AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

AGCBA

INFORME FINAL DE AUDITORIA

PROYECTO Nº 4.22.00.00

SISTEMAS INFORMÁTICOS DE LOS ÓRGANOS RECTORES

PERIODO 2001

Buenos Aires, diciembre de 2002

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

Av. Corrientes 640 piso 5º Capital Federal

Presidente

Dr. Vicente Mario Brusca

Auditores Generales:

Dr. Jorge Argüello

Dr. Nicolás Corradini

Dra. Noemí Fernández Cotonat

Dr. Daniel Rodríguez

Dra. Gabriela Serra

Dr. José María Pazos

FOLIO 3

CODIGO DE PROYECTO:
4.22.00.00

NOMBRE DEL PROYECTO:
Sistemas Informáticos de los Órganos Rectores

PERIODO BAJO EXAMEN:
Año 2001

FECHA DE PRESENTACIÓN DEL INFORME:

EQUIPO DESIGNADO:

Director de Proyecto:	Dr. Ricardo Martín, Lic. en Economía
Supervisor:	Dr. José Juffar, Contador Público
Auditores:	Ing. José Recasens
	Ing. Rodolfo Bella
	Ing. Adolfo Nicolosi
	Sr. Héctor Zancada
	Sr. Nicolás Diner
	Lic. Francisco Camean
	Sr. Oscar Ciarlotti

OBJETIVOS: Auditoría informática que permita opinar sobre los sistemas y sus condiciones de integración, funcionalidad, performance, seguridad y resguardo.

A.G.C.B.A.

Departamento Operaciones de Auditoría
INFORME FINAL
de la
Unidad Especial de Auditoría

Informe Final de Auditoria
Proyecto Nº 4.22.00.00

DESTINATARIO

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

En uso de las facultades conferidas por los artículos, 131,132 y 136 de la Ley 70, y conforme a lo dispuesto en el artículo 135 de la Constitución de la Ciudad, hemos procedido a hacer un examen en el ámbito de la Dirección General de Tesorería, la Dirección General de Contaduría y la Oficina de Gestión Pública y Presupuesto

I. OBJETO DE LA AUDITORÍA

Evaluación de los aplicativos y de los sistemas operativos, la seguridad física y lógica de los servidores involucrados en los sistemas informáticos de gestión y administración financiera usados por la Dirección General de Tesorería, la Dirección General de Contaduría y la Oficina de Gestión Pública y Presupuesto.

II. ALCANCE

El examen fue realizado de conformidad con las 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 161/00.

El trabajo se llevó a cabo en el período comprendido entre el 17 de Julio de 2001 y el 30 de Abril de 2002, habiéndose aplicado los procedimientos que se detallan en el Anexo I.

La revisión se practicó sobre las aplicaciones SISER (Dirección General de Contaduría), SIPRIN (Oficina de Gestión Pública y Presupuesto) y C.U.T. (Dirección General de Tesorería), y sobre los servidores que las soportan, comprendiendo los siguientes centros de procesamiento:

A.G.C.B.A.

Departamento Operaciones Especiales
INFORME FINAL
de la
Contaduría General de la Ciudad de Buenos Aires

- Red de Área Metropolitana (MAN), y Centro de Cómputos y Procesamiento de Datos de la Dirección General de Sistemas de Información (DGSI)
- Redes locales (LAN) de los principales organismos del sistema.

La evaluación de los mecanismos relacionados con la administración, el control de accesos y las rutinas de auditoría del aplicativo SISER se efectuó a partir de una muestra seleccionada en forma aleatoria mediante la utilización de técnicas de muestreo estadístico, que comprendió 88 usuarios del sistema, con un nivel de confianza del 95% y una precisión del 10%.

III. LIMITACIONES AL ALCANCE

El alcance previsto para el presente trabajo de auditoría se ha visto limitado debido a los siguientes factores:

a. La Contaduría General no ha suministrado una cantidad significativa de documentación respaldatoria de altas, asignación de perfiles y de passwords de usuarios del SISER, solicitados para su consulta.

   La documentación respaldatoria no recepcionada correspondiente a 49 usuarios representa el 56% de la muestra seleccionada. Esta documentación fue solicitada oportunamente mediante nota AGCBA N° 2889/01 del 23/10/01 y reiterada mediante nota AGCBA N° 3187/01.

b. La Contaduría General no ha suministrado, al cierre de las tareas de campo, la documentación referida a:

   - Descripción General de la Base de Datos del sistema SISER.
   - Detalle del software con que cuenta dicha base de datos.
   - Contenido de cada una de las tablas del sistema.

Cabe mencionar, no obstante, que con posterioridad a dicho cierre, con fecha 22/7/2002, se recibió vía correo electrónico el contenido de tablas del sistema aludido en el tercero de los puntos mencionados, el que no pudo ser considerado en razón de haber concluido los procedimientos de campo.

Esta documentación fue solicitada oportunamente mediante nota AGCBA N° 2801/01 del 18/10/01 y reiterada mediante notas AGCBA N° 3216/01 y AGCBA N° 954/02.

La carencia de esta documentación, y en particular el no haber podido contar en tiempo y forma con las estructuras de datos de cada una de las tablas del sistema, impidió realizar un análisis acabado de la calidad de los aplicativos y de su correspondencia con las técnicas en uso al momento de su desarrollo y en la actualidad.

IV. ACLARACIONES PREVIAS

Breve descripción de las áreas examinadas

Dirección General de Sistemas de Información (DGSI):

- **Red de área metropolitana (MAN). DGSI**

  La Red de Área Metropolitana (Red MAN) constituye el vínculo que permite establecer la conectividad digital entre las diferentes reparticiones y organismos del Gobierno de la Ciudad con el Centro de Procesamiento de Datos. Mediante la misma son posibles los servicios de comunicaciones y conectividad tales como: el Correo Electrónico, Internet y el procesamiento remoto en sistemas como SISER y SIPRIN, que comparten distintos organismos.

- **Centro de Cómputos y Procesamiento de Datos. Servidor para la aplicación Sistema Integral de Servicios (SISER). DGSI**

  El centro de procesamiento de datos del Gobierno de la Ciudad de Buenos Aires está situado en dependencias de la Dirección General de Sistemas de Información, en Av. Independencia 635. El mismo tiene a su cargo el funcionamiento operativo del servidor Sun Solaris que es el ordenador principal donde reside la aplicación llamada Sistema Integral de Servicios (SISER), que constituye el núcleo central de los aplicativos examinados.

Principales organismos usuarios del sistema:

- **Redes Locales (LAN)**

  Los sistemas informáticos de los órganos rectores son operados fundamentalmente por tres organismos: Oficina de Gestión Pública y Presupuesto (OGEPU), la Dirección General de Tesorería (Tesorería) y. la Dirección General de Contaduría (Contaduría. Antes de que se pusiera en marcha el SISER, estos tres organismos tenían sus propios sistemas y sus propias redes. Actualmente cada uno de ellos conserva su red local (LAN) con su administración independiente de cualquier otro organismo. OGEPU está en una ubicación geográfica distante de Tesorería y Contaduría, mientras que estos últimos tienen asiento en edificios contiguos en la Av. Belgrano 836/38. Cabe aclarar que la red de la Tesorería se vincula a la MAN por una conexión dependiente de la Contaduría.

  Estas tres redes de administración independiente se conectan al Centro de Cómputos de DGSI en la Av. Independencia 635 por la red MAN, para operar en el servidor la aplicación SISER. Las aplicaciones complementarias, SIPRIN y

CUT no residen en el centro de cómputos de DGSI; cada una de ellas reside en el servidor de la red local respectiva (CUT en Tesorería y SIPRIN en OGEPU).

Breve descripción de los Sistemas:

Los sistemas informáticos de los Órganos Rectores están constituidos por un sistema principal, llamado SISER (Sistema Integral de Servicios) y dos sistemas que lo complementan: CUT (Cuenta Única del Tesoro) y SIPRIN (Sistema de Programación de Inversiones).

SISER:

El SISER es la aplicación principal: en esta se registran los recursos y gastos, estos últimos en las etapas presupuestarias del compromiso preventivo, compromiso definitivo, devengado, liquidado y mandado a pagar. Además de la información del año en curso, se procesa en este aplicativo la información del presupuesto del año siguiente.

Este sistema fue utilizado por primera vez para procesar el presupuesto 2000. La contratación se efectuó para ..."garantizar el correcto funcionamiento de los sistemas vigentes en el marco del efecto 2000, en forma previa a la ejecución del proyecto integral de reforma de los sistemas de administración financiera y de gestión." En consecuencia, el SISER no fue concebido como una solución definitiva e integrada, al punto que preveía la programación de interfases con aplicaciones existentes, como los sistemas CUT (Tesorería) o Liquidación de Haberes, hasta tanto se contratara un sistema integral cuyo pliego habría de elaborarse. El proceso licitatorio del sistema definitivo no había sido iniciado al cierre de las tareas de campo.

Actualmente, el SISER guarda las registraciones correspondientes al ejercicio en curso, el siguiente, y los años anteriores a partir del 2000 inclusive.

Esta es una aplicación crítica ya que es el soporte fundamental de las registraciones contables y presupuestarias del Gobierno de la Ciudad. El ejercicio 2001 es el segundo presupuesto que se procesa en la misma. Eventuales fallas en el procesamiento de esta aplicación podrían implicar la paralización de los pagos del Gobierno de la Ciudad.

La administración del SISER está a cargo de la Contaduría y el equipo que lo procesa reside en la DGSI.

El aplicativo SISER utiliza la red MAN del Gobierno de la Ciudad de Buenos Aires, y el procesamiento se efectúa sobre un equipo SUN, con un Sistema operativo SUN Solaris (Unix). El lenguaje de desarrollo es C-Fix dentro del conjunto de herramientas denominado Ideafix de la firma Intersoft. El servicio de instalación y mantenimiento es provisto por la firma ASICOMP SRL. La Red de contaduría funciona en ambiente Novell.

CUT:

La aplicación CUT es la que administra la etapa del pagado, que se realiza a partir de las ordenes de pago (mandado a pagar) emitidas por Contaduría. Una vez procesado el pago una interfaz actualiza en el sistema SISER la operación. Esta interfaz informática fue desarrollada en Tesorería.

Los recursos ya no son registrados en esta aplicación, siendo ingresados directamente en el sistema SISER.

La administración de este aplicativo, residente en la red local de Tesorería, está a cargo de esta repartición.

La red y el aplicativo CUT funcionan en ambiente Windows NT. La aplicación está desarrollada en lenguaje Visual Basic.

SIPRIN:

En la aplicación SIPRIN se procesa la información presupuestaria de los proyectos cuya programación excede el año. El SIPRIN permite que cada repartición cargue sus proyectos con el detalle de cada año, permitiendo el seguimiento de los mismos.

SIPRIN fue desarrollado durante el año 2001 y se lo ha utilizado para el procesamiento de proyectos que afecten el presupuesto 2002 y años siguientes.

La información procesada en la aplicación SIPRIN se ingresa al SISER manualmente.

Este aplicativo funciona en un servidor independiente dentro de la red Windows NT perteneciente a la OGEPU, sobre Windows 98, y está desarrollado en Microsoft Access. Su administración está a cargo de la OGEPU.

Por último, la información histórica de los presupuestos anteriores a la implantación del SISER es administrada por la OGEPU. Allí reside un servidor RISC 6000 (IBM RS 6000) con el sistema que se usaba para procesar el presupuesto antes del SISER. Estos presupuestos (1999 y años anteriores) son consultados por las reparticiones cuando requieren dicha información.

El aplicativo SIPRIN utiliza la red MAN del Gobierno de la Ciudad de Buenos Aires.

Metodología

Para la elaboración del presente informe se utilizó el criterio de clasificación de riesgos de vulnerabilidad de los sistemas elaborado por la Sindicatura General de la Nación, que especifica los siguientes perfiles:

- **Alto:**
  Representa que el aspecto evaluado cuenta con importantes debilidades en los procedimientos de control, que pueden significar que la operatoria del organismo sufra un perjuicio grave.

- **Medio:**
  Se incluyen dentro de esta clasificación aquellas observaciones referidas a procedimientos de control que si bien existen y funcionan, no es posible asegurar que cubran la totalidad del objetivo de control que pretenden cubrir.

- **Bajo:**
  El aspecto evaluado no presenta debilidades o las existentes no tienen importancia relativa. Igualmente es conveniente aclarar que los controles manuales y computarizados están diseñados para proveer una seguridad razonable, pero no absoluta, de que no ocurrirán errores o irregularidades.

A los efectos de una mejor comprensión de las observaciones y sus respectivas recomendaciones, excepto las de carácter general, han sido ordenadas por cada ambiente que participa en el procesamiento de la información: Centro de Cómputos DGSI, Red Contaduría, Red Tesorería y Red OGEPU.

En Anexos II, III y IV se grafican los distintos vínculos y accesos al Sistema SISER, la relación entre las áreas usuarias, los sistemas y sus módulos, y la estructura del sector que administra, mantiene y desarrolla el aplicativo SISER.

FOLIO 10

V. OBSERVACIONES

Aspectos Generales.

1. Las aplicaciones informáticas de los Órganos Rectores no constituyen un sistema integrado.

   Los pagos se realizan mediante una aplicación llamada CUT (Cuenta Única del Tesoro), que funciona independientemente del SISER y los presupuestos cuya duración excede los 12 meses son cargados en la aplicación SIPRIN, que también es independiente del SISER.

   Además, algunos módulos principales que, por los volúmenes monetarios y la jerarquía del gasto, deberían estar integrados al SISER, no lo estaban al momento de esta auditoría (Ej.: Compras y Contrataciones, Liquidación de Haberes, Administración de Bienes).
   La falta de integración genera ineficiencia en el sistema de administración financiera, que se traduce en tareas duplicadas de carga de datos, con los consiguientes riesgos de inconsistencia y la necesidad de efectuar controles y operar interfases que podrían evitarse.

2. Se generan tareas redundantes o procedimientos diferentes para operaciones iguales (por ejemplo: tareas de back up, administración de la seguridad) con superposición de funciones.

   Los sistemas CUT, SISER y SIPRIN están instalados en redes y servidores independientes en edificios geográficamente dispersos, y tienen su procesamiento y su administración descentralizada en diferentes organismos, según se describe en el apartado de Aclaraciones Previas de este informe. Esto genera las redundancias y superposiciones mencionadas.

   No existe un procedimiento unificado para las tareas de resguardo de información (backup), y ésta responsabilidad no está centralizada en una única área. Cada aplicación y red de área local tiene un procedimiento propio e independiente.

   La falta de unificación de los procesos y procedimientos perjudica la eficiencia y produce un debilitamiento del control interno.

A.G.C.B.A.

3. No hay procedimientos escritos para las rutinas de resguardo de información (back up) en las redes locales, con la sola excepción de la red OGEPU. Esto

implica el riesgo de fallas en la ejecución de la tarea, en especial cuando se producen cambios en el personal que la realiza, al tiempo que diluye la responsabilidad del ejecutor por no estar descrito con precisión el alcance de la misma.

4. La falta de algunos elementos importantes y de bajo costo no se justifica frente al impacto económico de una posible pérdida de información.

   La falta de reposición adecuada de cintas para resguardo de información, cuyo valor es de U$S 100 por unidad, constituye un ejemplo de esta carencia, máxime si se tiene en cuenta que a través de estos sistemas y redes, se procesa la totalidad del presupuesto y el gasto del GCBA. Las cintas antes mencionadas son imprescindibles para mantener los resguardos de la información de los sistemas en niveles aceptables de seguridad; su carencia impide, entre otras cuestiones, guardar backup de cierres de ejercicio.

   Por otra parte, en Tesorería no se dispone de dispositivos adecuados para el manejo de información, tales como Zip Drive o grabador de CD ROM, y en Contaduría se carece de un dispositivo para el grabado de cintas magnéticas (Tape Backup).

5. No se aplica una política de capacitación de los agentes que tienen a su cargo la administración de las redes y las aplicaciones.

   Los sistemas y las redes van creciendo en complejidad sin el adecuado nivel de entrenamiento de sus responsables, al tiempo que continuamente se producen cambios tecnológicos que obligan a una actualización permanente.

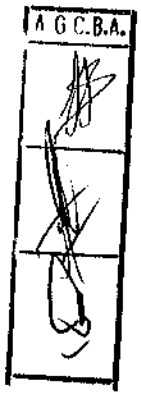
   La falta de capacitación se refleja en la no implementación de mejoras y actualizaciones en las redes y los sistemas, lo que reduce el aprovechamiento de las tecnologías informáticas.

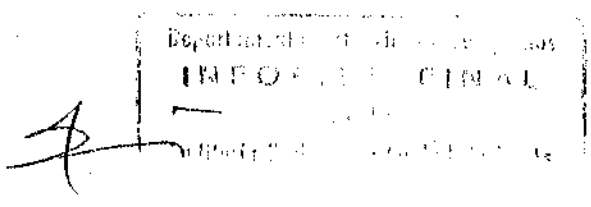
Red OGEPU:

6. No hay una sala especial para el servidor y los switches.

   Si bien estos se encuentran en un gabinete cerrado con llave, el cableado y el servidor no están protegidos contra eventuales intrusiones.

7. Existe subutilización de equipos.





La información de los presupuestos anteriores al 2000 es procesada en un servidor exclusivo (RISC 6000) con una impresora de formulario continuo de alta velocidad dedicada a esta única tarea. A partir de la implementación del SISER, el servidor utilizado pasó a ser un Sun Solaris residente en la DGSI, el cual contiene todos los presupuestos a partir del año 2000. En consecuencia, el equipo RISC 6000 dejó prácticamente de utilizarse, quedando disponible al solo efecto de entregar información de los presupuestos anteriores al 2000 guardados en él.

El equipo RISC 6000 trabaja con un sistema operativo desactualizado, emulando un computador Wang. Esta información es consultada muy ocasionalmente, y con el correr del tiempo lo será cada vez menos, por lo que no se justifica el porte del equipamiento destinado para este fin.

Además, la configuración aludida ocasiona problemas para su continuidad y obliga a mantener hardware y software innecesarios, creando un incremento de tareas y costos.

Aplicación SIPRIN:

8. SIPRIN es una aplicación no integrada al SISER, que carece de interfases para transferir a esta aplicación la información ingresada en ella.

   La falta de integración hace necesario el ingreso de datos y la realización de controles que podrían evitarse, con los consiguientes riesgos de discrepancia en la información redundante que albergan los sistemas.

   Esta debilidad está presente a pesar de que SIPRIN fue desarrollada con posterioridad al SISER, que constituye el sistema informático principal para la administración financiera.

9. Los niveles de seguridad son deficientes.

   El desarrollo no tiene seguridad lógica a nivel de la base de datos. Sólo se utiliza la seguridad del sistema operativo (Windows 98) para proteger la información. Este factor incrementa la vulnerabilidad y el riesgo de accesos indebidos y pérdida de información.

10. La aplicación SIPRIN fue desarrollada con una herramienta inadecuada para tareas corporativas (Access), ya que no soporta el procesamiento multiusuario.

    La aplicación SIPRIN debería ser utilizada en red y permitir el acceso simultáneo a la misma de múltiples organismos y reparticiones que, en algunos casos, se encuentran en edificios distantes del sitio en que se ubica el servidor que la

aloja. Sin embargo la herramienta informática con que fue desarrollada es inadecuada para funcionar en esta modalidad de uso.

Debido a ello surgen problemas funcionales que obligan a utilizar soluciones poco eficientes, como por ejemplo el uso de directorios separados por cada organismo o repartición.

11. El Sistema SIPRIN adolece de limitaciones funcionales.

    El Sistema permite totalizar la cantidad de proyectos cargados en la base de datos, pero no totalizar los montos que estos involucran.

    Esto genera dificultades en el manejo de la información y los recursos además de repetición de tareas, provocando ineficiencia en el trabajo.

12. La interfaz de uso de la aplicación SIPRIN no es funcional ni amigable.

    Esta aplicación no permite cargar información parcial de un proyecto, ya que los registros deben completarse para ser admitidos por la misma.

    Esto provoca pérdidas de tiempo y demoras en el trabajo que afectan la productividad administrativa.[1]

Red Contaduría:

13. Se comprobó la inexistencia de un Plan de Contingencia que indique las acciones y procedimientos que garanticen la continuidad de los servicios de procesamiento frente a situaciones imprevistas o de desastre.

    Asimismo se carece de un plan de evacuación y sus prácticas periódicas.

    Si se produjera un desastre, la falta de planificación reflejada en la carencia de estos planes pone en riesgo la información y la continuidad de los procesos.

14. La red de Contaduría carece de vínculo alternativo o de respaldo para su conexión con la DGSI, donde reside el servidor principal del SISER (ver gráfico en Anexo 1).

A G C.B.A.

[1] La OGEPU, con motivo del descargo a este informe, informa que hacia fines de agosto de 2002, ha incorporado un nuevo sistema SIPRIN.

Si el vínculo existente (red MAN) tuviera complicaciones, ni la Contaduría ni la Tesorería podrían operar el sistema.

15. El procedimiento de back-up ejecutado en Contaduría no brinda protección en caso de desastre, resultando además más costoso de lo necesario.

    El back-up consiste en una copia realizada sobre otro disco dentro del mismo servidor, lo cual es antieconómico, impidiendo además guardar un juego de back up en sede externa, a efectos de prevenir cualquier siniestro que pudiera afectar al mismo tiempo a ambos discos.

    Esto aumenta el riesgo de pérdida de la información.

16. No están separadas formal ni funcionalmente las tareas de mantenimiento edilicio, como reparación de cañerías, problemas de humedad y otros, y las correspondientes al área de sistemas, que tiene a su cargo la red, los servidores, y el correcto funcionamiento de los puestos de trabajo. Ambas tareas son ejecutadas por el mismo funcionario, que revista como responsable de mantenimiento del edificio.

    Esta superposición de funciones es inadecuada para las responsabilidades propias de la administración de una red de envergadura que se utiliza en tareas críticas, afectándose la eficiencia del área de sistemas.

Aplicación SISER:

17. La dependencia del Gobierno de la Ciudad Autónoma de Buenos Aires respecto de la empresa Asicomp S.R.L., proveedora del sistema SISER, es alta.
    Esta situación de dependencia es generada por los siguientes factores:

    - El SISER fue adquirido a la empresa Asicomp S.R.L. mediante la Licitación Privada N° 106/99. En este pliego está taxativamente indicado que "no se requiere la entrega de los programas fuentes". Como consecuencia de esta situación la empresa es, necesariamente, la encargada de realizar tanto el desarrollo como el mantenimiento del sistema.

    - El mercado de especialistas en Ideafix –nombre comercial del motor de la base de datos del aplicativo SISER, cuyo lenguaje de programación es el C-fix - es muy reducido, por lo que el Gobierno de la Ciudad está seriamente limitado para modificar la relación de dependencia que tiene con la empresa.

Como consecuencia de lo observado precedentemente, el Gobierno de la Ciudad se convierte en un cliente cautivo de la empresa Asicomp S.R.L. mientras utilice el aplicativo SISER.

18. No hay separación de ambientes entre Desarrollo y Producción del sistema SISER.

La buena práctica aconseja generar al menos un entorno de desarrollo separado del ambiente de producción, de modo que las modificaciones a los programas puedan compilarse y probarse con un conjunto coherente de datos antes de su traslado al entorno productivo. Esto minimiza el riesgo de problemas emergentes de cambios en el sistema, al par que hace posible quitar a los desarrolladores permiso sobre los archivos y demás objetos de producción.

La falta de una adecuada segregación de los ambientes mencionados en el título constituye una falla grave de la seguridad, ya que los desarrolladores estarían en condiciones de modificar la información real de los sistemas debido a que disponen de acceso a los datos y conocen en profundidad el funcionamiento de la aplicación.

19. No hay un adecuado control por oposición en la administración de la seguridad lógica del SISER.

El grupo de trabajo en Contaduría administra la seguridad del sistema operativo del servidor y de la aplicación SISER, al tiempo que es el encargado de efectuar el mantenimiento del aplicativo y el desarrollo de nuevos programas.

El manejo de la seguridad unificado con el desarrollo o mantenimiento de los programas constituye una seria debilidad del control interno.

20. Parte del personal que desempeña tareas de sistemas en la Dirección General de Contaduría no está formalizado.

Durante el desarrollo de la aplicación SISER se formó un grupo de trabajo con personal de distintas reparticiones (Tesorería, Contaduría, OGEPU, DGSI). Este personal revista en sus respectivas áreas de origen, a pesar de haberse terminado el desarrollo de la aplicación y de que cumplen su tarea en la Contaduría.

Esta situación genera inconsistencia entre la responsabilidad formal y la real.

21. No se halló evidencia de la existencia de procedimientos escritos para la definición de perfiles de usuarios.

    Esto impide que se pueda definir con precisión el alcance del accionar del nuevo usuario en el momento de solicitar el alta, lo que afecta el control sobre los accesos a la información.

22. No se cumple con los procedimientos escritos que establecen los pasos a seguir por los usuarios y por el grupo que administra el aplicativo SISER para la solicitud de altas de usuarios.

    Se detectó una cantidad significativa de usuarios dados de alta en el sistema sin la correspondiente solicitud, según se detalla en el punto a de las Limitaciones al Alcance.

23. El procedimiento para la baja de usuarios no garantiza que el listado de usuarios se encuentre debidamente actualizado.

    El mismo no incluye la comprobación sistemática mediante cruces con información proveniente del Sistema o del área de Personal, que permita asegurar que se cumple acabadamente con este requisito.

24. No se aplica el procedimiento para la baja de usuarios.

    Al analizar el "Listado de Comprobantes generados por Usuario" se detectaron 53 usuarios (el 60% de la muestra) que no registran movimientos en el periodo 01/01/2001 al 26/09/2001. Ninguno de estos usuarios figura como "inactivo", dado de baja o estado análogo en el Listado de Usuarios al 20/09/2001.

    Esto revela que los agentes que dejan de pertenecer a la Dirección o cambian de área podrían continuar accediendo a la misma información que utilizaban antes del cambio, aumentando el riesgo de accesos indebidos y la vulnerabilidad de los sistemas.

    La situación descripta implica una debilidad del control interno.

25. La responsabilidad de algunas tareas de administración de la seguridad y desarrollo del SISER está en manos de personal con contratos temporarios.

    La eventual interrupción de los servicios que presta este personal contratado por el GCBA podría acarrear serios problemas en las prestaciones, en caso de que

A.G.C.B.A.

los contratos se suspendan o discontinúen abruptamente, por motivos presupuestarios u otros.

26. La identificación de usuarios no es unívoca.

Se detectaron casos de usuarios repetidos, esto es, dos o más números de usuario distintos con dos o más claves y perfiles para un mismo agente.

Sobre un universo de 989 perfiles de usuario, 83 correspondían a personas con 2 o más perfiles, lo que representa el 8,4% del total.

Esta falta de unicidad en los números de identificación de usuario atenta contra el control interno, ya que tanto el listado de auditoria, como el listado de comprobantes generados por usuario, se obtienen ingresando al sistema el número del usuario en cuestión, con lo cual no existe seguridad de que en estos listados se puedan obtener todos los movimientos del agente consultado.

En Anexo V se señalan los casos mencionados.

27. Dentro del Sistema SISER no resulta amigable determinar los alcances de las funciones de consulta y de sus perfiles.

Las opciones de consulta con que cuenta cada usuario dentro del sistema no resultan fácilmente identificables tanto a nivel de usuario como de grupo. Si bien dentro del menú de "administración del sistema" existe una opción que permite ver el menú de opciones de cada perfil, resulta muy poco práctico (sobre todo debido a la rigidez de la interfaz con el usuario) analizar cada menú para determinar cuales son las opciones de consulta de cada usuario.

Asimismo, resulta dificultoso determinar el alcance de los perfiles de usuarios ya que no es posible consultarlo en forma individual. Esto significa que para ver los permisos de un usuario es necesario consultar a qué grupo pertenece el mismo, y ver qué permisos tiene asignado ese grupo. En la consulta de permisos por usuario sólo figuran los que el usuario en cuestión tiene por fuera del grupo al cual pertenece. Esto hace más complicada la verificación del perfil del usuario respectivo.

28. Se detectaron 16 casos de usuarios que realizaron transacciones dentro del sistema sin permiso o autorización explícita para su ejecución. Los casos fueron detectados sobre comprobantes que no eran críticos para la registración contable y presupuestaria del Gobierno de la Ciudad.

En Anexo VI se detallan los casos mencionados.

A G C.B.A.

29. Se detectaron elementos que ponen de manifiesto problemas de continuidad y performance del aplicativo SISER.

- Los datos históricos obtenidos de los registros estadísticos proporcionados por la Mesa de Ayuda del SISER, correspondientes a los años 2000 y 2001, presentan la siguiente información:

	Año 2000	***Año 2001***
Total Horas sin Sistema	172,3	337,45
Total Horas Laborables	1525	3000
Porcentaje de Horas sin Sistema	**11,30%**	**11,25%**
Total Días con Caídas	70	117
Total Días Laborables	122	240
Porcentaje de Días con Caídas	**57,40%**	**48,75%**

Es de destacar que no se produjo ninguna mejora significativa en el año 2001 respecto del año 2000 en cuanto a la estabilidad del aplicativo SISER.

- En ocasiones se produce una saturación del sistema como consecuencia de operaciones de carga de datos, que impiden a los usuarios realizar operaciones en forma normal.

Esta saturación se produce a pesar de tratarse del ingreso de una reducida cantidad de registros, tal como se observó en el Departamento Liquidador de Servicios Básicos de la Dirección General de Contaduría. En este sector se cargan desde un medio magnético (disquete), en un proceso batch, los datos de facturación telefónica, tardando en ocasiones más de 2 horas para procesar menos de 1,5 mb.

30. No se ha obtenido evidencia de la existencia de procedimientos escritos que establezcan los pasos a seguir por los usuarios para la solicitud de modificaciones correctivas e innovativas en el sistema SISER.

Se detectaron casos en que los usuarios recurren directamente a la empresa Asicomp S.R.L.– proveedora del aplicativo SISER y encargada de su mantenimiento y desarrollo- para solucionar estos inconvenientes.

A G C.B.A.

La ausencia de normas escritas repercute en una disminución de la eficiencia en el mantenimiento y desarrollo de los sistemas, generando un obstáculo para estimar plazos de ejecución, asignar adecuadamente recursos y aprovechar las ventajas de una correcta planificación.

31. Las rutinas de auditoría practicadas a nivel de administrador del sistema en el aplicativo SISER no son confiables:

    - Se detectaron diferencias entre la información surgida del "Listado de Comprobantes Generados por Usuario" y el "Listado de Auditoría por Usuario". En Anexo VII se detallan los casos señalados.
    - En el "Listado de Auditoría por Usuario" se observó la existencia de registros de transacciones que presentan información inconsistente. En el Anexo VIII se adjunta un listado con ejemplos de estos registros.
    - No se registran las transacciones de los usuarios relacionadas con consultas.

32. En el Departamento Responsables (Dirección General de Contaduría), mediante pruebas de control, se detectó un error en el control de consistencia, por el cual el sistema SISER permite registrar e imputar el Mandado a Pagar por un importe superior al del Compromiso Definitivo.

    Si bien los errores que pueden resultar de esta falla son detectados más adelante en el circuito administrativo mediante controles manuales, el hecho de que se produzcan deficiencias de validación en puntos tan críticos como el mencionado evidencia una debilidad del control interno.

33. En el ciclo de registración contable / presupuestaria el "Devengado" no se contabiliza en el momento oportuno.

    Esto se produce porque, si bien el articulo 31 del decreto 1000 reglamentario del articulo 59 de la ley 70 indica que el "Devengado" se produce a partir de la recepción en conformidad de bienes o servicios oportunamente contratados, en la práctica esta registración contable se realiza en el sistema SISER junto con el "Mandado a pagar". Esto se debe a que el sistema no tiene incorporada la posibilidad de emitir el correspondiente certificado de recepción definitiva, de tal manera de producir luego en forma automática el asiento contable o presupuestario correspondiente.

34. Se detectaron errores y deficiencias en las informaciones generadas por el sistema SISER que en algunos casos llegaban a hacer inutilizables las mismas por parte de los usuarios, tales como:

    - En la "Consulta de Cuotas – Ejecución" de la jurisdicción 40, programa 2371, inciso 2, no coincide el "Crédito Vigente" con la suma de las 4 cuotas trimestrales correspondientes, según se muestra a continuación:

      Crédito Vigente $33.108.753
      ∑ Cuotas (1-4) $31.037.360

Diferencia $ 2.071.393

- Cuando se emite una Orden de Pago a la que se le realizan descuentos en la Dirección General de Contaduría el "Importe Total " en letras no coincide con el "Total a Pagar".

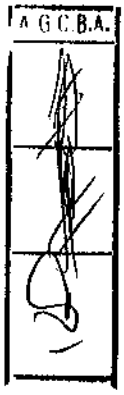
- Cuando se produce una desafectación parcial sobre un compromiso preventivo, la misma es registrada sin respetar el criterio cronológico. Esto se produce porque la desafectación es registrada en la misma fecha en que se realizó la afectación original y no en el momento en que ésta realmente se produjo.

Estas deficiencias disminuyen la confiabilidad de la información brindada por el sistema.

35. El nivel de complejidad de la interfaz con el usuario del aplicativo SISER es alto.

La interfaz de este aplicativo es de "sólo texto". Esta situación plantea limitaciones, principalmente en la presentación de datos (títulos mal encuadrados, mala distribución de la información presentada).

La situación comentada implica una importante merma en la facilidad de operación de las funciones del sistema, la cual resulta menos intuitiva que la permitida en la actualidad por los sistemas informáticos que cuentan con una interfaz gráfica.



FOLIO 21

Red Tesorería:

36. La función de mantenimiento y administración de este servicio carece de procedimientos escritos, y es ejecutada por una estructura que no está contemplada en el organigrama formal de la repartición.

    Esto implica que no se explicitan formalmente las responsabilidades, misiones y funciones, lo que desdibuja los límites y la definición de las tareas a cargo de los agentes, afectando la calidad de la gestión.

37. Se comprobó la inexistencia de un Plan de Contingencia que indique las acciones y procedimientos que garanticen la continuidad de los servicios de procesamiento frente a situaciones imprevistas o de desastre.

    Asimismo, el sector carece de un plan de evacuación. Estos planes, que deben ser periódicamente ensayados, son particularmente necesarios en dependencias como la aquí observada, que por sus características edilicias (rejas en las ventanas, escasa cantidad de salidas del edificio con falta de señalización, obstrucción de pasillos y puertas, etc.) y por la cantidad de personal que se desempeña en ella, dificultan una posible evacuación en caso de siniestro.

    Si se produjera un desastre, la falta de planificación reflejada en la carencia de estos planes pone en riesgo las vidas humanas, la información y la continuidad de los procesos.

38. El Centro de Cómputos que alberga a los servidores de la red de Tesorería y de la aplicación CUT, y a los respectivos switches, no cuenta con un lugar adecuado, debido a que presenta deficiencias en la regulación de la temperatura ambiente y no permite controlar el acceso de personas ajenas al sector.

    La falta de condiciones adecuadas pone en riesgo la seguridad de la red y de la información.

39. El área de sistemas carece de medios básicos y elementales para sus funciones (ejemplo: disquetes, zip drives, renovación de baterías de la UPS de los servidores).

    Estas carencias atentan contra la calidad del trabajo del área y la seguridad de la información, y obligan a buscar soluciones inadecuadas para el trabajo habitual.

40. No existe una red eléctrica que alimente en forma exclusiva la totalidad de la red de datos.

La misma red eléctrica es utilizada para los datos y para artefactos de uso cotidiano (calentadores, estufas de cuarzo, etc); consecuentemente, se generan picos de tensión por sobrecarga.

Esto incrementa el riesgo de caídas en la red e interrupción en las tareas de procesamiento, con pérdida de información y de tiempo por parte de los usuarios de la red.

41. No hay ningún mecanismo de protección de la información que se envía al Banco de la Ciudad para que haga efectivos los pagos a proveedores.

La información del sistema CUT se transmite al Banco de la Ciudad de Buenos Aires para que se efectúen los pagos, por un sistema de línea telefónica (dial up) sin ningún nivel de seguridad, protección, encriptación o firma digital.

Esto atenta contra la confiabilidad, la confidencialidad y la integridad de la información enviada.

42. No existe un procedimiento rutinario y formal para dar de baja a los usuarios de la red.

En consecuencia, los agentes que dejan de pertenecer a la Dirección o cambian de área, podrían continuar accediendo a la misma información.

Teniendo una carga innecesaria de usuarios se aumenta la exposición al riesgo y la vulnerabilidad de los sistemas.

Aplicación CUT:

43. La aplicación CUT no se encuentra integrada al SISER, lo que obliga a procesar una interfase con las transacciones del SISER que impactan en el sistema CUT, y posteriormente aquellas procesadas en esta aplicación que impactan en el SISER.

Esto incrementa el riesgo de inconsistencia de la información entre los dos sistemas por la posibilidad de errores en los procesos, ocasionando tareas redundantes y comprometiendo la integridad y confiabilidad de los datos.

44. No hay división de funciones entre la administración de la seguridad, la operación del sistema, y las eventuales tareas de mantenimiento.

Esto implica que todas las responsabilidades sobre la administración de este aplicativo recaen sobre la misma área.

Esta concentración de funciones atenta contra la integridad y confiabilidad de los datos.

45. No existe un doble juego de respaldo de los servidores de la red local; por consiguiente, tampoco existe guarda en sede externa de un respaldo de datos alternativo al de uso habitual.

Esta condición se establece para una mayor protección de la información en caso de desastre.

La situación observada aumenta el riesgo de pérdida de la información.

Centro de Cómputos en DGSI. Red MAN. Servidor SISER

46. El servidor SISER está visible en la red MAN para usuarios de la red del Gobierno de la Ciudad de Buenos Aires, que no son usuarios del sistema SISER, no obstante necesitarlo una cantidad acotada de organismos, y de usuarios dentro de cada uno de ellos.

Este factor aumenta su riesgo y vulnerabilidad, ya que se expone al servidor a un mayor número de posibles ataques.

47. No se emplea tecnología de protección de servidores al sistema SISER, respecto de los accesos que se efectúan a través de la red MAN.

Esta tecnología de protección de servidores en las redes consiste en establecer filtros para ingreso y egreso de información, direcciones IP, servicios, protocolos y otros.

La carencia de estas tecnologías aumenta el riesgo y la vulnerabilidad del servidor y la información contenida en él.

A.G.C.B.A.

48. Hay subutilización de equipamiento.

    Se está utilizando un computador Sun Ultra 5 como consola de acceso al servidor principal. La consola de acceso es el medio que utiliza el administrador para realizar tareas en el servidor. El personal responsable del servidor en DGSI suele acceder para estas tareas desde sus puestos de trabajo habituales, sin trasladarse físicamente al Centro de Cómputos, que está ubicado en otro piso del edificio.

    Este ordenador, emplazado junto al servidor principal, constituye una solución antieconómica, ya que se trata de un equipo de gran capacidad y alto costo.

49. El personal del área de Sistemas de Base y de Seguridad de DGSI es insuficiente para el normal desarrollo de las tareas.

    Frente a situaciones como vacaciones o enfermedad de alguno de ellos las áreas antes mencionadas quedan sin personal a cargo.

    Esto pone en riesgo la continuidad del servicio.

50. No se dispone de instrucciones escritas acerca de como proceder en caso de paradas de emergencia en el servidor SISER.

    Si se produjeran estas paradas en horarios o días en que el personal responsable del servidor no se encuentra disponible, el personal de guardia no tiene instrucciones escritas de los pasos a seguir para levantar nuevamente el servidor y sus servicios. Esto ocasionaría pérdidas de tiempo, atentando contra la continuidad de los servicios.

51. La ubicación física del servidor SISER (SUN) es inadecuada debido a la presencia de un mueble que obstruye el fácil acceso al dispositivo.

    Ello hace que resulte sumamente dificultoso el acceso al botón de apagado y encendido, y a sus cables y dispositivos.

    En caso de una emergencia, se pone en riesgo la seguridad del servidor y las conexiones del mismo.

52. Se comprobó la inexistencia de un Plan de Contingencia que indique las acciones y procedimientos que garanticen la continuidad de los servicios de procesamiento frente a situaciones imprevistas y de desastre. Asimismo, se carece de un plan de evacuación y sus prácticas periódicas.

Si se produjera un desastre, la falta de planificación reflejada en la carencia de estos planes pone en riesgo la información y la continuidad de los procesos.

53. El servidor principal en el que opera el SISER carece de procesamiento alternativo (server back up).

No existen convenios con algún otro centro de cómputos para asegurar un respaldo para el mismo.

Frente a una falla de hardware en el servidor Sun que requiera una reparación prolongada, todo el sistema quedaría fuera de operación.

54. No hay monitoreo del servidor ni análisis sistemático del log file en el sistema Sun Solaris. Además, se carece de parte diario, semanal o periódico de novedades del servidor o la aplicación y su correspondiente análisis.

El servidor genera en forma automática un archivo (log file) donde se detallan situaciones tales como accesos, paradas, modificaciones en los directorios, usuarios, problemas de sistemas, etc. Los administradores del sistema operativo y la aplicación (el grupo de trabajo en Contaduría) no analizan esta fuente de información para generar partes rutinarios que permitan tener estadísticas de uso del servidor y de la aplicación, estabilidad, paradas, etc.

Estos análisis permiten tomar medidas correctivas, prever situaciones de riesgo, mejorar la performance del equipo y los sistemas, detectar cuellos de botella por concurrencia simultanea de usuarios y realizar controles de seguridad, entre otras mejoras que se derivarían de la información que se podría obtener si se observaran estas rutinas.

55. No se halló evidencia de que se efectúe un adecuado seguimiento de la actividad de la red ni de los intentos de acceso fallidos al Servidor.

Lo observado incrementa el riesgo de intrusiones al equipo y a la información administrada en el mismo.

A G C.B.A.

56. Las cintas en uso para el back up del servidor son insuficientes, y se encuentran al límite de su vida útil.

Éstas superan el año y medio de uso ininterrumpido. Las que están en uso son las entregadas originalmente con el equipo servidor principal. Algunas de ellas ya han presentado fallas irrecuperables y fueron sustituidas por la cinta de otro

día (ej.: falla en la del día martes, se la sustituye en la rotación por la del día domingo y se deja de hacer respaldo de datos ese día). La cantidad de cintas sólo permiten un juego de back up diario.

Frente a la solicitud de compra de nuevos juegos de cinta en cantidad suficiente para cumplir con las normas habituales de seguridad en los back up, se adquirió (al momento de la auditoría en el Centro de Cómputos de DGSI) una sola cinta de valor aproximado a ese momento U$S 100 (en concordancia ver Observaciones, Aspectos Generales, punto 4).

Estas carencias comprometen la continuidad de los servicios y la seguridad de la información en sistemas críticos.

57. No hay segundo juego de respaldo de la información del SISER.

La inexistencia de un segundo juego de cintas de resguardo de la aplicación SISER impide la guarda en sede externa de un respaldo de datos alternativo al de uso habitual. Esta condición se establece para una mayor protección de la información en caso de desastre.

Esta carencia aumenta el riesgo de pérdida de la información y de ruptura de la continuidad de los servicios. Si hubiera alguna situación de desastre en el Centro de Cómputos se perdería toda la información existente sin posibilidad de recuperación.

58. No hay respaldo de datos para cortes históricos del sistema SISER (ejemplo: el corte de fin de mes o el de los trimestres).

Todas las cintas se usan en la rotación semanal del back up diario (esquema: una cinta para el Lunes, otra para el Martes, etc.), a pesar de que en los sistemas contables es necesario contar con respaldos que luego permitan reconstruir la información a un momento dado.

Esta falta atenta contra la seguridad de la información e impide la reconstrucción antes mencionada en caso de que fuera necesaria.

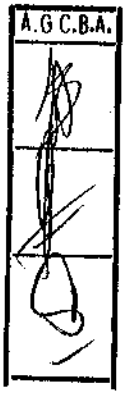
59. No hay un adecuado respaldo del sistema operativo.

A.G.C.B.A.

Actualmente hay un solo juego de resguardo para el mismo, y este back up se realiza mensualmente. No hay segundo juego de respaldo de la información del sistema operativo.

Por consiguiente, tampoco existe guarda en sede externa de un respaldo alternativo al de uso habitual, condición necesaria para la protección de la información en caso de desastre.

En consecuencia, si hubiera alguna situación de desastre en el Centro de Cómputos se perdería la configuración en uso del sistema operativo –tal como la definición de la seguridad-, dificultando y demorando innecesariamente la eventual recuperación.



VI. RECOMENDACIONES

Las recomendaciones que siguen, que se corresponden numéricamente con las observaciones respectivas, no poseen carácter vinculante, quedando a criterio del administrador el modo más conveniente de resolver los problemas señalados en cada caso.

Aspectos Generales.

1. Adoptar las acciones necesarias para implementar un sistema integrado que comprenda el sistema de pagos, el presupuesto plurianual y el sistema de registración presupuestaria (actualmente CUT, SIPRIN y SISER, respectivamente), configurando un sistema único de forma tal que se concentren bajo un mismo servidor y sistema operativo, soportados por la DGSI, las aplicaciones que procesen la totalidad del circuito contable y presupuestario. A este sistema central deberían integrarse luego todos los demás módulos de gestión financiera, así como el sistema de Liquidación de Haberes.

   Ello permitiría unificar las tareas habituales tales como back up, actualizaciones de sistemas operativos, configuración de la red, seguridad, etc., con el consiguiente ahorro de recursos informáticos, humanos y de procedimientos.

2. Evaluar la factibilidad de centralizar la administración y procesamiento de las aplicaciones en un único servidor, unificando las rutinas de mantenimiento y resguardo de la información con el consiguiente ahorro de tareas y recursos.

3. Las rutinas de resguardo de la información deben estar documentadas en todos los casos.

4. Realizar las acciones necesarias para obtener los medios y recursos que aseguren la continuidad y el funcionamiento de los sistemas informáticos.

5. Programar cursos de capacitación para los administradores de las redes y el personal de sistemas, a fin de proporcionarles las herramientas necesarias para hacer frente al crecimiento de la red, así como para incorporar las nuevas tecnologías que aparecen por la constante evolución de la técnica.

Red OGEPU:

6. Mudar los servidores y el hardware de red a la sala donde hoy está el servidor que contiene la información de los presupuestos anteriores. De esta forma se incrementaría la seguridad del acceso a los mismos.

A.G.C.B.A.

7. Considerar la factibilidad de migrar la información histórica al SISER, de modo de liberar el equipamiento dedicado hoy en exclusiva a su guarda y eventual consulta.

Aplicación SIPRIN:

8. Integrar en un sistema único, según se señala en la recomendación N° 1, el tratamiento de los proyectos de incidencia presupuestaria plurianual. Hasta tanto esto se realice, evaluar la conveniencia de transferir información automáticamente entre estas aplicaciones.

9. El nuevo desarrollo debe contemplar medidas de seguridad más sólidas que las actuales y mejoras en la interfaz de captura de datos.

10. El nuevo desarrollo debe ser realizado con una herramienta adecuada para actividades corporativas.

11. Tomar los recaudos necesarios para que en un nuevo desarrollo no se repitan las limitaciones funcionales de las que adolece el SIPRIN.

12. Un nuevo desarrollo debe contar con una interfaz con el usuario amigable y funcional.

Red Contaduría:

13. Generar un Plan de Contingencia.

14. Activar un vínculo alternativo con DGSI. En lo posible, utilizar hardware hoy en desuso, que se encuentra en el centro de cómputos.

15. Generar, con los medios adecuados y de uso común para estas tareas, un sistema de doble juego de back up. Uno de estos juegos debe guardarse en sede externa, que no corra el riesgo de ser afectada por el mismo siniestro que podría destruir la información original.

16. Formalizar las tareas y funciones del área de sistemas y su personal desligando al área de las funciones de mantenimiento edilicio.

Aplicación SISER:

17. Arbitrar los medios necesarios para modificar la relación de dependencia que en la actualidad tiene el Gobierno de la Ciudad con la empresa Asicomp S.R.L., proveedora del sistema SISER.

18. Separar adecuadamente los ambientes en desarrollo y producción para incrementar la seguridad y la confiabilidad de la información, adecuando, además, la organización y el procedimiento de puesta en producción de las aplicaciones.

19. Desafectar de la administración de la seguridad al grupo de trabajo y los desarrolladores, trasladando esta responsabilidad al área específica para esta función en el Centro de Cómputos de la DGSI. Evaluar la factibilidad de unificar, por razones de seguridad, metodología y economía, la administración de la seguridad de las aplicaciones relacionadas con los órganos rectores en el área de la DGSI especializada a ese efecto. Además, en lo posible, el área especializada en sistemas operativos de la DGSI, debiera encargarse del entorno operativo.

20. Formalizar el destino, las tareas y funciones del grupo de trabajo que contribuyó al desarrollo del SISER. Procurar la coincidencia entre la situación de revista formal y la real, asignando nuevas tareas en los casos en que se estime necesario.

21. Formalizar los procedimientos de asignación de perfiles.

22. Verificar el efectivo cumplimiento de los procedimientos escritos referidos al alta de usuarios en el sistema. Actualizar la documentación de los usuarios existentes en el sistema cuando corresponda.

23. Establecer un procedimiento periódico y formal para depurar las tablas de usuarios, definiendo previamente los criterios a emplear.

    Formalizar el procedimiento de bajas de usuarios de forma de asegurar que no permanezcan en las tablas aquellos agentes que por traslados, cambio de función u otro motivo deban resignar la facultad de acceder a la información. El mismo deberá contemplar la revisión periódica de los usuarios inactivos.

A.G.C.B.A.

24. Contenida en 23.

25. El personal temporario incorporado durante el desarrollo del SISER debe hacer un traspaso de conocimientos y responsabilidades críticas al personal estable designado a ese efecto.

26. Incluir dentro del procedimiento de asignación de claves un mecanismo de identificación de usuario que permita determinar indubitablemente a quién pertenece para asegurar que exista un perfil único para cada agente.

27. Generar un informe que permita conocer el alcance de la clave de forma clara y completa para cada usuario así como sus atribuciones para consultas.

28. Analizar las causas de estas acciones no contempladas en el alcance del perfil, y subsanarlas.

29. Instrumentar las medidas necesarias para que el gasto y el presupuesto públicos sean administrados por un sistema que cumpla los requisitos de continuidad y performance que su importancia amerita.

30. Establecer y normar mecanismos coherentes y eficientes para la solicitud y realización del mantenimiento correctivo e innovativo del sistema SISER.

31. Realizar los ajustes y cambios necesarios para que las rutinas de auditoría realizables al sistema SISER sean confiables.

32. Adoptar las medidas necesarias para solucionar la falla de control señalada.

33. Realizar los cambios necesarios para que el Devengado sea registrado en tiempo y forma, a partir de la emisión por el SISER del correspondiente certificado de recepción definitiva o documento análogo.

34. Adoptar los recaudos necesarios para solucionar los errores y deficiencias detectados en las informaciones emitidas por el SISER.

35. Evaluar las posibles soluciones al problema de la baja amigabilidad de la interfaz con el usuario que presenta el aplicativo SISER.

Red Tesorería:

36. Formalizar el área de sistemas, su personal, tareas, responsabilidades y funciones.

37. Generar un Plan de Contingencia.

38. La Tesorería y la Contaduría se encuentran en edificios contiguos; por lo tanto, parece aconsejable reubicar los servidores y switches de Tesorería, evaluando la factibilidad de emplazarlos físicamente en el Centro de Cómputos de Contaduría, el cual cuenta con un buen nivel de seguridad. Ello permitiría además liberar

para otros usos el espacio que hoy los aloja. Este traslado físico no implica el abandono de la administración de la red por parte del personal de la Tesorería.

También parece recomendable analizar la variante de trasladar el servidor que soporta la aplicación CUT a la DGSI (Independencia 635). Ello permitiría incorporar esta aplicación a la rutina de back up general de la institución y operarla con personal independiente del área usuaria.

39. Dotar al área de sistemas con los medios adecuados a las tareas que realizan.

40. Es altamente conveniente que la alimentación de energía a la red de datos esté completamente separada de la red eléctrica de uso común.

41. Implementar niveles de seguridad en la información y el vinculo entre la Tesorería y el Banco Ciudad por medio de controles de accesos, encriptación y firma digital.

42. Establecer un procedimiento periódico y formal para depurar las tablas de usuarios, definiendo previamente los criterios a emplear.

Aplicación CUT:

43. Integrar en un sistema único, según se señala en la recomendación N° 1, el tratamiento de la etapa presupuestaria del pagado.

44. En lo posible, transferir la administración de la seguridad al área pertinente de la DGSI.

45. Generar, con los medios adecuados y de uso común para estas tareas, un sistema de doble juego de back up del CUT y la red. Uno de estos juegos debe guardarse en sede externa.

Centro de Cómputos en DGSI. Red MAN. Servidor SISER

46. El servidor debería estar en una red segmentada restringiendo la conexión sólo a las reparticiones habilitadas, para no exponerlo a usuarios de la red que no son usuarios del sistema SISER, reduciendo así los niveles de riesgo y vulnerabilidad.

47. Implementar los medios que disminuyan la vulnerabilidad de los servidores involucrados en el procesamiento de la información, implementando tecnologías de protección de servidores (Por ejemplo: firewalls, VPN cliente servidor).

A.G.C.B.A.

48. Un simple teclado permitiría el acceso al servidor. Evaluar el aumento de la capacidad del computador SUN Netra I (usado actualmente como consola de acceso al servidor del SISER) para que pueda servir como servidor de desarrollo y servidor alternativo de respaldo del principal.

49. Asignar la dotación adecuada de personal idóneo de software de base y seguridad en DGSI, organizando la tarea de modo que exista suficiente relevo de los agentes. Asimismo, mantener a este personal en un plan de capacitación continua.

50. Documentar adecuadamente los procedimientos e instrucciones, no sólo los rutinarios sino también aquellos que deben ser utilizados en caso de emergencia o imprevistos.

51. Corregir la ubicación del servidor SISER. El lugar debe contemplar seguridad y espacio suficiente como para tener un fácil acceso al mismo.

52. Generar un Plan de Contingencia.

53. Ídem recomendación N° 48.

54. Generar un parte periódico de incidentes en el servidor y la aplicación, con su respectivo análisis.

55. Implementar un software y una rutina de monitoreo de la red que advierta sobre posibles intrusiones en el servidor SISER y otros servidores críticos. Además, implementar un análisis y seguimiento sistemático del log file para mejorar su seguridad y sus prestaciones.

56. Proveer los medios necesarios para las tareas de back up. Tener en disponibilidad un juego de cintas vírgenes para ir reemplazando a aquellas que llegan al fin de su vida útil recomendada, ya que la sobre utilización crea un riesgo innecesario.

57. Generar un doble juego de respaldo de la información SISER y del sistema operativo contemplando para uno de estos juegos la guarda en sede externa.

58. Efectuar un back up de los cortes de cierres contables como mínimo anualmente.

59. Efectuar un back up de respaldo para el Sistema operativo, cada quince días o semanalmente, con rotación de un segundo juego de respaldos, guardado en sede externa.

A.G.C.B.A.

VII. CONCLUSIONES

Vulnerabilidad:

De acuerdo a los niveles de vulnerabilidad mencionados en las Aclaraciones Previas, los ambientes auditados fueron evaluados como se expone a continuación:

- Centro de Cómputos (DGSI): nivel bajo, dado que cuenta con un buen entorno de seguridad, aunque no está totalmente aprovechado.
- Red MAN: nivel medio.
- Redes locales: nivel medio.
- SISER: nivel alto
- SIPRIN: nivel alto
- CUT: nivel alto

El nivel de vulnerabilidad alto asignado a los sistemas SISER, SIPRIN y CUT se desprende de las observaciones efectuadas. En particular, resultan de mayor relevancia las que se refieren al primero de ellos, descriptas en los puntos 18 a 29 del capítulo V. OBSERVACIONES, y dentro de éstas, las dos primeras. Esta auditoría considera aconsejable evaluar la factibilidad y conveniencia de trasladar al ámbito de la DGSI, que provee funciones de procesamiento central y conectividad a través de los servicios instalados en el equipo Sun Solaris y la red de área metropolitana (MAN), las funciones inherentes a la seguridad del SISER, normalizando y perfeccionando los procedimientos que se aplican y creando conciencia entre los usuarios acerca de la importancia de esta función.

Cabe señalar, por otra parte, que respecto de la evaluación de los procedimientos de altas de usuarios y asignación de perfiles en el sistema SISER, el trabajo de auditoría se ha visto limitado debido a que la Contaduría General no ha suministrado una cantidad significativa de documentación, según se señala en las Limitaciones al Alcance descriptas en el punto a del apartado III.

Sistemas de aplicación:

Respecto del software de aplicación, la no obtención en tiempo y forma de información referida al contenido de las tablas de la base de datos, mencionada en el punto b) del apartado III. LIMITACIONES AL ALCANCE, impide opinar respecto de la calidad del sistema SISER en lo referente al empleo de técnicas actuales de uso generalizado, tales como el diseño de la base de datos con arreglo al modelo relacional, la validación automática de la integridad referencial, o

la adopción de estándares de atributos y longitud para los tipos de datos de uso más frecuente.

Ello no obstante, la falta de integración señalada en el punto 1 del capítulo V. OBSERVACIONES y la excesiva dependencia del proveedor apuntada en 17, de las que adolece el sistema SISER, en consonancia con las demás debilidades de los diferentes aplicativos examinados en el marco de esta auditoría, como asimismo, el alto nivel de interrupción en el servicio y los problemas de performance que presenta la aplicación principal mencionados en 29, revelan la necesidad de encarar el desarrollo de un sistema integrado que provea una solución moderna y completa a los requerimientos informáticos de Contaduría, Tesorería y OGEPU, así como procedimientos automáticos y seguros para la transferencia de información desde y hacia los demás sistemas de Administración Financiera de la Ciudad y la aplicación de Liquidación de Haberes.

ANEXOS

ANEXO I: PROCEDIMIENTOS APLICADOS

ANEXO II: SISER, VINCULOS Y ACCESOS

ANEXO III: RELACIÓN ENTRE LAS ÁREAS USUARIAS, LOS SISTEMAS Y SUS MÓDULOS

ANEXO IV: ESTRUCTURA DEL SECTOR QUE ADMINISTRA, MANTIENE Y DESARROLLA EL APLICATIVO SISER

ANEXO V: AGENTES DETECTADOS CON MÁS DE UN USUARIO ASIGNADO

ANEXO VI: TRANSACCIONES REALIZADAS SIN PERMISOS

ANEXO VII: DIFERENCIAS ENTRE INFORMACIONES CONTENIDAS EN LOS DISTINTOS LISTADOS

ANEXO VIII: INCONSISTENCIAS EN REGISTROS DE TRANSACCIONES

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

ANEXO I - PROCEDIMIENTOS APLICADOS

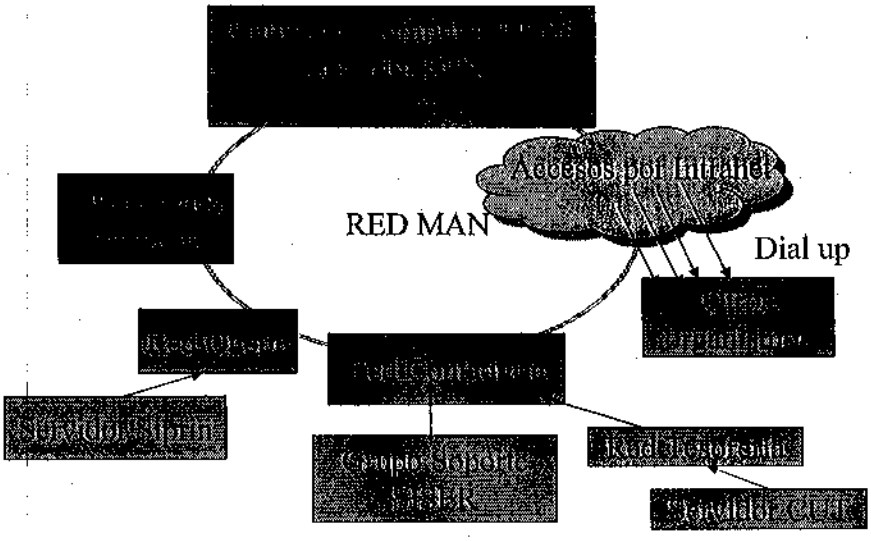
Los procedimientos aplicados fueron, entre otros, los siguientes:

- Relevamiento y obtención de documentación referida a la organización del área de sistemas de las dependencias involucradas.
- Recopilación y análisis de informes anteriores de auditorías.
- Utilización de cuestionarios para relevar la seguridad de operación de los sistemas informáticos.
- Relevamiento de las operaciones computarizadas actualmente en uso relacionadas con el objeto del presente informe.
- Análisis de la dependencia de proveedores externos en lo referido a propiedad del software y programas fuentes, administración, mantenimiento y actualización de la aplicación y del entorno operativo, etc.
- Verificación de la actualización de los registros de autorizaciones para acceder a los sistemas.
- Verificación de que las autorizaciones para acceder a los sistemas estén otorgadas por los niveles adecuados de autoridad.
- Verificación de la existencia de accesos inapropiados o no autorizados
- Verificación de que se cumplan los procedimientos para asignación de perfiles y passwords.
- Verificación de que existan registros informáticos de las actividades de los usuarios (logs) a nivel del sistema operativo.
- Entrevistas con usuarios y personal jerárquico y de nivel intermedio de las distintas reparticiones involucradas en el proceso de registración contable / presupuestaria del Gobierno de la Ciudad.
- Obtención, análisis y cruce de información de listados relacionados con permisos de usuarios, actividades realizadas en los sistemas y listados de usuarios.
- Identificación y análisis de los riesgos más relevantes de los aplicativos.
- Evaluación de las actividades de control de los aplicativos, tales como aprobaciones, autorizaciones, verificaciones, revisiones de desempeño operativo.

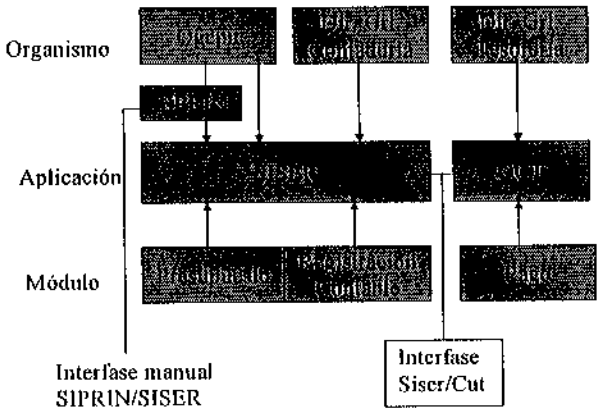
A G C.B.A.

- Evaluación del proceso de identificación, captura y comunicación de la información.
- Evaluación, a través de la selección de muestras de transacciones, de las actividades de control de los aplicativos.

ANEXO II - SISER, VINCULOS Y ACCESOS



Anexo III - RELACIÓN ENTRE LAS AREAS USUARIAS, LOS SISTEMAS Y SUS MÓDULOS



39

ANEXO IV - ESTRUCTURA DEL SECTOR QUE ADMINISTRA, MANTIENE Y DESARROLLA EL APLICATIVO SISER

Soporte Técnico: se ocupa de los aspectos relacionados con la conectividad del sistema, como la configuración de impresoras, la instalación del sistema en los equipos de los usuarios, etc.

Mesa de Ayuda: atiende a los usuarios con problemas y dudas y funciona como interfaz entre los usuarios y la administración del sistema. Cabe aclarar que se detectaron casos en que los usuarios recurren directamente a la empresa ASICOMP.

Administración Operativa: se ocupa de la administración de operaciones y procesamiento.

Seguridad y Soporte Gerencial: configura los perfiles, crea menús, da de alta usuarios en el sistema, se ocupa de algunos de los aspectos de seguridad del aplicativo.

Asicomp S.R.L.: se ocupa del desarrollo, y el mantenimiento correctivo y adaptativo de la aplicación.

Comisión SISER: está integrada por personal jerárquico de las Direcciones Generales de Tesorería, Contaduría, y Gestión Pública y Presupuesto.

40

ANEXO V - AGENTES DETECTADOS CON MÁS DE UN USUARIO ASIGNADO EN EL SISTEMA SISER

Nombre y Apellido	1° número	2° número	3° número
Raul Ríos	1002	1538	
Hugo Callegari	1005	1254	
José Servini	1005	1255	
Claudia Borello	1035	1404	
Juan P. Caviglia	1052	1796	
Teresa Cerchiaro	1056	1924	2021
Ana De Toro	1075	2090	
Claudia Justiniano	1118	1792	
Lidia Louzao	1127	1567	
Ricardo Luduena	1130	1735	
Maria L. Manquez	1134	1547	
Silvia Russo	1201	1202	
Gabriela Sciangalepre	1208	1413	
Claudio Bello	1239	1683	
Salvador Osnato	1261	2038	
Marcelo Traina	1302	1660	
Susana Sosa	1303	1661	
Martín Santamarina	1311	1717	
Adriana Porcel	1318	1895	1947
Sergio Enriquez	1372	1494	
Alejandro Cozzani	1391	1434	
Nora Niveiro	1421	1902	
Noemí Posse	1437	1970	
Marta Ainbinder	1463	1870	
Gustavo Velásquez	1523	1549	
Rosa Mansilla	1571	1573	
María del C. Diez	1585	2062	
Deborah Calzi	1756	1785	
Gladis Parra	1758	1762	
Claudia Vilella	1772	1868	
María M. Canepa	1777	1855	
Myriam Martín	1786	2017	
Alejandro Aisen	1804	2016	
Gabriel Muntaabski	1805	2015	
Bettina Kropft	1824	1932	1933
Mauricio Swirido	1897	1948	
Teresa Cerchiaro	1924	2021	
Mirta Sesino	1925	2022	
Valeria Kovacs	1949	2108	
Bárbara Aída	1955	2023	

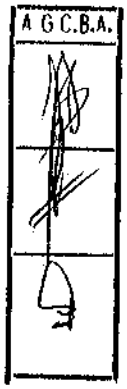
A G.C.B.A.

FOLIO 41

ANEXO VI - TRANSACCIONES REALIZADAS SIN PERMISOS

En el siguiente cuadro se presentan los casos de transacciones realizadas en el sistema para las cuales el usuario en cuestión no cuenta con los permisos correspondientes.

Usuario	Comprobante con el que trabajó sin que consten permisos en el sistema
1023	9
1038	9
1051	9
1057	9
1087	9
1089	9
1093	9
1126	9
1162	9
1166	9
1179	9
1222	9
1411	9
1420	9
1775	9
1005	1; 2001; 2011



42

ANEXO VII: DIFERENCIAS ENTRE INFORMACIONES CONTENIDAS EN LOS DISTINTOS LISTADOS

Usuario	Diferencias Detectadas
1005	No muestra movimientos en el "Listado de Comprobantes Generados por Usuario", pero en el "Listado de Auditoría por Usuario" constan 475 procesos relacionados con los comprobantes 2002 (Unidades de Medida), 1 (Definitivo), 2001 (Unidades Ejecutoras) y 2011 (Programas).
1051	Muestra en el Listado de Auditoría por Usuario 38 procesos relacionados con el comprobante 16 (Ordenes de Pago). Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran.
1093	Muestra en el Listado de Auditoría por Usuario 6 procesos relacionados con el comprobante 16 (Ordenes de Pago). Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran.
1251	Muestra en el Listado de Auditoría por Usuario 4 procesos relacionados con el comprobante 1 (Definitivo). Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran.
1266	Muestra en el Listado de Auditoría por Usuario 1 proceso relacionado con el comprobante 57 (Ampliación del Cálculo de Recursos). Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran.
1314	Muestra en el Listado de Auditoría por Usuario 19 procesos relacionados con los comprobantes 10 (Pedido de Provisión) y 12 (Contratos) en los meses 7 y 8 de 2001. Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran en estos meses.
1505	Muestra en el Listado de Auditoría por Usuario 53 procesos relacionados con el comprobante 48 (Certificado de Devolución de Fondos). Esta información no guarda consistencia con la brindada por el Listado de Comprobantes Generados por Usuario, ya que en este último, estos movimientos no figuran.
1543	No muestra movimientos en el "Listado de Comprobantes Generados por Usuario", pero en el "Listado de Auditoría por Usuario" constan 1277 procesos relacionados con el comprobante 10 (Comprobante de Egresos).

A.G.C.B.A.

43

ANEXO VIII: INCONSISTENCIAS EN REGISTROS DE TRANSACCIONES

En el siguiente cuadro se presentan algunos de los registros de transacciones encontrados que presentan información inconsistente, donde el año de imputación es el año 0 ó el numero de transacción asignado por el sistema es el 0.

USUARIO	FECHA	HORA	TRANSACCIÓN	AÑO	TIPO	NÚMERO
1717	28/08/2001	11:29	1 datos variables de objetos.	0	82	182
1717	28/08/2001	11:29	1 datos variables de objetos.	0	83	754
1717	28/08/2001	11:39	1 datos variables de objetos.	0	81	2285
1341	06/07/2001	15:00	1 datos variables de objetos.	0	1	23422
1341	16/07/2001	15:33	1 datos variables de objetos.	0	1	23506
1341	16/07/2001	15:36	1 datos variables de objetos.	0	1	23507
1341	16/07/2001	15:37	1 datos variables de objetos.	0	1	23508
1717	09/08/2001	17:30	35 cuentas contables de cultura	2001	2	0
1450	03/07/2001	11:13	1 datos variables de objetos.	0	1	17971
1450	23/08/2001	10:23	1 datos variables de objetos.	0	1	12062
1717	02/08/2001	12:35	35 cuentas contables de cultura	2001	2	0
1736	20/07/2001	17:44	1 datos variables de objetos.	0	81	2191
1736	20/07/2001	18:06	1 datos variables de objetos.	0	84	3670

A G C.B.A.