INFORME FINAL
DE AUDITORIA

Proyecto 4.03.23a

SISTEMAS DE INFORMACIÓN DEL GCBA.
SEGUIMIENTO DEL INFORME N° 4.10.2.99

AÑO 2003

AUDITORÍA GENERAL
DE LA CIUDAD AUTÓNOMA DE
BUENOS AIRES

Av. Corrientes 640 piso 5º Capital Federal

Presidente

Lic. Matías Barroetaveña

Auditores Generales

Dra. Alicia M. J. Boero

Dr. Vicente M. Brusca

Dr. Rubén A. Campos

Dr. Nicolás Corradini

Lic. José Luis Giusti

Lic. Josefa A. Prada

CODIGO DEL PROYECTO:
4.03.23.

NOMBRE DEL PROYECTO:
Sistemas de Información del G.C.B.A.

Seguimiento de las observaciones incluidas en el informe final de Auditoría N° 4.10.2.99 Red MAN y Mainframe (Equipo Central) en la Dirección General de Estructuras y Sistemas de Información.

DURACIÓN DEL PROYECTO:
1° de agosto al 10 de diciembre de 2003

PERIODO BAJO EXAMEN:
Año 2003.

EQUIPO:

- **Supervisor Coordinador**: Dr. Pablo Madera, Abogado
- **Supervisor:** Dr. José Juffar, Contador Público

- **Auditores**: Ing. José Recasens
  Lic. Francisco Camean Ariza
  Sr. Héctor Zancada
  Ing. Rodolfo Bella
  Sr. Oscar Ciarlotti
  Lic. Martín Bordoy
  Srta. Carmen Fernández

Informe Final de Auditoria
Proyecto Nº 4.03.23

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

En uso de las facultades conferidas por la Ley 70, artículos 132 y 136 de la Ciudad de Buenos Aires, relacionadas con lo dispuesto en el artículo 135 de la Constitución de la Ciudad, la AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES procedió a efectuar un examen en el ámbito de Dirección General de Sistemas de Información dependiente de la Secretaria de Hacienda y Finanzas, con el objeto que se detalla en el apartado siguiente.

OBJETIVO:
Seguimiento de las observaciones incluidas en el informe final de auditoría N° 4.10.2.99 “Red MAN y Mainframe (Equipo Central) en la Dirección General de Estructuras y Sistemas de Información”, análisis de las medidas implementadas y sus respectivos grados de avance.

I. OBJETO DE LA AUDITORÍA

Relevar y evaluar las medidas adoptadas por la Dirección General de Sistemas de Información de la Secretaría de Hacienda y Finanzas con referencia al Informe N° 4.10.2.99 “Red MAN y Mainframe (Equipo Central) en la Dirección General de Estructuras y Sistemas de Información”, aprobado por el Colegio de Auditores de la A.G.C.B.A. el 5/9/2000.

II. ALCANCE

El examen fue realizado de conformidad con las normas de auditoría externa de la AUDITORÍA GENERAL DE LA CIUDAD AUTÓNOMA 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 A.G.C.

El trabajo se desarrolló en el ámbito de la Dirección General de Sistemas de Información, habiéndose aplicado los procedimientos que se detallan en **Anexo I**.

III. ACLARACIONES PREVIAS

1. Breve descripción de las áreas examinadas

- **Red de área metropolitana.(MAN)**

La red de área metropolitana constituye el vínculo que permite establecer la conectividad digital de datos de las diferentes dependencias del Gobierno de la Ciudad entre sí y con el Centro de Procesamiento de Datos. Esta red es utilizada por la mayoría de las áreas del Gobierno de la Ciudad. La misma hace posible el procesamiento remoto de sistemas como Control Presupuestario, Seguimiento de Expedientes y provee los servicios de Correo Electrónico e Internet. Ha crecido de modo importante en los últimos 3 años, según se expone en **Anexo II.**

- **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 entre otros los sistemas de Sueldos y el Sistema Único de Mesa de Entradas. (SUME)

2. Cambios en la Dirección General de Sistemas de Información

Las áreas de procesamiento y comunicaciones de la Dirección General de Sistemas de Información (DGSI) han cambiado en los aspectos que se comentan a continuación de un modo sustantivo desde el año 1999 en que se realizó la auditoría anterior:

2.1. Procesamiento.

2.1.1. El área de procesamiento tiene actualmente 41 servidores, muchos de los cuales fueron enviados a ese centro en los últimos tres años desde otros organismos del G.C.B.A.. Algunos de estos se corresponden con servicios que habían sido subcontratados a empresas privadas cuyos contratos se hallaban vencidos y que fueron retomados por el G.C.B.A.. Un ejemplo en este sentido es el correspondiente a los Sistemas de Administración Geográficos y Catastrales que sirven como base de cálculo para la determinación de la tasa de Alumbrado Barrido y Limpieza (ABL).

La proliferación de servidores de diferente tipo, dimensión y sistema operativo en el ámbito del G.C.B.A., algunos de los cuales han sido trasladados al Centro de Cómputos (DGSI), se ha producido sin un adecuado encuadre tecnológico que de homogeneidad al crecimiento del hardware y del software.

La concentración de servidores en un lugar físico con condiciones adecuadas constituye un cambio positivo y económicamente conveniente pues se aprovecha de un modo mas eficiente la inversión realizada en el Centro de Cómputos relativa a alimentación eléctrica, seguridad física, y otros. Este cambio de locación debe ser acompañado por un crecimiento acorde de la capacidad de transporte de las redes de comunicaciones. Pero por otro lado, cabe señalar que la concentración de equipamiento incrementa el riesgo de pérdida de la continuidad del procesamiento de la información en caso de siniestro, por lo que se torna crítica la disponibilidad de procesamiento y conectividad contingente así como el cumplimiento estricto de la política de resguardo de información.

Las responsabilidades de la DGSI con relación a los equipos trasladados, en algunos casos, se limita a proveer el espacio físico para su instalación, la conectividad necesaria para su utilización desde el área usuaria y el personal para el manipuleo de insumos como cartuchos de cinta, ya que no se ocupa, en general, del resto de las tareas relativas a su administración, mantenimiento y resguardo.

2.1.2. No fueron relevadas, ya que excedían el alcance de este trabajo, las áreas que se encargan desde sitios remotos de la ejecución de las copias de respaldo, del soporte técnico, del mantenimiento del software y el hardware, por citar algunas de las funciones conexas con los sistemas transferidos. Cabe destacar que la DGSI no se encuentra a cargo de estas funciones y su relación con las mismas es complementaria e informal. Tampoco es responsable de verificar, que su ejecución sea eficiente y segura; estos aspectos, por su jerarquía, deberán ser motivo de futuras auditorías.

2.1.3. Cabe destacar que tanto en este examen como en el anterior, se observa que el equipo principal de la DGSI , un IBM/390, continúa subutilizado ya que solamente se aprovecha aproximadamente 1/5 de su capacidad en los picos de uso.

Este equipo fue ampliado en ocasión del proyecto cuyo objetivo era procesar los sistemas de la Dirección General de Rentas en la DGSI , luego abortado en virtud del contrato de servicio de procesamiento firmado con el Banco de la Ciudad de Bs. As.

Dentro del marco de ese contrato se determinó su uso como equipo de contingencia. Se debe señalar que no se ha realizado ninguna tarea apuntando al cumplimiento de este requisito contractual. En la actualidad el Mainframe se utiliza para la liquidación de sueldos y el SUME (Sistema Único de Mesa de Entradas) y algunos sistemas menores como la base de datos del Sistema de Programación de Inversiones (SIPRIN).

2.2. Red MAN

Las redes de comunicación constituyen un elemento clave en la integración, coordinación y mejora de la eficiencia del accionar de las organizaciones.

Los principales nodos (puntos de enlace) de la red MAN se encuentran en el edificio de la DGSI, en el Palacio de Gobierno y en el edificio de Carlos Pellegrini y Perón (ex Mercado del Plata). Desde estos nodos se establecen los vínculos con las áreas de salud, rentas, los centros de gestión y participación, registros civiles, cementerios y otros, según se expone en **ANEXO II**.

La red de comunicación digital ha crecido hasta alcanzar los 120 vínculos punto a punto.

Para aquellos nodos donde no es posible establecer enlaces punto a punto por restricciones técnicas o económicas, se está utilizando la tecnología VPN (Virtual Private Network), enlace virtual seguro a través de Internet.

Los enlaces principales actualmente alcanzan una velocidad de comunicación de 155 Mb/seg y existen planes de expansión para evolucionar a tecnologías Gigabit.

Se utilizan diversos medios para el establecimiento de las comunicaciones como fibra óptica, cable de cobre y medios inalámbricos.

Se han instalado algunos vínculos alternativos para proveer contingencia a las comunicaciones de los nodos claves y se ha incorporado software de monitoreo para detectar intentos de intrusión, saturación de vínculos y otros inconvenientes.

3. Metodologías de evaluación

3.1. A los efectos de evaluar las decisiones adoptadas y las acciones encaradas por la Dirección General de Sistemas de Información a las observaciones manifestadas por esta Auditoría en el Informe del Proyecto N° 4.10.2.99 se utilizaron los siguientes criterios:

- El progreso es satisfactorio: Las acciones encaradas y las decisiones adoptadas hasta el momento por la entidad responden en forma adecuada a las observaciones efectuadas.
- El progreso es incipiente: Se han adoptado algunas decisiones en línea con las observaciones efectuadas, aunque el proceso deberá ser continuado en el futuro.
- El progreso no es satisfactorio: La entidad no ha dado respuesta a las observaciones efectuadas.

3.2. Para la medición de los niveles de riesgo señalados en el apartado V.- **CONCLUSIONES** 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.

IV. SEGUIMIENTO DE LAS OBSERVACIONES

1. Aspectos Generales

1.1. Seguros

Observación :

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

Recomendación :

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.

Comentarios del organismo auditado:

No se formularon comentarios.

Comentario de la Auditoría :

El progreso no es satisfactorio

Al día de la fecha no existe ningún seguro contratado. Se prevé la contratación de un paquete de seguros para el año 2004.

2. Entorno de Seguridad

2.1. Seguridad Lógica

Observación: .

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 .

Recomendación:

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

Comentarios del organismo auditado:

Con referencia a la seguridad en la entrega de acceso al servicio de correo, se informa que a la fecha, los datos de las cuentas de correo electrónico (nombre de usuario y contraseña) se entregan en sobre cerrado, únicamente al titular de la mismas (en el caso de cuentas personales), o al responsable del sector si se trata de una cuenta genérica.

Comentario de la Auditoría :

El progreso es incipiente

Las claves son entregadas en sobre cerrado pero no son secretas, ya que al momento de su emisión son conocidas por el encargado del otorgamiento. Recomendamos que se configure la seguridad de modo que el usuario deba modificar la clave cuando ingresa al sistema por primera vez.

Observación:

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.

Recomendación:

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

Comentarios del organismo auditado:

Con respecto a la administración de la seguridad cabe aclarar que según la disposición Nº 092 DGSINF- 2001 las Direcciones de Soporte Técnico y Planeamiento y Desarrollo son responsables en forma conjunta de la responsabilidad por la seguridad ,a excepción de la seguridad del Mainframe, que está a cargo de un grupo de trabajo formado por personal de ambas Direcciones.

Comentario de la Auditoría :

El progreso no es satisfactorio

La Administración de la Seguridad del correo electrónico e Internet está compartida entre la Dirección de Soporte Técnico y la Dirección Planeamiento y Desarrollo en forma conjunta, desde un punto de vista formal, aunque en la práctica la tarea es ejecutada por la Dirección de Planeamiento y Desarrollo. Por su parte el área específica de Seguridad dependiente de la Dirección de soporte Técnico se encarga únicamente de la seguridad del equipo IBM 390 (MAINFRAME). Asimismo han sido trasladados al Centro de Cómputos una gran cantidad de equipos cuya seguridad no es administrada centralmente. Este aspecto excede el marco de esta auditoría y será materia de futuros exámenes. Mantenemos y extendemos la vigencia de la recomendación efectuada hace tres años destacando la importancia del cumplimiento de la misma. Ratificamos que la dimensión del G.C.B.A. en general y del centro de procesamiento de información de la DGSI amerita la creación de la estructura necesaria para la administración centralizada de la seguridad, con un adecuado aprovechamiento de la escala, unificando los procedimientos, desarrollando personal especializado al efecto y, fundamentalmente, con absoluta independencia de las áreas usuarias, de procesamiento, de desarrollo, y demás, tal como lo requiere la normativa. Se debería evaluar la posibilidad de que el área que administre la seguridad se constituya en una estructura externa a la DGSI, tal como recomiendan las normas en la materia, y no comparta la dependencia de las áreas de procesamiento y mantenimiento, lo que aseguraría una mayor y más efectiva independencia funcional.

Observación:

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 .

Recomendación:

2.1.3. Generar las claves de acuerdo a las normativas de la DGEYSI

Comentarios del organismo auditado:

Atento al cumplimiento de las normas para la asignación de claves de acceso del servicio de correo se informa que los criterios que se aplican son los siguientes:

**Una vez que el usuario ha recibido el sobre conteniendo los datos de su cuenta de correo electrónico (nombre de usuario y contraseña), podrá cambiar, si así lo deseará, su contraseña. Esto lo podrá realizar a través de la página:

MAIL.G.C.B.A..GOV.AR, seleccionando la opción “CAMBIO DE PASSWORD”, identificada con un ícono de candado.

**La asignación de claves de acceso está a cargo del grupo de Administradores del correo, para que la tarea de registración de usuarios se efectúe eficaz y eficientemente .

** Las claves de acceso de correo que asignan no tienen una longitud menor de ocho caracteres , a fin de proveerle al usuario un adecuado nivel de seguridad.

** Las claves de acceso son únicas para cada usuario.

** Al momento de acceder al correo, la clave de acceso no es desplegada en la pantalla.

Comentario de la Auditoría :

El progreso es satisfactorio

Se verificó que las claves son entregadas bajo sobre cerrado. La estructura de password es alfanumérica de ocho (8) caracteres y se ha dado cumplimiento a los aspectos mencionados en la recomendación.

Observación:

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.

Recomendación:

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

Comentarios del organismo auditado:

Con referencia a la existencia de un procedimiento normal de bajas de usuarios se consigna que toda vez que un usuario deja de pertenecer al G.C.B.A. o a un área, se da de baja su cuenta. También periódicamente se controla la actividad de las cuentas de correo, y en caso de la existencia de cuentas activas, se contacta al usuario a efectos de ratificar o rectificar su cuenta de correo.

Comentario de la Auditoría :

El progreso es satisfactorio

Se ha incorporado un procedimiento de bajas.

2.2. Seguridad Física

Observación:

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.

Recomendación:

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.

Comentarios del organismo auditado:

Se colocaron dos llaves, en caja de vidrio para ser roto en caso de emergencia , en las puertas que comunican el Centro de Cómputos con la cochera y la cochera exterior. La caja de vidrio se encuentra instalada junto a las puertas. Se ha previsto instalar una cámara de video para monitorear el área.

Comentario de la Auditoría :

El progreso es satisfactorio

Se verificó visualmente la existencia de las llaves en la puerta de emergencias.

Observación:

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.

Recomendación:

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

Comentarios del organismo auditado:
No se formularon comentarios.

Comentario de la Auditoría :

El progreso no es satisfactorio

No se observaron modificaciones desde el anterior informe de Auditoría.

Observación:
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.

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

Comentarios del organismo auditado:
No se formularon comentarios.

Comentario de la Auditoría

El progreso no es satisfactorio

No se han efectuado modificaciones respecto del sistema de extinción de incendios.

Observación:

2.2.4. No existe un sistema de iluminación de emergencia.

Recomendación:

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

Comentarios del organismo auditado:
Se instaló un sistema de iluminación en todas las salas de del Centro de Cómputos.

Comentario de la Auditoría

El progreso es satisfactorio

Se verificó visualmente la instalación de tubos de luz de emergencia en las salas del Centro de Cómputos.

Observación:

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

Recomendación :

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

Comentarios del organismo auditado:
Se instalaron carteles de señalización.

Comentario de la Auditoría :

El progreso es satisfactorio

Se verificó visualmente la existencia de carteles que indican las salidas en caso de emergencia.

Observación:

2.2.6. No existe un plan de evacuación del edificio.

Recomendación :

2.2.6. Diseñar y probar plan de evacuación del edificio.

Comentarios del organismo auditado:
No se formularon comentarios.

Comentario de la Auditoría :

El progreso no es satisfactorio

No se ha elaborado un plan de evacuación ni existen constancias de convocatoria a Defensa Civil.

3. Centro de Cómputos

3.1. Utilización del Equipamiento

Observación:

3.1.1.De acuerdo a la información suministrada por la DGSEYS 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

Recomendación:

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

Comentarios del organismo auditado:
Durante el primer trimestre del año 2000 se trabajó en la elaboración de un pliego para la contratación de un cluster para la realizar la consolidación de aplicaciones y bases de datos residentes en el mainframe y la incorporación de nuevos sistemas(Ej: el SIDIF).

Comentario de la Auditoría :

El progreso no es satisfactorio

A la fecha de realización de las tareas de campo el servidor no excede del 20% de utilización del CPU.

3.2. Documentación para asistir las actividades del Centro de Cómputos

Observación:
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.
Recomendación:
3.2.1. Redactar y catalogar la información existente, clasificándola temáticamente

Comentarios del organismo auditado:
Se procedió a la redacción uniforme de la información existente.

Comentario de la Auditoría :

El progreso es satisfactorio

Se verificó la existencia de la clasificación temática.

3.3. Herramientas de análisis de uso

Observación:
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

Recomendación:

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

Comentarios del organismo auditado:
Se encuentra en confección un pliego para la contratación de una solución integral.

Comentario de la Auditoría :

El progreso no es satisfactorio

Por el incremento de la cantidad de servidores (40) y por el cambio del sistema, no se instaló un software a tal efecto.

3.4. Plan de contingencia

Observación:

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.

Recomendación :

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).

Comentarios del organismo auditado:
Se elaboró un plan de contingencia para los sistemas críticos.

Comentario de la Auditoría :

El progreso no es satisfactorio

Se exhibió un borrador de plan de contingencia que no se encuentra vigente por no haber sido aprobado por la Dirección General. Se desconoce asimismo si este borrador se convertirá en la versión definitiva.

3.5. Respaldo de Información

Observación :

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

Recomendación:

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..

Comentarios del organismo auditado:
Desde diciembre de 2001 se remite en forma mensual una copia de resguardo a sede externa .

Comentario de la Auditoría :

El progreso es satisfactorio

Debemos destacar que la tarea fue realizada para el Mainframe existente hace tres años pero no para todos los servidores ni tampoco para todos los que fueron trasladados al Centro de Cómputos con posterioridad, tarea que se estaba llevando a cabo al momento de la ejecución de las tareas de campo. La DGSI en general, no se encarga de un modo completo de la ejecución de las copias de respaldo de algunos servidores que fueron trasladados al Centro de Cómputos de la DGSI, efectuando un control parcial sobre los mismos. Este aspecto excede el alcance de la actual auditoría y será motivo de evaluación en futuros exámenes. En líneas generales es necesario disponer una política de back up unificada, ejecutada por un equipo capacitado al efecto con un

adecuado nivel de automatización de esta tarea para todos los servidores, salvo justificada excepción. Existen en la actualidad mecanismos robotizados que minimizan los errores, disminuyen el manipuleo y la cantidad de cartidges (u otros soportes) y hacen más eficiente la función. Asimismo, por razones de economía, la ejecución de las copias de respaldo, las pruebas de recupero, el procedimiento de resguardo en sede externa y otros, deben unificarse y estar a cargo del centro de procesamiento de datos, salvo excepción justificada debidamente.

4. Red de Área Metropolitana (MAN)

4.1 . Administración de la Red

Observación :

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.

Recomendación:

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.

Comentarios del organismo auditado:

Para la administración de la RED MAN se utilizan los software HP Open View y Solar Wins; se realizó la segmentación de la red para incrementar la seguridad y facilitar la administración; se prevé la adquisición de un software de (IDS).

Comentario de la Auditoría

El progreso es satisfactorio

Se instalaron dos herramientas (HP OPEN VIEW y SOLAR WINS), que permiten el testeo, monitoreo y administración de vínculos.

4.2. Plan de contingencias

Observación :

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

Recomendación:

4.2.1. Confeccionar un plan de contingencia

Comentarios del organismo auditado:

A fin de contar con adecuadas alternativas de comunicación ante fallas en las comunicaciones se instalaron enlaces redundantes con los organismos que procesan los sistemas mas críticos.

Comentario de la Auditoría :

El progreso es incipiente

Se han instalado vínculos que proveen contingencia para las comunicaciones principales pero no se dispone de un plan de contingencia formal que contenga análisis de riesgos, impacto, nivel de continuidad requerido, pasos y responsables para la puesta en marcha de la solución contingente y retorno a la situación normal. Asimismo no existen actas en las que se haya constatado la efectividad de las medidas adoptadas. La normativa exige la ejecución de pruebas formales al menos una vez al año, en las que se verifique la efectividad del plan en el mantenimiento de la operatividad, con participación de las áreas usuarias y auditoría interna que deben suscribir las actas respectivas.

4.3. Respaldo de Información

Observación :

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 sólo uno cuenta con doble respaldo de datos

Recomendación:

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

Comentarios del organismo auditado:
No se realizan back up de los servidores de comunicaciones porque en caso de caídas sólo se reinstalan los servidores de soporte técnico, Gateway, y servidores de DNS.

Comentario de la Auditoría :

El progreso no es satisfactorio

No hay un sistema de back-up para los servidores GATEWAY y DNS que, ante una caída, deben reinstalarse y reconfigurarse por completo.(Ej: Disaster Recovery) .

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

Comentarios del organismo auditado:

No se formularon comentarios.

Comentario de la Auditoría

El progreso no es satisfactorio

Se verificó que no se produjeron modificaciones respecto del informe de auditoría anterior

4.4. Documentación

Observación :

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

Recomendación:

4.4.1. Confeccionar manuales operativos de la red.

Comentarios del organismo auditado:

No hay un manual operativo de la red debido a que bajo el alcance del control de los componentes de monitoreo, nos plantea hoy una red con una realidad semejante a la de Internet, en cuanto a su manejo y distribución.

Comentario de la Auditoría :

El progreso no es satisfactorio

Se verificó que no se han confeccionado manuales operativos de la red.

Observación :

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.

Recomendación :

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.

Comentarios del organismo auditado:

Se confeccionaron los planos de red y el inventario del equipamiento.

Comentario de la Auditoría :

El progreso es satisfactorio

Se verificó la existencia del plano lógico de la red.

V.-CONCLUSIONES

Niveles de Cumplimiento

Se ha solucionado el 41% de las observaciones efectuadas, restando aún la resolución de algunos aspectos muy importantes como los relativos a la organización de la seguridad y al aprovechamiento de los recursos tecnológicos según surge de la revisión practicada.

Por otra parte, cabe señalar que el tratamiento dado por la Dirección General de Sistemas al Informe de Auditoría N° 4.10.2.99 no ha sido el adecuado, ya que no se elaboró un plan de acción, no se elevó un proyecto con propuestas a la Subsecretaría de Gestión Operativa, ni se efectuó un seguimiento periódico de los avances en la resolución de los aspectos observados en el informe mencionado.

Niveles de Riesgo

De acuerdo a los niveles de riesgo de vulnerabilidad de los sistemas establecidos en el apartado III.-**ACLARACIONES PREVIAS**, y en función de los aspectos evaluados en el presente informe, se concluye que la situación general ha mejorado aunque no se han alcanzado todavía niveles aceptables .

- El Centro de Cómputos (Mainframe) debe calificarse como de riesgo Medio (cuenta con un aceptable entorno de seguridad, aunque no está totalmente aprovechado).

- Red MAN: debe calificarse como de riesgo Medio.

La Dirección General de 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), debe mejorar su 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 tecnológicos (Mainframe y Red MAN) y de la escala, profesionalizando y especializando sus recursos humanos.

ANEXO I

PROCEDIMIENTOS DE AUDITORÍA APLICADOS

- Entrevistas con el personal jerárquico y operativo de las áreas involucradas.

- Relevamiento de los aspectos necesarios de las instalaciones del Centro de Cómputos.

- Obtención y análisis de Organigramas, Manuales Operativos, Normas de Procedimiento y Planes de Contingencia.

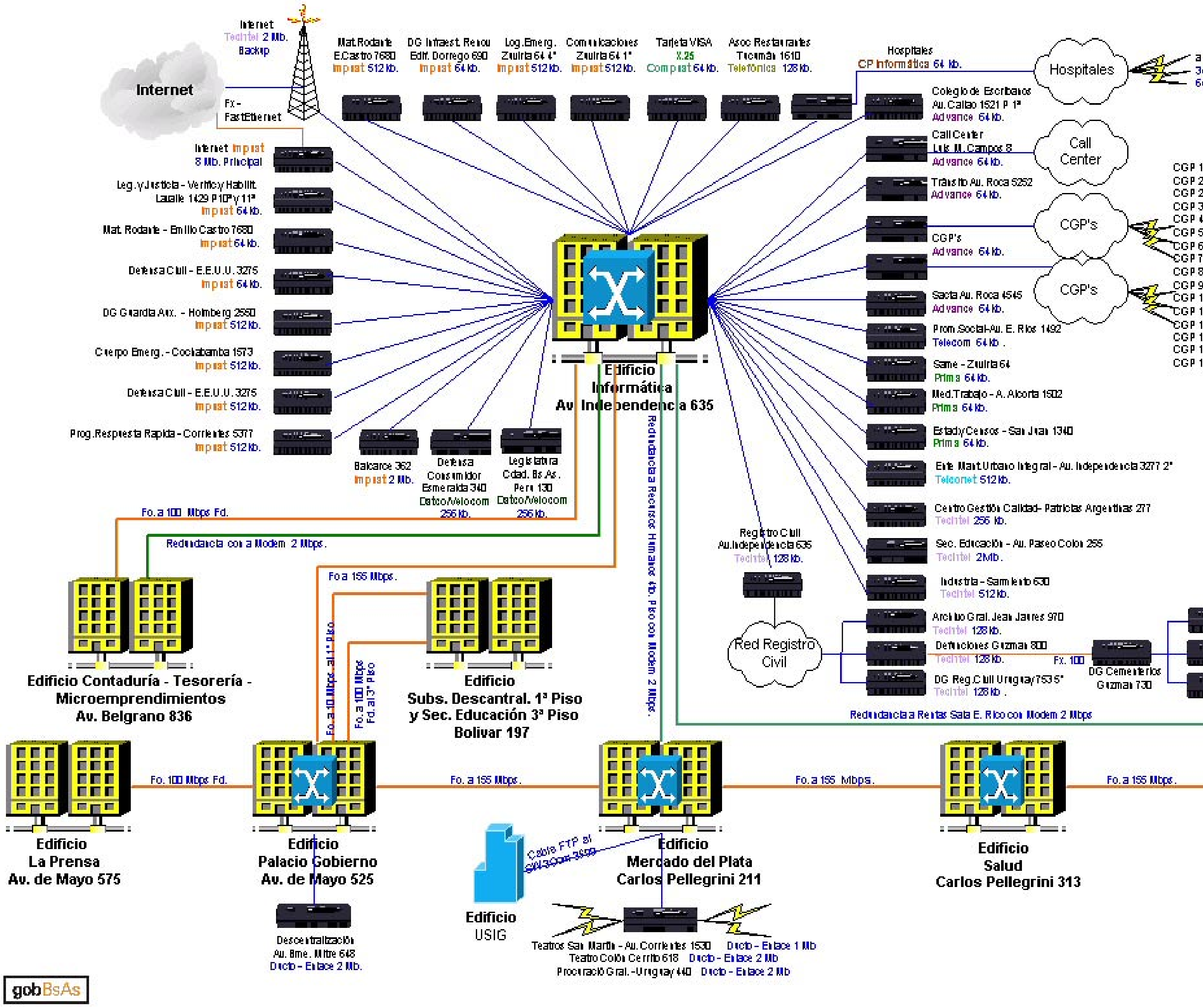
- Verificación de los mecanismos de otorgamiento de claves y habilitación de usuarios.

- Verificación del cumplimiento de normas internas y externas y confrontación con estándares que surgen de las normas nacionales e internacionales.

- Inspecciones oculares.

- Ejecución de software de reconocimiento de redes, análisis de tráfico, Auditoría de passwords, control de puertos sobre servidores y control de seguridad de switches y routers.

ANEXO II


Internet
Internet Techtel 2 Mb. Backup
Fx - FastEthernet
Internet Impsat 8 Mb. Principal
Edificio Informática Av. Independencia 635
Edificio Contaduría - Tesorería - Microemprendimientos Av. Belgrano 836
Edificio Subs. Descantral. 1° Piso y Sec. Educación 3° Piso Bolivar 197
Edificio La Prensa Av. de Mayo 575
Edificio Palacio Gobierno Av. de Mayo 525
Edificio USIG
Edificio Mercado del Plata Carlos Pellegrini 211
Edificio Salud Carlos Pellegrini 313
Hospitales
Call Center
CGP's
Red Registro Civil
Fo. a 100 Mbps Fd.
Redundancia con a Modem 2 Mbps.
Fo. a 155 Mbps.
Redundancia a Rentas Sala E. Rico con Modem 2 Mbps
gobBsAs