INFORME FINAL
DE AUDITORIA

Red MAN y Mainframe (Equipo Central) en la Dirección General de Estructuras y Sistemas de Información

Buenos Aires, 12 de Julio de 2000

2

AUDITORÍA GENERAL DE LA CIUDAD DE BUENOS AIRES

Presidente

Dr. Vicente Brusca

Auditores Generales

Dr. Jorge Argüello

Dr. Nicolás Corradini

Dra. Noemí Fernández Cotonat

Dr. José María Pazos

Lic. Daniel Rodríguez

Dra. Gabriela Serra

CODIGO DE PROYECTO: 4.10.2.99

NOMBRE DE PROYECTO:

Evaluación de la gestión en materia de eficiencia y eficacia de los sistemas de informatización.

DURACIÓN DEL PROYECTO: 01/04/00 al 30/06/00

PERIODO BAJO EXAMEN: 01/04/00 al 30/06/00

FECHA DE PRESENTACIÓN INFORME: 12 de julio de 2000

OBJETIVOS:

Evaluar diseño, arquitectura, organización, documentación y seguridad del Sistema Central de Procesamiento (Mainframe) y la Red Troncal (Red Man)

A.G.C.B.A.

Departamento Aplicaciones Tecnológicas
INFORME FINAL
de la
Auditoría Gral. de la Ciudad de Bs. As.

Auditoria General de la Ciudad de Buenos Aires

INFORME DE AUDITORIA
PROYECTO Nº 4.10.2.99

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

En uso de las facultades conferidas por la Constitución de la Ciudad Autónoma de Buenos Aires de acuerdo al artículo 135, la ley número 325 del 18 de febrero de 2000 dictada por la Honorable Legislatura de la Ciudad Autónoma de Buenos Aires en su artículo número 6 y, supletoriamente, la ley 24.156 (AGN) la Auditoría General de la Ciudad procedió a efectuar un examen en el ámbito de la Dirección General de Estructuras y Sistemas de Información de la Secretaría de Hacienda con el siguiente objeto:

I.- OBJETO DE LA AUDITORIA

Realizar una auditoría informática sobre el diseño, arquitectura, organización, documentación y seguridad del Sistema Central de Procesamiento (mainframe) y la Red Troncal (red Man)

II.- ALCANCE

A los efectos de la presente auditoría de sistemas se seleccionaron las siguientes áreas de trabajo:

- Red de área metropolitana.(MAN)

La red de área metropolitana constituye el vínculo que permite establecer la conectividad digital de las diferentes dependencias del Gobierno de la Ciudad entre sí y con el Centro de Procesamiento de Datos. Es utilizada por la mayoría de las áreas del Gobierno de la Ciudad. Gracias a la misma son posibles los servicios de Correo Electrónico, Internet y el procesamiento remoto de Sistemas como Control Presupuestario, etc.

- Centro de Procesamiento de Datos. (Mainframe)

El centro de procesamiento de datos está situado en Independencia 635 y en el mismo tiene asiento el equipo central de procesamiento (Mainframe). El Mainframe constituye el equipo principal en el que se procesan los sistemas de Sueldos y el Sistema Único de Mesa de Entradas. (SUME)

Esta auditoría de sistemas se efectuó sobre la situación vigente al momento de su realización, que comprendió el período de marzo a julio de 2000.

Se utilizaron las normas generales de auditoría de la AGCBA, comprendidas en la ley 70, ley 325 y complementarias.

También se utilizaron las normas establecidas por la Dirección General de Estructuras y Sistemas de información, en adelante DGEySI.

Complementariamente se utilizaron:

- Manual de Seguridad de Redes de la Subsecretaría de la Gestión Pública dependiente de Jefatura de Gabinete de Ministros, que son utilizados en el ámbito de la administración pública nacional.
- Manual de Auditoría Informática de la Sindicatura General de la Nación, SIGEN.

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:

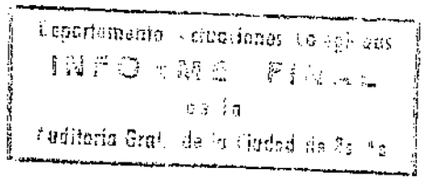
- Alto:
  - Representa que el aspecto evaluado cuenta con debilidades fuertes en los procedimientos de control, que pueden permitir que la operatoria del organismo sufra un perjuicio grave.

- 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 cuenta con debilidades o las existentes no tienen importancia relativa. Igualmente es conveniente aclarar que los controles manuales y computadorizados están diseñados para proveer una seguridad razonable, pero no absoluta, de que no ocurrirán errores o irregularidades.

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

- Se solicitó por nota la documentación relativa al objeto de esta auditoría.
- Se efectuaron entrevistas con el personal jerárquico y operativo de las áreas involucradas de la DGEySI, previa determinación de las responsabilidades de las mismas.
- Se solicitaron claves para el equipo de auditoría para verificar los mecanismos de otorgamiento y habilitación de usuarios.



- Se verificaron en el lugar y personalmente medidas de seguridad física generales con incidencia en el objeto de esta auditoria.

Se excluyeron los siguientes procedimientos:

- No se verificaron licencias de uso del software instalado.
- No se ejecutaron procesos (por parte de los auditores) en los servidores ni en el mainframe.

III.- LIMITACIONES AL ALCANCE

Los siguientes factores limitaron la tarea de auditoría:

- Ausencia de documentación escrita de los distintos procesos, circuitos, procedimientos y sistemas.
- Falta de estructura formal por debajo del nivel de Dirección.
- Diferencias entre la estructura formal y real.
- Existencia de tareas y áreas no comprendidas en la estructura ni en las metas y funciones, como por ejemplo el desarrollo Internet.
- Falta de auditorias recientes sobre las áreas seleccionadas para la presente.
- Indisponibilidad de software adecuado para revisar procesos y uso de la red y los servidores.

IV.- ACLARACIONES PREVIAS

Para la realización de las visitas y entrevistas efectuadas para relevar la información necesaria, se cumplimentaron todos los pasos administrativos imprescindibles para lograr las correspondientes autorizaciones.

El Dirección auditada facilitó nuestra tarea proveyéndonos de la información y los elementos necesarios para su ejecución. Asimismo la actitud del personal entrevistado fue abierta y positiva.

Se tomó conocimiento del funcionamiento y la seguridad de los sistemas a través de entrevistas con los responsables de área, verificación del cumplimiento de normativas y confrontación con los estándares que surgen de las prácticas más usuales.

V.- OBSERVACIONES

1. Aspectos Generales.

1.1. Seguros.

1.1.1. Se verificó que no se han contratado seguros para cubrir los riesgos de eventuales siniestros o accidentes.

2. Entorno de Seguridad

2.1. Seguridad Lógica

2.1.1. Las claves para ingresar al servicio de correo electrónico no son entregadas en sobre cerrado, permitiendo, de esta forma, que puedan ser conocidas por personas no autorizadas.

2.1.2. Si bien hay un área abocada específicamente a la seguridad (Seguridad Informática) en los hechos la administración de la misma está dividida: la seguridad de los accesos a Internet es administrada por Seguridad Informática, mientras que el control de los accesos al correo electrónico es administrado por los encargados del proyecto Internet. Los procedimientos utilizados por unos y otros son diferentes.

2.1.3. Las claves de acceso entregadas no cumplen en forma total con los requisitos establecidos en las normas elaboradas por la DGEySI, como por ejemplo, la longitud y conformación de las mismas.

2.1.4. No se pudo verificar la existencia de un procedimiento rutinario y formal para dar de baja a los usuarios. por lo que, tanto los agentes que dejan de pertenecer a la Administración o cambian de área podrían continuar haciendo uso de los servicios.

2.2. Seguridad Física

2.2.1. Se pudo constatar la existencia de una salida de emergencia en el Centro de Cómputos, aunque cerrada con llave para prevenir su uso no autorizado, ya que comunica a la zona de cocheras, que no cuenta con servicio de vigilancia. Dicha llave se encuentra depositada en Vigilancia, fuera del área del CC, lo que dificultaría, e incluso podría imposibilitar, su uso en caso de ser necesario ante algún eventual siniestro.

2.2.2. El sistema de detección de humo y calor carece de mantenimiento, por lo que no se puede garantizar su funcionamiento en caso de siniestro.

2.2.3. Si bien existieron proyectos para su modificación, el sistema de extinción automático de incendios continúa utilizando gas Halon,

cuyo uso ha sido prohibido por tener consecuencias letales para el ser humano, ya que funciona por eliminación del oxígeno en el ambiente. Por este motivo ha sido conectado en la modalidad de activación manual.

2.2.4. No existe un sistema de iluminación de emergencia.

2.2.5. No existe señalización para indicar las salidas a utilizar en caso de emergencia.

2.2.6. No existe un plan de evacuación del edificio.

3. Centro de Cómputos

3.1. Utilización del equipamiento.

3.1.1. De acuerdo a la información suministrada por la DGEySI sobre el comportamiento del equipo durante el año 1999, se verificó que el mayor promedio diario de uso de CPU no excede el 20%, sensiblemente inferior a los niveles que las prácticas usuales estiman como aprovechamiento óptimo, generando una importante sub-utilización del mainframe.

3.2. Documentación para asistir las actividades del Centro de Cómputos.

3.2.1. Se verificó la existencia de documentación desarrollada por la propia área para dar apoyo a tareas de operación y mantenimiento del equipo central, aunque no se encuentra redactada y catalogada de manera de ofrecer un rápido y sencillo acceso.

3.3. Herramientas de análisis de uso.

3.3.1. Se tomó conocimiento de que, a partir del cambio del sistema operativo, realizado para lograr compatibilidad con el año 2000, no fue reinstalado el software necesario para efectuar análisis de comportamiento del equipamiento, por lo que, actualmente, no se pueden elaborar las estadísticas de rendimiento del equipamiento.

3.4. Plan de contingencia.

3.4.1. Se constató la existencia de un plan, diseñado para dar solución a eventuales inconvenientes que pudieran surgir a partir de la problemática presentada por el año 2000, para atender hipotéticas situaciones de salida de servicio del equipo central. Sin embargo, no se pudo verificar la existencia de convenios con algún otro centro de cómputos para asegurar un backup para el procesamiento, que era parte sustancial del mencionado plan.

3.5. Respaldo de información.

3.5.1. Se pudo comprobar la existencia de un adecuado esquema de respaldo de información, en términos de periodicidad y clasificación de los archivos en términos de criticidad. Si bien los resguardos de información se realizan por duplicado y una de las copias es mantenida en caja ignífuga, ambas permanecen en el mismo ámbito edilicio. Esta copia en sede externa está dispuesta por la normativa interna.

4. Red de Área Metropolitana (MAN).

4.1. Administración de la Red.

4.1.1. Se verificó la contratación del licenciamiento para el uso de un producto para administrar el funcionamiento de la red y generar información de control y estadística (log files). Sin embargo, éste no fue instalado hasta el momento, por lo que no es posible efectuar tareas de administración, tales como control a distancia de terminales, localización y corrección temprana y remota de fallas, verificación de funcionamiento de todo el equipamiento instalado, confección de estadísticas de uso, por citar solo algunas.

4.2. Plan de contingencia.

4.2.1. No se dispone de un plan de contingencia para la red para atender posibles caídas del servicio.

4.3. Respaldo de información.

4.3.1. No existe un procedimiento unificado para las tareas de backup y esta responsabilidad no está centralizada en una única área. Se pudo verificar que de los siete servidores instalados solo uno cuenta con doble respaldo de datos.

4.3.2. No hay servidores de respaldo para equipos que efectúan tareas críticas como, por ejemplo, el que soporta al Sistema de Administración del Gasto por lo que, ante una eventual caída, no existe posibilidad de procesamiento alternativo.

4.4. Documentación.

4.4.1. No se dispone de manuales operativos de la red.

4.4.2. No se pudo verificar la existencia de un plano lógico de la red que incluya la circulación de la información, los puntos de acceso, usuarios y servidores. Esto dificulta la detección de fallas, la comprensión de las rutas.

VI.- RECOMENDACIONES

1. Aspectos Generales.

1.1. Seguros.

1.1.1. Contratar los seguros necesarios para cumplimentar tanto las normativas internas como las disposiciones generales emitidas por el Gobierno de la Ciudad en materia edilicia.

2. Entorno de Seguridad

2.1. Seguridad Lógica

2.1.1. Establecer un sistema de entrega de las claves que permita asegurar su confidencialidad.

2.1.2. Unificar la administración de la seguridad en el área especializada a ese efecto.

2.1.3. Generar las claves de acuerdo a las normativas de la DGE y SI

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

2.2. Seguridad Física

2.2.1. Instalar mecanismos que permitan controlar el uso de la salida de emergencia como por ejemplo, con alguna señalización en Vigilancia cada vez que sea accionada, y, además, colocar la llave en algún lugar accesible desde el recinto del Centro de Cómputos.

2.2.2. Disponer la reanudación de los controles y mantenimiento periódicos del sistema de detección de humo y calor.

2.2.3. Dotar al Centro de Cómputos de un sistema de extinción automático de uso permitido y con probada eficacia en ámbitos similares.

2.2.4. Instalar sistema de iluminación de emergencia, de acuerdo a las normativas vigentes.

2.2.5. Instalar sistema de señalización para indicar las salidas a utilizar en caso de emergencia.

2.2.6. Diseñar y probar plan de evacuación del edificio.

3. Centro de Cómputos

3.1. Utilización de equipamiento.
   3.1.1. Estudiar, de acuerdo a la planificación prevista para el área, la posibilidad de redimensionar la actual configuración o reemplazarla.

3.2. Documentación para asistir las actividades del Centro de Cómputos.
   3.2.1. Redactar y catalogar la información existente, clasificándola temáticamente.

3.3. Herramientas de análisis de uso.
   3.3.1. Instalar las herramientas para el análisis de uso del equipamiento.

3.4. Plan de contingencia.
   3.4.1. Diseñar un plan de contingencia para atender cualquier situación que pueda presentarse. Establecer algún convenio con otro Centro de características similares que aseguren el back up del procesamiento, privilegiando los que puedan celebrarse con organismos oficiales, dependientes, preferentemente, del Gobierno de la Ciudad de Buenos Aires (por ejemplo: Banco de la Ciudad de Buenos Aires).

3.5. Respaldo de información.
   3.5.1. Designar una sede externa y mantener en ella copia de los archivos de mayor criticidad, debiendo hacerlo, por lo menos, con una copia completa del resguardo mensual.

4. Red de Área Metropolitana (MAN).

4.1. Administración de la Red.
   4.1.1. Instalar el producto contratado para la administración de la Red. Asegurar el entrenamiento del personal que tendrá a su cargo la ejecución.

4.2. Plan de contingencia.
   4.2.1. Confeccionar un plan de contingencia.

4.3. Respaldo de información.
   4.3.1. Unificar las tareas de backup de todos los servidores en una sola área específica. Definiendo, previamente, las políticas en la materia.

   4.3.2. Asegurarse la existencia de, por lo menos, un servidor de respaldo.

4.4. Documentación.
   4.4.1. Confeccionar manuales operativos de la red.

4.4.2. Elaborar un plano lógico de la red detallando la circulación de la información, rutas alternativas, puntos de acceso, usuarios y toda la información necesaria para una correcta administración de la misma.

VII.- CONCLUSIONES

De acuerdo a los niveles de vulnerabilidad establecidos en el Alcance, se evaluó que:

- El Centro de Cómputos (Mainframe) debe calificarse como bajo (cuenta con un buen entorno de seguridad, aunque no esta totalmente aprovechado).

- Red MAN: medio.

El nivel de vulnerabilidad medio asignado a la Red MAN se desprende de las observaciones efectuadas en los párrafos V.2.1 y V.4.-

La Dirección General de Estructuras y Sistemas de Información que provee funciones de procesamiento central y conectividad a través de los servicios instalados en el equipo central (mainframe) y la red de área metropolitana (MAN), debería reforzar su esquema de seguridad y evaluar la conveniencia de centralizar su administración, normalizando y perfeccionando sus prácticas administrativas y concientizando a los usuarios acerca de su importancia. Asimismo debe procurarse el aprovechamiento pleno de estos recursos (Mainframe y Red MAN).

Dr. JORGE HORACIO DELORD
DIRECTOR DE ESTRUCTURAS ADMINISTRATIVAS
Y SISTEMAS DE INFORMACION
AUDITORIA GRAL. DE LA CIUDAD DE BS. AS.

A.G.B.A.

Departamento Auditorías Informáticas
de la
Auditoría Gral. de la Ciudad de Bs. As.