

INFORME FINAL DE AUDITORIA

Código del Proyecto: 5.05.07
Dirección General de Sistemas
de Información Geográfica
Auditoria de Sistemas de Información

Ciudad Autónoma de Buenos Aires

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

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

Presidente

Lic. Matías Barroetaveña

Auditores Generales:

Dra. Alicia M. J. Boero

Dr. Vicente Mario Brusca

Dr. Rubén A. Campos

Dr. Nicolás Corradini

Dr. José Luis Giusti

Lic. Josefa A. Prada

CÓDIGO DEL PROYECTO:

5.05.07

NOMBRE DEL PROYECTO:

Dirección General de Sistemas de Información Geográfica
Auditoría de Sistemas de Información

OBJETO:

Dirección General de Sistemas de Información Geográfica.

OBJETIVO:

Evaluar la adecuación de los recursos informáticos al cumplimiento de los objetivos institucionales y operativos del programa en términos de eficacia y eficiencia.

ALCANCE:

Examinar, en general, la Arquitectura de Hardware y los Sistemas Operativos. Se efectuará lo propio con las cuestiones relativas a la red de comunicación de datos y a la seguridad. Se revisará el cumplimiento de las prácticas críticas de seguridad y la continuidad de los servicios.

PERÍODO BAJO EXAMEN:

Octubre - Diciembre 2005

EQUIPO DESIGNADO:

Auditor Supervisor:	Guillermo A. García
Coordinador:	José Recasens

JURISDICCIÓN:

20 Jefatura de Gobierno

UNIDAD EJECUTORA:

125 Unidad de Sistemas de Información Geográfica

PROGRAMA:

SPP 2078 Sistemas de Información Geográfica

INFORME EJECUTIVO

Lugar y Fecha de emisión	Buenos Aires, Febrero de 2007
Código del Proyecto	5.05.07
Denominación del Proyecto	Dirección General Sistemas de Información Geográfica. Auditoría de Sistemas
Período Examinado	2005
Unidad Ejecutora	125 – Unidad de Sistemas de Información Geográfica
Programa Auditado	SPP 2078 Sistemas de Información Geográfica
Objetivo de la auditoría	Evaluar la adecuación de los recursos informáticos al cumplimiento de los objetivos institucionales y operativos del programa en términos de eficacia y eficiencia.
Alcance	Examinar, en general, la Arquitectura de Hardware y los Sistemas Operativos. Se efectuará lo propio con las cuestiones relativas a la red de comunicación de datos y a la seguridad. Se revisará el cumplimiento de las prácticas críticas de seguridad y la continuidad de los servicios.
Período desarrollo tareas de auditoría	01-Oct-2005 al 15-Diciembre-2005
Limitaciones al alcance	No existieron.
Aclaraciones Previas	Originalmente, la USIG (Unidad de Sistemas de Información Geográfica) se organizó para tomar los servicios concesionados a la firma CATREL S.A. Esta firma proveía el servicio de información geográfica desde el año 1991¹. Vencida la concesión en el año 2001, se prorrogó la misma hasta el 2003. A partir de esa fecha se hace cargo de los servicios concesionados la USIG. Posteriormente la USIG deviene en la actual DGSIG (Dirección General de Sistemas de Información Geográficas) dependiente del Vice Jefe de Gabinete del Gobierno de la Ciudad. Esta unidad tiene nivel de Dirección General y depende del Vice Jefe de Gabinete. Dispone de un presupuesto aproximado de \$2.900.000 (año 2005). Se desempeñan en la misma aproximadamente 80 personas, que revistan en carácter de contratados y 2 personas con nombramiento. La Dirección cuenta además con 10 pasantes, que rotan en distintas áreas. La Dirección tiene áreas que constituyen una unidad de apoyo técnico de la Dirección General de Rentas. Se encargan de llevar la cuenta corriente de los contribuyentes de ABL en lo que corresponde a las actualizaciones catastrales (avalúos),

¹ Los antecedentes relativos al traspaso se encuentran en el informe AGCBA 5.04.06 que se puede consultar en el sitio web www.agcba.gov.ar.

	detección de obras nuevas, ampliaciones, refacciones, impresión de las boletas, seguimiento de los pagos, seguimiento de planes de pagos, la relación con los mandatarios etc. Estas funciones relacionadas con las liquidaciones y los planes de pago son inherentes a la DGR. Área de Sistemas. El área de sistemas consta de cuatro sectores: • Desarrollo alfanumérico. • Desarrollo Gráfico. • Seguridad en Redes. • Soporte técnico. El área de sistemas de información geográfica consta de tres sectores: • Generación de Información: Genera nuevas capas de información geográfica como por ejemplo el mapa de calles actualizado o el historial del código de planeamiento urbano. • Interacción con otras áreas: Responde consultas y solicitudes de información, instala y capacita en el uso del sistema. • Sistema USIG: Se encarga del mantenimiento del sistema de información geográfico (USIG) de Internet (de uso público) e Intranet (de uso restringido al GCBA).
Conclusiones	La DGSIG perdió el rango de Dirección General pasando a depender de la Dirección General de Estadísticas y Censos, dependiente a su vez de la Subsecretaría de Inversión Pública y Análisis Fiscal del Ministerio de Hacienda. Esta nueva jerarquía refleja la poca entidad y el rol secundario que se otorga a las tecnologías de la información y las comunicaciones en el actual proyecto de Gobierno. Su ubicación actual, por otra parte, la sitúa dentro de un área usuaria por lo que carece de la independencia que respecto de las mismas sugieren la normativa y las buenas prácticas. Asimismo al instalarla dentro del Ministerio de Hacienda y Finanzas se prioriza su relación con la recaudación desdibujándose su función esencial de carácter tecnológico y al servicio de la ciudadanía, del conjunto del GCBA y de otros estamentos Públicos y Privados que pueden usufructuar este servicio. La Ex DGSIG brinda servicio de información geográfica al conjunto del GCBA así como a toda la comunidad con menos recursos que el anterior prestador lo que marca una mejora en su eficiencia global. La Ex DGSIG además ha introducido mejoras en los servicios mediante la incorporación de capas de información y ha extendido los mismos a una mayor cantidad de usuarios dentro y fuera del GCBA. Como herencia del antiguo modelo de gestión y como tarea

	complementaria a la de proveer sistemas gráficos, efectúa el procesamiento de los avalúos y sus respectivas cuentas corrientes, función que es competencia de Hacienda y Finanzas y debe integrarse a los sistemas de recaudación por lo que debe trasladarse a dicha órbita, lo que se encuentra en ejecución. Esto es fundamental para que la ex DGSIG libere recursos y se aboque específicamente a las cuestiones estrictamente tecnológicas de los sistemas geográficos y su relación con las bases alfanuméricas y continúe expandiendo sus servicios a lo largo y a lo ancho del GCBA y la ciudadanía. La Ex DGSIG posee parte del procesamiento a nivel de la propia Dirección lo que resulta antieconómico debido a que resulta muy costoso cumplir con todos los requisitos de seguridad para los mismos entre los que se encuentran a modo de ejemplo piso elevado, cableado de alimentación independiente, corriente estabilizada, servicio de energía ininterrumpido, acceso restringido con los adecuados controles, operatoria de respaldo, acondicionamiento del aire, y otros. Esto se potencia por el hecho de que sus oficinas son alquiladas y la inversión, de efectuarse, sería de muy dudoso recupero. Esto asimismo afecta la independencia del área de procesamiento de las áreas de desarrollo lo que es exigido para garantizar la confidencialidad, integridad, y adecuado tratamiento de la información. Una opción razonable consiste en usufructuar plenamente el centro de procesamiento de Datos que posee la DGSIG dentro del GCBA situando la totalidad del equipamiento central en dicha dependencia. También es necesario que exista una adecuada independencia del área de seguridad con lo que se completan y perfeccionan los requisitos básicos en materia de organización. Por otra parte es importante la planificación formal a corto medio y largo plazo aprobada por la superioridad y revisada en períodos prefijados para asegurar la alineación de las acciones de la Dirección con la política institucional. La planificación es un proceso y debe estar formalizado como tal. Se requieren además mecanismos formales para la administración, seguimiento, cuantificación y control bajo la óptica de la mejora continua de los principales procesos como la evaluación de mejoras tecnológicas, los pedidos de adecuación del software, el seguimiento de las actividades locales, y otros. Por otra parte en centros de cómputo de mediana envergadura resulta complejo alcanzar niveles adecuados de organización normativa debido a la carencia de personal y a la imposibilidad de atender muchos frentes diferentes con dotaciones reducidas. En este sentido es positivo revisar y ajustar normativa existente utilizada por áreas con mayor desarrollo de la misma en lo que puede colaborar la DGSIG. Esto asimismo potencia el uso de la especialización funcional.
--	---

	Por último es necesario revisar las razones de la importante rotación de recursos humanos para limitar la migración de los mismos, en especial los claves, para el desarrollo de la gestión. En la obtención de resultados la buena voluntad personal resulta inconducente. Para obtener resultados se requiere adecuados niveles de organización y especialización. Capacitación adecuada, compromiso y motivación del personal.
--	--

**INFORME FINAL DE AUDITORIA
PROYECTO N° 5.05.07**

DESTINATARIO

**Señor
Vicepresidente 1° de la Legislatura de la
Ciudad Autónoma de Buenos Aires
Dip. Santiago Manuel de Estrada
S / D**

En uso de las facultades conferidas por la Constitución de la Ciudad Autónoma de Buenos Aires de acuerdo al artículo 135, la ley número 325 del 18 de febrero de 2000 dictada por la Legislatura de la Ciudad Autónoma de Buenos Aires en su artículo número 6 y, supletoriamente, la ley 70, esta Auditoría General de la Ciudad procedió a efectuar un examen en el ámbito de las áreas de la Dirección General de Sistemas de Información Geográfica de la Ciudad de Buenos Aires con el objetivo que más abajo se describe:

1.- OBJETO

Dirección General de Sistemas de Información Geográfica. Auditoría de Sistemas, Jurisdicción 20, Jefatura de Gobierno.

2.- OBJETIVO

Evaluar la adecuación de los recursos informáticos al cumplimiento de los objetivos institucionales y operativos del programa en términos de eficacia, eficiencia y economía.

3.- ALCANCE

Se examinará la Arquitectura de Hardware y los Sistemas Operativos. Se efectuará lo propio con las cuestiones relativas a la red de comunicación de datos y a la seguridad. Se revisará el cumplimiento de las prácticas críticas de seguridad y la continuidad de los servicios.

Las tareas se efectuaron sobre el contexto vigente al momento de su realización, comprendiendo el período de Octubre-Diciembre del año 2005.

4.- ACLARACIONES PREVIAS

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

Subsidiariamente se utilizaron:

- ▣ Las normas y recomendaciones de seguridad establecidas por la DGSInf.
- ▣ Normas Informáticas de la Sindicatura General de la Nación (SIGEN).
- ▣ Manual CISA. Edición 2003.
- ▣ Manual COBIT. (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Association. Capítulo Buenos Aires.
- ▣ Normativa Magerit. (Manual de Gestión de Riesgos en Tecnologías de la Información)

La normativa en la materia establece que los procedimientos que deben llevarse a cabo para el desarrollo de las tareas y el control de las áreas de sistemas de información y comunicaciones deben involucrar a toda la organización, desde el personal directivo hasta los integrantes del área de sistemas de información y el personal de todos los niveles de las áreas usuarias. Asimismo establece que estos procedimientos se deben diseñar para proveer un grado razonable de seguridad en el logro de los objetivos de la organización y el uso eficiente de los recursos utilizados para ello. Para ello deben estar aplicados para dar cumplimiento a los siguientes requisitos:

- Eficacia: La información y los procesos relacionados deben ser relevantes y pertinentes para el desarrollo de la actividad. Deben presentarse en forma correcta, coherente, completa y oportuna.
- Eficiencia: El proceso de la información debe realizarse mediante una óptima utilización de los recursos.
- Confidencialidad: La información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.
- Integridad: Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.
- Disponibilidad: Los recursos y la información deben estar disponibles en tiempo y forma, cada vez que sean requeridos.
- Cumplimiento: Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades públicas.
- Confiabilidad: Los sistemas deben brindar información correcta para que se la utilice en la operatoria de la entidad, en los informes a los usuarios internos y a los organismos reguladores.

Todos los recursos intervinientes, tales como datos, sistemas de aplicación, tecnología, instalaciones y personas deben satisfacer y contribuir al

cumplimiento de cada uno de estos aspectos en los procesos de tecnología informática.

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.

Se utilizó software de auditoría de sistemas y tecnologías de la información.

4.1- Procedimientos:

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

- Se solicitó por nota la documentación relacionada con el objeto de esta auditoría.
- Se realizó la entrevista protocolar explicando los procedimientos, el objeto, el objetivo y el alcance del proyecto.
- Se efectuaron entrevistas con el personal jerárquico y operativo de las áreas involucradas.
- Se efectuaron verificaciones “in situ” de la instalación del equipamiento informático, de las comunicaciones y la conectividad, en la sede de la DGSIG y en la Dirección de Sistemas de Información (DGSInf) dependiente de la Secretaría de Hacienda.
- Se efectuó el análisis de la documentación provista por el área.

4.2- Descripción General

Originalmente, la USIG (Unidad de Sistemas de Información Geográfica) se organizó para tomar los servicios concesionados a la firma CATREL S.A. Esta firma proveía el servicio de información geográfica desde el año 1991². Vencida la concesión en el año 2001, se prorrogó la misma hasta el 2003. A partir de esa fecha se hace cargo de los servicios concesionados la USIG.

² Los antecedentes relativos al traspaso se encuentran en el informe AGCBA 5.04.06 que se puede consultar en el sitio web www.agcba.gov.ar.

Posteriormente la USIG deviene en la actual DGSIG (Dirección General de Sistemas de Información Geográficas) dependiente del Vice Jefe de Gabinete del Gobierno de la Ciudad.

Esta unidad tiene nivel de Dirección General y depende del Vice Jefe de Gabinete. Dispone de un presupuesto aproximado de \$2.900.000 (año 2005). Se desempeñan en la misma aproximadamente 80 personas, que revistan en carácter de contratados y 2 personas con nombramiento. La Dirección cuenta además con 10 pasantes, que rotan en distintas áreas.

La Dirección tiene áreas que constituyen una unidad de apoyo técnico de la Dirección General de Rentas. Se encargan de llevar la cuenta corriente de los contribuyentes de ABL en lo que corresponde a las actualizaciones catastrales (avalúos), detección de obras nuevas, ampliaciones, refacciones, impresión de las boletas, seguimiento de los pagos, seguimiento de planes de pagos, la relación con los mandatarios etc. Estas funciones relacionadas con las liquidaciones y los planes de pago son inherentes a la DGR.

Área de Sistemas.

El área de sistemas consta de cuatro sectores:

- Desarrollo alfanumérico.
- Desarrollo Gráfico.
- Seguridad en Redes.
- Soporte técnico.

El área de sistemas de información geográfica consta de tres sectores:

- Generación de Información: Genera nuevas capas de información geográfica como por ejemplo el mapa de calles actualizado o el historial del código de planeamiento urbano.
- Interacción con otras áreas: Responde consultas y solicitudes de información, instala y capacita en el uso del sistema.
- Sistema USIG: Se encarga del mantenimiento del sistema de información geográfico (USIG) de Internet (de uso público) e Intranet (de uso restringido al GCBA).

Servicios contratados a terceros: No tiene servicios contratados a terceros.

Comunicaciones: El sistema utiliza para sus operaciones la red de datos del GCBA, la MAN (Metropolitan Area Network). Muchas de las funciones de sus sistemas cuentan con interfases Web y son accesibles a través de Internet.

Descripción de la Red Interna de Datos: La DGSIG brinda servicio de información geográfica con acceso al mapa interactivo a la ciudadanía a través de internet y al GCBA a través de la Intranet. La información alfanumérica que

se relaciona con el mapa interactivo está organizada en capas. Cada capa contiene información relativa a un tema de interés, como por ejemplo la forestación, la densidad de población y otros. La ciudadanía accede a 37 capas mientras que los usuarios del GCBA acceden a todas las capas con excepción de algunas de ellas como la relativa a habilitaciones que tienen el acceso restringido.

El servicio de la DGSIG (Dirección General de Sistemas de Información): La DGSIG provee servicio de alojamiento (housing) a los servidores de la DGSIG. Hay 5 equipos en el centro de cómputos sito en la Av. Independencia 635 PB para esta finalidad³.

Efectúan copias de respaldo según instructivos de la DGSIG. Estas copias de respaldo incluyen un juego que se utiliza para guarda en sede externa con frecuencia mensual. El proceso de generación de copias de resguardo está desdoblado en una parte manual y otra que se efectúa automáticamente mediante un robot. Como sede externa se utiliza la contaduría del GCBA situada en Belgrano al 800.

Cabe resalta que respecto a la contingencia y el proceso de recuperación de desastre se encuentra a cargo de la DGSIG.

Software de base y servicios: Se encuentran orientados a sistemas de arquitectura abierta (denominado así ya que se puede acceder y modificar el código -órdenes escritas dentro de los programas-) siguiendo recomendaciones realizadas por la DGSIG (Sistema Operativo, aplicaciones ofimáticas y sistema USIG Internet). Combinan el uso de estos sistemas con sistemas propietarios (sistema USIG Intranet).

Decreto N° 350-GCABA-2006: Por último, la organización auditada (DGSIG) pierde el rango de Dirección General en el nuevo organigrama de la ley de Ministerios hecho que se produjo luego del cierre de las tareas de campo. Las competencias relativas a la gestión y administración de las bases de datos georeferenciales existentes en el Gobierno de la Ciudad de Buenos Aires pasaron de la ex Secretaría Jefe de Gabinete al actual Ministerio de Hacienda, bajo cuya órbita se estableció el objetivo de "diseñar, planificar, aplicar y coordinar los sistemas estadísticos, censos e integración de bases de datos georeferenciales" (Conf. artículo 16, inc. j) de la Ley N° 1.925). El área pasó a depender en su totalidad de la Dirección General de Estadísticas y Censos, dependiente de la Subsecretaría de Inversión Pública y Análisis Fiscal.⁴ Una

³ Considerando que dichos equipos funcionan en conjunto cumpliendo diferentes funciones y que resulta muy dificultosa su evaluación por separado se efectuó una serie de pruebas chequeando la disponibilidad del servicio y si la respuesta era satisfactoria. Las pruebas fueron satisfactorias.

⁴ La misma tiene entre sus responsabilidades primarias la de "promover, coordinar, administrar e integrar las bases de datos geo-referenciales existentes en las diferentes áreas del Gobierno de la Ciudad de Buenos Aires" (Conf. Anexo 2/6 Decreto N° 350/06).

disposición posterior de la Dirección General de Rentas designa una coordinación para asegurar la obtención de los productos esenciales para la liquidación de las tasas a partir de la información que producía la Dirección disuelta.

5.- OBSERVACIONES

5.1. Tecnologías de la Información y red de datos

5.1.1. Aspectos Generales.

Descripción: En este marco se revisa la situación del área de tecnologías de la Información y comunicaciones (TICs) en el organismo, la dependencia del área de seguridad, los nuevos proyectos y sus tratamientos, la existencia de políticas formales documentadas para la administración de los sistemas, etc.

- 1- *La infraestructura de comunicaciones de voz (telefonía) es inadecuada y antieconómica.* Cuentan con sólo 4 líneas analógicas de entrada y salida de comunicaciones.
La DGSIG se vincula con nodos de la red Man con un enlace de datos punto a punto, por lo que de igual manera podrían enlazar sus comunicaciones de voz para integrarse a la red con que cuenta el GCBA.
- 2- *No hay control sobre el gasto de comunicaciones de voz.* Las facturas telefónicas de la DGSIG no son conformadas por la Dirección para su control y posterior aprobación o rechazo del gasto. Las facturas son enviadas directamente a la Contaduría General sin su respectivo visado administrativo por parte del usuario del servicio. Esta falta de control no es responsabilidad de la DGSIG que ha hecho esfuerzos en ese sentido. Además de la falta de control interno y sus consumos, cabe la posibilidad de que, eventualmente, la empresa proveedora pueda facturar comunicaciones erróneamente o que no fueron realizadas por el usuario.
- 3- *Plan Estratégico de Tecnologías de la Información y las Comunicaciones (TICs).* No existe un plan estratégico de TICs formalmente aprobado por las máximas autoridades, que contenga los proyectos principales, los cronogramas de su implementación y los responsables para un período de corto, mediano y largo plazo.
La Dirección conoce sus prioridades y elabora el presupuesto anual basado en los desarrollos a realizar en el período presupuestado. Sin embargo, la falta de un Plan formal de TIC que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, responsables, sectores involucrados y la totalidad de las tareas a llevarse a cabo, no permite una supervisión continua y directa de las tareas que se realizan.
- 4- *Política formal de seguridad.* El organismo cuenta con rutinas de seguridad. Sin embargo, no existe una política formal de seguridad de la

información en la que se precise, entre otros, el compromiso⁵ de la dirección, la estructura, los recursos y el marco tecnológico y organizativo en que se desenvolverá la función. La política formal de seguridad debe acompañarse de un Análisis de Riesgos formalmente aprobado.

- 5- *Áreas no técnicas.* La dirección de sistemas de información geográfica heredó de su predecesora CATREL SA un conjunto de funciones que corresponden a la Dirección General de Rentas como el registro de la cuenta corriente de ABL de los contribuyentes que efectúan mejoras, el seguimiento de sus pagos, el otorgamiento de planes de pago, y otras. También heredó funciones propias de las áreas de fiscalización de obras y catastro como la detección de mejoras edilicias.
- 6- *Función de Seguridad Informática.* Existe una función denominada "Responsable de la Seguridad de Redes" dentro del área de sistemas. No obstante, es necesario la independencia del responsable de la seguridad⁶ respecto del área de sistemas para garantizar un adecuado control por oposición.
- 7- *Proceso de evaluación de incorporación de tecnología.* No se dispone de un procedimiento sistemático y formal de evaluación de factibilidad de nuevos proyectos tecnológicos. El proceso formal permite asegurar que son analizadas las novedades tecnológicas y que se incorporan aquellas que mejoran la eficiencia y los servicios.
- 8- *La infraestructura edilicia en la que desarrollan las tareas el personal de la DGSIG es inadecuada.* La planta se encuentra separada en dos sectores, dividida por el hall de acceso de los ascensores. Falta espacio físico suficiente para el personal, el equipamiento y los insumos. Los practicantes fueron derivados a instalaciones en el edificio del Mercado del Plata. El organismo auditado ha realizado distintas propuestas infructuosamente fin de resolver este problema.

5.1.2. Organización y personal

Descripción: Las observaciones en este título están referidas a aspectos generales de la organización, la situación del personal del área de sistemas, su grado de capacitación en relación a las tareas, la segregación de funciones, etc.

- 1- *Plan de capacitación de los agentes.* No hay un plan formal de capacitación de los agentes que tienen a su cargo la administración y mantenimiento de los sistemas, la red, la conectividad y las comunicaciones.

⁵ Normas como el COBIT y las ISO hablan del compromiso de la dirección con las políticas de seguridad.

⁶ La segregación de funciones entre seguridad y administración está establecida en la normativa Cobit y debe ser observada siempre porque constituye una pieza esencial de la seguridad. Además las buenas prácticas y las normas así lo exigen.

La falta de capacitación afecta la implementación de mejoras y actualizaciones de la red y los sistemas, y reduce la posibilidad de aprovechamiento de las tecnologías asociadas a la información y las comunicaciones.

- 2- *Segregación de funciones.* Si bien existe una distribución informal de tareas, se producen superposiciones. El área no tiene formalizada la delimitación entre las tareas de mantenimiento de sistemas, operaciones, soporte técnico y supervisión, de manera de garantizar una adecuada segregación de funciones y un control por oposición de intereses.
- 3- *Situación del personal.* La falta de formalización de la relación laboral de los agentes a cargo de tareas críticas pone en riesgo la continuidad de tareas en razón de la debilidad del vínculo con el organismo. Asimismo, la inadecuación de los montos contractuales en esas tareas genera pérdida de personal valioso (se registraron 14 renunciaciones de personal especializado en 2 trimestres), de costoso entrenamiento y en muchos casos de difícil sustitución. A pesar de que el organismo auditado ha elevado propuestas con medidas correctivas para este problema, la situación subsiste.

5.1.3. Equipamiento (Hardware)

- 1- *Inventario de equipamiento.* El organismo cuenta con un adecuado registro de altas y bajas de hardware que lleva año a año en planillas separadas. Este registro es adecuado para su ingreso contable y patrimonial ya que consigna en forma correcta el tipo de bien, su descripción, su número de serie y la fuente de financiación. Sin embargo, se debe contar con un inventario de hardware unificado que consigne número de serie, área, puesto de trabajo, número IP, etc. en sincronización con el mapa físico y lógico de la red, este inventario es puramente operativo por lo tanto debe consignar el equipamiento en uso.

5.1.4. Red de datos

Descripción: En esta sección se revisa todo lo referido a la red interna de datos del organismo y su conectividad con otras redes. También se verifican aspectos referidos a la documentación, la verificación del funcionamiento de los vínculos, la seguridad de la red, etc.

- 1- *Encriptación de información.* No se utilizan técnicas de encriptación de la información que circula por la red o que se envía a otras reparticiones.
- 2- *Monitoreo de red local.* No se verifican procedimientos de seguimiento formal, sistemático y rutinario de la actividad de la red local. Tampoco hay registro formal de los incidentes más frecuentes que se presentan.

- 3- *Documentación de intentos de acceso indebido.* No se documenta formalmente el seguimiento de los intentos de acceso indebidos a los servidores.

5.1.5. Continuidad de la operación

Descripción: Los aspectos referidos a la continuidad de las operaciones sistematizadas en el organismo son aquellos que hacen a la no interrupción de los servicios; se revisan para que en caso de contingencias la información no se pierda y se pueda recuperar en el menor tiempo posible la normalidad de los procesos.

- 1- *Procedimientos de respaldo y recuperación de la información.* La información de los servidores residentes en DGSInf se respalda con un doble juego de copias. La información de los servidores residentes en DGSIG se respalda espejando discos pero no tiene doble copia. Esta metodología es inadecuada ya que así se carece de copia en sede externa.
Además no se efectúan pruebas de recupero de datos de modo planificado y sistemático con frecuencia periódica tal como lo estipulan las buenas prácticas en la materia.
- 2- *Plan de Contingencias, Plan de Evacuación y Plan de Recuperación de Desastres.* No se cuenta con un plan formalmente aprobado de contingencias, un plan de evacuación y un plan de recuperación de desastres y sus correspondientes pruebas periódicas, sistemáticas y formales.

5.1.6. Seguridad lógica

Descripción: La seguridad lógica contempla todo lo atinente a los aspectos de seguridad en la administración de los sistemas, los servidores y la red. Aspectos como las claves de acceso, la información y sus responsables, las altas y bajas de usuarios, etc. son revisados en este título.

- 1- *Clasificación de la información* El organismo cuenta con información propia y de terceros, en estos casos son los otros organismos los que establecen las restricciones de usuarios para acceder a la misma. El tratamiento de los permisos es en esos casos adecuado, sin embargo no se ha efectuado una clasificación formal de la información de manera tal que se pueda precisar el nivel de confidencialidad necesario de los datos y de la información en los diferentes procesos, computarizados o manuales. Tampoco se dispone de un procedimiento formal para su ejecución.
- 2- *Definición del dueño de los datos.* El auditado cuenta con mecanismos para conocer a los responsables de los datos. Sin embargo, no se definió formalmente, en cada caso, al propietario de los datos, es decir, el funcionario responsable que participará en la determinación de los niveles de acceso a la información para cada función y proceso.

- 3- *Claves.* Las claves no son en todos los casos personales y secretas. No se brindan ejemplos puntuales por razones de seguridad⁷.
En este sentido, el organismo se encuentra abocado a la tarea de desarrollar un sistema de claves personales, secretas y univocas que en un futuro cercano entrará en producción.
- 4- *Intentos de Acceso Fallidos.* No se encuentra normado formalmente el bloqueo de usuarios por intentos de acceso fallidos a la red y a los sistemas. Los procedimientos de bloqueo deben ser notificados formalmente a los usuarios del sistema. Tampoco hay un procedimiento formal para la rehabilitación de claves.
- 5- *Procedimiento de puesta en producción.* No existen procedimientos de control formal para garantizar el efectivo y correcto control de cambios cuando corresponde.
- 6- *Falta de separación entre áreas de sistemas y usuarias.* No existe una completa división entre las funciones de Sistemas y las correspondientes a las áreas Usuarias.
La Dirección efectúa tareas propias de un área de Sistemas, como procesamiento de información, conjuntamente con actividades propias de las áreas usuarias como captura y actualización de información. Un ejemplo de tarea propia del área usuaria es la recolección de información de las imágenes correspondientes a los frentes y su actualización.
Esto debilita el control por oposición natural existente entre las áreas mencionadas anteriormente.
- 7- *Ejecución de tareas incompatibles con el procesamiento de datos de sistemas geográficos.* La DGSIG efectúa tareas que corresponden a la DGR tales como llevar la cuenta corriente de los avalúos de ABL.
La DGSIG, además de llevar la base de cálculo física de la tasa de ABL, calcula, emite, registra y efectúa el seguimiento de la cobranza de los avalúos (incrementos por mejoras o aumento de superficie de los inmuebles).
Estas funciones fueron heredadas del modelo privado y constituyen una debilidad del control interno por excesiva concentración de funciones y así como una falla grave de organización debido a que son tareas que corresponden a otra área (la DGR).
- 8- *Funciones de producción desconcentradas.* La DGSIG efectúa parte de las funciones de producción, como back ups de servidores situados en la DGSI, back up en sede externa, mientras que la DGSIG efectúa otra parte

⁷ Las claves deben ser personales y secretas, es decir que sólo el usuario pueda conocerla. El alcance del secreto incluye al administrador del servicio, que debe tener una clave genérica a fin de habilitar al usuario para que ingrese a una primera sesión y que en ese momento el usuario debe cambiar esa clave genérica por una personal, de esta forma el administrador se abstiene de conocer la clave de los usuarios. El conocimiento de las claves de los usuarios lleva a situaciones de no repudio, es decir que de producirse incidentes no podría identificarse en forma cierta e indubitable a un único responsable.

como el back up del equipo situado en RS Peña, el mantenimiento de equipos, el ajuste fino de los sistemas, el recupero de datos, y otros.

Resulta antieconómico que estas funciones estén repartidas ya que implica una menor escala y un menor grado de especialización además de áreas parcialmente superpuestas. Resulta conveniente concentrar las funciones de producción en la DGSi permitiendo que la DGSi enfoque su esfuerzo en las restantes.

5.1.7. Seguridad Física Edificio de R. S. Peña

Descripción: La seguridad física contempla todo el entorno en donde se desarrollan las tareas de administración de los sistemas y la red donde están funcionando los servidores, las medidas de seguridad contra el fuego (detectores, matafuegos), la ubicación de los dispositivos de red, los accesos del personal del organismo y/o terceros, las medidas preventivas como luces y salidas de emergencia, los planes de evacuación y sus prácticas etc.

- 1- *Resguardo de documentación.* No se dispone de instalaciones adecuadas para guardar los listados y documentación de datos, programas y sistemas.
- 2- *Procedimiento de depuración de la información.* Falta un procedimiento formal, rutinario y sistemático para depurar la información y si corresponde proceder a la destrucción de la información impresa o grabada. El procedimiento formal debe fijar para la información un ciclo de vida.
- 3- *Servidores en sede descentralizada.* Existen servidores de sistemas de información geográfica que tienen su asiento en la dependencia sita en Roque Sáenz Peña. Allí sólo deberían funcionar los servidores propios de la administración de la red local.
La preparación de la seguridad física, en cuanto a control de accesos, ejecución de back ups, instalación eléctrica independiente, aseguramiento de provisión eléctrica, y otros de la sede para servir de asiento a servidores resulta antieconómica debido a que el GCBA cuenta con sitios preparados a tal fin, como el existente en la DGSi.
Esto se agrava por tratarse de oficinas alquiladas en las que parte de esta inversión se perdería.

5.1.8. Sistemas aplicativos

Descripción: En esta sección se revisa lo atinente a los sistemas, los programas, desarrollos, software en uso, aplicaciones, etc que utiliza el organismo.

- 1- *Registro de cambios.* El sistema no cuenta con reportes (logs) que permitan identificar unívocamente al autor de acciones o cambios dentro

del Sistema de modo que se pueda determinar la responsabilidad por acciones en caso de necesidad.

- 2- *Integración con los Sistemas del GCBA.* El sistema de información geográfico está operando con 100 capas (aprox.) pero su potencialidad aún no se desarrolló de modo completo ya que no funciona integrado completamente con la totalidad de los sistemas del GCBA. Esta falta de integración no es responsabilidad de la propia Dirección General, es el GCBA quien debe fomentar y desarrollar la integración de los sistemas para evitar redundancia de tareas y para una mejor utilización de la información.

6. RECOMENDACIONES

6.1. Tecnologías de la Información y red de datos

- 1- Se recomienda hacer un estudio del uso y los requerimientos de telefonía del organismo, conociendo estos parámetros sugerimos hacer uso de las facilidades imperantes en el mercado de comunicaciones de voz y datos como una forma de mejorar la prestación y disminuir los costos.
- 2- Se recomienda que se contacte al proveedor del servicio y se disponga que las facturas sean remitidas al organismo para su control antes del envío a la Contaduría General. Asimismo, debería cursarse nota a la Contaduría General expresando la necesidad de la aprobación de las facturas de consumo antes del pago.
Por otra parte, aunque el sistema se resolviera con un enlace o una integración a las redes de comunicaciones del GCBA, igualmente las mismas deberían ser controladas por el organismo a fin de evitar comunicaciones indebidas o costos innecesarios.
- 3- Implementar un plan de corto plazo con fechas programadas para las distintas tareas, detallando etapas, recursos humanos y materiales asignados que permita supervisar los avances, revisar las metas y monitorear su alineación con los objetivos de la Dirección. También, debe realizarse un plan estratégico de mediano/largo plazo según los lineamientos de las máximas autoridades del organismo.
- 4- Carencia de política formal de seguridad. Formalizar una política de seguridad con los lineamientos tecnológicos, el compromiso de la dirección, los recursos y las definiciones de riesgo correspondientes.
- 5- El organismo se encuentra (desde septiembre de 2005) dando los pasos necesarios para realizar la transferencia de esas tareas a la unidad de proyectos especiales del BCBA que presta servicios informáticos a la DGR. La dirección debe ajustarse a las tareas técnicas para la cual está capacitada, todas las otras tareas recibidas por situaciones heredadas

generan una dispersión de sus recursos humanos, tecnológicos y económicos innecesarios. Por ello, se recomienda acelerar el proceso de transferencias de las tareas mencionadas.

- 6- Independencia de la función seguridad informática. Incorporar o designar formalmente un responsable independiente del área de sistemas y del sector usuario, que se haga cargo de la seguridad informática, el acceso a los datos y el resguardo de la información.
- 7- Carencia de un proceso de evaluación de incorporación de tecnología. Dado la velocidad con que se producen cambios en las tecnologías de la información y las comunicaciones (TICs), se debe desarrollar e implementar un proceso de detección de novedades tecnológicas, herramientas y soluciones que continuamente aparecen en el mercado y posteriormente proceder a su evaluación. Las mismas deben tener un tratamiento formal con una metodología de decisión adecuada.
- 8- Se recomienda intensificar la búsqueda de una solución teniendo en cuenta que las instalaciones edilicias deben ser acordes a las tareas desempeñadas. Esta adecuación entre tareas e infraestructura debe manifestarse en temas tales como: relación entre metros cuadrados disponibles y cantidad de personal, luz ambiente natural para aquellas tareas de uso intensivo de computadoras, espacios diferenciados para cada área, espacio para archivos, guarda de documentación, áreas de impresión, etc.

6.1.2. Organización y personal

- 1- *Falta de un plan de capacitación de los agentes de las áreas Tics (Tecnologías de la Información y las comunicaciones):* Los cambios continuos en las áreas de las comunicaciones, las redes y las tecnologías asociadas con la información obliga al organismo a contar con un plan de capacitación para desarrollar las habilidades del recurso humano en función de las necesidades de la organización.
Se recomienda confeccionar un plan formal de capacitación que contemple la actualización de los conocimientos y las técnicas según las funciones que desempeña cada agente, tanto en la actualidad como a futuro, en función de los proyectos del área. Contemplar para ello las características personales, formación previa y la vocación de los involucrados.
- 2- *Falta de segregación de funciones.* Las funciones en el área de sistemas deben estar claramente diferenciadas asegurándose que estas se encuentran segregadas de modo tal de generar un adecuado control por oposición. Se recomienda, segregar adecuadamente las funciones que sean incompatibles entre sí, desconcentrando tareas y generando controles por oposición.

- 3- *Personal contratado.* La falta de personal estable en las áreas críticas de sistemas supone riesgos y posible pérdida de conocimientos en el tratamiento de la información. Para solucionarlo, se deben tomar todas las medidas posibles para lograr que haya personal estable a cargo de las funciones críticas del área de sistemas. En todos los casos se debe evaluar la modalidad y la remuneración de contratación del personal crítico de forma de no comprometer la continuidad de los servicios informáticos y técnicos.

6.1.3. Equipamiento (Hardware)

- 1- Las planillas de altas y bajas anuales de hardware con que cuenta el organismo son un buen punto de partida para generar a partir de ellas un inventario operativo de equipamiento.
Se recomienda confeccionar y mantener permanentemente actualizado un inventario físico del equipamiento con un adecuado nivel de detalle, para ello se cuenta con planillas anuales que facilitan la tarea.

6.1.4. Red de datos

- 1- *Encriptación de información.* En los casos en que se maneja información crítica se debe evaluar la necesidad de encriptarla. Las técnicas de encriptación son niveles de seguridad que se suman y operan en forma concomitante con otras medidas que se toman para resguardar la información. Además proveen de mecanismos de autenticación a quienes envían y quienes reciben la información. Proveen la seguridad que la información no ha sido alterada y permite garantizar el no repudio del intercambio.
- 2- *Falta de monitoreo de red.* Se debe incorporar el monitoreo rutinario, sistemático y completo de la red por medio de software específico para este fin. Este, debidamente configurado genera alertas para distintas situaciones. Además de monitorear la red, se debe tener un registro formal de todas las novedades que se producen para luego analizarlas y tomar medidas acordes con ellas.
- 3- *Ausencia de documentación de análisis de intentos de acceso indebido.* Se recomienda analizar y documentar los intentos de acceso no permitidos y las acciones tomadas para neutralizarlos y proteger la red. Esta recomendación acompaña y complementa a la formulada para el monitoreo de red (ver ut supra).

6.1.5. Continuidad de la operación

- 1- *Procedimientos de resguardo incompletos.* Formalizar una política y un procedimiento para la generación de las copias de resguardo de la información.

Confeccionar e implementar procedimientos de resguardo de la información que incluyan nivel de riesgo, definición de soportes, responsable de ejecución, mecanismo de control y supervisión y demás aspectos.

Incluir en los procedimientos de resguardo de la información la guarda en sede externa. Esta se cumplimenta efectuando la conservación de la información en un edificio diferente de aquel en el que tiene asiento el centro de cómputos.

Falta de copia de respaldo en sede externa. Las reglas del arte indican que una buena política de respaldo de la información debe incorporar la práctica del resguardo en sede externa previa definición de lugar de guarda, la frecuencia y otros factores.

Procedimiento de recuperación incompleto. Incorporar procedimientos formales de recuperación de datos, que deben ser testeados semestralmente (como mínimo) en forma rutinaria y sistemática. En ellos se debe dar participación a las áreas usuarias y a los responsables de los controles internos del organismo que deberán ratificar el éxito de la prueba y suscribir el acta. En caso de fallas se deberá efectuar un informe de las mismas, para su corrección y prueba.

- 2- Los planes de contingencia prevén los pasos a seguir frente a situaciones de emergencia o desastre (inundaciones de la sala donde reside la central, incendio, cortes prolongados de energía, etc). Estos planes apuntan a la continuidad de los servicios en esas eventualidades.

Planificar, probar y evaluar un plan de contingencias, un plan de evacuación, con medidas especiales para el centro de cómputos si el mismo las requiriese, y un plan de recuperación de desastre que permita el retorno a la operación normal en los plazos previstos. Estos planes deben probarse al menos una vez al año.

Los organismos basan gran parte de su accionar en los vínculos y las comunicaciones, dada su importancia estos deben contar con un plan de contingencia y un plan de recuperación de desastres formalmente aprobado y este debe ser verificado periódicamente a fin de asegurar su adecuado funcionamiento.

El personal debe conocer y realizar los debidos procedimientos en caso de emergencia para atenuar los efectos y daños que esta puede producir. Estos planes deben ser periódicamente probados para ir adecuándolos a las distintas circunstancias.

Plan de contingencias incompleto. Elaborar un plan de contingencias, evacuación y de recuperación de desastres y efectuar pruebas integrales de los mismos por lo menos una vez al año. Las pruebas deben ser formales e incluyen a la totalidad del personal involucrado, los planes deben tener un responsable formal y contemplar el rol de cada agente al momento de tener que ejecutarlo. Para la confección de estos planes se puede solicitar la colaboración de la Dirección General de Sistemas de Información y la Dirección General de Defensa Civil del GCBA.

6.1.6. Seguridad lógica

- 1- *Falta de clasificación formal de la información.* Clasificar la información según el grado de confidencialidad (por ejemplo: en pública, reservada y confidencial). Esto debe incluir toda la información que administre la institución con independencia de su soporte que puede ser o no informático. En caso de manejar información de otros organismos de gobierno se debe solicitar a estos que remitan formalmente la clasificación que tiene la información enviada firmada por su responsable. Los mismos recaudos deben tenerse en cuenta para la información que la DGSIG envía a otros organismos.
- 2- *Falta de definición del dueño del dato.* Definir formalmente al propietario de los datos que se generan en cada área y el alcance de su participación en los diferentes procedimientos de seguridad lógica. También, definir quienes serán los responsables por la fijación de pautas de resguardo de la información de la institución y del tratamiento adecuado de la misma en función de su grado de confidencialidad.
- 3- Se recomienda acelerar los pasos necesarios para que el nuevo sistema de claves entre en vigencia en el menor tiempo posible, teniendo en cuenta los factores observados. La identificación de cada usuario debe ser unívoca, y formal de modo de evitar la negación de pertenencia de la clave por parte del usuario. Además se sugiere incorporar al desarrollo un plazo de renovación periódico de la clave por parte de los usuarios de los distintos sistemas y también un plazo de caducidad de las claves que no fueron usadas en un tiempo previamente determinado. La incorporación de estas funciones genera la necesidad de advertir al usuario de las condiciones de uso al momento del alta. Normar formalmente las características que se determinen para las claves de seguridad como período de caducidad, cantidad y tipo de caracteres requeridos, y otros.
- 4- *Bloqueo por Intentos de Acceso Fallidos.* Formalizar las condiciones del bloqueo (por ejemplo tres intentos) y desbloqueo por intentos de acceso fallidos. Notificar las novedades de acceso a los usuarios del sistema.
- 5- *Procedimiento de puesta en producción.* Incorporar un procedimiento formal para la puesta en producción de nuevas aplicaciones o

modificaciones a las existentes, indicando versión, fecha de puesta en producción, responsables involucrados, etc. Incorporar logs de auditoría para los cambios que se efectúan en aplicativos centrales.

- 6- Efectuar una clara delimitación de las áreas usuarias que deben manipular información, ingresarla y procesarla a través de los aplicativos con independencia de las funciones propias de Sistemas.
- 7- Estas funciones corresponden a Hacienda y Finanzas ya que se trata de sistemas de recaudación y deben integrarse a los sistemas que administran la misma. La DGSIG informó que ya se están efectuando tareas en este sentido y que el procesamiento efectuado hasta el presente se realizó bajo el control de Rentas.
- 8- Concentrar las funciones correspondientes a producción, como procesamiento, copias de respaldo y otros, en la DGSI aprovechando la infraestructura de seguridad física instalada y mantener descentralizadas las funciones de Planificación, Desarrollo, Incorporación de tecnología y otros relativa a Sistemas Geográficos.

6.1.7. Seguridad Física Edificio de R. S. Peña

- 1- Incorporar instalaciones adecuadas para la conservación de la documentación como carpetas de sistemas, programas, información de control, listados y otros.
- 2- Se recomienda fijar un procedimiento formal que determine los pasos a seguir para depurar la información. Asimismo, en forma concordante este documento debe expresar el ciclo de vida de la información que se maneja en el organismo.
Confeccionar un procedimiento de desecho de información impresa y/o en soportes magnéticos que asegure su destrucción en especial cuando los soportes contengan información confidencial.
- 3- Evaluar el traslado de todos los servidores al centro de cómputos de la DGSI disminuyendo los requisitos de seguridad física del edificio alquilado. Incrementar, de resultar necesario, el ancho de banda del vínculo de comunicación existente entre las dos sedes.

6.1.8. Sistemas aplicativos

- 1- Incorporar paulatinamente logs en las funciones críticas del sistema, las que deberán determinarse previamente.
- 2- Se recomienda tender a la integración de la información de los diferentes sistemas del GCBA, potenciando la funcionalidad de los mismos y

explotando en forma exhaustiva la información disponible. Corresponde aclarar que esta función no es de la exclusiva responsabilidad de la DGSIG. Esta integración debe procurarse aunque la información se encuentre soportada por diferentes entornos y equipos.

7.- CONCLUSIONES

La DGSIG perdió el rango de Dirección General pasando a depender de la Dirección General de Estadísticas y Censos, dependiente a su vez de la Subsecretaría de Inversión Pública y Análisis Fiscal del Ministerio de Hacienda. Esta nueva jerarquía refleja la poca entidad y el rol secundario que se otorga a las tecnologías de la información y las comunicaciones en el actual proyecto de Gobierno. Su ubicación actual, por otra parte, la sitúa dentro de un área usuaria por lo que carece de la independencia que respecto de las mismas sugieren la normativa y las buenas prácticas. Asimismo al instalarla dentro del Ministerio de Hacienda y Finanzas se prioriza su relación con la recaudación desdibujándose su función esencial de carácter tecnológico y al servicio de la ciudadanía, del conjunto del GCBA y de otros estamentos Públicos y Privados que pueden usufructuar este servicio.

La Ex DGSIG brinda servicio de información geográfica al conjunto del GCBA así como a toda la comunidad con menos recursos que el anterior prestador lo que marca una mejora en su eficiencia global. La Ex DGSIG además ha introducido mejoras en los servicios mediante la incorporación de capas de información y ha extendido los mismos a una mayor cantidad de usuarios dentro y fuera del GCBA.

Como herencia del antiguo modelo de gestión y como tarea complementaria a la de proveer sistemas gráficos, efectúa el procesamiento de los avalúos y sus respectivas cuentas corrientes, función que es competencia de Hacienda y Finanzas y debe integrarse a los sistemas de recaudación por lo que debe trasladarse a dicha órbita, lo que se encuentra en ejecución. Esto es fundamental para que la ex DGSIG libere recursos y se aboque específicamente a las cuestiones estrictamente tecnológicas de los sistemas geográficos y su relación con las bases alfanuméricas y continúe expandiendo sus servicios a lo largo y a lo ancho del GCBA y la ciudadanía.

La Ex DGSIG posee parte del procesamiento a nivel de la propia Dirección lo que resulta antieconómico debido a que resulta muy costoso cumplir con todos los requisitos de seguridad para los mismos entre los que se encuentran a modo de ejemplo piso elevado, cableado de alimentación independiente, corriente estabilizada, servicio de energía ininterrumpido, acceso restringido con los adecuados controles, operatoria de respaldo, acondicionamiento del aire, y otros. Esto se potencia por el hecho de que sus oficinas son alquiladas y la inversión, de efectuarse, sería de muy dudoso recupero. Esto asimismo afecta la independencia del área de procesamiento de las áreas de desarrollo lo que es exigido para garantizar la confidencialidad, integridad, y adecuado

tratamiento de la información. Una opción razonable consiste en usufructuar plenamente el centro de procesamiento de Datos que posee la DGSi dentro del GCBA situando la totalidad del equipamiento central en dicha dependencia.

También es necesario que exista una adecuada independencia del área de seguridad con lo que se completan y perfeccionan los requisitos básicos en materia de organización.

Por otra parte es importante la planificación formal a corto medio y largo plazo aprobada por la superioridad y revisada en períodos prefijados para asegurar la alineación de las acciones de la Dirección con la política institucional. La planificación es un proceso y debe estar formalizado como tal.

Se requieren además mecanismos formales para la administración, seguimiento, cuantificación y control bajo la óptica de la mejora continua de los principales procesos como la evaluación de mejoras tecnológicas, los pedidos de adecuación del software, el seguimiento de las actividades locales, y otros.

Por otra parte en centros de cómputo de mediana envergadura resulta complejo alcanzar niveles adecuados de organización normativa debido a la carencia de personal y a la imposibilidad de atender muchos frentes diferentes con dotaciones reducidas. En este sentido es positivo revisar y ajustar normativa existente utilizada por áreas con mayor desarrollo de la misma en lo que puede colaborar la DGSi. Esto asimismo potencia el uso de la especialización funcional.

Por último es necesario revisar las razones de la importante rotación de recursos humanos para limitar la migración de los mismos, en especial los claves, para el desarrollo de la gestión. En la obtención de resultados la buena voluntad personal resulta inconducente. Para obtener resultados se requiere adecuados niveles de organización y especialización. Capacitación adecuada, compromiso y motivación del personal.