INFORME FINAL

DEFENSORÍA DEL PUEBLO
SISTEMAS DE TELEFONÍA Y COMUNICACIONES INSTITUCIONALES

AUDITORÍA DE SISTEMAS

CIUDAD AUTÓNOMA DE BUENOS AIRES
AGOSTO DE 2004

AUDITORÍA 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

INFORME EJECUTIVO

PROYECTO N° 5-04-28
DEFENSORÍA DEL PUEBLO - SISTEMAS DE TELEFONÍA Y COMUNICACIONES INSTITUCIONALES.

CONCLUSIONES: Se han realizado múltiples observaciones, que requerirán de un proceso que se desarrollará en el tiempo. Sin embargo, el tenerlas en cuenta e ir corrigiendo los sistemas y las tecnologías poco a poco supone un proceso de establecer prácticas de acuerdo a las reglas del arte. La Defensoría del Pueblo debe formalizar las políticas de sistemas incluyendo la organización, el marco tecnológico y la seguridad. Por otra parte es importante evaluar un segundo nivel de integración con otros Sistemas del GCBA no solamente para la obtención de información sino también para incorporarse en calidad de Organismo Usuario. Razones de economía y eficiencia indican que los Sistemas como Control Presupuestario, Sueldos, Internet y otros, utilizados por toda la administración deben tender a ser paulatinamente comunes a todo el GCBA a través de un servicio centralizado a cargo de un único prestador.

OBJETO: Examinar la organización, funcionamiento y resguardo de los recursos informáticos, como así también la alineación de las acciones en pos del logro de los objetivos institucionales de la organización. Verificar el cumplimiento de las buenas prácticas en materia de seguridad, continuidad y eficiencia. Analizar las comunicaciones de voz.

OBSERVACIONES:

Las principales observaciones realizadas están referidas a:

- Telefonía y Comunicaciones: La administración de la telefonía y la red de datos no se encuentra centralizada en un único responsable tecnológico. Se registran llamadas a líneas externas 0610, número que identifica a los proveedores del servicio de acceso a Internet (Internet Service Providers ISP). Estas llamadas deberían estar bloqueadas ya que la Defensoría cuenta con un vínculo directo a Internet, por lo cual ocasionan gastos innecesarios y exponen al conjunto de la red del organismo a riesgos de ataques y/o violaciones de información.
- Seguridad Física: La ubicación de las centrales así como los centros de cómputos no cuentan con adecuados niveles de seguridad de acceso para evitar riesgos y reducir la vulnerabilidad de los sistemas. No existe un plan de contingencia formal para las comunicaciones y la conectividad Internet.
- Seguridad Lógica: El organismo no cuenta con el software que permite configurar la Central telefónica no obstante que el contrato preveía que la empresa proveedora entregase el software para poder configurar la misma. No se ha efectuado una adecuada clasificación de la información; No se definió al propietario de los datos, funcionario que participará en la determinación de los niveles de acceso a la información para cada función y proceso; El procedimiento para la determinación de los perfiles de usuario para cada función no se encuentra formalizado y es incompleto ya que debe especificar las áreas que intervienen y los

responsables de definir la información que se accederá y la modalidad y el alcance bajo la cual será accedida; No hay procedimientos formales que establezcan cuales son los pasos a seguir por los agentes para solicitar el ingreso como usuario a la red y a los sistemas de información perjudicando gravemente ~~a~~ la seguridad y confiabilidad de la información de los sistemas; No se dispone de compromiso de confidencialidad formal para los usuarios por la no-difusión de la información reservada; Se ha verificado la existencia de claves compartidas entre agentes que comparten el usuario y la clave para algunas tareas.

- Tecnologías de la Información y Comunicación de Datos: No existe una política formal de seguridad de la información; No existe una función formal, en la estructura del organismo, para la administración y control de la seguridad de acceso a los datos y la información; El área de Sistemas no dispone de una adecuada metodología para la administración de proyectos, de un procedimiento adecuado para la registración de las necesidades y adecuaciones, de un método para planificar las tareas, de una clara definición del rol del usuario y otras cuestiones relativas a esta problemática.
- Organización y Personal: Ausencia de un plan formal de capacitación de los agentes que tienen a su cargo la administración y mantenimiento de los sistemas y la red; La totalidad de los integrantes del área de sistemas está constituida por personal contratado lo que no garantiza una razonable continuidad en el funcionamiento de la misma.
- Software y Hardware: No se lleva el inventario y el control del software instalado en los equipos de computación. El inventario del hardware es incompleto. No incluye los equipos de las áreas usuarias, de los que tampoco se detalla su ubicación ni números de serie.
- Red de Datos: No se dispone de un equipo de protección (firewall) que filtre los datos que vienen desde Internet; El mapa lógico y el mapa físico de la red de comunicación de datos son incompletos; No se utilizan técnicas de encriptación de la información que circula por la red.
- Sistemas aplicativos: Las operaciones esenciales y de misión crítica de la entidad deben registrarse, administrarse y procesarse en los sistemas aplicativos correspondientes, no debiendo registrarse / administrarse ninguna operación en forma manual, en planillas de calculo o con otro "software" utilitario; No se halló evidencia de que el Sistema URIX cuente con reportes (logs) que registren los cambios efectuados e identifiquen unívocamente al autor de los mismos; No se dispone de manuales con estándares de metodología para la adquisición o el diseño, desarrollo y mantenimiento de los sistemas aplicativos.

CÓDIGO DEL PROYECTO:
5-04-28

NOMBRE DEL PROYECTO:
Defensoría del Pueblo - Sistemas de Telefonía y Comunicaciones Institucionales.

OBJETO:
Examinar la organización, funcionamiento y resguardo de los recursos informáticos, como así también la alineación de las acciones en pos del logro de los objetivos institucionales de la organización. Verificar el cumplimiento de las buenas prácticas en materia de seguridad, continuidad y eficiencia. Analizar las comunicaciones de voz.

ALCANCE:
Se examinará la metodología de trabajo y el cumplimiento de las prácticas usuales en seguridad; se evaluará la existencia de medidas que garanticen la continuidad de los servicios; Se examinará la arquitectura de hardware, los sistemas operativos, el planeamiento, el servicio a las áreas operativas. Se efectuará lo propio con las cuestiones relativas a la red de comunicación de datos y a la seguridad lógica y física. Se examinará el actual sistema de comunicación de voz.

PERÍODO BAJO EXAMEN:
Febrero - Abril de 2004

EQUIPO DESIGNADO:

Auditor Supervisor:	Guillermo A. García
Coordinador:	José Recasens
Auditores:	Zancada Héctor
	Bella Rodolfo
	Francisco Cameán Ariza
	Oscar Ciarlotti
	Carmen Fernández

INFORME FINAL DE AUDITORIA
Proyecto Nº 5.04.28

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

En uso de las facultades conferidas por la Constitución de la Ciudad Autónoma de Buenos Aires de acuerdo al artículo 135, la ley número 325 del 18 de febrero de 2000 dictada por la Legislatura de la Ciudad Autónoma de Buenos Aires en su artículo número 6 y, supletoriamente, la ley 70, esta Auditoria General de la Ciudad procedió a efectuar un examen en el ámbito de las áreas de Sistemas y Comunicaciones de La Defensoría del Pueblo con el siguiente objeto:

1.- OBJETO

Sistemas de telefonía y comunicaciones institucionales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

2.- OBJETIVO

Examinar la organización, funcionamiento y resguardo de los recursos informáticos, como así también la alineación de las acciones en pos del logro de los objetivos institucionales de la organización. Verificar el cumplimiento de las buenas prácticas en materia de seguridad, continuidad y eficiencia. Analizar las comunicaciones de voz y los contratos involucrados.

3.- ALCANCE

El presente examen fue solicitado por la Defensora del Pueblo de la Ciudad de Buenos Aires a partir del inicio de una nueva gestión en dicha organización a fin de examinar la metodología de trabajo y el cumplimiento de las prácticas usuales en seguridad evaluando la existencia de medidas que garanticen la continuidad de los servicios, examinando la arquitectura de hardware, los sistemas operativos, el planeamiento, el servicio a las áreas operativas como así también efectuar lo propio con las cuestiones relativas a la red de comunicación de datos y a la seguridad lógica y física incluyendo el examen del actual sistema de comunicación de voz.

El presente trabajo comprende el uso de las Tecnologías de la Información y las Comunicaciones (TIC´s) por lo tanto se incluye el servicio de comunicaciones (telefonía) y conectividad (Internet).

Las tareas se efectuaron sobre el contexto vigente al momento de su realización, comprendiendo el período de febrero a abril del año 2004.

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

Subsidiariamente se utilizaron:

- Las normas y recomendaciones de seguridad establecidas por la DGEySI.
- Manual de Auditoria Informática de la Sindicatura General de la Nación (SIGEN).
- Manual CISA. Edición 2003.
- Manual COBIT. (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Association. Capítulo Buenos Aires.

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 lo 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 optima utilización de los recursos.
- Confidencialidad: La información critica 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.

3.1- Procedimientos:

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

- Se solicitó por nota documentación relacionada con el objeto de esta auditoria.
- Se efectuaron entrevistas con el personal jerárquico y operativo de las áreas involucradas.
- Se efectuaron verificaciones “in situ” de la Instalación del equipamiento informático, de las comunicaciones y la conectividad.

- Se verificó la documentación de los sistemas.
- Se efectuó el análisis de la documentación provista por el área.

3.2- Limitaciones al Alcance:

Los siguientes factores limitaron la tarea de auditoria:

- Falta de documentación correspondiente al contrato anterior de la central telefónica.

4.- ACLARACIONES PREVIAS

El presente informe se estructura en dos partes, refiriéndose la primera a las comunicaciones telefónicas mientras que la segunda lo hace con respecto a la red informática del organismo y su conectividad tanto interna como externa (vínculo Internet). En ambas se observan aspectos generales, seguridad física, lógica y otros aspectos. En los casos en que la observación abarca ambos temas (telefonía y datos), se ha optado por hacer una única observación y se aclara explícitamente su referencia a ambos capítulos.

Esta división en dos capítulos es meramente metodológica y fue realizada para una mejor comprensión del lector y para no tener que reiterar en cada observación si esta se refiere a uno u otro tema.

Cabe aclarar que desde que se ha instalado la tecnología digital en el mundo de las comunicaciones se viene produciendo un fenómeno que se ha dado en llamar “convergencia digital” y que en términos generales significa que toda la información, cualquiera sea su forma, voz (telefonía), imágenes (video, fotografía, tv, etc), textos, datos, etc. va convergiendo en una sola y única tecnología para su gobierno, difusión y administración.

4.1- Introducción:

La Defensoría del Pueblo es un organismo de reciente creación. El artículo 137 de la Constitución de la Ciudad de Buenos Aires establece que su misión es la defensa, protección y promoción de los derechos humanos y demás derechos e intereses frente a actos, hechos u omisiones de la administración o de prestadores de servicios públicos. Posteriormente, la ley 3 de la Legislatura de la Ciudad Autónoma de Buenos Aires reglamentó su funcionamiento.

Se trata de un organismo a cargo de un Defensor designado por la Legislatura con los votos de las dos terceras partes del total de sus miembros. Es un órgano unipersonal e independiente con autonomía funcional y autarquía financiera. El Defensor del Pueblo es secundado en su labor por cuatro

defensores adjuntos cada uno de los cuales se ocupa de un área temática específica como Políticas Sociales, Servicios Públicos, Seguridad y Derechos Humanos, y Ambiente, Comunicaciones, Hábitat y Urbanismo.

Las funciones, competencias y atribuciones de los diferentes niveles se establecieron por medio de un reglamento interno (Resolución N° 52).

La Defensoría cuenta con dos Direcciones Generales con dependencia directa de la Defensora del Pueblo llamadas de Áreas Temáticas y Técnico Administrativa respectivamente. Tanto las comunicaciones, la conectividad como el área de sistemas dependen de la Dirección Técnico Administrativa.

4.2- Comunicaciones: Telefonía

El servicio de Telefonía depende de Servicios Generales y ésta de la Dirección General Técnico Administrativa. La central telefónica que administra las comunicaciones internas y externas fue instalada en el año 2001. Esta instalación tuvo lugar a partir de una propuesta de Telefónica de Argentina en reemplazo de la central existente a esa fecha.

Se trata de una central LUCENT, Modelo Merlín Magic, con 160 líneas internas que acceden al exterior a través treinta canales de comunicación simultáneos (entrantes y salientes, trama E1). La trama asimismo provee cien números telefónicos consecutivos. El organismo posee también líneas analógicas adicionales. Esta central es modular y ampliable.

La instalación de la central y las líneas internas se abonaron por medio de un contrato de leasing de 36 meses con la empresa The Capita Corporation. Este establece el pago de un canon mensual, con opción de compra. El valor residual, si se ejerce la opción de compra al finalizar el contrato, es igual al precio a valor de plaza de la central. Cabe aclarar que la opción de leasing fue pactada en dólares.

El mantenimiento del equipo así como la programación de la central es efectuado por la firma AVAYA.

Internamente un agente se encarga de tareas de cableado e instalación de nuevos puestos de teléfonos y de la comunicación técnica con el proveedor.

4.3- Área de Sistemas:

El área de Sistemas depende de la Dirección Técnico Administrativa. Esta área no fue incluida en la resolución 52 (mencionada anteriormente en el acápite IV Aclaraciones Previas, Introducción) sino que se generó con posterioridad a esta por lo cual no está debidamente formalizada. La integran tres agentes.

Poseen cuatro servidores:

- Servidor de correo electrónico
- Servidor de archivos
- Servidor Web
- Servidor de aplicaciones

a) Software de Aplicación:

- Utilizan el Sistema Urix para el seguimiento de las actuaciones internas.
- Poseen un software de liquidación de haberes comercial llamado Salary Easy Soft de la firma Buenos Aires Software SRL.
- Asimismo disponen de un software de información geográfico llamado Compumap de la firma Mapas y Sistemas.
- También se utilizan las clásicas herramientas de ofimática para la edición de texto y planilla de cálculo.

b) Hardware:

- Los servidores son equipos IBM (2) y HACER (2) basados en procesadores Pentium II y Pentium III con discos entre 10 y 18 gigabytes.

c) Software de base y servicios:

- Se encuentran orientados a sistemas de arquitectura abierta (Sistema Operativo UNÍX) y el uso de software libre y abierto (Software con código abierto al público y derecho de uso sin pago de licencia o con cánones de bajo costo. En general son desarrollos cooperativos). También combinan el uso de estos sistemas con sistemas propietarios.
- El software utilizado para estos fines es:
  - Send Mail para correo electrónico.
  - Apache para el Servidor Web.
  - Windows 98, 2000, XP y LINUX Mandrake y Linux Red Hat como Sistemas Operativos.
  - Samba File Server Servidor de archivos.
  - MySQL y SQL Server para motor de Base de Datos.
  - Poseen asimismo un antivirus corporativo.

d) Comunicaciones:

La red interna vincula a los cuatro servidores antes mencionados con los puestos de trabajo. Dispone de una capacidad de conectividad para 142 puestos. Poseen una salida a Internet de 512 kb contratada a la empresa MetroRed.

5.- OBSERVACIONES

5.1 Telefonía y Comunicaciones. Aspectos Generales:

5.1.1 *Evaluación sistemática de las comunicaciones:* No se analizan en forma rutinaria y sistemática las comunicaciones, lo que puede provocar que, por ejemplo, se abonen llamadas indebidas y/o innecesarias.

5.1.2 *Administración descentralizada:* La administración de la telefonía y la red de datos no se encuentra centralizada en un único responsable tecnológico. La actual convergencia tecnológica entre comunicaciones y conectividad (la llamada convergencia digital, ver "Aclaraciones Previas") propone la centralización de la responsabilidad de las tecnologías de la información y las comunicaciones (TICs) en una conducción unificada que facilite la integración física y lógica de los distintos sistemas.

5.1.3 *Llamadas de acceso a Internet:* Se registran llamadas a líneas externas 0610, número que identifica a los proveedores del servicio de acceso a Internet (Internet Service Providers ISP). Estas llamadas deberían estar bloqueadas por la central telefónica por dos motivos: a) la Defensoría cuenta con un vínculo directo a Internet, por lo cual ocasionan gastos innecesarios; b) exponen al conjunto de la red del organismo a riesgos de ataques y/o violaciones de información ya que son efectuadas desde una terminal de la red interna de la Defensoría a través de un vínculo no protegido que puede facilitar un acceso indebido (falla de seguridad lógica).

5.2 Seguridad lógica:

5.2.1 *Acceso lógico a través de la conexión vía MODEM:* Si bien es habitual que las centrales telefónicas cuenten con facilidades de acceso remoto a su configuración[1], este tipo de accesos debería estar limitado en el tiempo (sólo cuando el personal de mantenimiento telefónico no se encuentra en el organismo), y protegido por claves de seguridad de acceso limitado a personal responsable del organismo y que en caso de tener que permitir el acceso a terceros, por ejemplo: la empresa que brinda soporte técnico, debiendo estas claves ser cambiadas luego de cada uso. La falta de estos procedimientos hace que el servicio telefónico no tenga niveles de seguridad adecuados a sus funciones.

[1] La Central telefónica tiene (en su interior) permanentemente conectada una línea analógica a un MODEM que permite el acceso remoto a sus funciones y su configuración.

5.2.2 *Software de administración de la central:* El organismo no cuenta con el software que permite configurar la Central telefónica no obstante que el contrato preveía que la empresa proveedora entregase el software para poder configurar la misma. Sin embargo, el mismo no fue entregado generándose así una dependencia innecesaria con la firma proveedora de la Central.

5.2.3 *Cursos de capacitación para la programación de la central:* No se capacitó al personal del organismo para poder programar y/o configurar la Central telefónica. El contrato de leasing con la empresa proveedora contemplaba la capacitación de personal técnico del organismo para poder administrar y programar la Central.

5.3 Seguridad física:

5.3.1 *Acceso físico a la central:* La central telefónica se encuentra en la misma sala donde hay operadores trabajando, lo que hace que esa oficina se encuentre abierta la mayor parte del tiempo. Esta situación no permite adecuados niveles de seguridad para la protección de la Central. La ubicación de las centrales así como los centros de cómputos deben contar con adecuados niveles de seguridad de acceso para evitar riesgos y reducir la vulnerabilidad de los sistemas.

5.3.2 *Acceso físico a la consola de programación:* La programación de la central telefónica puede ser realizada desde teléfonos digitales especiales que funcionan como consola de acceso a la programación de las funciones de la Central. Estas consolas se usan como teléfonos normales por las operadoras de recepción de llamadas. Esta situación no constituye un adecuado nivel de seguridad para proteger la configuración de la Central.

5.3.3 *Verificación del sistema ininterrumpido de energía (UPS):* No hay procedimientos de verificación y pruebas rutinarias de funcionamiento de la unidad de provisión de energía interrumpida (UPS). Las Centrales telefónicas deben contar, entre otras medidas de seguridad física, con sistemas ininterrumpidos de provisión de energía. La falta de procedimientos de monitoreo y prueba de los sistemas de energía disminuyen su eficacia y eficiencia para cuando tienen que entrar en funcionamiento real.

5.3.4 *Plan de contingencia (comunicaciones y conectividad):* No existe un plan de contingencia formal para las comunicaciones y la conectividad Internet. La falta de un plan de contingencia aumenta los riesgos y daños que pueden producirse en casos de emergencia, incrementan la vulnerabilidad de los servicios y afectan así la vuelta a la normalidad del funcionamiento del organismo.

5.3.5 *Plan de recuperación de desastre:* No hay un plan de recuperación de desastre para las comunicaciones y conectividad. La falta de estos planes aumenta la vulnerabilidad y retrasa la vuelta a la normalidad en forma rápida y ordenada en caso de desastre.

5.4 Tecnologías de la Información y Comunicación de Datos. Aspectos Generales:

5.4.1 *Plan de Tecnologías de la Información y las Comunicaciones (TICs):* No existe un Plan de TIC formal que permita una supervisión continua y directa de las tareas que se realizan y que contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrado y la totalidad de las tareas a llevarse a cabo a corto plazo (por ejemplo: un año). Tampoco existe un plan estratégico de sistemas, que contenga los proyectos principales y los cronogramas de su implementación para un período de mediano / largo plazo (por ejemplo: tres años).

5.4.2 *Política formal de seguridad:* No existe una política formal de seguridad de la información en la que se precise, entre otros, el compromiso de la dirección, la estructura, los recursos y el marco tecnológico y organizativo en que se desenvolverá la función. Dicha carencia implica el riesgo de que no se expliciten las pautas y el nivel de riesgo que el organismo está dispuesto a asumir.

5.4.3 *Función de Seguridad Informática:* No existe una función formal, en la estructura del organismo, para la administración y control de la seguridad de acceso a los datos y la información.

5.4.4 *Procedimientos para nuevos requerimientos:* No se ha obtenido evidencia formal de la existencia de procedimientos que establezcan los pasos a seguir para dar adecuado tratamiento a los requerimientos de los usuarios para la solicitud de nuevos servicios o necesidades de los sistemas de información. La ausencia de un procedimiento que permita formalizar, evaluar y tomar acción frente a las nuevas necesidades o problemas de los usuarios implica una limitación a la evolución del nivel de servicio debido a la falta de un mecanismo sistemático del tratamiento de la mejora continua.

5.4.5 *Metodologías de administración y seguimientos de proyectos:* El área de Sistemas no dispone de una adecuada metodología para la administración de proyectos, de un procedimiento adecuado para la registración de las necesidades y adecuaciones, de un método para planificar las tareas, de una clara definición del rol del usuario y otras cuestiones relativas a esta problemática. Asimismo, no se encuentra en condiciones de dar cumplimiento a la tarea de adecuación de los

sistemas existentes y la implantación de nuevos sistemas con su conformación actual, ya que no cuenta con la dotación suficiente de personal así como tampoco con especialistas orientados a esta función. Por consiguiente la adecuación de los sistemas a las necesidades de los usuarios se ven restringida limitándose el nivel de servicio en este aspecto.

5.4.6 *Función de Organización:* El organismo no posee la función de organización que sea responsable de la confección de la normativa interna y que establezca los procedimientos requeridos para cada proceso con apoyo informático. Esto impide delimitar la responsabilidad y las tareas de cada una de las áreas en los diferentes procesos que se ejecutan. Esta situación repercute en el área de sistemas bajo la forma de un limitado nivel de organización que se observa en la falta de formalización de los cargos, carencia de correspondencia entre los cargos y las funciones, ausencia de normas y procedimientos formales de seguridad, continuidad, operación, mantenimiento, contingencia y soporte entre otros.

5.4.7 *Proceso de evaluación de incorporación de tecnología:* No se dispone de un procedimiento sistemático y formal de evaluación de factibilidad de nuevos proyectos tecnológicos[2]. Ello implica el riesgo de postergar la incorporación de herramientas y soluciones que puedan contribuir a la mejora de la eficiencia y a la baja de los costos en la organización.

5.5 Organización y personal:

5.5.1 *Plan de capacitación de los agentes:* Ausencia de un plan formal de capacitación de los agentes que tienen a su cargo la administración y mantenimiento de los sistemas y la red[3]. La falta de capacitación puede afectar la implementación de mejoras y actualizaciones de la red y los sistemas, y reducir la posibilidad de aprovechamiento de las tecnologías asociadas a la información y las comunicaciones

5.5.2 *Dependencia funcional formal:* No está formalizada la dependencia funcional del área de Sistemas de información y comunicaciones.

5.5.3 *Personal contratado:* La totalidad de los integrantes del área de sistemas está constituida por personal contratado lo que no garantiza una razonable continuidad en el funcionamiento de la misma. El personal contratado mantiene un vínculo contractual débil que pone en riesgo el mantenimiento del soporte, del procesamiento y de todas las tareas

[2] A modo de ejemplo, no se evaluó la factibilidad de incorporar servicios importantes para una institución de este tipo como por ejemplo la posibilidad de digitalizar documentación, la utilización de facilidades de gobierno electrónico, herramientas de control de proyectos y otros. Esta falencia también se observa en las comunicaciones y la conectividad del organismo.

[3] Los sistemas y las redes van creciendo en complejidad, al mismo tiempo, continuamente se producen cambios tecnológicos, lo que obliga a una actualización permanente y un adecuado nivel de entrenamiento de sus responsables.

esenciales para el sostén del servicio en caso de desvinculación de los mismos.

5.5.4 *Segregación de funciones:* El área no presenta una clara delimitación de las tareas entre mantenimiento de sistemas, operaciones, soporte técnico y supervisión, que permita garantizar una adecuada segregación de funciones y un control por oposición de intereses. La concentración de funciones implica un riesgo para la integridad de la información y disminuye la confiabilidad de su procesamiento.

5.5.5 *Control del área:* La ausencia parcial o total de documentación del área de Sistemas implica una limitación para evaluar las acciones del área y su alineación con las políticas del organismo.

5.5.6 *Control de operaciones computarizadas y/o procesos:* No existe una adecuada documentación escrita y actualizada de los controles de las actividades y procesos que se desarrollan normalmente en el centro de procesamiento de información.

5.6 Equipamiento (Hardware):

5.6.1 *Inventario de equipamiento:* El inventario del hardware es incompleto. No incluye los equipos de las áreas usuarias, de los que tampoco se detalla su ubicación ni números de serie. El Inventario de "hardware" no especifica las áreas que están a cargo del equipamiento ni la configuración interna del mismo.

5.7 Programas (Software):

5.7.1 *Control de Software Instalado:* No se lleva el inventario y el control del software instalado en los equipos de computación. La falta de registro y control del software instalado implica la imposibilidad de un adecuado resguardo y protección. Asimismo implica el riesgo de que se ingresen virus por instalación de programas infectados o que se afecte la estabilidad de la red por la utilización de software inapropiado.

5.8 Red de datos:

5.8.1 *Documentación de la red de datos:* El mapa lógico y el mapa físico de la red de comunicación de datos son incompletos. No se especifica el tipo de cableado, cantidad de líneas, cantidad y tipo de bocas identificación precisa de cada dispositivo entre otros, lo que genera la imposibilidad de conocer el detalle de la misma y el flujo de la información entre sus nodos. Esto dificulta el mantenimiento, la detección y solución de

problemas. También, dificulta el análisis y la evaluación de posibles ampliaciones futuras.

5.8.2 *Dispositivo de protección de la red (pared cortafuego, firewall):* No se dispone de un equipo de protección (firewall) que filtre los datos que vienen desde Internet. Las redes conectadas a Internet deben extremar sus medidas de seguridad ya que los niveles de riesgos se incrementan al usar la red de redes.

5.8.3 *Encriptación de información:* No se utilizan técnicas de encriptación de la información que circula por la red. Habiendo información crítica y/o altamente confidencial debería instrumentarse un mecanismo de protección de los datos que impida el acceso indebido a la información que circula por la red. El uso de técnicas adecuadas de encriptación, ya sea por "hardware" y/o "software",provee de este tipo de protección. En caso de no utilizarse se deberá documentar la decisión que debe ser tomada por el nivel correspondiente.

5.8.4 *Monitoreo de red:* No se halló evidencia de que se efectúe un seguimiento, sistemático y rutinario, de la actividad de la red. No se dispone de un software de monitoreo de la red que permita determinar excesos de tráfico, intentos de acceso indebidos, modificaciones al hardware interconectado y otros. Esto impide alertar y diagnosticar automáticamente problemas en la red de comunicaciones afectando la seguridad de la misma y la continuidad y eficiencia de los servicios.

5.8.5 *Documentación de intentos de acceso indebido:* No se documentan ni analizan los intentos de acceso indebidos Esta circunstancia incrementa la posibilidad de que no se detecten intentos de accesos indebidos y no se tomen las medidas preventivas adecuadas para evitarlos.

5.9 Continuidad de la operación:

5.9.1 *Procedimientos de resguardo de la información:* No existe una política formal de resguardo de la información. Los procedimientos de resguardo y respaldo de datos en uso (backup) son incompletos. La ausencia y/o falencias en los procedimientos de back-up aumentan el riesgo de pérdida de la información en caso de emergencias, desperfectos o de desastres además de demorar el retorno del servicio requiriendo mayor cantidad de horas hombre para su recuperación.

5.9.2 *Copia de respaldo en sede externa:* Los procedimientos de copia y resguardo de datos actualmente en uso, no incluyen copia en sede externa. Cabe aclarar que se dispone de una copia adicional pero la misma se encuentra dentro del edificio. Esto implica el riesgo de pérdida de información en caso de siniestro grave como por ejemplo un incendio importante. Las reglas del arte establecen que una copia de la

información debe ser resguardada en sede externa, lo que significa en un sitio distante fuera del edificio.

5.9.3 *Procedimientos de recuperación de la información:* La documentación referida a los procesos de recuperación de datos y archivos es incompleta[4]. Estas faltas implican el riesgo de no poder efectuar el recupero por fallas no detectadas en las copias de respaldo o en el procedimiento de recuperación.

5.9.4 *Plan de Contingencias, Plan de Evacuación y Plan de Recuperación de Desastres:* No se cuenta con un plan formal y completo de contingencias, un plan de evacuación y un plan de recuperación de desastres y sus correspondientes pruebas. Tampoco se dispone de equipamiento alternativo (servidores de respaldo, propios o por convenios formales con terceros) para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales.

5.10 Seguridad Lógica:

5.10.1 *Clasificación de la información:* No se ha efectuado una adecuada clasificación de la información de forma tal que se pueda precisar el nivel de confidencialidad necesario de los datos y de la información en los diferentes procesos, computarizados o manuales.

5.10.2 *Definición del dueño de los datos:* No se definió al propietario de los datos, funcionario que participará en la determinación de los niveles de acceso a la información para cada función y proceso. El propietario de los datos es el responsable por el uso indebido de los mismos, de allí que en cada caso se deba definir el funcionario que asume esa responsabilidad.

5.10.3 *Procedimiento de definición de Perfiles de Usuarios:* El procedimiento para la determinación de los perfiles de usuario para cada función no se encuentra formalizado y es incompleto ya que debe especificar las áreas que intervienen y los responsables de definir la información que se accederá y la modalidad y el alcance bajo la cual será accedida. La falta de un proceso formal y completo impide que se pueda definir con precisión el alcance del accionar del nuevo usuario en el momento de solicitar el alta, lo que afecta el control sobre los accesos y la seguridad de la información.

5.10.4 *Procedimiento de Altas de Usuarios:* No hay procedimientos formales que establezcan cuales son los pasos a seguir por los agentes para

[4] Por ejemplo: los dispositivos físicos deben estar rotulados y dichos rótulos constar en el procedimiento. Asimismo debe precisarse la circunstancia de aplicación, el nivel que toma la decisión y el responsable de la ejecución de la misma.

solicitar el ingreso como usuario a la red y a los sistemas de información perjudicando gravemente ~~a~~ la seguridad y confiabilidad de la información de los sistemas.

5.10.5 *Procedimiento de Bajas de Usuarios:* No existe un procedimiento formal para la baja de usuarios[5].

5.10.6 *Compromiso de confidencialidad y uso responsable:* No se dispone de compromiso de confidencialidad formal para los usuarios por la no-difusión de la información reservada; tampoco se dispone de un compromiso formal por el uso responsable de los recursos, la clave de seguridad y el acceso a Internet.

5.10.7 *Claves compartidas:* Se ha verificado la existencia de claves compartidas entre agentes que comparten el usuario y la clave para algunas tareas. El incumplimiento de esta regla implica el riesgo de que la responsabilidad resulte indeterminada al no poder identificar al autor del acto.

5.10.8 *Identificación de usuarios unívoca:* Hay agentes con más de una identificación de usuario en la red. El incumplimiento de esta norma posibilita el repudio de acciones efectuadas bajo una identificación de usuario que no se encuentra debidamente relacionada con una persona física. Asimismo se constata la existencia de usuarios genéricos haciendo impersonal cualquier acción efectuada bajo esa registración.

5.10.9 *Discos y Directorios:* Un alto porcentaje de los equipos comparten discos y directorios, sin ningún tipo de restricción. Esta situación puede facilitar accesos indebidos o modificación o daño de la información (no se citan ejemplos en resguardo de la seguridad).

5.10.10 *Puertos lógicos:* Se observan equipos con puertos lógicos abiertos innecesariamente lo que implica un riesgo ya que se facilita el acceso indebido (no se citan ejemplos en resguardo de la seguridad).

5.10.11 *Usuario Administrador:* La falta de este cambio de usuario facilita que quien desee ingresar indebidamente tenga la facilidad de conocer la denominación de la identificación del usuario de mayor categoría y responsabilidad del servidor principal, situación que facilita su tarea ya que de las dos condiciones posibles de acceso (usuario y clave) una está resuelta. (No se citan ejemplos en resguardo de la seguridad).

[5] Esto podría implicar que los usuarios que dejan de pertenecer a la institución ingresen a los sistemas de información y provoquen daños o tengan acceso a información privada. Asimismo implica el riesgo de que otro usuario utilice la clave del agente dado de baja con lo que se habilita el repudio de todo lo actuado.

5.10.12 *Usuarios locales:* Hay usuarios locales repetidos en el dominio de equipos secundarios por fuera del servidor principal.

5.10.13 *Características mínimas en la clave:* No se encuentran normadas las características mínimas que deben respetar las claves de acceso y autenticación de los usuarios.

5.10.14 *Intentos de Acceso Fallidos:* No se encuentra normado el bloqueo de usuarios por intentos de acceso fallidos a la red y a los sistemas. Tampoco existe un procedimiento formal para la rehabilitación de claves. La inexistencia de un procedimiento de bloqueo de usuarios por intentos fallidos incrementa la vulnerabilidad de los sistemas, posibilitando el ingreso de usuarios no autorizados, además, posibilita el romper la clave con el uso de técnicas de "fuerza bruta" (no se citan ejemplos en resguardo de la seguridad). El ingreso de usuarios no autorizados puede permitir daños, pérdida, destrucción y/o divulgación de información crítica.

5.10.15 *Procedimientos ante alarmas por virus:* Se carece de un procedimiento formal y sistemático que establezca los pasos y las acciones en caso de alarma por virus. La falta de este procedimiento implica el riesgo de no actuar a tiempo y en forma debida evitando daños mayores por difusión del problema.

5.10.16 *Medidas antivirus:* Se carece de medidas habituales que reduzcan el riesgo de infección y/o difusión de los virus, troyanos, gusanos y otros. Tales medidas incluyen una adecuada capacitación de los usuarios, restricciones a la instalación de software, restricción del tipo de archivo que se baja desde Internet, restricción del uso de la disquetera de 3½ y otros.

5.10.17 *Procedimiento de puesta en producción:* No existen procedimientos de control para garantizar el efectivo y correcto control de cambios cuando corresponda[6].

5.10.18 *Acceso y modificación de los datos por fuera del aplicativo:* No se encuentra debidamente restringido el acceso a utilitarios sensitivos que permiten modificar datos en el ambiente de producción. Este tipo de operación está desaconsejada y debe efectuarse en caso de no contar con ninguna otra alternativa siendo necesario documentar toda acción relativa a este tipo de actividad cuando ello ocurra.

5.10.19 *Seguridad en los servidores abiertos a Internet:* Se detectaron fallas en los niveles de seguridad del servidor del sitio Internet (web server) (no se citan ejemplos en resguardo de la seguridad).

[6] Estos procedimientos incluyen situaciones tales como: cambios de programas en bibliotecas de producción, archivos, definiciones de diccionarios de datos, ordenes de corrida de programas, etc.

5.11 Seguridad Física:

5.11.1 *Protección de dispositivos de red:* Las instalaciones no poseen una apropiada seguridad física y ambiental. Los dispositivos de comunicaciones digitales (hubs y switches) no se encuentran protegidos dentro de un mueble cerrado con llave (rack de comunicaciones) por lo que están al alcance de cualquier agente que pase por el lugar en el que se hallan. Esto potencia el riesgo de daño a la red.

5.11.2 *Seguridad en los accesos físicos:* No se dispone de adecuados controles de acceso[7].

5.11.3 *Sala de servidores:* El área de servidores sirve al mismo tiempo como depósito de materiales. El tipo de tarea que se realiza en la misma es incompatible con el uso de deposito, además algunos de estos materiales son combustibles (papel). También hay instalaciones resueltas en forma precaria, por ejemplo el equipo de aire acondicionado tiene instalado un tacho de recolección de agua dentro de la misma sala de servidores.

5.11.4 *Resguardo de documentación:* Los listados y documentación de datos, programas y sistemas deben estar guardados con adecuadas medidas de seguridad.

5.11.5 *Procedimiento de depuración de la información:* Falta un procedimiento formal y rutinario para depurar y si corresponde proceder a la destrucción de la información impresa o grabada, una vez cumplido su periodo de retención y/o su ciclo de vida.

5.11.6 *Salidas, luces y señalización de Emergencia:* Se comprobó la falta de una salida de escape de emergencia del edificio. Esto implica el riesgo de vida para las personas que trabajan en el edificio. Actualmente, no existe señalización ni luces de emergencia que conduzcan a la salida del edificio.

5.11.7 *Elementos de seguridad:* Se comprobó la falta parcial de elementos de seguridad. El edificio cuenta con matafuegos pero no con mangueras y otros elementos. Asimismo se carece de dispositivos de detección automática de humo / calor en la sala de servidores.

5.11.8 *Red eléctrica:* No existe una red eléctrica que alimente en forma exclusiva y diferenciada la totalidad de la red de datos ni siquiera en el área de servidores. La misma red eléctrica es utilizada para los datos y para artefactos de uso cotidiano (cafeteras, calentadores, estufas de cuarzo, etc.). Esto incrementa el riesgo de incendios y de

[7] En tal sentido, el área de servidores es utilizada también como sala de reuniones.

caídas en la red e interrupción en las tareas de procesamiento, con pérdida de información y de tiempo por parte de los usuarios de la red por suspensión del servicio.

5.11.9 *Fuente alternativa de energía de la red de datos:* No se cuenta con una fuente alternativa de energía para la red de datos. Ante una eventual caída del suministro eléctrico la falta de una fuente de energía alternativa ocasionaría la caída de la red y de las computadoras, con riesgo de perdida de información y posibles fallas en los dispositivos electrónicos. Asimismo cesaría por completo la operación de los sistemas.

5.12 Proveedores:

5.12.1 *Falta de recaudos contractuales:* El contrato con el proveedor del sistema URIX en el año 2002 no dispone de los recaudos formales que aseguren a la entidad la continuidad del procesamiento ante cualquier situación que pudiera sufrir el proveedor por la cual dejara de prestar sus servicios en el mercado.

5.12.2 *Adecuación del software a las necesidades del organismo:* La modalidad de contratación del mantenimiento del aplicativo URIX no contempló un mecanismo para adecuar el aplicativo a los requerimientos de los usuarios por lo que el mismo se tornó rígido y perdió funcionalidad.

5.13 Sistemas aplicativos:

5.13.1 *Operaciones de los aplicativos centrales:* Las operaciones esenciales y de misión crítica de la entidad deben registrarse, administrarse y procesarse en los sistemas aplicativos correspondientes, no debiendo registrarse / administrarse ninguna operación en forma manual, en planillas de calculo o con otro "software" utilitario[8]. La falta de este recaudo disminuye la confiabilidad de la información.

5.13.2 *Documentación:* En algunos casos, la documentación de los aplicativos es incompleta[9]. Esto resulta ineficiente ya que limita la capacidad de adecuación del aplicativo y demora la obtención de las soluciones posibles.

5.13.3 *Registro de cambios:* No se halló evidencia de que el Sistema URIX cuente con reportes (logs) que registren los cambios efectuados e identifiquen unívocamente al autor de los mismos, de modo que se

[8] Un ejemplo de estos usos por fuera de la aplicación central es la elaboración de estadísticas.
[9] El aplicativo URIX no cuenta con la documentación adecuada lo que implica la necesidad de investigar su arquitectura cada vez que es necesario efectuar alguna tarea con el mismo.

pueda determinar la responsabilidad por acciones en caso de necesidad.

5.13.4 *Sistema integrador:* No se cuenta con un sistema de información de gestión para ser utilizado por las máximas autoridades en la toma de decisiones, que obtenga e integre en forma totalmente automatizada los datos que residen en los distintos archivos o bases de datos de sus aplicaciones.

5.13.5 *Integración con los Sistemas del GCBA:* No se ha evaluado la alternativa de adherir al uso de sistemas centrales del GCBA tales como el Sistema de Administración Geográfico, el sistema de Control Presupuestario, el sistema de Administración de Inversiones y otros del GCBA[10].

5.13.6 *Falta de estándares de metodología:* No se dispone de manuales con estándares de metodología para la adquisición o el diseño, desarrollo y mantenimiento de los sistemas aplicativos. Esto implica el riesgo de no dar los pasos tendientes la obtención de las soluciones más adecuadas o hacerlo de un modo poco eficiente.

5.14 Internet:

5.14.1 *Subdominio org.ar:* El subdominio registrado y en uso por la Defensoría es incorrecto **(VER ANEXO I)**.

5.14.2 *Dominios defensoria.gov.ar y defensoria.org.ar:* La elección del dominio "defensoria", tanto en el caso de las direcciones defensoria.org.ar (en uso actualmente) como para el caso de defensoria.gov.ar, resulta inadecuado y no facilita que los usuarios puedan encontrar el sitio en un entorno de información global como el que ofrece Internet **(VER ANEXO II)**.

5.14.3 *Servidor del sitio Internet:* El servidor del sitio Internet de la Defensoría se encuentra en una red privada cuando podría ser conveniente que su ubicación en el entorno de la red del Gobierno de la Ciudad de Buenos Aires. El utilizar un prestador privado para el servicio de conexión Internet (ISP) no significa que los servidores de los sitios públicos del organismo tengan que necesariamente estar en la red de este. El ubicar al servidor en la red del GCBA trae aparejado una economía de esfuerzos y de costos, sin perder la autonomía del manejo y la administración de la información del sitio.

[10] Estos sistemas poseen una importante funcionalidad al mismo tiempo que implican el aprovechamiento en mayor escala de los recursos con la consiguiente economía. Este comentario es válido para todos los sistemas de gestión del GCBA mencionados en la ley 70 (Título III, Capítulo 1, art. 27).

5.14.4 *Persona responsable del dominio:* No es correcta la designación de la Persona Responsable en el registro del dominio defensoria.org.ar. NIC Argentina establece que: "La Persona Responsable es la persona que designa la entidad registradora como persona de contacto para resolver cuestiones administrativas que tengan que ver con el dominio"[11]. Es decir sus funciones están relacionadas con la administración del dominio elegido y registrado, desde este punto de vista y dado que esa administración se relaciona con cuestiones técnicas y de responsabilidad tales como dar de baja el dominio ("Delegar un dominio no delegado. Modificar o dar de baja la delegación del Dominio del que es responsable. Dar de baja el Dominio. Cambiar la Persona Responsable por otra. Cambiar la entidad administradora del dominio. Cambiar el Contacto Técnico del dominio. Cambiar los DNS que resuelven el dominio")[12] la Persona Responsable inscripta en NIC debería ser el propio Defensor del Pueblo o en su defecto este delegar formalmente esa responsabilidad, delimitando claramente el alcance, en alguien del área de Sistemas.

6.- RECOMENDACIONES

6.1 Telefonía y Comunicaciones. Aspectos Generales:

6.1.1 *Evaluación sistemática de las comunicaciones:* Las comunicaciones de voz deben analizarse en forma rutinaria y sistemática a fin de detectar cuellos de botella, documentar caídas de la central, números frecuentes, llamadas innecesarias, errores de facturación por parte del proveedor, etc. A tal fin, muchas centrales permiten conectar una Pc con un software "facturador" para hacer el seguimiento de las llamadas y realizar el análisis de las mismas.

6.1.2 *Administración descentralizada:* La actual convergencia tecnológica entre comunicaciones y conectividad (la llamada convergencia digital, ver "Aclaraciones Generales") propone la centralización de la responsabilidad de las tecnologías de la información y las comunicaciones (TIC) en una conducción unificada que facilite la integración física y lógica de los distintos sistemas. Las comunicaciones y los datos están en un franco proceso de convergencia razón por la cual todo lo atinente a estos rubros es conveniente centralizarlo. Asimismo, debe haber un único responsable tecnológico, esta responsabilidad debe ser formal y real, con incumbencia en todos los sistemas, tecnologías y vínculos, tanto de voz como de datos. La

[11] Ver: http://www.nic.ar, documento: Preguntas Frecuentes.
[12] Ver: http://www.nic.ar, documento: Preguntas Frecuentes

conducción unificada permite una mayor integración en todo lo referente a los usos de las tecnologías.

6.1.3 *Llamadas de acceso a Internet:* Si bien el organismo ha comenzado un proceso de solución de este problema, sugerimos utilizar el bloqueo de las llamadas al 0610 así como a los números que identifican a distintos Proveedores de Servicios de Internet (ISP) inhibiendo su acceso. También se debe instruir a los usuarios acerca de los riesgos a los que se expone la red con este tipo de conexiones. Por otra parte se recomienda en las compras futuras de hardware, no incluir el modem en la configuración de puestos de trabajo (Pc), así se logra una economía en los costos de los mismos y además se evitan riesgos en la red.

6.2 Seguridad lógica:

6.2.1 *Acceso lógico a través de la conexión vía MODEM:* Limitar la posibilidad de acceso a la central por la conexión vía modem al mínimo imprescindible. Establecer pautas y compromisos formales con la empresa que brinda el soporte técnico fijando los casos, días y horarios en que ellos puedan acceder a la configuración de la central. Cerrar la posibilidad de acceso con claves de seguridad o la desconexión física del dispositivo. Cambiar las claves, luego de cada acceso, sobre todo en caso de que sea utilizada por terceros.

6.2.2 *Software de administración de la central:* generar los reclamos formales necesarios para que la empresa proveedora haga entrega del software de administración y configuración de la central telefónica. En caso que la empresa no cumpla con sus responsabilidades contractuales, buscar software alternativo que supla esta carencia. El auditado informa que este ítem se encuentra en vías de solución.

6.2.3 *Cursos de capacitación para la programación de la central:* generar los reclamos formales necesarios para que la empresa proveedora capacite en la administración y configuración de la central telefónica. Esta capacitación debe ser tomada por dos agentes del área responsable como mínimo. En caso que la empresa no cumpla con sus responsabilidades contractuales, buscar capacitación alternativa que supla esta carencia.

6.3 Seguridad física:

6.3.1 *Acceso físico a la central:* Dado que la Defensoría cuenta con un proyecto en desarrollo de remodelación de las salas de la central telefónica y los servidores, sugerimos que en el proyecto se contemple ubicarlas en áreas de acceso restringido y dotarlas con adecuadas medidas de seguridad física y de acceso.

6.3.2 *Acceso físico a la consola de programación:* Minimizar la utilización de las consolas de programación de la central por parte de personas ajenas a la administración de la misma. Evitar el uso de esas consolas como teléfonos comunes y, en caso que esas consolas deban ser usadas por las operadoras, bloquear las funciones de acceso a la programación.

6.3.3 *Verificación del sistema ininterrumpido de energía (UPS):* Debe generarse un procedimiento de verificación y prueba en forma sistemática y rutinaria de los sistemas UPS para corroborar su adecuado funcionamiento en caso de un corte de energía. Estos sistemas funcionan con baterías que pueden no tener la carga completa o haber excedido su vida útil. Las pruebas deben ser documentadas. Además, estos dispositivos cuentan con un software de administración que permiten configurar sus funciones para que, en caso de corte de energía se pueda hacer un cierre ordenado de los sistemas que mantiene. Las pruebas y verificaciones periódicas deben incluir tanto al dispositivo como al software y su configuración.

6.3.4 *Plan de contingencia (comunicaciones y conectividad):* 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. 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. Los vínculos y las comunicaciones deben contar con un plan de contingencia formalmente aprobado y este debe ser verificado periódicamente a fin de asegurar su adecuado funcionamiento. Los centros de comunicaciones deben contar con un plan de contingencia que permita al personal conocer y realizar los debidos procedimientos en caso de emergencia para atenuar los efectos y daños que esta puede producir. Estos planes deben estar formalmente aprobados y ser periódicamente probados para ir adecuándolos a las distintas circunstancias.

6.3.5 *Plan de recuperación de desastre:* El plan de recuperación de desastres debe ser formalmente aprobado y verificado periódicamente para asegurar su adecuación a las necesidades del organismo. Estos planes prevén los pasos a seguir para la vuelta a la normalidad del organismo en caso de desastres y luego de haber puesto en práctica el plan de contingencia.

6.4 Tecnologías de la Información y Comunicación de Datos. Aspectos Generales:

6.4.1 *Plan de Tecnologías de la Información y las Comunicaciones (TICs):* Falta de un Plan de Sistemas. Implementar un plan de corto plazo con plazos para las distintas tareas y etapas y 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.

6.4.2 *Política formal de seguridad:* 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.

6.4.3 *Función de Seguridad Informática:* Falta de la función seguridad informática. Incorporar 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.

6.4.4 *Procedimientos para nuevos requerimientos:* Falta de tratamiento formal a los nuevos requerimientos. Implementar procedimientos de tratamiento formal de los nuevos requerimientos de los usuarios. Los requerimientos de los usuarios de una organización evolucionan y cambian constantemente, por ello es necesario crear canales formales para dar curso a esas necesidades.

6.4.5 *Metodologías de administración y seguimientos de proyectos:* Falta de Metodologías de administración y seguimientos de proyectos. Si bien el organismo ha comenzado a incorporar personal idóneo al área de sistemas para mejorar la calidad de las prestaciones, se recomienda generar una metodología de administración y seguimiento de proyectos, con cronogramas, responsables, recursos y metas a cumplir.

6.4.6 *Función de Organización:* Falta de un área de Organización. Generar la formación de un área y/o función de organización que contribuya a formalizar los procesos con apoyo informático. La misma deberá confeccionar las normas y procedimientos de la institución, los circuitos administrativos y los niveles de decisión de cada trámite. Estos circuitos deberán funcionar en consonancia con la apoyatura informática.

6.4.7 *Proceso de evaluación de incorporación de tecnología:* 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.

6.5 Organización y personal:

6.5.1 *Plan de capacitación de los agentes:* Falta de un plan de capacitación de los agentes de las áreas de sistemas 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 y las capacidades y la vocación del personal.

6.5.2 *Dependencia funcional formal:* Falta de dependencia funcional formal del área de sistemas. Definir la dependencia del área de sistemas de información y del área de seguridad de sistemas que debe ser independiente del área de sistemas y depender del máximo nivel posible. El organismo nos informa que este item se encuentra en vìas de solución.

6.5.3 *Personal contratado:* Personal contratado. La falta de personal estable en las áreas críticas de sistemas supone riesgos y posible perdida 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.

6.5.4 *Segregación de funciones:* 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. Nos informan que este ítem se encuentra en vías de solución.

6.5.5 *Control del área:* Control del área parcialmente formal. El área de sistemas debe llevar un adecuado registro formal, rutinario y sistemático de las tareas, los cambios y las novedades. Esto posibilita un control de gestión y fortalece la seguridad en el área.

6.5.6 *Control de operaciones computarizadas y/o procesos:* Control formal parcial de operaciones computarizadas o procesos. Se recomienda formalizar los controles de proceso y las operaciones del centro de cómputos de manera de garantizar su ejecución y supervisión.

6.6 Equipamiento (Hardware):

6.6.1 *Inventario de equipamiento:* Incompleto inventario físico del equipamiento. El organismo nos informa en el descargo que ha comenzado a reformular el inventario. Se recomienda confeccionar y

mantener permanentemente actualizado un inventario físico del equipamiento con un adecuado nivel de detalle, para ello se cuenta con múltiples herramientas informáticas que facilitan la tarea. Las altas y bajas de ese inventario deben ser notificadas al área encargada de llevar el registro patrimonial del organismo.

6.7 Programas (Software):

6.7.1 *Control de Software Instalado:* Inadecuado Control del Software Instalado. Se recomienda restringir la instalación de software y controlar con medios informáticos el software instalado en cada equipo. Los equipos de computación no pertenecen al usuario sino al organismo y a la función que el mismo desempeña. En consecuencia debe estar pautado el software que tendrá instalado cada puesto de trabajo para un acabado cumplimiento de la misma. Llevar a cabo este control facilita la seguridad de la red. El organismo nos informa que el ítem se encuentra en vías de solución.

6.8 Red de datos:

6.8.1 *Encriptación de información:* En los casos en que se maneje 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.

6.8.2 *Monitoreo de red:* Se debe incorporar el monitoreo rutinario, sistemático y completo de la red por medio de software especifico para este fin. Este, debidamente configurado genera alertas para distintas situaciones. Además de monitorear la red, se debe tener un registro de todas las novedades que se producen para luego analizarlas y tomar medidas acordes con ellas.

6.8.3 *Documentación 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).

6.9 Continuidad de la operación:

6.9.1 *Procedimientos de resguardo de la información:* Procedimientos de resguardo incompletos. 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.

6.9.2 *Copia de respaldo en sede externa:* 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.

6.9.3 *Procedimientos de recuperación de la información:* Procedimiento de recuperación incompleto. Incorporar procedimientos formales de recuperación de datos, que deben ser testeados anualmente 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.

6.9.4 *Plan de Contingencias, Plan de Evacuación y Plan de Recuperación de Desastres:* 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.

6.10 Seguridad Lógica:

6.10.01 *Clasificación 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.

6.10.02 *Definición del dueño de los datos:* 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.

6.10.03 *Procedimiento de definición de Perfiles de Usuarios:* Confeccionar un procedimiento para definir los perfiles de usuario en el que cada dueño de dato especifique las facultades que dispondrá cada función con relación al tratamiento de la información. Se deberán precisar cómo se definen los perfiles y quién determina cual es la información a la que pueden acceder y con qué grado de libertad.

6.10.04 *Procedimiento de Altas de Usuarios:* Confeccionar e implementar un procedimiento formal de altas de usuario.

6.10.05 *Procedimiento de Bajas de Usuarios:* Confeccionar e implementar un procedimiento formal de bajas de usuario.

6.10.06 *Compromiso de confidencialidad y uso responsable:* Incorporar la práctica de la firma del compromiso de confidencialidad que incluya la no-difusión de la clave de seguridad. Asimismo se deberá resaltar la responsabilidad que le cabe a cada agente en caso de uso indebido de su habilitación como usuario de los sistemas a los que accede. Solicitar la intervención del área legal para su redacción.

6.10.07 *Claves compartidas:* Eliminar las claves compartidas efectuando la renovación de las mismas.

6.10.08 *Identificación de usuarios unívoca:* 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.

6.10.09 *Discos y Directorios:* Deben eliminarse las facilidades de acceso genéricas, especialmente aquellas instaladas en equipos personales. La información se debe compartir bajo el control de la administración de la seguridad.

6.10.10 *Puertos lógicos:* Cerrar los puertos lógicos que se hallen innecesariamente abiertos, especialmente en los servidores.

6.10.11 *Usuario Administrador:* Modificar la identificación de la función administrador y guardar reserva de la misma.

6.10.12 *Usuarios locales:* Eliminar los usuarios repetidos y en caso de requerir usuarios especiales justificar debidamente la excepción.

6.10.13 *Características mínimas en la clave:* Normar las características que se determinen para las claves de seguridad como período de caducidad, cantidad y tipo de caracteres requeridos, y otros.

6.10.14 *Intentos de Acceso Fallidos:* Formalizar las condiciones del bloqueo y desbloqueo por intentos de acceso fallidos. Definir el procedimiento de desbloqueo.

6.10.15 *Procedimientos ante alarmas por virus:* Se debe prever el mecanismo de acción ante alarmas y su difusión. La responsabilidad debe estar predeterminada y ser única. Se deberán nombrar reemplazos para casos de ausencia del responsable principal.

6.10.16 *Medidas antivirus:* Si bien la entidad cuenta un antivirus corporativo que funciona satisfactoriamente, Se sugiere revisar otras medidas usuales para la prevención de virus mencionadas en la observación.

6.10.17 *Procedimiento de puesta en producción:* Incorporar un procedimiento para la puesta en producción de nuevas aplicaciones o modificaciones a las existentes.

6.10.18 *Acceso y modificación de los datos por fuera del aplicativo:* Los datos deben ser accedidos únicamente por las áreas usuarias y a través de los aplicativos. Los responsables de producción deben contar con facilidades de acceso para el cumplimiento de sus funciones exclusivamente. El acceso a los datos por personal no usuario y a través de herramientas especiales debe ser restringido. En el caso excepcional en que este procedimiento sea necesario debe justificarse, autorizarse y documentar el alcance de la tarea.

6.10.19 *Seguridad en los servidores abiertos a Internet:* Los servidores de los sitios y páginas web están expuestos a los máximos riesgos por estar abiertos a Internet y a la posibilidad de ataques e intrusiones, por ello se deben extremar las medidas de seguridad ya que muchos de estos ataques están dirigidos a sitios de gobierno.

6.11 Seguridad Física:

6.11.01 *Protección de dispositivos de red:* Incorporar muebles para los dispositivos electrónicos de comunicaciones. Los mismos deberán estar cerrados con llave y en la medida de lo posible fuera del acceso del personal no técnico.

6.11.02 *Seguridad en los accesos físicos:* Incorporar medidas de control de acceso al área de servidores y separar la misma del área de trabajo y reunión.

6.11.03 *Sala de servidores:* No guardar elementos que no sean indispensables para la operación en la sala de servidores. Resolver adecuadamente la deposición del agua condensada por el equipo acondicionador de aire.

6.11.04 *Procedimiento de depuración de la información:* Confeccionar un procedimiento de desecho de información impresa y en soportes magnéticos que asegure su destrucción en especial cuando los soportes contengan información confidencial.

6.11.05 *Salidas, luces y señalización de Emergencia:* Evaluar la instalación de salidas de emergencia, luces y señalización. Establecer y señalizar las salidas de emergencias para que puedan ser utilizadas a tal fin.

Capacitar al personal para su uso adecuado en caso de ser necesario.

6.11.06 *Elementos de seguridad:* Elementos de seguridad del edificio. Revisar y completar los elementos de seguridad del edificio.

6.11.07 *Red eléctrica:* Evaluar la instalación de una red estabilizada e independiente para la red de datos. Se deberá dar prioridad en este contexto a los servidores, los dispositivos de comunicación y los puestos de trabajo en ese orden.

6.11.08 *Fuente alternativa de energía de la red de datos:* Evaluar la instalación de una fuente alternativa de energía para la red de datos. Este tipo de medida constituye una previsión ante la posibilidad de cortes prolongados.

6.11.09 *Fuente de energía transitoria de los dispositivos de comunicaciones:* Evaluar la incorporación de dispositivos UPS para los elementos electrónicos de comunicaciones.

6.12 Proveedores:

6.12.01 Falta de recaudos contractuales: Considerar en próximos contratos la incorporación de medidas que prevean la continuidad del servicio y el acceso irrestricto de una auditoria tal como si se tratara de un servicio prestado internamente.

6.12.02 A*decuación del software a las necesidades del organismo:* Incorporar un modelo de gestión externo o interno para la satisfacción de este requisito.

6.13 Sistemas aplicativos:

6.13.01 *Operaciones de los aplicativos centrales:* Tender paulatinamente a la eliminación del tratamiento de la información fuera de los aplicativos centrales.

6.13.02 *Documentación:* Completar la documentación de los aplicativos. En caso de que los mismos sean provistos externamente reclamar la documentación al proveedor.

6.13.03 *Registro de cambios:* Incorporar logs de auditoría para los cambios que se efectúan en aplicativos centrales.

6.13.04 *Sistema integrador:* Producir la integración de la información de gestión por niveles de manera de contar con indicadores de gestión

generados por los aplicativos que faciliten la conducción del organismo.

6.13.05 *Integración con los Sistemas del GCBA:* Evaluar la integración con algunos sistemas del GCBA como por ejemplo el sistema de información geográfica, el sistema de gestión presupuestaria, y otros.

6.13.06 *Falta de estándares de metodología:* Incorporar estándares de metodología para el desarrollo y la adquisición de aplicativos.

6.14 Internet:

6.14.01 *Subdominio org.ar:* Por las razones expuestas en el Anexo I, se recomienda utilizar el dominio de www.defensoria.gov.ar o defensoriaciudad.gov.ar (ver recomendación siguiente) en la papelería, folletería, papeles oficiales, publicidad, etc. del organismo.

6.14.02 *Dominios defensoria.gov.ar y defensoria.org.ar:* Si bien luego de las tareas de campo los nombres de dominio de titularidad de la Defensoría fueron unificados lo que significa un avance en la posibilidad de ser ubicados por los ciudadanos, se sugiere que se registre algún nombre siguiendo las recomendaciones de NIC Argentina a tal efecto **(ver Anexo II)** para ello se debería registrar un nombre identificatorio del organismo (Defensoría) combinado con un nombre identificatorio de la localización geográfica (ciudad de buenos aires).

6.14.03 *Servidor del sitio Internet:* Los proveedores de Internet (ISP) brindan entre otros servicios conectividad y hosting (posibilidad de ubicar el servidor web en el centro de cómputos del proveedor). Caben dos sugerencias: a) Conectividad: Los vínculos de Internet, al igual que cualquier otro servicio, deben ser contratados en un marco de oferta pública y competencia abierta de precios y calidad de servicio. b) Hosting: la observación estaba dirigida expresamente a trasladar el servidor de páginas web del organismo al ámbito del Gobierno de la Ciudad (revisar el tema con la Dirección General de Sistemas de Información) tal como hacen otros muchos organismos de la Ciudad. Resulta antieconómico tener un servidor en el ámbito de una red privada cuando el GCBA cuenta con suficientes facilidades como para hacerse cargo de ellos.

6.14.04 Persona responsable del dominio: Se sugiere que el responsable del dominio sea el Defensor del Pueblo, este cuenta con un mandato que al finalizar se traslada a un nuevo Defensor que elige la Legislatura de la Ciudad (cada XXX años). Al producirse el traspaso de un Defensor a otro muchas situaciones del organismo requieren de un traspaso formal (por ejemplo, cuentas bancarias, registro de firmas,

etc.), el nombre de domino bien puede ser incluido en esos traspasos de una administración a otra.

7.- CONCLUSIONES

El nivel de servicio de las Tecnologías de la Información y Comunicación de la Defensoría del Pueblo resulta aceptable, especialmente en cuanto a los servicios básicos se refiere (ejemplo: correo electrónico, servicio web, sistemas estándar, telefonía, etc.), sin embargo resulta limitado en el apoyo tecnológico brindado a los aspectos centrales de la gestión. Se debería concentrar la atención en los sistemas que apoyen la estrategia institucional en sus funciones relevantes.

Se han realizado múltiples observaciones, que requerirán de un proceso que se desarrollará en el tiempo. Sin embargo el tenerlas en cuenta e ir corrigiendo los sistemas y las tecnologías poco a poco supone un proceso de establecer prácticas de acuerdo a las reglas del arte.

Las comunicaciones y los datos están en un franco proceso de convergencia razón por la cual todo lo atinente a estos rubros es conveniente centralizarlo. Además, se deben aprovechar las diferentes opciones que ofrece la tecnología actual y la desregulación imperante en el mercado de comunicaciones de voz y datos para buscar soluciones más innovadoras, tendientes a mejorar las prestaciones y reducir los costos.

También es necesario mejorar aspectos relativos a la seguridad física y lógica así como prever posibles situaciones contingentes como por ejemplo cortes de energía eléctrica más o menos prolongados.

El nivel de aprovechamiento de la potencialidad de la red de comunicación de datos en la Defensoría del Pueblo es medio y el nivel de riesgo debido a debilidades en la seguridad de la información y protección de activos informáticos es alto (Criterio de la SIGEN ver Alcance) según se desprende de las observaciones del presente informe.

La Defensoría del Pueblo debe formalizar las políticas de sistemas incluyendo la organización, el marco tecnológico y la seguridad. Es necesario incrementar la relación con el usuario, focalizarse en sus necesidades, generar procesos formales de decisión y de revisión de la estrategia informática. Debe definirse el modelo de gestión para dar cobertura a los diferentes aspectos que se encuentran parcialmente atendidos a la fecha de este informe tales como la capacidad de planificación, el mantenimiento y desarrollo de sistemas, las tareas de organización y métodos y otros.

Se debe procurar la integración de la información minimizando las redundancias como una forma de mejorar la eficiencia y la oportunidad de la misma incrementando su confiabilidad en un adecuado marco de control.

También se debe evaluar el aprovechamiento de los sistemas existentes en el GCBA como factor generador de integración y economía de escala. Existe información en el ámbito del GCBA cuyo acceso se puede efectuar a través de los sistemas existentes.

Por otra parte es importante evaluar un segundo nivel de integración con otros Sistemas del GCBA no solamente para la obtención de información sino también para incorporarse en calidad de Organismo Usuario.

Razones de economía y eficiencia indican que los Sistemas como Control Presupuestario, Sueldos, Internet y otros, utilizados por toda la administración deben tender a ser paulatinamente comunes a todo el GCBA a través de un servicio centralizado a cargo de un único prestador.

La integración de las diferentes aplicaciones dentro de los organismos y entre estos y los diferentes organismos del GCBA es un paso esencial para el logro de un aspecto clave de la modernización del estado: la mejora de la productividad administrativa. De este modo se brindarán mejores servicios a la comunidad con un mejor aprovechamiento de los recursos.

Se deben mejorar asimismo los mecanismos de seguridad físicos y lógicos. La Defensoría del Pueblo debe trabajar en forma integrada con otras áreas especializadas del Gobierno que pueden colaborar para el trabajo que es necesario llevar a cabo.

El área de sistemas de la Defensoría del Pueblo deberá poner su esfuerzo en formalizar muchas de sus rutinas cotidianas para poder lograr un mejor desempeño. También, el organismo debe apoyar la constante actualización y capacitación de los miembros de esta área.

ANEXO I

El acceso por Internet al sitio de la Defensoría se realiza escribiendo en la barra de direcciones del explorador la siguiente dirección: "http://www.defensoria.org.ar". Este es el nombre de dominio y el subdominio en uso actualmente por el organismo.

El registro en el subdominio org.ar contradice la normativa vigente en la materia. "NIC Argentina[13] es la sigla que, siguiendo las prácticas internacionales en la materia, identifica al Ministerio de Relaciones Exteriores, Comercio Internacional y Culto en su carácter de administrador del dominio Argentina de INTERNET"[14]. Es el organismo que tiene a su cargo todo lo atinente con el registro y administración de los nombres de dominio de la Argentina en Internet, estableciendo las recomendaciones, normas y usos para su registración.

Los subdominios utilizados en la dirección de Internet indican la especialidad de la organización (por ejemplo, mil.ar identifica a los organismos pertenecientes a las fuerzas armadas de la Argentina).

La Defensoría tiene en uso como única dirección de acceso el subdominio org en su dirección Internet.

Los subdominios en uso (ejemplo: .com, .mil, .edu, .net, etc.) son iguales en el todos los países del mundo. Ahora bien, Nic establece para ese subdominio: "Denominaciones debajo del ORG.AR: sólo podrán registrar nombres dentro del subdominio ORG.AR las entidades que sean organizaciones sin fines de lucro argentinas o extranjeras. No podrán registrar nombres debajo del ORG.AR las personas físicas por más que la actividad que las mismas desempeñen carezca de fines de lucro[15]" También, en forma concordante: "La entidad registradora deberá poseer personería jurídica sin fines de lucro y el solicitante del dominio deberá consignar el CUIT"[16].

También se agrega: "Las denominaciones bajo "GOV.AR" sólo se registrarán cuando identifiquen a dependencias estatales, sean éstas de carácter nacional, provincial o municipal, no pudiendo utilizarse para identificar a entidades que no pertenezcan a los Poderes Ejecutivo, Legislativo o Judicial"[17].

Por otro lado, debe mencionarse que el dominio y subdominio defensoría.gov.ar se encontraba registrado desde 1999 por el Gobierno de la Ciudad de Buenos Aires, por lo tanto no se requería ningún tramite de registro para su utilización.

[13] Dirección Internet: http://www.nic.ar.
[14] Ver: http://www.nic.ar, documento: Normativa vigente.
[15] Ver: http://www.nic.ar, documento: Normativa vigente adenda del 29/10/2001.
[16] Ver: http://www.nic.ar, documento: Preguntas frecuentes.
[17] Ver: http://www.nic.ar, documento: Normativa vigente. Regla 7.

La defensoría no es una organización sin fines de lucro, es un organismo del gobierno de la Ciudad. Además, tampoco se unificaron los nombres de dominio, es decir que tanto defensoria.gov.ar como defensoria.org.ar apunten al mismo sitio Internet, como podría haberse hecho si se deseaba usar ambas denominaciones.

Esto posibilitaría que los usuarios encuentren el sitio indistintamente del nombre que usen. Al día de hoy si se pide en el buscador defensoría.gov.ar el sitio no se resuelve, el software declara no poder encontrar el servidor. La elección del nombre de dominio y el subdominio correspondiente no es caprichosa, se relaciona directamente con la posibilidad de que los usuarios puedan encontrar el sitio correcto que buscan en un entorno de información global.

ANEXO II

Las recomendaciones de NIC (ver antecedentes en la observación anterior) establecen que: “En el caso de dependencias estatales, el nombre a registrar debe permitir identificar fácil y unívocamente a la dependencia que solicite el nombre de dominio, a efectos de evitar confusiones con otras dependencias de similares denominaciones en otros ámbitos de la Administración”[18].

Desde este punto de vista el dominio “defensoría” no cumple con la norma identificando fácil y unívocamente a la Defensoría del Pueblo de la Ciudad de Buenos Aires ya que se eligió como dominio el uso de una palabra genérica que no caracteriza plenamente al organismo en cuestión, para ello debió habérsele sumado al genérico una identificación de localización geográfica (ejemplo: bsas, buenosaires, etc.). Para más, el propio sitio de la Defensoría muestra otros muchos organismos “Defensoría” del país. Hay que tomar conciencia que Internet es un recurso de información de uso global, de allí la necesidad de identificar lo más unívocamente posible los sitios institucionales de los organismos.

Los sitios de Internet son medios de difusión, de comunicación y de intercambio entre los organismos y los usuarios, por ello la identificación debe ser lo más precisa posible, para que sea funcional y que los usuarios puedan acceder con facilidad e intuitivamente a ellos.

[18] Ver: http://www.nic.ar, documento: Normativa vigente. Regla 7.