INFORME FINAL DE AUDITORIA

Código de Proyecto: 5.04.32
"Ente Único Regulador de los Servicios Públicos"

Auditoría de Sistemas de Información y Comunicaciones (voz y datos).

Ciudad Autónoma de Buenos Aires
Marzo de 2005

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

CÓDIGO DEL PROYECTO:
5-04-32

NOMBRE DEL PROYECTO:
Ente Único Regulador de los Servicios Públicos – Auditoría de Sistemas de Información y Comunicaciones (Voz y datos).

OBJETO:
Hardware, software y dispositivos de red en el ámbito del Ente Único Regulador de Servicios Públicos de la Ciudad Autónoma de Buenos Aires.

OBJETIVO:
Examinar las funciones a cargo del área de sistemas, la arquitectura tecnológica y organizativa, la seguridad en el resguardo de la información y los activos informáticos, las buenas prácticas administrativas, la organización y la continuidad del servicio informático y las comunicaciones en el ámbito del Ente Único Regulador de los Servicios Públicos de la Ciudad de Buenos Aires.

ALCANCE:
Se examinará 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:
Septiembre - Octubre 2004

EQUIPO DESIGNADO:

Auditor Supervisor:	Guillermo A. García
Coordinador:	José Recasens
Auditores:	Zancada Héctor Oscar Ciarlotti

INFORME EJECUTIVO

PROYECTO N° 5-04-32
ENTE ÚNICO REGULADOR DE LOS SERVICIOS PÚBLICOS – AUDITORÍA DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (VOZ Y DATOS) .

CONCLUSIONES: El nivel de servicio de las Tecnologías de la Información y Comunicaciones del Ente Único Regulador de los Servicios Públicos es limitado. Esto se debe principalmente al bajo desarrollo del hardware que no se ha extendido a toda la organización y a servicios que se brindan en sus aspectos básicos como el correo electrónico, servicio web, sistemas estándar y telefonía. Asimismo la estrategia informática fijada por el ente no se ha centrado en apoyar los aspectos esenciales de la organización. En el presente informe se han realizado múltiples observaciones, que requerirán de un proceso que se desarrollará en el tiempo. Este proceso desembocará en mejores servicios, prácticas administrativas de acuerdo a las reglas del arte, las buenas prácticas y un entorno más seguro y eficiente.

OBJETO: Hardware, software y dispositivos de red en el ámbito del Ente Único Regulador de Servicios Públicos de la Ciudad Autónoma de Buenos Aires.

OBJETIVO: Examinar las funciones a cargo del área de sistemas, la arquitectura tecnológica y organizativa, la seguridad en el resguardo de la información y los activos informáticos, las buenas prácticas administrativas, la organización y la continuidad del servicio informático y las comunicaciones en el ámbito del Ente Único Regulador de los Servicios Públicos de la Ciudad de Buenos Aires.

OBSERVACIONES:
Las principales observaciones realizadas están referidas a:

- Mejorar aspectos relativos a la seguridad física y lógica así como prever posibles situaciones contingentes como por ejemplo la posibilidad de un incendio en el centro de cómputos. La experiencia demuestra que existe una gran diferencia en la reacción ante una situación anormal si la misma fue prevista. En todos los casos deben tenerse en cuenta las necesidades específicas de un centro de cómputos. El Ente debe trabajar en forma integrada con otras áreas especializadas del Gobierno que pueden colaborar para el trabajo que es necesario llevar a cabo.
- Aprovechar las diferentes opciones que ofrece la tecnología actual y la desregulación imperante en el mercado de comunicaciones de voz y datos. Por otra parte las comunicaciones de voz y datos están en un franco proceso de convergencia razón por la cual todo lo atinente a estos rubros es conveniente centralizarlo para buscar soluciones más innovadoras, tendientes a mejorar las prestaciones y reducir los costos.
- Aprovechar todas las posibilidades de la red de comunicación de datos, desde que el Ente no dispone de una adecuada salida a Internet y sus servicios Web y de correo adolecen de debilidades que se explicitaron en las observaciones del presente informe.

- Formalizar las políticas de sistemas de información y comunicaciones, incluyendo la organización, el marco tecnológico y la seguridad dando amplia participación a toda la organización en este proceso. Será necesario generar procesos formales de decisión y de revisión de la estrategia informática y definir 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. Dentro de este encuadre deberá tener especial preponderancia la constante actualización y capacitación de los miembros del área de Sistemas condición sin la cual no se podrán implementar muchas de las mejoras necesarias.
- Procurar la integración de la información dispersa en diferentes sistemas, internos y externos a la organización, 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.
- Integrar 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 a fin de brindar mejores servicios a la comunidad con un mejor aprovechamiento de los recursos.

INFORME FINAL DE AUDITORIA
PROYECTO Nº 5.04.32

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 del Ente Único Regulador de los Servicios Públicos de la Ciudad de Buenos Aires con el siguiente objeto:

1.- OBJETO

Hardware, software y dispositivos de red en el ámbito del Ente Único Regulador de Servicios Públicos de la Ciudad Autónoma de Buenos Aires.

2.- OBJETIVO

Auditoria del área de sistemas del organismo, incluyendo su arquitectura tecnológica y organizativa, la seguridad en el resguardo de la información y los activos informáticos, las buenas prácticas administrativas, la organización y la continuidad del servicio informático y las comunicaciones en el ámbito del Ente Único Regulador de los Servicios Públicos.

3.- ALCANCE

El presente examen fue solicitado por el Ente Único Regulador de los Servicios Públicos de la Ciudad de Buenos Aires en virtud del comienzo 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 septiembre a octubre 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 normativa complementaria.

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 efectuó el análisis de la documentación provista por el área.

3.2- Limitaciones al Alcance:

Los siguientes factores limitaron la tarea de auditoria:

- Diferencias entre la estructura formal y la real.
- Carencia de normas, manuales y procedimientos escritos formales.
- La falta 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.
- 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.
- La inexistencia de un mapa lógico y físico de la red trae aparejado la imposibilidad de conocer el detalle de las mismas 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.

4.- ACLARACIONES PREVIAS

Los sistemas en que la institución basa su gestión son críticos y deben responder a las necesidades institucionales de modo amplio y flexible. Si esto no sucede se podrían ver comprometidas la eficiencia y la dinámica de la organización para el cumplimiento de sus objetivos.

4.1- Área de Sistemas

Conforme el organigrama de la organización, el área de Sistemas depende de la Gerencia de Administración. La misma se integra con cuatro agentes (dos contratados y dos de planta), encontrándose actualmente a cargo de un agente (licenciado en sistemas) sin designación formal.

La red tiene 23 puestos de trabajo propios y otros 20 puestos que son equipos que fueron incorporados a la red y que son de propiedad del personal del organismo. Cabe consignar que la red cuenta con aproximadamente 110 usuarios que comparten los puestos de trabajo mencionados anteriormente.

Poseen seis servidores:

- Un Servidor de correo electrónico (Mail Server);
- Un Servidor de archivos (File Server);
- Un SQL Server;
- Dos Servidores Linux con funciones de Firewall para las líneas ADSL;

- Un Servidor Linux para administrar los sistemas y funciones de Firewall para la tercer línea ADSL.

El servidor del sitio web del organismo está residente (hosting) en una red privada contratada a ese efecto, ese mismo proveedor da servicios de mail externos.

4.2- Software de Aplicación

Se utilizan las clásicas herramientas de ofimática para la edición de texto y planilla de cálculo.

Utilizan un desarrollo propio para el seguimiento de expedientes.

Poseen un software para las tareas de administración contable y liquidación de sueldos (Software de Gestión Contable Waldbott).

4.3- Hardware

Los servidores son equipos de marca, alguno de ellos con inconvenientes de capacidad de disco (File Server). Asimismo presentan un cierto nivel de obsolescencia.

Los puestos de trabajo son computadores de marca y equipos genéricos.

4.4- Software de base y servicios

Se encuentran orientados a sistemas de arquitectura abierta (Sistema Operativo Linux). Combinan el uso de estos sistemas con sistemas propietarios.

4.5- Comunicaciones

Una central telefónica Meridian administra las comunicaciones internas y externas del Ente, posee 52 líneas internas que acceden al exterior a través treinta canales de comunicación simultáneos (entrantes y salientes, trama E1). Dicha trama provee asimismo cien números telefónicos consecutivos. La central es modular y ampliable.

El organismo posee también ocho líneas analógicas adicionales de las cuales tres son utilizadas para el servicio ADSL (conexión a Internet por banda ancha a través del vínculo físico telefónico) de 512 kb cada una contratadas a la empresa Telefónica de Argentina -Speedy-.

No se encuentran conectados a la red MAN del GCBA.

La red interna vincula a los servidores antes mencionados con los puestos de trabajo.

El mantenimiento del equipo así como la programación de la central es efectuado por un tercero[1] contratado al efecto.

5.- OBSERVACIONES

5.1. Tecnologías de la Información y red de datos

5.1.1. Aspectos Generales

1- Plan de Tecnologías de la Información y las Comunicaciones (TICs)
Ausencia de un Plan formal ni informal de TIC 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 involucrados y la totalidad de las tareas a llevarse a cabo a corto plazo (por ejemplo: un año).
No se verifica la existencia un plan estratégico de sistemas, que contenga los proyectos principales y los cronogramas de su implementación para un período de mediano y largo plazo (por ejemplo: tres años).

2- Alineación de los sistemas de información

Carencia de sistemas para apoyar la gestión esencial del mismo en forma integral, limitándose al apoyo de las áreas de servicios como la Administración. El único sistema de apoyo a la gestión del organismo es un sistema de seguimiento de expedientes con desarrollo interno que no se encuentra documentado.

3- 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.

4- 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- Procedimientos para nuevos requerimientos

Ausencia de procedimientos formales que establezcan los pasos a seguir para dar adecuado tratamiento a los requerimientos de los usuarios (cliente interno)

[1] Un técnico a quien se recurre cada vez que hay que cambiar la configuración o alguna eventualidad. Este servicio no se encuentra abonado.

para la solicitud de nuevos servicios o necesidades de los sistemas de información.

6- Metodologías de administración y seguimientos de proyectos

Carencia de una metodología para la administración de proyectos, de un procedimiento para el registro 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.

Ausencia de condiciones para dar cumplimiento a la tarea de adecuación de los sistemas existentes y la implantación de nuevos sistemas con su conformación actual, careciendo de la dotación suficiente de personal especializado orientados a esta función e imposibilitad de contratar el servicio.

7- Función de Organización

El organismo no posee un área de organización y métodos 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.

Limitado nivel de organización que se observa en la falta de formalización de los cargos, carencia de correspondencia entre los cargos y las funciones, la falta de normas y procedimientos formales de seguridad, continuidad, operación, mantenimiento, contingencia y soporte entre otros.

8- Proceso de evaluación de incorporación de tecnología

No se dispone de un procedimiento sistemático y formal de evaluación de factibilidad de nuevos proyectos tecnológicos.

5.1.2. Organización y personal

1- Plan de capacitación de los agentes

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

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- Dependencia funcional formal

No está formalizada la dependencia funcional del área de Sistemas de información y comunicaciones.

3- Segregación de funciones

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. Si bien existe una distribución informal de tareas, se producen algunas superposiciones.

4- Control del área

El área de sistemas no cuenta con procedimientos documentados. Asimismo, existe total carencia de la documentación usual en el Sistema de Seguimiento de Expedientes.

5- Control de operaciones computarizadas y/o procesos

No existe una adecuado registro actualizado de los controles de las actividades y procesos que se desarrollan normalmente en el centro de procesamiento de información.

5.1.3. Equipamiento (Hardware)

1- Inventario de equipamiento

El inventario del hardware es incompleto, no incluye los números de serie. Asimismo tampoco especifica qué áreas están a cargo del equipamiento.

Se ha verificado la existencia de un número significativo de equipos informáticos (PC's) propiedad de los agentes del organismo.

5.1.4. Programas (Software)

1- Control de Software Instalado:

El inventario de software no especifica el vencimiento de las licencias y la última fecha de actualización de la versión. Esto implica el riesgo de utilizar software con licencias vencidas o en versiones desactualizadas con riesgo de mantener debilidades que ya se hubieran corregido.

5.1.5. Red de datos

1- Documentación de la red de datos

No existe un mapa lógico ni el mapa físico de la red de comunicación de datos (donde se debe especificar, por ejemplo: el tipo de cableado, cantidad de líneas, cantidad y tipo de bocas identificación precisa de cada dispositivo y otros).

2- Encriptación de información:

No se utilizan técnicas de encriptación de la información que circula por la red.

3- Monitoreo de red

No se verifican procedimientos de seguimiento formal, sistemático y rutinario de la actividad de la red. Tampoco hay registro de los incidentes más frecuentes que se presentan.

Inexistencia de un software de monitoreo de la red y que efectúe revisiones frecuentes.

Ausencia de herramientas que permitan determinar excesos de tráfico, intentos de acceso indebidos, modificaciones al hardware interconectado y otros. Esto permite alertar y diagnosticar automáticamente problemas en la red de comunicaciones.

4- Documentación de intentos de acceso indebido

No se documenta formalmente el seguimiento de los intentos de acceso indebidos.

5.1.6. Continuidad de la operación

1- Procedimientos de resguardo de la información

No existe una política y procedimientos formales de resguardo y respaldo de la información. Cabe consignar que se realizan rutinas de back up en forma correcta, sin embargo estas rutinas no llegan a constituir una completa política de resguardo de la información.

2- Copia de respaldo en sede externa

Los procedimientos de copia y resguardo de datos actualmente en uso, no incluyen copia en sede externa.

3- Procedimientos de recuperación de la información

No se dispone de un procedimiento formal de recuperación de datos y archivos.

4- Plan de Contingencias, Plan de Evacuación y Plan de Recuperación de Desastres

No se cuenta con un plan de contingencias, un plan de evacuación y un plan de recuperación de desastres y sus correspondientes pruebas.

5- Servidores alternativos[2]

No se dispone de equipamiento alternativo (servidores de respaldo, propios o por convenios formales con terceros) para el procesamiento y las telecomunicaciones.

5.1.7. Seguridad lógica

1- Clasificación de la información

No se ha efectuado una 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. Tampoco se dispone de un procedimiento para su ejecución.

2- Definición del dueño de los datos

No se definió al propietario de los datos, es decir, el funcionario que participará en la determinación de los niveles de acceso a la información para cada función y proceso.

3- Procedimiento de definición de Perfiles de Usuarios

El procedimiento para la determinación de los perfiles de usuario para cada función no es formal y es incompleto ya que no se especifican las áreas que intervienen y los responsables de definir la información a la que se accederá y la modalidad y el alcance bajo la cual será accedida.

4- Procedimiento de Altas de Usuarios

Ausencia de 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.

5- Procedimiento de Bajas de Usuarios

Inexistencia de un procedimiento formal para la baja de usuarios.

[2] Los servidores alternativos se utilizan a los efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales.

6- Compromiso de confidencialidad y uso responsable

El compromiso de confidencialidad para el tratamiento reservado de la información confidencial no cuenta con la aprobación formal de las autoridades.

7- Compromiso de uso responsable de la red, de la conexión Internet y del correo electrónico que provee el organismo

No hay un compromiso formal firmado por los usuarios sobre el uso responsable de la red, la información, el acceso a Internet y el correo electrónico.

8- Claves compartidas

Uso de claves compartido. En efecto, las claves no son en todos los casos personales y secretas. Hay agentes que comparten el usuario y la clave para algunas tareas.

9- 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 se encuentra resuelta. (No se citan ejemplos en resguardo de la seguridad).

La falta de estos cambios aumenta los riesgos y la seguridad en la red.

10- Características mínimas en la clave

No se encuentran normadas formalmente las características mínimas que deben respetar las claves de acceso y autenticación de los usuarios.

11- 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 hay un procedimiento formal para la rehabilitación de claves.

12- 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.

13- Medidas antivirus

Los procedimientos antivirus son informales e incompletos.

Se carece de alguna de las medidas habituales que reducen los riesgos de infección y difusión de los virus, troyanos, gusanos y otros.

14- Procedimiento de puesta en producción

No existen procedimientos de control para garantizar el efectivo y correcto control de cambios cuando corresponde.

15- Acceso y modificación de los datos por fuera del aplicativo

No se encuentra debidamente restringido el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción.

16- Seguridad en los servidores abiertos a Internet

El contrato por el servicio de hospedaje del sitio web (hosting) no incluye condiciones referidas a la seguridad. Tampoco especifica el derecho del cliente a auditar tales condiciones en la instalación del proveedor.

5.1.8. Seguridad Física

1- Seguridad en los accesos físicos

No disponen de controles de acceso formales, donde se determine el área restringida. El área de procesamiento debe separarse del área de trabajo. Se debe permitir el acceso al área de procesamiento solo al personal formalmente autorizado.

2- Resguardo de documentación

No se dispone de instalaciones adecuadas para guardar los listados y documentación de datos, programas y sistemas.

Estos deben almacenarse con adecuadas medidas de seguridad.

3- Procedimiento de depuración de la información

Falta un procedimiento formal y rutinario para depurar la información 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.

4- Salidas, luces y señalización de Emergencia

Se comprobó la falta de salida de escape de emergencia del edificio. Actualmente, no existe señalización ni luces de emergencia que conduzcan a la salida del edificio

5- Elementos de seguridad

Se comprobó la falta parcial de elementos de seguridad en la sala de servidores. Asimismo se carece de dispositivos de detección automática de humo / calor en la sala de servidores.

6- Fuente alternativa de energía de la red de datos

No se prueba rutinariamente el correcto funcionamiento de los equipos de fuente de energía interrumpida. Las pruebas se efectúan sólo por cortes del suministro eléctrico.

5.1.9. Sistemas aplicativos

1- Documentación

En el sistema de seguimiento de expedientes la documentación es inexistente.

2- Registro de cambios

El sistema Waldbott no cuenta con reportes (log) que permita 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.

3- Sistema integrador

No se cuenta con un sistema integrador de la información para toma de decisiones.

4- Integración con los Sistemas del GCBA

No se ha evaluado la alternativa de adherir al uso de sistemas centrales del GCBA como por ejemplo el Sistema de Administración Geográfico, el sistema de control presupuestario, el sistema de Administración de Inversiones salidas y servidores de la Red MAN y otros servicios del GCBA Dirección General de Sistemas de Información (DGSinf).

5- 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.

5.1.10. Internet

1- Falta de especificidad en el dominio

El dominio registrado carece de especificidad ya que no identifica al ente y a la ciudad de Buenos Aires en forma univoca. En consecuencia podría tratarse de cualquier ente de una ciudad cualquiera.

Esto dificulta la ubicación del dominio en el ciberespacio debido a la superabundancia de información publicada en el mismo.

El acceso por Internet al sitio del Ente se realiza escribiendo en la barra de direcciones del explorador la dirección (Uniform Resource Locator, URL) http://www.entedelaciudad.gov.ar[3].

2- Persona responsable del dominio

No es correcta la designación de la Persona Responsable en el registro del dominio "entedelaciudad.gov.ar".

En el registro figura como responsable técnico y responsable administrativo una persona ajena al organismo.

Esta delegación de funciones no fue aprobada formalmente por las autoridades.

5.2- Comunicaciones y conectividad externa:

5.2.1. Aspectos Generales:

1- Contratación del servicio telefónico

El servicio de telefonía no fue contratado en un marco de competencia de precios y servicios entre distintos proveedores. El contrato de adhesión que une al Ente Único Regulador de los Servicios Públicos con el prestador del servicio de telefonía fue suscripto en un mercado monopólico y que actualmente se encuentra desregulado.

2- Líneas analógicas

El mantener líneas analógicas[4] innecesarias deriva en gastos indebidos ya que son recursos que se abonan y podrían reemplazarse con la utilización eficiente

[3] Este es el nombre de dominio y el subdominio en uso actualmente por el organismo.

de la trama. Además se dificulta el control y el uso de las comunicaciones telefónicas.

3- Evaluación sistemática de las comunicaciones

Inexistencia de estadísticas. No se analizan en forma rutinaria y sistemática las comunicaciones, lo que puede provocar que, por ejemplo, se abonen llamadas indebidas y/o innecesarias. Además el análisis sistemático y rutinario de las comunicaciones permite revisar el flujo, las horas pico, posibles cuellos de botella, indicar si es necesario ampliar los servicios con nuevas tramas, etc.

4- Administración Informal

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.

La administración de la telefonía y la red de datos está unificada en la práctica, aunque no se encuentra formalizada.

5- Conectividad Internet

La conectividad Internet actualmente en uso es ineficiente y antieconómica.

Se utilizan líneas ADSL (3), estas líneas son habitualmente utilizadas para conectividad Internet de banda ancha en hogares o en redes pequeñas y de pocos usuarios. Para compensar esta falencia se han contratado tres líneas sin resolver el problema de base. Hay que mencionar que para proteger la red interna se instaló un servidor por cada una de estas líneas. También además del abono por cada servicio ADSL se paga un abono de línea telefónica.

Existen opciones más eficientes y más económicas en el mercado para resolver la conectividad Internet.

6- Correo electrónico externo

El organismo carece de correo electrónico externo, su servidor cubre el correo interno y baja el correo que viene de afuera del organismo y lo distribuye internamente. Para ello se está pagando y utilizando un servidor externo que provee una red privada.

5.2.2. Seguridad lógica:

[4] Ver Punto 4.5- Comunicaciones.

1- Procedimiento formal para configurar y administrar el servicio telefónico

Ausencia de un procedimiento formal para definir, instrumentar y controlar los servicios telefónicos disponibles para cada interno o agente, en función de las necesidades de las diferentes áreas. Inexistencia de una configuración formal aprobada que contemple qué permisos dispondrán los integrantes de cada área y los tipos de llamada que podrá efectuar. (Larga distancia local, Internacional, llamadas a celulares y otros).

No se verifican procedimientos formales para el acceso y la administración de la configuración, aunque solo el personal de sistemas accede a la misma.

La configuración de la central y de los permisos de usuarios es informal.

Los sistemas de comunicaciones y conectividad de los organismos deben contar con una configuración formal aprobada por las autoridades del mismo según los servicios que se prestan

2- Acceso lógico a la central

No se modifican las claves de acceso a la central cada vez que terceros efectúan una modificación en la configuración de la misma.

3- Software de administración de la central

El organismo no cuenta con el software que permite configurar la Central telefónica.

4- Cursos de capacitación para la programación de la central

El personal del organismo no se encuentra capacitado para programar y/o configurar la Central telefónica.

5.2.3. Seguridad física:

1-Acceso físico a la central no formalizado

No se encuentra formalizada la restricción de acceso y la lista de agentes exceptuados. La central telefónica se encuentra en la sala de servidores donde solamente ingresan quienes poseen la llave sin que se haya determinado formalmente quienes deben ser los que la posean.

2- Ubicación inadecuada y falta de verificación del sistema ininterrumpido de energía (UPS)

Inexistencia de procedimientos formales de verificación y pruebas rutinarias de funcionamiento del la unidad de provisión de energía interrumpida (UPS). Además, este dispositivo se encuentra en una habitación contigua en la que se

guardan elementos de limpieza, la misma está cerrada con llave y el personal responsable del sistema no tiene esas llaves. Tampoco se cuenta con software para administrar los dispositivos.

3- Plan de contingencia (comunicaciones y conectividad)

Inexistencia de un plan de contingencia formal ni informal para las comunicaciones y la conectividad Internet.

4- Plan de recuperación de desastre

Inexistencia de un plan de recuperación de desastre para las comunicaciones y conectividad.

6. RECOMENDACIONES

6.1. Tecnologías de la Información y red de datos

6.1.1. Aspectos Generales

1- Implementar un plan de corto plazo, que contenga tiempos y metas para las distintas tareas y etapas, recursos humanos y materiales asignados que permita supervisar los avances, revisar las metas y verificar su alineación con los objetivos de la Dirección. Asimismo, debe realizarse un plan estratégico de mediano / largo plazo según los lineamientos que fijen las máximas autoridades del organismo.

2- El sistema en uso debe documentarse y mejorarse en su performance para que con los adecuados niveles de seguridad y adecuación sea incorporado formalmente al uso cotidiano. Si esto no pudiera lograrse, incorporar software con todas las características de las reglas del arte, buscando constantemente la alineación de las incorporaciones con los fines de la organización.

3- Si bien existen prácticas y rutinas de seguridad, no hay una política formal a este respecto, por lo tanto, se debe formalizar una política de seguridad con los lineamientos tecnológicos, el compromiso de la dirección, los recursos y las definiciones de riesgo correspondientes.

4- Incorporar formalmente, un responsable de la seguridad informática, independiente del área de sistemas y del sector usuario, que se haga cargo de esa responsabilidad, del acceso a los datos y del resguardo de la información.

5- 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- 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 materiales y humanos suficientes y metas a cumplir.

7- Generar 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.

8- Dada 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.

6.1.2. Organización y personal

1. 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.

2. Definir la dependencia del área de sistemas de información y del área de seguridad de sistemas a un adecuado nivel que asegure su alineamiento con el objetivo de la organización y su independencia de las áreas usuarias (ejemplo: sistemas no debe depender de administración).

3. 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. Esto debe adaptarse a las posibilidades del área comenzando por separar las funciones más importantes (producción, desarrollo y soporte) y efectuarlo en la medida que la dimensión de la misma lo permita.

4. El área de sistemas debe llevar un adecuado registro formal, rutinario y sistemático de las tareas, los cambios y las novedades. Además todos los

sistemas en uso deben estar documentados. Esto posibilita un control de gestión y fortalece la seguridad en el área.

5. Se recomienda formalizar los controles de proceso y las operaciones del centro de cómputos de manera de garantizar su ejecución y supervisión.

6.1.3. Equipamiento (Hardware)

1. 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 notificados al área encargada de llevar el registro patrimonial del organismo.

6.1.4. Programas (Software)

1. Se recomienda restringir la instalación de software y controlar con medios informáticos el software instalado en cada equipo, incluyendo el número de versión y el vencimiento de las licencias y sus renovaciones.
   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. En el caso de licencias vencidas o a vencerse, se recuerda que hay una recomendación de la Dirección General de Sistemas de Información (DGSinf) de realizar la migración al software abierto, lo que redundaría en un ahorro económico importante para el organismo, esta misma recomendación debe ser tenida en cuenta frente a la incorporación de equipos nuevos.

6.1.5. Red de datos

1. Elaborar un mapa físico y un mapa lógico de la red con el máximo nivel de detalle posible. El contar con ambos mapas de red permite abordar y planificar soluciones en forma competente y adecuada, además de facilitar las tareas de administración de la misma.

2. Evaluar la utilización de técnicas de encriptación de la información que circula por la red de datos. En los casos en que se maneje información muy crítica se debe proveer las herramientas necesarias para 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 la utilización de herramientas de encriptación no redunda en mayores costos para el organismo ya que al igual que en el caso de las herramientas ofimáticas existe en la actualidad software abierto y gratuito para este uso.

3. Si bien se efectúan revisiones periódicas de la 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.

4. Si bien se revisan los intentos de acceso indebido, se recomienda analizar y documentar formalmente los intentos de acceso no permitidos y las acciones tomadas para neutralizarlos y proteger la red. Esta recomendación acompaña y complementa la formulada para el monitoreo de red (ver ut supra).

6.1.6. Continuidad de la operación

1. Confeccionar e implementar procedimientos de resguardo de la información que incluyan: niveles de riesgo formalmente aceptados por la organización, definición de soportes, responsables de ejecución, mecanismos de control y supervisión entre otros aspectos. No debe olvidarse que para el estado y los organismos que lo componen la información es un activo valioso para su desenvolvimiento y que como tal debe ser cuidado y preservado.

2. Las reglas del arte y las buenas prácticas de administración de las organizaciones, 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, frecuencia y otros factores. Al igual que en el caso anterior se recuerda que la información es un activo valioso.

3. Si bien, en los hechos, los resguardos son utilizados con habitualidad para recuperar información de los usuarios; se deben incorporar procedimientos formales de recuperación de datos, que deben ser verificados periódicamente (se sugiere, como mínimo 2 veces al año) 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 un acta. En caso de fallas se deberá efectuar un informe de las mismas, para realizar su corrección y nueva prueba.

4. Elaborar un plan de contingencias, un plan de evacuación y un plan de recuperación de desastres y efectuar pruebas integrales de los mismos por lo menos dos veces 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 y de otros organismos.

5. Se debe elaborar un plan que frente a posibles caídas o paradas de los sistemas, el organismo pueda continuar con sus operaciones habituales en servidores alternativos. Estos servidores alternativos pueden ser propios o, por un ahorro de costos, pueden ser de terceros (por ejemplo, otros organismos), en cuyo caso deben elaborarse acuerdos formales que contemplen este tipo de colaboración.

6.1.7. Seguridad lógica

1. Realizar una clasificación formal de la información según el grado de confidencialidad, de jerarquía y de criticidad (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.

2. Definir quienes son los responsables por la fijación de pautas de resguardo y protección de la información de la institución y del tratamiento adecuado de la misma en función de su grado de confidencialidad, criticidad, etc.

3. Confeccionar un procedimiento formal 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.

4. Confeccionar e implementar un procedimiento formal de altas de usuario.

5. Confeccionar e implementar un procedimiento formal de bajas de usuario.

6. Incorporar la práctica de la firma del compromiso de confidencialidad que incluya la no difusión de la clave de seguridad, entre otras pautas. 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.

7. Al igual que en la recomendación anterior, se solicita incorporar un compromiso formal sobre el uso responsable de la red, el correo electrónico e Internet. Este documento deberá ser firmado por el usuario al momento de recibir su alta en la red y los sistemas.

8. Eliminar totalmente las claves compartidas efectuando la renovación periódica y rutinaria de las mismas. Asimismo, instruir y capacitar a los

usuarios sobre los peligros para la seguridad que conllevan este tipo de malas prácticas.

9. Modificar la identificación de la función administrador y guardar reserva de la misma. El administrador, al igual que los demás usuarios debe cambiar periódicamente sus claves de acceso en resguardo de la seguridad, además puede incorporar como buena práctica el cambio periódico del nombre de usuario con los atributos del administrador.

10. Normar las características que se determinen para las claves de seguridad como período de caducidad, cantidad y tipo de caracteres requeridos, y otros.

11. Formalizar las condiciones del bloqueo y desbloqueo por intentos de acceso fallidos. Definir el procedimiento de desbloqueo y las autorizaciones y sus responsables.

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

13. 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 (a modo de ejemplo, inhabilitar las disqueteras, etc).

14. Incorporar un procedimiento formal para la puesta en producción de nuevas aplicaciones o modificaciones a las existentes. Estos procedimientos deben contemplar, por ejemplo, la documentación completa de la aplicación y sus cambios, la versión en uso, la fecha de puesta en producción, entre otros.

15. Los datos deben ser accedidos únicamente por las áreas usuarias responsables y a través de los aplicativos. Los responsables de producción deben contar, exclusivamente, con facilidades de acceso para el cumplimiento de sus funciones. 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. Se recomienda mantener unificado el tratamiento de la información dentro de los sistemas principales.

16. Los servidores de los sitios y páginas web están expuestos a los máximos riesgos y a la posibilidad de ataques e intrusiones por estar abiertos a Internet. Por ello se deben extremar las medidas de seguridad ya que muchos de estos ataques están dirigidos a sitios de gobierno, estas medidas de seguridad incluyen en todos los casos a los proveedores de servicios relacionados.

6.1.8. Seguridad Física

1. Incorporar medidas de control de acceso al área de servidores y separar la misma del área de trabajo y reunión. Dotar al área de los medios adecuados para poder implementar las medidas de seguridad física correspondientes.

2. La documentación de los sistemas debe guardarse fuera de las áreas usuarias, se debe proveer a la administración de los sistemas con los medios adecuados para que lleve a cabo esta tarea.

3. Confeccionar un procedimiento formal aprobado por las máximas autoridades para el desecho y la destrucción de información impresa y en soportes magnéticos. Los procedimientos deben asegurar su destrucción, en especial cuando los soportes contengan información confidencial.

4. Evaluar la instalación de salidas de emergencia, luces y señalización. Establecer y señalizar las salidas para que puedan ser utilizadas a tal fin en casos de emergencia, peligro o desastres. Capacitar al personal para su uso adecuado en caso de ser necesario.

5. Revisar y completar los elementos de seguridad del edificio, especialmente en la sala de servidores.

6. Las UPS deben ser probadas en forma rutinaria y periódica para observar su correcto funcionamiento y para solucionar las fallas que se presenten. Este tipo de medidas constituyen una previsión ante la posibilidad de cortes de energía.

61.9. Sistemas aplicativos

1. Completar la documentación de los aplicativos. En caso en que los mismos hayan sido provistos externamente y/o por terceros, reclamar la documentación al responsable del desarrollo de esas aplicaciones.

2. Incorporar logs de auditoría para los cambios que se efectúan en aplicativos centrales. Los logs deben permitir la completa e univoca identificación de quien realizó cambios en la información, estos sistemas de seguridad apuntan a eliminar la posibilidad del repudio de las acciones realizadas por los usuarios.

3. 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.

4. Evaluar la integración con aquellos sistemas y servicios del GCBA que sean funcionales al organismo y que permitan aumentar la seguridad, la eficiencia y la economía en la administración de estos recursos.

5. Incorporar estándares de metodología para el desarrollo y la adquisición de aplicativos.

6.1.10. Internet

1. Se sugiere que se registre algún nombre siguiendo las normas y recomendaciones de NIC Argentina a tal efecto (ver Anexo) para ello se debería registrar un nombre identificatorio del organismo (Ente) combinado con un nombre identificatorio de la localización geográfica (ejemplo: Ciudad de Buenos Aires). 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.

2. Se sugiere que el responsable[5] del dominio sea uno de los 5 Directores del Ente, este cuenta con un mandato que al finalizar se traslada a un nuevo Director que elige la Legislatura de la Ciudad (cada 4 años). Al producirse el traspaso de un Director 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. El nombre de dominio que el Ente utiliza para Internet es un activo, es similar a una marca registrada ya que los dominios son únicos e irrepetibles mundialmente, por ello no debe ser delegada las facultades que lo conciernen en personas ajenas a la institución.

6.2- <u>Comunicaciones y conectividad externa:</u>

6.2.1. Aspectos Generales:

1. La observación está referida al servicio telefónico que era prestado en exclusividad por las empresas Telefónica de Argentina S.A. y Telecom S.A. y actualmente desregulado.
   En este sentido, sugerimos hacer uso de la desregulación imperante en el mercado de comunicaciones de voz y datos como una forma de disminuir los costos y mejorar la prestación. Por ello, se recomienda hacer un estudio del uso y los requerimientos de telefonía del organismo, conociendo estos parámetros, llamar, en el marco normativo correspondiente, a un concurso público y abierto de precios y servicios para satisfacer las necesidades especificas del organismo.

[5] "Persona Responsable: es la persona física de contacto designada por la entidad registrante, que atenderá todas las cuestiones relacionadas con el dominio".

2. Eliminar las líneas analógicas conservando una o dos líneas para el caso en que la centralita quede fuera de servicio por corte de energía. Eliminar las líneas utilizadas para las conexiones ADSL luego de reemplazar a estas por una solución adecuada para el organismo.

3. 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.

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

5. Se sugiere contratar, en el marco de la normativa vigente, una salida Internet de banda ancha de las muchas que se encuentran en este mercado desregulado. Asimismo, no deberá contratarse soluciones de banda ancha de uso domestico (ADSL o Cablemodem) ya que estas están destinadas al uso hogareño y son inadecuadas para las necesidades del organismo.

6. Establecer un servidor de correo electrónico propio en salvaguarda de la seguridad y la confidencialidad de la correspondencia electrónica del organismo. La solución actualmente en uso es no solo antieconómica sino también inadecuada. El organismo puede acordar con la Dirección General de Sistemas de Información (DGSinf) una solución a este problema.

6.2.2. Seguridad lógica:

1. El responsable tecnológico debe contar con procedimientos formales para acceder, administrar y cambiar la configuración de la central telefónica, estos procedimientos deben incluir los respectivos permisos de uso de las distintas modalidades (DDI, DDN, llamadas de fijo a celulares, horarios de uso, llamadas entrantes, etc) para los usuarios y las áreas. Los permisos de uso deben estar formalmente aprobados por las autoridades del organismo. En este sentido es necesario generar canales formales para la toma del conocimiento de las novedades y los cambios que se producen y un proceso de evaluación formal de las mismas.

2. Se recomienda, por razones de seguridad, modificar la clave de acceso a la configuración de la central luego de cada intervención o cambio en la misma, este procedimiento debe ser tenido en cuenta especialmente en los casos de intervención por personal ajeno al organismo.

3. Generar los mecanismos formales necesarios para que la empresa proveedora haga entrega del software de administración y configuración de la central telefónica. En caso que no fuera posible, buscar software alternativo que supla esta carencia.

4. Generar los mecanismos 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 realice esta capacitación, buscar capacitación alternativa que supla esta carencia.

6.2.3. Seguridad física:

1. Se sugiere que se contemple ubicarla en áreas de acceso restringido y dotarlas con adecuadas medidas de seguridad física y de acceso formalizando la lista de agentes que pueden acceder a su ubicación física.

2. La UPS debe ser mudada a la sala donde reside la central y donde el acceso está restringido. 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.

3. Elaborar un plan de contingencia formal que debe ser aprobado por las máximas autoridades del organismo ya que en el se explicita el riesgo que se está dispuesto a asumir en caso de contingencias.
   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.

4. Elaborar un plan de recuperación de desastres y realizar pruebas y verificaciones periódicas del mismo.
   El plan de recuperación de desastres debe ser formalmente aprobado y verificado formalmente 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.

7.- CONCLUSIONES

El nivel de servicio de las Tecnologías de la Información y Comunicaciones del Ente Único Regulador de los Servicios Públicos es limitado. Esto se debe principalmente al bajo desarrollo del hardware que no se ha extendido a toda la organización y a servicios que se brindan en sus aspectos básicos como el correo electrónico, servicio web, sistemas estándar y telefonía.

Asimismo la estrategia informática fijada por el ente no se ha centrado en apoyar los aspectos esenciales de la organización.

En el presente informe se han realizado múltiples observaciones, que requerirán de un proceso que se desarrollará en el tiempo. Este proceso desembocará en mejores servicios, prácticas administrativas de acuerdo a las reglas del arte, las buenas prácticas y un entorno más seguro y eficiente.

Es necesario mejorar aspectos relativos a la seguridad física y lógica así como prever posibles situaciones contingentes como por ejemplo la posibilidad de un incendio en el centro de cómputos. La experiencia demuestra que existe una gran diferencia en la reacción ante una situación anormal si la misma fue prevista. En todos los casos deben tenerse en cuenta las necesidades específicas de un centro de cómputos. El Ente debe trabajar en forma integrada con otras áreas especializadas del Gobierno que pueden colaborar para el trabajo que es necesario llevar a cabo.

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

El Ente no aprovecha todas las posibilidades de la red de comunicación de datos. No dispone de una adecuada salida a Internet y sus servicios Web y de correo adolecen de debilidades que se explicitaron en las observaciones del presente informe.

El Ente debe formalizar las políticas de sistemas de información y comunicaciones, incluyendo la organización, el marco tecnológico y la seguridad dando amplia participación a toda la organización en este proceso. Es necesario generar procesos formales de decisión y de revisión de la estrategia informática y definir 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. Dentro de este encuadre debe tener especial preponderancia la constante actualización y capacitación de los miembros del área de Sistemas condición sin la cual no se podrán implementar muchas de las mejoras necesarias.

Se debe procurar la integración de la información dispersa en diferentes sistemas, internos y externos a la organización, 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. 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.

ANEXO I

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

"NIC Argentina[6] 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"[7]. 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). Los subdominios en uso (ejemplo: .com, .mil, .edu, .net, etc.) son iguales en el todos los países del mundo.

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"[8].

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. A tal respecto NIC aclara "Las denominaciones que contengan las palabras, letras, o nombres distintivos que usen o deban usar la Nación, las provincias y los municipios, sólo podrán ser registradas por las entidades públicas que correspondan. 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. 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."

[6] Dirección Internet: http://www.nic.ar.
[7] Ver: http://www.nic.ar, documento: Normativa vigente.
[8] Ver: http://www.nic.ar, documento: Normativa vigente. Regla 7.