INFORME FINAL DE AUDITORÍA

Con Informe Ejecutivo

Seguimiento de las Observaciones Informáticas del Proyecto 5.04.32
Ente Único Regulador de Servicios Públicos

Auditoria de Sistemas y Comunicaciones

Proyecto Nº 10.12.02

Auditoría de Seguimiento

Buenos Aires, Mayo 2013

Corrientes 640, Piso 5º - (C1043AAT) Ciudad Autónoma de Buenos Aires

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

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

PRESIDENTE

Lic. Cecilia Segura Rattagan

AUDITORES GENERALES

Dr. Santiago de Estrada

Lic. Eduardo Epszteyn

Dr. Alejandro Fernández

Ing. Adriano Jaichenco

Dra. María Victoria Marcó

Dra. Paula Oliveto Lago

Código de Proyecto: 10.12.02

Nombre del Proyecto Auditoria: Seguimiento de las observaciones informáticas del proyecto 5.04.32 Ente Único Regulador de Servicios Públicos. Auditoría de Sistemas y Comunicaciones.

Tipo: Seguimiento

Objeto: Sistemas y comunicaciones del EURSP.
Jurisdicción: Jurisdicción 20 –Jefatura de Gobierno 113.
Ente Único Regulador de los Servicios Públicos

Presupuesto: No aplicable.

Objetivo: Determinar si la Entidad auditada ha tomado acciones correctivas respecto de las observaciones consignadas en el Informe 5.04.32.

Alcance: Verificar el grado de cumplimiento de las recomendaciones y medidas adoptadas frente a las observaciones del informe 5.04.32

Período bajo examen: 2011

EQUIPO DESIGNADO:
Directora de Proyecto: Dra. Gabriela Custer
Auditor a Cargo: Lic. Héctor S. Zancada

Aprobado por unanimidad en la Sesión de Colegio de Auditores Generales de fecha 15/05/2013.

RESOLUCION AGC N° 150/13

INFORME EJECUTIVO

Lugar y fecha de emisión	Ciudad Autónoma de Buenos Aires, Mayo de 2013.
Código del Proyecto	10.12.02
Denominación	Seguimiento de las observaciones informáticas del proyecto 5.04.32 Ente Único Regulador de Servicios Públicos. Auditoría de Sistemas y Comunicaciones.
Tipo	Auditoría de Seguimiento
Período examinado	2011
Objeto:	Sistemas y comunicaciones del EURSP
Jurisdicción:	Jurisdicción 20 –Jefatura de Gobierno 113. Ente Único Regulador de los Servicios Públicos
Unidad Ejecutora	
Programa Presupuestario	No aplicable
Objetivo	Determinar si la Entidad auditada ha tomado acciones correctivas respecto de las observaciones consignadas en el Informe 5.04.32.
Alcance	Verificar el grado de cumplimiento de las recomendaciones y medidas adoptadas frente a las observaciones del informe 5.04.32
Desarrollo de tareas	Las tareas de auditoría fueron realizadas entre abril 2012 y octubre de 2012.
Aclaraciones previas	**4.2** El informe 5.04.32 fue realizado sobre la situación del año 2004, referida a las TICs del Ente, por lo tanto incluyó el servicio de comunicaciones (telefonía) y de conectividad (Internet). Las Observaciones fueron agrupadas en dos grandes temas: - Tecnologías de la Información y red de datos (Título 5.1) y - Comunicaciones y conectividad externa (Título 5.2). **4.3** El Organismo cuenta con una red dividida en dos subredes. Tienen conectadas a ellas 190 puestos de trabajo y catorce servidores. Cuentan con 440 usuarios. Tienen conexión Internet de banda ancha corporativa con su correspondiente vínculo de respaldo. También cuentan con conexión a la red MAN del GCBA, utilizada para acceder a las aplicaciones SADE y SIGAF.

Principales Conclusiones	Se resolvieron 52 de un total de 67 observaciones del Informe 5.04.32. De las 15 restantes, 6 tuvieron avances o resoluciones parciales (avances incipientes) quedando 9 observaciones sin resolver o sin mejoras (avances no satisfactorios). El informe cuyo seguimiento se efectuó había sido un exhaustivo análisis de las TICs del Ente.
Principales Observaciones	Entre las tareas pendientes que están referidas a observaciones que no han registrado ningún grado de avance, merecen un comentario las referidas a la falta de planes de contingencia y planes de recuperación de desastres, tanto de las comunicaciones y la conectividad como de la red y los servidores propios. Estos planes y sus pruebas periódicas revisten particular importancia ya que son los que garantizan la continuidad de los servicios frente a los distintos eventos que puedan presentarse.

INFORME FINAL DE AUDITORIA
SEGUIMIENTO DE LAS OBSERVACIONES INFORMATICAS DEL PROYECTO 5.04.32. ENTE UNICO REGULADOR DE SERVICIOS PUBLICOS- AUDITORIA DE SISTEMAS Y COMUNICACIONES
PROYECTO Nº 2.12.10

DESTINATARIO

Señora
Presidente
Legislatura de la Ciudad Autónoma de Buenos Aires
Lic. Maria Eugenia Vidal
S_____ /_____ D

En uso de las facultades conferidas por los artículos 131, 132 y 136 de la Ley 70 de la Ciudad Autónoma de Buenos Aires, y conforme a lo dispuesto en el artículo 135 de la Constitución de la Ciudad, la Auditoría General de la Ciudad de Buenos Aires ha procedido a efectuar una auditoría de seguimiento de la Auditoría 5.04.32 en el ámbito del organismo a su cargo con el objeto detallado en el apartado siguiente.

I. OBJETO DE AUDITORÍA

Sistemas y comunicaciones del EURSP.

II. OBJETIVO DE LA AUDITORÍA

Determinar si la Entidad auditada ha tomado acciones correctivas respecto de las observaciones consignadas en el Informe 5.04.32.

III. ALCANCE DEL EXAMEN

Verificar el grado de cumplimiento de las recomendaciones y medidas adoptadas frente a las observaciones del informe 5.04.32

Las tareas de auditoría se llevaron a cabo los meses de abril a octubre de 2012.

3.1 Procedimientos

3.1.1 Se enviaron Notas de presentación del proyecto de auditoría y de pedido de información relacionadas con los avances habidos referidos a las observaciones del informe 5.04.32 Ente Único Regulador de Servicios Públicos realizado en el año 2004.

3.1.2 Se realizó una entrevista con el Presidente del Organismo para presentar al equipo a cargo de las tareas y explicar el alcance de las mismas.

3.1.3 Se concedieron dos prórrogas a la solicitud de información, la última con vencimiento el 7 de junio de 2012.

3.1.4 Se realizaron entrevistas con el responsable y personal del área de Sistemas del Organismo con el fin de presentar al equipo de trabajo encargado del proyecto y para recabar información general del área.

3.1.5 Se elaboró un cuestionario relacionado con el funcionamiento de la seguridad física y lógica del Organismo. Se realizaron listas de verificación relacionadas con las comunicaciones, el manejo de la información, administración de servidores, seguridad en la red, almacenamiento, respaldos, soporte técnico, etc. Se relevó información de la Organización, Aplicativos, Planeamiento, Control, Proyectos, etc.

3.1.6 Se realizaron visitas al centro de servidores con listas de control para verificar la seguridad física del mismo.

3.1.7 Se realizaron entrevistas con el responsable del área y el administrador de redes para relevar la seguridad lógica en uso.

3.1.8 Se solicitó información relativa a los sistemas de respaldo de la información, su guarda, periodicidad, contenidos, pruebas de recupero, etc.

3.1.9 Se verificó in situ, la implementación y uso de los sistemas, la red, la administración telefónica, la encriptación, las medidas de antivirus y otras relacionadas con la seguridad.

3.1.10 Se analizó la Res. CABA 8/2007 "Manual de Políticas de Seguridad Informática" publicada en el BOCBA 2629 del 21/02/2006.

3.1.11 Se analizó la Res. 106 EURSPCABA/08 "Manual de Procedimientos del Ente Único Regulador de los Servicios Públicos de la CABA" publicado en el BOCBA 3015 del 16/9/2008.

3.1.12 Se analizaron los contenidos del Acta 497 del 4/9/2012, de la Resolución 112 del 6/7/2012, el Acta 494 del 15/8/2012 y la Resolución 47 del 27/4/2012.

3.1.13 Se elaboró un cuestionario tomando como base la respuesta a la solicitud de información relacionada con las Observaciones del Informe 5.04.32.

3.1.14 Se relevó información relativa a la inscripción del registro del dominio Internet del Ente en NIC. Este relevamiento está relacionado con Observaciones consignadas en el Informe 5.04.32.

3.1.15 En el mes de julio de 2012 el área de sistemas cambió su dependencia funcional de la Dirección de Administración a la recientemente creada área de Innovación Tecnológica dependiente de la Gerencia de Proyectos. Este cambio motivo que se realizaran varias entrevistas con el Gerente de Planificación y el titular del área de Innovación Tecnológica.

IV Aclaraciones Previas:

4.1 En cumplimiento con la Res. 218 del 2005 (Anexo II "Pautas para Auditoría de Seguimiento") de la AGCBA se utilizará la siguiente grilla:

"Grilla de evaluación de observaciones
Se hará una consideración de las observaciones que ya no tienen vigencia, explicitando los criterios por los que se toma esa decisión.
Se mantendrá el criterio de no agregar observaciones, salvo hallazgos que lo ameriten.
En cuanto a la calificación que las observaciones realizadas en el informe de origen obtengan, harán referencia al grado de avance de la situación, y serán:

- grado de avance no satisfactorio (para el caso en que el ente auditado no haya iniciado modificaciones a partir de la observación realizada, o, en caso de haberlas realizado, estas no sean satisfactorias). Se mantiene la observación
- grado de avance incipiente (para el caso en que el ente auditado haya iniciado modificaciones siguiendo la observación realizada por el equipo auditor, pero estas no resulten suficientes)
- grado de avance satisfactorio (para el caso en que el ente auditado haya resuelto la observación). Se resolvió la observación"

4.2 El Informe 5.04.32 fue realizado sobre la situación del año 2004, referida a las TICs del Ente, por lo tanto incluyó el servicio de comunicaciones (telefonía) y conectividad (Internet).

Las Observaciones fueron agrupadas en dos grandes temas:
- Tecnologías de la Información y red de datos (Título 5.1) y
- Comunicaciones y conectividad externa (Título 5.2).

4.3 El Organismo cuenta con una red dividida en dos subredes. Tienen conectadas a ellas 190 puestos de trabajo y catorce servidores.
Cuentan con 440 usuarios.
Tienen conexión Internet de banda ancha corporativa con su correspondiente vínculo de respaldo. También cuentan con conexión a la red MAN del GCBA, se la utiliza para acceder a las aplicaciones SADE y SIGAF.

V. OBSERVACIONES

SEGUIMIENTO DE OBSERVACIONES

A fin de lograr mayor claridad en la comprensión de este seguimiento, se incluye en cada observación su correspondiente recomendación, la evaluación y los comentarios al respecto.

Las Observaciones conservan los títulos y la numeración original del informe de referencia.

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)
Observación: 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).
Recomendación: 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.
Comentario del Ente: Se elevó al Directorio del Organismo un "Plan Estratégico de Tecnologías de la Información y las Comunicaciones" (PETIC) que fue aprobado por Acta de Directorio Nº 513 del 21 de diciembre de 2012.
Avance Satisfactorio Se resolvió la observación

2- Alineación de los sistemas de información
Observación: 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.

Recomendación: 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.
Comentario de la AGC: El software de seguimiento de expedientes fue sustituido por el Sistema Único de Control de Expedientes (SUCE, lenguaje SQL) que cuenta con los manuales del usuario (entregaron copia del manual del usuario) y está en uso. También cuentan para la gestión con el Sistema de Administración de Documentos Electrónicos (SADE) para la gestión de entrada y salida de expedientes del organismo. Además utilizan la red Man del GCBA. Fue verificado el uso SIGAF y otras aplicaciones de apoyo a la gestión. SUCE entregaron Resoluciones que implementan la utilización del sistema para la gestión de expedientes.
Avance Satisfactorio Se resolvió la observación

3- Política formal de seguridad
Observación: 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.
Recomendación: 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.
Comentario del Ente: Posteriormente se elevó al Directorio del organismo el "Manual de Políticas y Normas de Seguridad Informática" versión 2. La nueva versión fue aprobada por Acta de Directorio 513 del 21 de diciembre de 2012 y se derogó la Resolución que ponía en vigencia la versión 1 del mismo Manual.
Comentario de la AGC: Se aprobó la norma que formaliza el procedimiento "Manual de Políticas y Normas de Seguridad informática" (Res.Nº 8 del 2007 del 29/01/2007 publicado en el BOCBA Nº 2629 del 21/02/2007).

Avance Satisfactorio Se resolvió la observación

4- Función de Seguridad Informática
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se emitió la Resolución Nº 112 del 2/7/2012 que designa un responsable para la administración de la seguridad.
Avance Satisfactorio Se resolvió la observación

5- Procedimientos para nuevos requerimientos
Observación: Ausencia de procedimientos formales que establezcan los pasos a seguir para dar adecuado tratamiento a los requerimientos de los usuarios (cliente interno) para la solicitud de nuevos servicios o necesidades de los sistemas de información.
Recomendación: 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.
Comentario de la AGC: El Manual de Procedimientos aprobado formalmente incluye un proceso para los requerimientos de los usuarios y estos quedan registrados en un sistema de tickets (GLPI).
Avance Satisfactorio Se resolvió la observación

6- Metodologías de administración y seguimientos de proyectos
Observación: 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.
Recomendación: 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.
Comentario de la AGC: No se pudo verificar la existencia de un procedimiento formal para la administración y seguimientos de proyectos.
Avance No Satisfactorio Se mantiene la observación

7- Función de Organización
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se elaboró un Manual de Procedimientos para los procesos del área de tecnología y para los procesos administrativos de compras y de recursos humanos entre otros. El responsable de mantenerlo actualizado o de incorporar nuevos procedimientos o circuitos fue formalizado por la Res.Nº 112.
Avance Satisfactorio Se resolvió la observación

8- Proceso de evaluación de incorporación de tecnología
Observación: No se dispone de un procedimiento sistemático y formal de evaluación de factibilidad de nuevos proyectos tecnológicos.
Recomendación: 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.
Comentario de la AGC: El proceso de evaluación de nuevos proyectos relacionados con las TICs fue incorporado a las misiones y funciones del Área de Innovación Tecnológica. Estos cambios en la organización fueron formalizados por Res. Nº 112.
Avance Satisfactorio Se resolvió la observación

5.1.2. Organización y personal

1- Plan de capacitación de los agentes
Observación: 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.
Recomendación: 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.
Comentario de la AGC: El organismo presentó un plan de capacitación de los agentes del área de tecnología para finales del 2012 y para el año 2013, elevado al directorio sin aprobación formal.
Avance Incipiente

2- Dependencia funcional formal
Observación: No está formalizada la dependencia funcional del área de Sistemas de información y comunicaciones.
Comentario de la AGC: Hay Resolución Nº 112 del 2/7/2012 que pasa el área de sistemas a depender del área de Innovación Tecnológica y ésta de la Gerencia de Proyectos.
Avance Satisfactorio Se resolvió la observación

3- Segregación de funciones
Observación: 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.
Recomendación: 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.
Comentario de la AGC: La Resolución Nº112 del 2/7/2012 formaliza las funciones del área de sistemas.
Avance Satisfactorio Se resolvió la observación

4- Control del área
Observación: El área de sistemas no cuenta con procedimientos documentados. Asimismo, existe total carencia de la documentación usual en el Sistema de Seguimiento de Expedientes.
Recomendación: 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.
Comentario de la AGC: Se abandonó el Sistema de seguimiento de expedientes que dio origen a esta Observación. Actualmente usan el Sistema Único de Seguimiento de Expedientes (SUCE). Se verificó la existencia de su documentación.
Avance Satisfactorio Se resolvió la observación

5- Control de operaciones computarizadas y/o procesos
Observación: No existe un adecuado registro actualizado de los controles de las actividades y procesos que se desarrollan normalmente en el centro de procesamiento de información.
Recomendación: Se recomienda formalizar los controles de proceso y las operaciones del centro de cómputos de manera de garantizar su ejecución y supervisión.
Comentario de la AGC: Se mantienen procesos no formalizados.
Avance Incipiente

5.1.3. Equipamiento (Hardware)

1- Inventario de equipamiento
Observación: 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.
Recomendación: 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.
Comentario de la AGC: El Manual de Procedimientos incluye un proceso formal de inventario del hardware. Se realizó un inventario usando GLPI (verificado uso in situ). El equipamiento está identificado con código de barras

para el seguimiento de inventario. La Resolución Nº47/ERSP/12 del 27/04/2012 aprueba el inventario de hardware.
Avance Satisfactorio Se resolvió la observación

5.1.4. Programas (Software)

1- Control de Software Instalado:
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se constató la existencia de un inventario general del software y de las licencias del organismo. Además, se realizó un inventario por puestos.
Avance Satisfactorio Se resolvió la observación

5.1.5. Red de datos

1- Documentación de la red de datos
Observación: 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).
Recomendación: 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.
Comentario de la AGC: El Ente elaboró y presentó un mapa físico y lógico de la red de datos.
Avance Satisfactorio Se resolvió la observación

2- Encriptación de información:
Observación: No se utilizan técnicas de encriptación de la información que circula por la red.
Recomendación: 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.
Comentario de la AGC: Instalaron e implementaron software de encriptación (AXCrypt). Además utilizan la encriptación de la información que se pasa al BCBA para el pago de sueldo.
Avance Satisfactorio Se resolvió la observación

3- Monitoreo de red
Observación: 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 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.
Recomendación: 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.
Comentario de la AGC: Utilizan software para monitorear la red (NTop) que cuenta con registro de incidentes.
Avance Satisfactorio Se resolvió la observación

4- Documentación de intentos de acceso indebido
Observación: No se documenta formalmente el seguimiento de los intentos de acceso indebidos.
Recomendación: 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).
Comentario de la AGC: Utilizan software LDAP que valida los accesos y registra los intentos de acceso indebidos.
Avance Satisfactorio Se resolvió la observación

5.1.6. Continuidad de la operación

1- Procedimientos de resguardo de la información
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se dictó una norma que formaliza el procedimiento "Manual de Políticas y Normas de seguridad informática" (Res.Nº 8 del 2007 del 29/01/2007 publicado en el BOCBA Nº 2629 del 21/02/2007). También el Manual de Procedimientos formaliza este proceso. Se verificó la aplicación de las normas.
Avance Satisfactorio Se resolvió la observación

2- Copia de respaldo en sede externa
Observación: Los procedimientos de copia y resguardo de datos actualmente en uso, no incluyen copia en sede externa.
Recomendación: 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.
Comentario de la AGC: Se dictó una norma que formaliza el procedimiento "Manual de Políticas y Normas de seguridad informática". Se hace back up en disco portable, se lleva el mismo a otro piso (PB) distinto de la sede de la Sala de servidores (piso 9). Se guarda el disco en caja fuerte PB.
Avance Satisfactorio Se resolvió la observación

3- Procedimientos de recuperación de la información
Observación: No se dispone de un procedimiento formal de recuperación de datos y archivos.
Recomendación: 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.
Comentario de la AGC: Se realizan pruebas formales y se las documenta.
Avance Satisfactorio Se resolvió la observación

4- Plan de Contingencias, Plan de Evacuación y Plan de Recuperación de Desastres
Observación: No se cuenta con un plan de contingencias, un plan de evacuación y un plan de recuperación de desastres y sus correspondientes pruebas.
Recomendación: 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.
Comentario de la AGC: Se elaboró un Plan de Evacuación aprobado por Defensa Civil. El organismo adhirió al Plan de Evacuación General del Edificio, es un plan que realiza simulacros formales de pruebas. Se mantiene observación ya que falta elaborar los otros planes solicitados usando como guía las normas de seguridad informática del organismo antes mencionada.
Avance Incipiente

5- Servidores alternativos
Observación: No se dispone de equipamiento alternativo (servidores de respaldo, propios o por convenios formales con terceros) para el procesamiento y las telecomunicaciones.
Recomendación: 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.
Comentario de la AGC: Se incorporó un servidor alternativo en la PB del edificio. Falta la elaboración de un plan que establezca los procedimientos para la puesta en marcha del proceso de uso.
Avance Incipiente

5.1.7. Seguridad lógica

1- Clasificación de la información
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Realizaron un clasificación formalizada en el Acta del Directorio Nº 494 Anexo II
Avance Satisfactorio Se resolvió la observación

2- Definición del dueño de los datos
Observación: 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.
Recomendación: Definir 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.
Comentario de la AGC: Realizaron una definición de los dueños de los datos formalizada en el Acta del Directorio Nº 494 Anexo II
Avance Satisfactorio Se resolvió la observación

3- Procedimiento de definición de Perfiles de Usuarios
Observación: 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.
Recomendación: 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.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo II
Avance Satisfactorio Se resolvió la observación

4- Procedimiento de Altas de Usuarios
Observación: 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.
Recomendación: Confeccionar e implementar un procedimiento formal de altas de usuario.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

5- Procedimiento de Bajas de Usuarios
Observación: Inexistencia de un procedimiento formal para la baja de usuarios.
Recomendación: Confeccionar e implementar un procedimiento formal de bajas de usuario.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

6- Compromiso de confidencialidad y uso responsable
Observación: El compromiso de confidencialidad para el tratamiento reservado de la información confidencial no cuenta con la aprobación formal de las autoridades.
Recomendación: 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.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

7- Compromiso de uso responsable de la red, de la conexión Internet y del correo electrónico que provee el organismo
Observación: 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.
Recomendación: 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.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

8- Claves compartidas
Observación: 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.

Recomendación: 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.
Comentario de la AGC: No se detectaron usos de claves compartidas. Se sugiere mantener la instrucción a los usuarios sobre las buenas prácticas de las medidas de seguridad. La prohibición de uso de claves compartidas quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

9- Usuario Administrador
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se cambiaron los usuarios y claves del administrador. Se implementaron sobres cerrados y firmados con las claves de los administradores.
Avance Satisfactorio Se resolvió la observación

10- Características mínimas en la clave
Observación: No se encuentran normadas formalmente las características mínimas que deben respetar las claves de acceso y autenticación de los usuarios.
Recomendación: Normar las características que se determinen para las claves de seguridad como período de caducidad, cantidad y tipo de caracteres

requeridos, y otros.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

11- Intentos de Acceso Fallidos
Observación: 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.
Recomendación: Formalizar las condiciones del bloqueo y desbloqueo por intentos de acceso fallidos. Definir el procedimiento de desbloqueo y las autorizaciones y sus responsables.
Comentario de la AGC: El procedimiento quedó formalizado en el Acta del Directorio Nº 494 Anexo I
Avance Satisfactorio Se resolvió la observación

12- Procedimientos ante alarmas por virus
Observación: Se carece de un procedimiento formal y sistemático que establezca los pasos y las acciones en caso de alarma por virus.
Recomendación: 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.
Comentario de la AGC: No presenta ninguna evidencia de procedimientos formales de acciones por alarmas por virus.
Avance No Satisfactorio Se mantiene la observación

13- Medidas antivirus

Observación: 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.
Recomendación: 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).
Comentario de la AGC: Se constató un antivirus no corporativo, es individual y está instalado en los puestos, también poseen antivirus en los servidores de correo. Hay otras medidas de seguridad complementarias. Sin embargo, la falta de antivirus corporativo pone en riesgo al total de la red ya que cada puesto tiene que realizar sus actualizaciones en lugar de poder automatizar y garantizar la función.
Avance Incipiente

14- Procedimiento de puesta en producción
Observación: No existen procedimientos de control para garantizar el efectivo y correcto control de cambios cuando corresponde.
Recomendación: 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.
Comentario de la AGC: La Res. Nº106 del 2008 fue actualizada por el ACTA Nº497 Anexo I pero estos procedimientos no fueron puestos en marcha por la organización.
Avance Incipiente

15- Acceso y modificación de los datos por fuera del aplicativo
Observación: No se encuentra debidamente restringido el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción.
Recomendación: 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.
Comentario de la AGC: Llevan log de transacciones en aplicaciones críticas. No se puede acceder a los datos en ambiente de producción.
Avance Satisfactorio Se resolvió la observación

16- Seguridad en los servidores abiertos a Internet
Observación: 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.
Recomendación: 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.
Avance No Satisfactorio Se mantiene la observación

5.1.8. Seguridad Física

1- Seguridad en los accesos físicos
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se formalizan los accesos mediante el Acta de Directorio Nº497.
Avance Satisfactorio Se resolvió la observación

2- Resguardo de documentación
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se verificó la guarda adecuada de la documentación.
Avance Satisfactorio Se resolvió la observación

3- Procedimiento de depuración de la información
Observación: 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.
Recomendación: 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.
Comentario de la AGC: El procedimiento fue formalizado por el Acta de Directorio Nº494.
Avance Satisfactorio Se resolvió la observación

4- Salidas, luces y señalización de Emergencia
Observación: 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
Recomendación: 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.
Comentario de la AGC: Se instaló señalización que fue verificada y salidas de emergencia con plano de evacuación en cada piso.
Avance Satisfactorio Se resolvió la observación

5- Elementos de seguridad
Observación: 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.
Recomendación: Revisar y completar los elementos de seguridad del edificio, especialmente en la sala de servidores.
Comentario de la AGC: Se verificó la existencia de matafuegos y sensores de humo en la sala de servidores.
Avance Satisfactorio Se resolvió la observación

6- Fuente alternativa de energía de la red de datos
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se constató la existencia de pruebas rutinarias formales y documentadas.
Avance Satisfactorio Se resolvió la observación

5.1.9. Sistemas aplicativos

1- Documentación
Observación: En el sistema de seguimiento de expedientes la documentación es inexistente.

Recomendación: 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.
Comentario de la AGC: El sistema que dio origen a esta observación fue sustituido por el SUCE que cuenta con documentación adecuada. Res. N° 259/ERSP/10
Avance Satisfactorio Se resolvió la observación

2- Registro de cambios
Observación: El sistema Waldbott no cuenta con reportes (log) que permitan identificar unívocamente al autor de acciones o cambios dentro del Sistema de modo que se pueda determinar la responsabilidad por acciones en caso de necesidad.
Recomendación: 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.
Comentario de la AGC: Se implementó el log transaccional de Waldbott
Avance Satisfactorio Se resolvió la observación

3- Sistema integrador
Observación: No se cuenta con un sistema integrador de la información para toma de decisiones.
Recomendación: 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.
Comentario de la AGC: Sin avances al respecto
Avance No Satisfactorio Se mantiene la observación

4- Integración con los Sistemas del GCBA
Observación: 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).
Recomendación: 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.
Comentario de la AGC: Se adhirió a sistemas centrales del GCBA: SADE para las entradas y salidas de documentación del Organismo. El SIGAF se encuentra en uso. Hay integración a la Red Man.
Avance Satisfactorio Se resolvió la observación

5- Falta de estándares de metodología
Observación: 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.
Recomendación: Incorporar estándares de metodología para el desarrollo y la adquisición de aplicativos.
Comentario de la AGC: Sin avances al respecto
Avance No Satisfactorio Se mantiene la observación

5.1.10. Internet

1- Falta de especificidad en el dominio
Observación: 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.

Recomendación: 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.
Comentario de la AGC: Han registrado nuevos dominios. Fue verificado y estos se encuentran a la espera de confirmación con NIC.
Avance Satisfactorio Se resolvió la observación

2- Persona responsable del dominio
Observación: 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.
Recomendación: Se sugiere que el responsable 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.
Comentario del Ente: El Ente informa que ha registrado en el NIC los cambios correspondientes en el responsable del dominio.
Comentario de la AGC: Se verificaron los cambios realizados en el NIC
Avance Satisfactorio Se resolvió la observación

5.2- Comunicaciones y conectividad externa:

5.2.1. Aspectos Generales:

1- Contratación del servicio telefónico
Observación: 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.
Recomendación: 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 específicas del organismo.
Comentario de la AGC: Sin cambios al respecto.
Avance No Satisfactorio Se mantiene la observación

2- Líneas analógicas
Observación: El mantener líneas analógicas innecesarias deriva en gastos indebidos ya que son recursos que se abonan y podrían reemplazarse con la utilización eficiente de la trama. Además se dificulta el control y el uso de las comunicaciones telefónicas.
Recomendación: 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.
Comentario de la AGC: Se conserva un solo ADSL como respaldo a la conexión de Internet contratada. Las líneas analógicas fueron distribuidas en los pisos para el caso de un fallo en el suministro de energía eléctrica.

Avance Satisfactorio Se resolvió la observación

3- Evaluación sistemática de las comunicaciones
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Falta realizar y formalizar el procedimiento. Sin avances al respecto.
Avance No Satisfactorio Se mantiene la observación

4- Administración Informal
Observación: 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 están unificadas en la práctica, aunque no se encuentra formalizada.
Recomendación: 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.
Comentario de la AGC: Se encuentra unificada la responsabilidad y la administración. Formalizada por la Res. del Directorio Nº112 donde se fijan las misiones y funciones del área y nivel de responsabilidad
Avance Satisfactorio Se resolvió la observación

5- Conectividad Internet
Observación: 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.
Recomendación: 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 Cable modem) ya que estas están destinadas al uso hogareño y son inadecuadas para las necesidades del organismo.
Comentario de la AGC: Hay banda ancha corporativa. Se eliminaron las ADSL no utilizadas.
Avance Satisfactorio Se resolvió la observación

6- Correo electrónico externo
Observación: 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.

Recomendación: 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.
Comentario de la AGC: Se constató la existencia de correo electrónico (mail Server) propio administrado por el organismo.
Avance Satisfactorio Se resolvió la observación

5.2.2. Seguridad lógica:

1- Procedimiento formal para configurar y administrar el servicio telefónico
Observación: 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
Recomendación: 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.
Comentario de la AGC: El procedimiento está formalizado por el Acta del Directorio Nº497. Los permisos de utilización de cada usuario están formalizados en el formulario unificado de Alta Baja y Modificación (ABM) en uso.
Avance Satisfactorio Se resolvió la observación

2- Acceso lógico a la central
Observación: No se modifican las claves de acceso a la central cada vez que terceros efectúan una modificación en la configuración de la misma.
Recomendación: 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.
Comentario de la AGC: Se constató la existencia de sobres cerrados con las claves.
Avance Satisfactorio Se resolvió la observación

3- Software de administración de la central
Observación: El organismo no cuenta con el software que permite configurar la Central telefónica.
Recomendación: 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.
Comentario de la AGC: Tienen el software para administrar la Central de Telefonía, y personal capacitado que se ocupa de la configuración y administración.
Avance Satisfactorio Se resolvió la observación

4- Cursos de capacitación para la programación de la central
Observación: El personal del organismo no se encuentra capacitado para programar y/o configurar la Central telefónica.
Recomendación: 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.
Comentario de la AGC: Se dispone del software para administrar la Central de Telefonía y personal capacitado que se ocupa de la configuración y

administración.
Avance Satisfactorio Se resolvió la observación

5.2.3. Seguridad física:

1-Acceso físico a la central no formalizado
Observación: 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.
Recomendación: 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.
Comentario de la AGC: Se verificó el cambio de la central a un lugar de acceso restringido.
Avance Satisfactorio Se resolvió la observación

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

Recomendación: 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.
Comentario de la AGC: Se verificó el cambio de la UPS a un lugar de acceso restringido y se verificaron las pruebas de funcionamiento.
Avance Satisfactorio Se resolvió la observación

3- Plan de contingencia (comunicaciones y conectividad)
Observación: Inexistencia de un plan de contingencia formal ni informal para las comunicaciones y la conectividad Internet.
Recomendación: 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.
Comentario de la AGC: Se constató la existencia de procedimientos sin formalizar que no constituyen un Plan de Contingencia de las comunicaciones e Internet.

Avance No Satisfactorio Se mantiene la observación

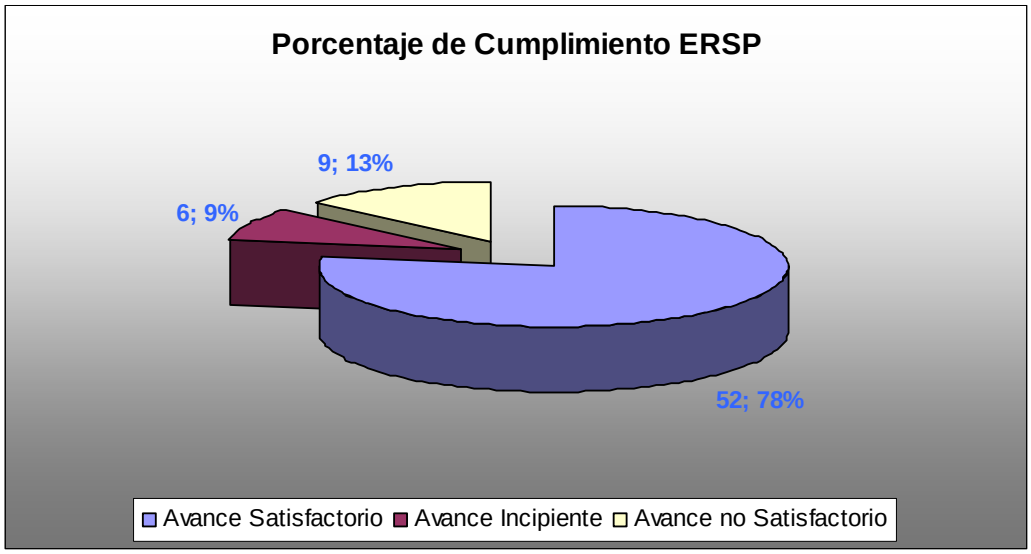
4- Plan de recuperación de desastre
Observación: Inexistencia de un plan de recuperación de desastre para las comunicaciones y conectividad.
Recomendación: Elaborar un plan de recuperación de desastres y realizar pruebas y verificaciones periódicas del mismo. El plan de recuperación de desastres debe 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.
Avance No Satisfactorio Se mantiene la observación

VI CONCLUSIONES

El informe cuyo seguimiento se efectuó consistió en un exhaustivo análisis de las TICs del Ente.

Se resolvieron 52 de un total de 67 observaciones del informe 5.04.32. De las 15 restantes, 6 tuvieron avances o resoluciones parciales (avances incipientes) quedando 9 observaciones sin resolver o sin mejoras (avances no satisfactorios).

Avance Satisfactorio	Avance Incipiente	Avance no Satisfactorio
52	**6**	**9**



El Organismo había elaborado dos normas internas: El "Manual de Políticas de Seguridad Informática" en el 2007 y el "Manual de Procedimientos del Ente Único Regulador de los Servicios Públicos de la CABA" en el 2008. El Manual de Políticas de Seguridad estaba exclusivamente referido al área de Sistemas del Organismo, el Manual de Procedimientos, en cambio contenía procedimientos propios del circuito administrativo y algunos procedimientos referidos al área de sistemas.

Ambas normas internas habían tenido aplicación parcial y en algunos casos nula hasta el comienzo de la presente auditoría de seguimiento.

Sin embargo, en el transcurso de la presente auditoría el Organismo produjo cambios en su organigrama que resultaron beneficiosos para el desarrollo de las tareas de resolución de observaciones:

El Departamento de Sistemas pasó a depender del Área de Innovación Tecnológica, que reporta a la Gerencia de Proyectos, abandonando su anterior ubicación en la Dirección de Administración (lo cual había sido observado).

La nueva conducción del área y la incorporación de agentes con experiencia impulsaron la resolución de una gran parte de las observaciones durante el desarrollo de las tareas de auditoría. A ese efecto tomaron como base de trabajo las normas internas preexistentes y aplicaron muchas de ellas, también formalizaron procesos que existían como rutinas informales. Además, sumaron medidas de seguridad física y lógica que habían sido extensamente observadas en el informe mencionado anteriormente.

Entre las tareas pendientes que están referidas a observaciones que no han registrado ningún grado de avance, merecen un comentario las referidas a la falta de Planes de Contingencia y Planes de Recuperación de Desastres, tanto

de las comunicaciones y la conectividad como de la red y los servidores propios.

Estos planes y sus pruebas periódicas revisten particular importancia ya que son los que garantizan la continuidad de los servicios frente a los distintos eventos que puedan presentarse.

ANEXO
NORMAS

1. Normas Básicas de Auditoría Externa de la AGCBA
2. Normas Básicas de Auditoría de Sistemas de la AGCBA.

3. Manual COBIT IV. (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Association. Capítulo Buenos Aires.

Supletoriamente se utilizaron:

1. Las normas y recomendaciones de seguridad establecidas por la ASI (Ex DGEySI).
2. Manual de auditoría Informática de la Sindicatura General de la Nación, SIGEN.
3. Manual CISA. (Manual de Control Information System Auditor)

Normas del Ente:

1. Res. CABA Nº8/2007 "Manual de Políticas de Seguridad Informática" publicada en el BOCBA Nº2629 del 21/02/2007.

2. Res.Nº 106 EURSPCABA/08 "Manual de Procedimientos del Ente Único Regulador de los Servicios Públicos de la CABA" publicado en el BOCBA Nº 3015 del 16/9/2008.