.

3.6. Eliminar los usuarios definidos fuera de los servidores destinados a esa finalidad.

3.7. Incorporar a los planes de capacitación políticas de seguridad destinadas a los usuarios finales, evaluando alternativas como la utilización de correo electrónico o Intranet.

3.8. Revisar el procedimiento de graboverificación e instrumentar formalmente los controles que se aplican sobre el ingreso y verificación de la información.

4. Aspectos relacionados con la red de cajeros automáticos

Advertir al administrador de la red las debilidades señaladas, instando a su rápida resolución. Adicionalmente, correspondería implementar o mejorar los procedimientos tendientes a la rápida resolución de conflictos como los que se plantean, de modo que la imagen institucional no resulte dañada.

5. Transferencias entre dependencias

Completar lo antes posible la implementación definitiva del nuevo sistema TRIN, evaluando la resolución de las debilidades planteadas en el presente informe.

6. Interfases con el sistema contable (People Soft)

6.1. Implementar formalmente los procedimientos a realizar en la Coordinación de Procesamiento de Datos para la ejecución y el control de las interfases de los aplicativos con el sistema contable.

6.2. Automatizar a la brevedad los procesos pendientes, a efectos de minimizar las tareas manuales de ejecución y control, reduciendo éstas a situaciones de excepción debidamente autorizadas.

A.G.C.B.A.

CONCLUSIONES:

De los procedimientos desarrollados en esta etapa surgen las observaciones que se exponen en forma detallada en el Capítulo pertinente, destacándose entre las más relevantes, las siguientes:

- Debilidades en el marco normativo y la documentación relacionada con los sistemas de información.
- Incumplimiento de algunos aspectos que surgen de las normas dictadas por el BCRA sobre seguridad física.
- Falta de participación en la administración de la seguridad de algunos servicios ofrecidos por proveedores externos.
- Dificultades en el servicio ofrecido por las redes Link y Maestro que afectan la imagen institucional, involucrando cuentas de depósitos de clientes que acceden a las mismas.
- Falta de automaticidad en el proceso de transferencias entre sucursales.
- Numerosos procesos manuales en la conciliación y registro de operaciones rechazadas en las interfases con el sistema contable.

La adopción de recaudos tendientes a resolver estos aspectos, algunos en vías de implementación, redundará en mejoras en las seguridades física y lógica, a la vez que dotará de mayor eficiencia al traspaso de la información y su intercambio.

A.G.C.B.A.

Dr. Vicente M. Brusca
Presidente
Auditoría General de la
Ciudad Autónoma de Buenos Aires

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

- Entrevistas con el personal jerárquico y operativo de todas las áreas involucradas de las Gerencias de Área de Sistemas, de Seguridad en Tecnologías de Información y Gerentes de Sucursal.
- Revisión de las medidas de seguridad generales.
- Relevamiento y lectura de los siguientes informes producidos por al Gerencia de Auditoría Interna: N° 53/124 (24/07/00), 39/125 (31/05/01) y 66/125 (31/07/01).
- Revisión de las instalaciones del Centro de Cómputos, las áreas informáticas del piso 4° del edificio de Sarmiento 640 y las Sucursales Centro, N° 14 (Barracas), N° 35 (La Lucila) y N° 22 (Once).
- Revisión de la documentación de las interfases con el sistema contable, el recupero de la información rechazada proveniente de las Sucursales, los controles y su automatización.
- Lectura de Manuales Operativos, Normas de Procedimiento y Planes de Contingencia.