INFORME FINAL

Administración de Infracciones

AUDITORÍA INFORMÁTICA

CIUDAD AUTÓNOMA DE BUENOS AIRES
OCTUBRE DE 2004

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

Av. Corrientes 640 - 5to. Piso
Ciudad Autónoma de Buenos Aires

PRESIDENTE:

Lic. Matías Barroetaveña

AUDITORES GENERALES:

Dra. Alicia M. J. Boero

Dr. Vicente Mario Brusca

Dr. Rubén A. Campos

Dr. Nicolás Corradini

Dr. José Luis Giusti

Lic. Josefa A. Prada

CÓDIGO DE PROYECTO:
5-03-26

NOMBRE DEL PROYECTO:
Administración de Infracciones – Auditoría Informática.

OBJETO:
Sistemas de Administración de Infracciones de la Dirección General Administrativa de Infracciones.

OBJETIVO:
a) Evaluar el diseño, arquitectura, organización, documentación, operación y seguridad del Sistema de Administración de Infracciones y subsistemas conexos; b) Examinar el proceso de migración al nuevo sistema, las medidas previstas para dotarlo de adecuada seguridad en el resguardo de la información y las buenas prácticas administrativas relacionadas con el desarrollo del nuevo sistema y el resguardo de los activos informáticos en el ámbito de la Dirección General de Administración de Infracciones.

ALCANCE:
La naturaleza y el alcance de los procedimientos de auditoría aplicados fueron determinados sobre la base de un relevamiento previo de los aspectos normativos, de procedimientos y control, relacionados con las operaciones y funcionamiento de la entidad relevada aplicados sobre la situación vigente al momento de su realización, que comprendió el período de agosto a diciembre del año 2003. (Ver Informes N° 82: Informe 5.07.0.00 Contrataciones de Servicio - DG Administrativa de Infracciones. Auditoria Legal y Financiera - Ejercicio 1999/2000; N° 254: Informe 5.12.01.00 Contratación del Servicio de Control Inteligente de Infracciones de Tránsito; N° 317 Informe 5.21.00.02 DG Administrativa de Infracciones. Relevamiento. Periodo 2001/02).

PERÍODO BAJO EXAMEN:
Agosto - Diciembre 2003.

UNIDAD EJECUTORA:
Dirección General de Administración de Infracciones

EQUIPO DESIGNADO:

Auditor Supervisor:	Dr. Guillermo A. García
Coordinador:	José Recasens
Auditores de campo:	Héctor Zancada Francisco Camean Ariza Oscar Ciarlotti

INFORME FINAL DE AUDITORIA
PROYECTO Nº 5.03.26

Sr. Presidente
De la Legislatura de la Ciudad
Autónoma de Buenos Aires
Lic. Jorge Telerman
S / D

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 Legislatura de la Ciudad Autónoma de Buenos Aires en su artículo número 6 y, supletoriamente la ley 70, esta Auditoria General de la Ciudad procedió a efectuar un examen en el ámbito de la Dirección General de Administración de Infracciones con el siguiente objeto:

I.- OBJETO DE LA AUDITORIA

Sistema de Administración de Infracciones de la Dirección General de Administración de Infracciones.

II.- OBJETIVO DE LA AUDITORIA

a) Evaluar el diseño, arquitectura, organización, documentación, operación y seguridad del Sistema de Administración de Infracciones y subsistemas conexos; b) Examinar el proceso de migración al nuevo sistema, las medidas previstas para dotarlo de adecuada seguridad en el resguardo de la información y las buenas prácticas administrativas relacionadas con el desarrollo del nuevo sistema y el resguardo de los activos informáticos en el ámbito de la Dirección General de Administración de Infracciones.

III.- ALCANCE

Esta auditoria se efectuó sobre la situación vigente al momento de su realización, que comprendió el período de Agosto - Diciembre del año 2003.

Se utilizaron las Normas Básicas de Auditoria Externa de la AGCBA y las Normas Básicas de Auditoria de Sistemas de la AGCBA, comprendidas en la ley 70, ley 325 y complementarias.

Complementariamente se utilizaron:

- Las normas y recomendaciones de seguridad establecidas por la DGEySI.

- Manual de Auditoria Informática de la Sindicatura General de la Nación, SIGEN.
- Manual CISA Edición 2002 y 2003.
- 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.
- Manual COBIT (Control Objectives Information Technologies).

Para la obtención de la información se cumplimentaron los siguientes procedimientos:

- Se solicitó por nota documentación relacionada con el objeto de esta auditoria.
- Se efectuaron entrevistas con el personal jerárquico y operativo del área.
- Se verificó la documentación del sistema de administración de infracciones a implementar en un futuro.
- Se efectuó el análisis de la documentación provista por el área.
  - Expediente 68274/2001;
  - Propuesta técnica UTN-FRBA;
  - Contrato suscripto entre el GBCA y la UTN-FRBA;
  - Actas de Comité de Seguimiento;
  - Vista de documentación de la Dirección General Administración de Infracciones;
  - Resúmenes de cuenta entregados por la Dirección General de Contaduría.

IV.- LIMITACIONES AL ALCANCE:

Los siguientes factores limitaron las tareas de auditoria:

a) Carencia de normas y procedimientos escritos en el circuito administrativo.

V.- ACLARACIONES PREVIAS

El servicio del Sistema de Administración de Infracciones permite la administración de las faltas (principalmente de tránsito vehicular) cuyo tratamiento es competencia del Gobierno de la Ciudad de Buenos Aires (GCBA) a través de la (DGAI) Dirección General de Administración de Infracciones.

Sin embargo, cabe aclarar que las infracciones comprenden no solo las faltas de Tránsito, sino también las infracciones a los códigos de Planeamiento Urbano, publicidad en la vía pública y otros. No incluye las faltas que son competencia de la justicia contravencional que son tratadas por los tribunales respectivos.

Las infracciones de tránsito constituyen el mayor porcentaje de los trámites atendidos por la DGAI las que se confeccionan manualmente y por medio de sistemas fotográficos digitales (concesionados). Esta última modalidad fue introducida recientemente a través de contratos con dos firmas privadas.

El servicio informático para la administración de infracciones está contratado desde el año 1990 a un proveedor externo (UTE-DAI), manteniéndose desde esa fecha, con modificaciones de servicio y de precio respecto de su contratación original[1]. A la fecha de conclusión de las labores de campo dicha contratación se hallaba vencida desde el mes de febrero de 2000 registrándose pagos devengados con la modalidad de “legítimo abono”.

Las infracciones se dividen en manuales (aquellas realizadas por la Policía Federal) y fotográficas (las realizadas por empresas que brindan dicho servicio al GCBA). Las infracciones manuales suman aproximadamente 50.000 por mes mientras que las fotográficas ascienden aproximadamente a 200.000 en el mismo lapso de tiempo.

El Sistema informático en uso (UTE DAI) hasta diciembre de 2003 opera sobre un servidor Mainframe (IBM 390), con programas desarrollados en lenguaje de programación Cobol, estos programas operan sobre base de datos DB2 y archivos VSAM. El servicio que presta la UTE incluye la distribución de las multas manuales a domicilio.

Cuando se implementaron las multas fotográficas el sistema colapsó por el elevado volumen de faltas que ingresaban, lo que generó un caudal de público que sobrepasó la capacidad del servicio y la posibilidad de atención de la dependencia.

La DGAI decidió adecuar el servicio y los sistemas de información a la nueva modalidad administrativa y al procesamiento del mayor volumen de

[1] Para más detalle se puede consultar los siguientes informes de auditoria en www.agcba.gov.ar (informes finales):
- N° 82: Informe 5.07.0.00 Contrataciones de Servicio - DG Administrativa de Infracciones. Auditoria Legal y Financiera - Ejercicio 1999/2000;
- N° 254: Informe 5.12.01.00 Contratación del Servicio de Control Inteligente de Infracciones de Tránsito;
- N° 317 Informe 5.21.00.02 DG Administrativa de Infracciones. Relevamiento. Periodo 2001/02.

infracciones. Para ello solicitó adecuaciones del sistema a la UTE para que se adapte al nuevo régimen operativo y ampliaciones en su capacidad para agilizar los trámites y atender la mayor afluencia de público en junio de 2001. Entre estas modificaciones se incluía la incorporación de más puestos de trabajo con capacidad de consulta (incluyendo la posibilidad de visualizar el acta de infracción), impresión de las multas en línea haciendo más eficiente la tramitación ya que se reemplazaba la búsqueda y manipuleo manual de las actas por su acceso en línea.

La UTE efectuó una propuesta económica mediante la cual llevaba el precio del contrato a $919.660 ($760.050 mas IVA) durante un año y lo reducía a $765.895 ($632.941 más IVA) a partir de ese primer año. El GCBA la aceptó a través de una nota del Secretario del área. La UTE efectuó la inversión y las reformas solicitadas. El GCBA no convalidó los cambios efectuados con la firma de un nuevo contrato tal cual fuera la intención según lo expresado en las notas intercambiadas. Esto generó un reclamo administrativo por parte de la UTE por el capital invertido y los mayores costos que le generaron los cambios en el sistema.

Proyecto Nuevo UTN - FRBA

Contemporáneamente con estos hechos, la Universidad Tecnológica Nacional (UTN) por intermedio de la Facultad Regional de Buenos Aires (UTN-FRBA) efectuó una propuesta para brindar un nuevo servicio de procesamiento en reemplazo del que en ese momento brindaba la UTE. La misma fue realizada en el marco del Convenio de Cooperación Tecnológica existente entre el GCBA y la FRBA suscripto el 18-12-1996. Dicha propuesta, que tenía como objetivo modernizar el Sistema Informático y brindar el Servicio Integral de Procesamiento y Administración de Infracciones fue aceptada y aprobada mediante la suscripción del contrato respectivo de fecha 30-12-2002.

El servicio ofrecido por la UTN-FRBA consiste en el procesamiento de las infracciones, la captura de las infracciones confeccionadas manualmente y la distribución postal de las infracciones llamadas manuales, que son aquellas actas de infracción labradas por la Policía Federal en la Ciudad de Buenos Aires. La distribución postal de las infracciones o multas fotográficas no forman parte del servicio contratado a la UTN-FRBA. El costo del servicio antes descrito asciende a la suma de $602.750 mensuales (ver contrato) alcanzando $7.233.000 al año.

El proyecto UTN-FRBA prevé la reprogramación de los sistemas y su traslado a una plataforma de arquitectura abierta. (Se denominan así a las plataformas basadas en sistemas operativos UNÍX) que corresponde a una tecnología moderna, en lugar de la utilizada hasta el momento (que fue desarrollada en la década del ´70).

En los considerandos de la contratación entre el GCBA y la FRBA para la prestación del servicio integral de procesamiento y administración de infracciones se argumentó que la propuesta era técnicamente satisfactoria como asimismo la existencia de razones de mérito, oportunidad y conveniencia.

El contrato establece un precio mensual de $602.750 para los primeros 36 meses y de $518.365 para los restantes 24 meses. Indica que esta diferencia se podrá destinar "a producir una actualización tecnológica del equipamiento". Para financiar su ejecución el GCBA el 31-12-02 pagó una cuota anticipada del contrato de $602.750. Se trata de un contrato de cinco años por un monto total de $34.139.760,00 (considerando el año de prorroga contemplado en el contrato el monto total ascendería a $40.360.140,00).

No obstante que la nueva contratación estipulaba un inicio de operación a partir del 14 de mayo de 2003, al momento de finalizar las tareas de campo el servicio contratado a la UTN-FRBA no había entrado en operaciones, verificándose una demora de 215 días, contados desde la fecha de inicio del servicio programada hasta el 15 de diciembre de 2003.

VI - OBSERVACIONES

1- Diseño, arquitectura, organización, documentación, operación y seguridad del sistema de administración

1.1- Falta de pautas tecnológicas:
El área competente del GCBA (DGSI - Dirección General Sistemas de Información) no especificó en el contrato las pautas tecnológicas bajo las cuales desarrollar este proyecto. La falta de pautas formales favorece la proliferación de sistemas operativos, bases de datos, lenguajes así como una cantidad desproporcionada de equipos para la atención de las diferentes necesidades del GCBA lo que resulta inadecuados desde el punto de vista técnico. Fecha del examen: Agosto-Diciembre 2003.

1.2- Falta de capacitación:
Al tiempo de culminación de las labores de campo de la presente auditoría, los usuarios de la UACF no han sido capacitados en la operación del Sistema a pesar de que la fecha de lanzamiento según lo informado por los responsables del proyecto sería inminente. Fecha del examen: Agosto-Diciembre 2003.

1.3- Aprobación formal de las nuevas aplicaciones:
No fue aprobada por los usuarios la funcionalidad de los programas de la UACF. Es fundamental que los usuarios aprueben la funcionalidad de la aplicación antes de que la misma se ponga en marcha para asegurar la

satisfacción de los requerimientos exigidos en la ejecución de las tareas que serán apoyadas por el sistema. Fecha del examen: Agosto-Diciembre 2003.

1.4- Pruebas de simulación de proceso real:
No se efectuaron procesos de prueba de operación simulando situaciones reales de modo de determinar las fallas en la operación y en los programas. Fecha del examen: Agosto-Diciembre 2003.

1.5- Pruebas de stress y volumen:
No se efectuaron pruebas de Stress y de volumen de transacciones necesarias para asegurar una adecuada prestación en condiciones de exigencia para las comunicaciones y los procesos. Estas pruebas son imprescindibles en desarrollos de esta envergadura y complejidad. Fecha del examen: Agosto-Diciembre 2003.

1.6- Falta de políticas de seguridad:
No se dispone de una política de seguridad de la información como lo establecía el contrato (ver Anexo III inciso d)[2]. Fecha del examen: Agosto-Diciembre 2003.

1.7- Falta de Requisitos de seguridad:
No se han efectuado los pasos requeridos para la administración de la seguridad de la información ya que:

- No se definió al responsable o "dueño del dato".
- No se efectuó la clasificación de la información en función de su confidencialidad.
- No se definieron formalmente los perfiles de los diferentes usuarios del sistema.
- Fecha del examen: Agosto-Diciembre 2003.

1.8- Falta de procedimientos para la definición de perfiles:
No se dispone de procedimientos para la definición de perfiles. La falta de un análisis de los perfiles de los diferentes usuarios implica el riesgo de que se produzcan accesos indebidos a la información. Fecha del examen: Agosto-Diciembre 2003.

1.9- Falta de procedimientos para otorgamiento de claves:

[2] Las políticas de seguridad son necesarias para organizar la asignación de recursos a la función y encuadrar tecnológicamente la misma, asimismo son indispensables para la protección de la información confidencial perteneciente al GCBA y los ciudadanos de Buenos Aires.

No se dispone de procedimientos formales para el otorgamiento de claves de usuario. La carencia de procedimientos para el otorgamiento de claves impide asegurar que se cumplen con los requisitos que debe guardar la misma (secreta, personal, unívoca, única y otros). Esto facilita el repudio en caso de atentados, destrucción o alteración de la información y releva de la responsabilidad que les corresponde a los usuarios del sistema. Fecha del examen: Agosto-Diciembre 2003.

1.10- Falta de procedimientos para adecuación de las aplicaciones:
No se dispone de procedimientos formales para el control de cambios en los programas de las aplicaciones. Fecha del examen: Agosto-Diciembre 2003.

1.11- Ausencia de procedimientos de copias de respaldo:
No existen procedimientos formales de generación de copias de respaldo (back up). Esto impide asegurar que los mismos serán ejecutados de un modo adecuado, que minimice el riesgo de pérdida de información. Asimismo no se puede asegurar que se cumplirán los requisitos usuales en la materia como por ejemplo, reemplazo y rotación de soportes, existencia de copia en sede externa, ejecución con las frecuencias adecuadas, recuperación de datos según la normativa y otros. Fecha del examen: Agosto-Diciembre 2003.

1.12- Falta de plan de contingencia:
No se dispone de un Plan de Contingencia aprobado por el GCBA. La falta de este plan pone en riesgo la continuidad del servicio que puede verse afectado por diferentes circunstancias. El mismo debe contener el análisis de los escenarios de riesgo, la alternativa de acción para ellos, los factores críticos, el disparador de la ejecución, el rol de cada agente o funcionario en la ejecución, y otros. Fecha del examen: Agosto-Diciembre 2003.

1.13- Carencia de un plan de recuperación de desastre:
No se dispone de un Plan de Recuperación de Desastre. Esta carencia hace que no este asegurada la restitución del servicio de un modo eficiente luego de que se superen las causas de su suspensión por contingencia. Fecha del examen: Agosto-Diciembre 2003.

1.14- Propiedad de los programas fuente:
El contrato no especifica la propiedad de los programas fuente ni la responsabilidad por el resguardo de los mismos durante el contrato. El contrato no aclara la propiedad de los programas fuente sino que hace referencia a que los aplicativos o programas en general pasarán a ser propiedad del GCBA al finalizar el contrato, lo que implica el riesgo de que se entreguen programas objeto y se excluyan los programas fuente. Los programas fuente son esenciales para poder efectuar el mantenimiento de la aplicación y deben

mencionarse taxativamente en los contratos. Las reglas del arte de la informática especifican además que el servicio de desarrollo que se contrata a un tercero incluye la tenencia de una copia de los programas fuente en sede de terceros especificando las circunstancias bajo las cuales el contratante puede solicitarlos. La falta de este recaudo puede impedir la continuidad del servicio por causas ajenas al GCBA. Asimismo, al final del contrato el desarrollo queda en poder del GCBA para lo cual este deberá contar con los programas fuente para poder seguir operando o introducir modificaciones.

1.15- Derechos de copyright:
El contrato no incluye el copyright de los desarrollos y programas a favor de la Ciudad. Los desarrollos contratados fueron pagados por la Ciudad, por lo tanto es esta la dueña de los programas. La propiedad de los mismos impide que estos sean vendidos o utilizados sin pagar por ellos o en forma no autorizada. Fecha del examen: Agosto-Diciembre 2003.

1.16- Relación con el proveedor a cargo de personal transitorio:
El tratamiento de la relación con el proveedor en la DGAI no incluye a personal de planta. La falta de personal que tenga continuidad en la gestión en el tratamiento de las cuestiones relativas al sistema implica que se pierda la experiencia obtenida a través del tiempo por el hecho de trabajar con el mismo al producirse cambios de funcionarios. Fecha del examen: Agosto-Diciembre 2003.

2- Proceso de migración. Seguridad en el resguardo de la información y resguardo de los activos informáticos.

2.1- Falta de políticas de seguridad:
No se dispone de un manual de políticas de seguridad. Las políticas de seguridad son necesarias para organizar la asignación de recursos a la función, encuadrar tecnológicamente la misma y definir el nivel de riesgo que se va a asumir. Fecha del examen: Agosto-Diciembre 2003.

2.2- Falta de Requisitos de seguridad:
No se han efectuado los pasos requeridos para la administración de la seguridad de la información ya que:

- No se definió al responsable o “dueño del dato”.
- No se efectuó la clasificación de la información en función de su confidencialidad.

No se definieron formalmente el alcance de la funcionalidad permitida a cada perfil en función de los dos puntos anteriores. Fecha del examen: Agosto-Diciembre 2003.

2.3- Falta de procedimientos para la definición de perfiles:
No se dispone de procedimientos formales para la definición de perfiles. La falta de un análisis de los perfiles a habilitar a los diferentes usuarios implica el riesgo de que se produzcan accesos indebidos a la información por falta de correspondencia entre la función y las funciones habilitadas por el sistema al perfil. Fecha del examen: Agosto-Diciembre 2003.

2.4- Falta de procedimientos para el otorgamiento de claves:
No se dispone de procedimientos formales para el otorgamiento de claves de usuario. La carencia de procedimientos para el otorgamiento de claves impide asegurar que se cumplen con los requisitos que debe guardar la misma (secreta, personal, unívoca, única y otros.) Esto facilita el repudio en caso de alteración de la información y releva de la responsabilidad que les corresponde a los usuarios del sistema. Fecha del examen: Agosto-Diciembre 2003.

2.5- Falta de procedimientos para la adecuación de aplicativos:
No se dispone de procedimientos formales para el control de cambios en los programas de los aplicativos. Este requisito es necesario para asegurar una actualización eficiente del aplicativo y evitar que la misma se produce en condiciones inseguras para la funcionalidad y la información. Fecha del examen: Agosto-Diciembre 2003.

2.6- Falta de planes de contingencia, evacuación y recuperación de desastre:
No se dispone de un Plan de contingencia, Plan de Evacuación, Plan de Recuperación de Desastres. Esto implica riesgos para la continuidad de la operación y en caso de producirse un corte prolongado recuperar eficientemente el estado previo al colapso. Fecha del examen: Agosto-Diciembre 2003.

VII- RECOMENDACIONES

1- Diseño, arquitectura, organización, documentación, operación y seguridad del sistema de administración

1.1- Falta de pautas tecnológicas:
La DGSI (Dirección General de Sistemas de Información dependiente de la Subsecretaría de Gestión Operativa de la Secretaría de Hacienda) debe definir el marco tecnológico en el que se desenvolverán los proyectos actuales y futuros del GCBA como parte de una política formal para los sistemas de información.

1.2- Falta de capacitación:
Se deben capacitar adecuadamente todos los usuarios del sistema en el uso del nuevo aplicativo de modo de poder iniciar la operación sin contratiempos.

La aprobación de la capacitación debe respetar las mismas formalidades del punto anterior[3].

1.3- Aprobación formal de las nuevas aplicaciones:
Obtener la aprobación formal de los usuarios del sistema de la funcionalidad del nuevo aplicativo. Hacer constar en actas dicha aprobación y hacerla suscribir asimismo por auditoria interna. Se debe dar cumplimiento a todos los requisitos de una adecuada metodología antes de la puesta en marcha del servicio de forma de minimizar los riesgos de fracaso y detectar los inconvenientes antes de que impacten en la operación real[4].

1.4- Pruebas de simulación de proceso real:
Efectuar pruebas de simulación de proceso real una vez se haya finalizado la migración de datos en un ambiente de prueba. Este paso permite ajustar detalles y detectar fallas de cualquier índole y evitar que impacten en el proceso real.

1.5- Pruebas de Stress y volumen:
La metodología requiere efectuar y aprobar formalmente las pruebas de stress y volumen antes del inicio de la operación. El ente auditado informa que no fue posible efectuar en tiempo y forma las pruebas debido al retraso en la recepción de la información. Las futuras adecuaciones deberán incluir este paso antes de la puesta marcha de las mismas.

1.6- Falta de políticas de seguridad:
Definir políticas de seguridad formales. La carencia de políticas de seguridad impide que la función se desarrolle con los recursos adecuados en un marco tecnológico claro y que quede difuso el nivel que debe alcanzar[5].

1.7- Falta de Requisitos de seguridad:
Dar cumplimiento a los requisitos de seguridad mencionados de modo de comenzar la operación garantizando la integridad, confidencialidad, y calidad de la información del GCBA y los ciudadanos, ya que haber mantenido los perfiles de usuario existentes en el sistema anterior no garantiza el cumplimiento de los requisitos observados.

1.8- y 1.9- Falta de procedimientos para la definición de perfiles y claves:

[3] En oportunidad del descargo del presente informe, el auditado remitió fotocopia de un cronograma de capacitación UACF realizada entre el 26-01-04 al 04-02-04 adjuntando una serie de planillas de asistencia. Al no informar si alcanzó a toda la planta y si resultó efectiva, se mantiene tanto la observación como la recomendación efectuada, la que será objeto de seguimiento en futuras auditorias.

[4] En oportunidad del descargo del presente informe, el auditado afirma haber realizado la aprobación funcional firmada por los usuarios referentes de la UACF. En este sentido, puede observarse que dicha aprobación fue efectuada con la salvedad que la firma de cada usuario solo avala "la impresión de la pantalla" conforme surge de la documentación remitida. Consecuentemente, no se ha aprobado la funcionalidad, por lo que se mantiene tanto la observación como la recomendación efectuada, la que será objeto de seguimiento en futuras auditorias.

[5] En oportunidad del descargo del presente informe, el auditado remitió fotocopia de un documento de normas de seguridad. Si bien dichas normas, en general, son correctas, no resultan suficientes para conformar una política, por lo que se mantiene tanto la observación como la recomendación efectuada, la que será objeto de seguimiento en futuras auditorias.

Definir y aprobar procedimientos para la definición de perfiles formales y el otorgamiento de claves[6].

1.10- Falta de procedimientos para adecuación de aplicaciones:
Definir y aprobar procedimientos formales para la adecuación de aplicativos.

1.11- Ausencia de procedimientos de copias de respaldo:
Incorporar procedimientos formales para la ejecución de las copias de respaldo de modo de minimizar la posibilidad de pérdida de información especificando reemplazo y rotación de soportes, copia en sede externa, frecuencias, responsables de la ejecución, procedimiento de recuperación de datos y otros. El auditado informa haber actualizado a posteriori este tema y adjunta en el descargo procedimientos cuya eficacia y eficiencia será objeto de futuras auditorias de seguimiento.

1.12- Falta de plan de contingencia:
Confeccionar un plan de contingencia. Someterlo a aprobación de la autoridad correspondiente.

1.13- Carencia de un plan de recuperación de desastre:
Confeccionar un plan de recuperación de desastre que especifique los pasos necesarios para la restitución del servicio en forma ordenada, rápida y efectiva de tal manera que se minimice el período de aplicación de la modalidad contingente.

1.14- Propiedad de los programas fuente y 1.15- Derechos de Copyright:
Confeccionar una adenda al contrato que aclare que el GCBA es propietario de los programas fuente y dueño del copyright. Asegurar que se disponga siempre de una versión actualizada de los programas fuente.

1.16- Relación con el proveedor a cargo personal transitorio:
Incorporar personal de planta en el tratamiento de los temas referidos a la operación, adecuación, reforma, etc., independientemente de la inclusión de otros funcionarios que la autoridad decida incorporar.

2- Proceso de migración: Seguridad en el resguardo de la información y resguardo de los activos informáticos

2.1- Falta de políticas de seguridad:
Definir políticas de seguridad formales. La carencia de políticas de seguridad impide que la función se desarrolle con los recursos adecuados en un marco tecnológico claro y que quede difuso el nivel que debe alcanzar.

2.2- Falta de Requisitos de seguridad:

[6] Dicho procedimiento se encuentra insinuado en el documento de normas de seguridad remitido en oportunidad del descargo del presente. Sin embargo, no se encuentra redactado como procedimiento por lo que se mantiene tanto la observación como la recomendación efectuada, la que será objeto de seguimiento en futuras auditorias.

Dar cumplimiento a los requisitos de seguridad mencionados de modo de comenzar la operación garantizando la integridad, confidencialidad, y calidad de la información del GCBA y los ciudadanos.

2.3- Falta de procedimientos para la definición de perfiles:
Definir y aprobar procedimientos para la definición de perfiles formales.

2.4- Falta de procedimientos para el otorgamiento de claves:
Definir y aprobar procedimientos para el otorgamiento de claves.

2.5- Falta de procedimientos para la adecuación de aplicativos:
Definir y aprobar procedimientos formales para la adecuación de aplicativos.

2.6- Falta de planes de contingencia, evacuación y recuperación de desastre:
Confeccionar un plan de contingencia. Someterlo a aprobación de la autoridad correspondiente. Confeccionar un plan de recuperación de desastre que especifique los pasos necesarios para la restitución del servicio en forma ordenada, rápida y efectiva de tal manera que se minimice el período de aplicación de la modalidad contingente.

VIII- CONCLUSIONES

Del análisis realizado surge que la Universidad Tecnológica Nacional - Facultad Regional Buenos Aires ha acumulado un importante atraso en el cumplimiento del contrato suscripto el 30 de diciembre de 2002 que preveía como fecha de inicio de la prestación del servicio el 14 de mayo de 2003 desde que el mismo entró en operaciones recién a principios del corriente año.

Al cierre de las tareas de campo de este trabajo de auditoria la última fecha para dar comienzo a la migración de los sistemas para que la UTN-FRBA se haga cargo de los mismos fue fijada para mediados de enero de 2004. En efecto aún restan muchas tareas por realizar especialmente dentro de la UACF. Todavía hay módulos que no fueron aprobados formalmente por los usuarios como los de la UACF, no se han hecho pruebas piloto con intervención de los usuarios, no se cuenta con una adecuada capacitación de los usuarios de la UACF.

Los antecedentes del contrato exhiben contradicciones respecto de lo decidido con otros importantes servicios de procesamiento tercerizados como el SIAC (Sistema Integral de Administración de Cobranzas), de la Dirección General de Rentas ya que en el presente contrato no se mantuvo la arquitectura de procesamiento. El GCBA dispone de un equipo con esa arquitectura con el 80% de su capacidad de procesamiento ociosa que podría haber soportado el proceso con ligeros ajustes. El gasto en equipamiento, la conversión del software y el trabajo de implantación del nuevo sistema son inversiones que finalmente recaen sobre el GCBA.

La Dirección General Sistemas Informáticos dio su visto bueno sin intervenir en la decisión ya que no fijó criterios tecnológicos, no solicitó ni verificó la capacidad técnica y la experiencia del futuro proveedor ni efectuó un análisis de costos minucioso. Con el proyecto ya avanzado (24 de junio de 2003) se incorporó al comité de seguimiento para solicitar el cumplimiento de algunos aspectos metodológicos descuidados por el proveedor.

A la fecha de la aprobación final del este informe, como es de público conocimiento, el Sistema de Administración de infracciones está siendo operado por el nuevo proveedor que comenzó a brindar el servicio a fines de Febrero de 2004.

HECHOS POSTERIORES AL EXAMEN DE AUDITORÍA:

La Dirección General auditada informó en su descargo del 9 de agosto de 2004 las diversas acciones y modificaciones implementadas sobre el objeto de la presente Auditoría. Dichas acciones fueron realizadas con posterioridad al cierre de la tarea de campo del presente examen lo que implica que su verificación se realizará en oportunidad de la próxima auditoria que se planifique para dicha organización.

Las modificaciones y/o implementaciones realizadas son las siguientes:

1- La capacitación se efectuó enero de 2004. Adjunta planilla de asistencia.

2- La aprobación formal de las nuevas aplicaciones se efectuó firmando las pantallas. El usuario aclaró que su firma solamente avalaba “la impresión de la pantalla”. Se adjunta manual de usuarios (versión julio/2004) con instructivo para uso UACF para el perfil controlador. No hay ningún otro perfil.

3- Debido a la demora del proveedor anterior en efectuar la entrega de los diseños de archivos y los datos para la migración, se produjo un atraso en la puesta en marcha del sistema de stress y volumen, con la consecuencia de que se realizaron sólo en forma parcial. Como resultado de ello, se realizaron correcciones en la conectividad y en la configuración del equipamiento utilizado para la prestación del servicio.

4- Se adjunta Proyecto Normas Sobre Seguridad Informática, elaborado por Universidad Tecnológica Nacional.

5- Con respecto a los Requisitos de seguridad se mantuvieron perfiles del sistema anterior.

6- En relación con los procedimientos para la definición de perfiles *se* adjunta normas de seguridad donde estos procedimientos están descriptos.

7- Se adjunta procedimientos descritos para el otorgamiento de claves.

8- Se adjunta documento de Control de Cambios, para los procedimientos de adecuación de las aplicaciones, cuya segunda versión (1.1) se encuentra en proceso de aprobación.

9- Con respecto a la Propiedad de los programas fuente *se* expresa que tanto los programas fuente como los derechos de copyright serán de propiedad del GCBA. La documentación correspondiente está en proceso de redacción y suscripción por las partes; será incorporada como addendum al contrato suscripto, junto con las definiciones de "dueño del dato", confidencialidad de la información.

10- Lo mismo ocurre con los Derechos de copyright.

11- Relación con el proveedor a cargo de personal transitorio: La relación con el proveedor involucra personal de planta, tanto del área de Sistemas de la DGAI, como de diversas direcciones pertenecientes a la Dirección General de Sistemas de Información.

12- Con respecto a las políticas de seguridad se adjunta el documento con las Normas de Seguridad.

13- Requisitos de seguridad. Se mantuvieron los perfiles de usuario existentes en el sistema anterior.

14- Procedimientos para la definición de perfiles. Se define en el mencionado documento de Normas de Seguridad.

15- Procedimientos para el otorgamiento de claves; también mencionado en las Normas de Seguridad.

16- Procedimientos para la adecuación de aplicativos: Se adjunta documento de Control de Cambios, cuya segunda versión (1.1) se encuentra en proceso de aprobación.