INFORME FINAL DE AUDITORÍA

Código de proyecto:3.07.02.00.02

Nombre de Proyecto: Atención Médica de Emergencia. Auditoría de Sistemas. Año 2002.

Buenos Aires, 20 de junio de 2003

CODIGO DEL PROYECTO: 3.07.02.00.02

NOMBRE DEL PROYECTO: Atención Médica de Emergencia. Auditoría de Sistemas.

PERÍODO BAJO EXAMEN: Marzo - Junio de 2003

FECHA DE PRESENTACIÓN DEL INFORME: 22/06/2003

EQUIPO DESIGNADO:

Coordinador	**:** *Recasens José*
Auditores	**:** *Zancada Héctor*
	: *Bella Rodolfo*
	: *Bordoy Martín*
	: *Mara Melul*
	: *Carmen Fernández*

OBJETIVO: Examinar 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 digitales en el ámbito del SAME.

Informe Final de Auditoria

Proyecto Nº 3.07.02.00.02

A la Señora

Presidente de la Legislatura

De la Ciudad Autónoma de Buenos Aires

Lic. María Cecilia Felgueras
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 24.156 (AGN) la Auditoria General de la Ciudad procedió a efectuar un examen en el ámbito de Sistema de Atención Médica de Emergencias con el siguiente objeto:

I.-OBJETO DE LA AUDITORIA

Auditoria de la seguridad del 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 SAME.

II.-ALCANCE

Esta auditoria se efectuó sobre la situación vigente al momento de su realización, que comprendió el período de Marzo- Junio del año 2003.

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

Complementariamente 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 CISSA Edición 2002.
- Guía de Aproximación a la Seguridad de los Sistemas de Información (MAGERIT versión 1.0) del Ministerio de Administraciones Públicas de España.

- Manual de apoyo al curso “Seguridad Informática en Nuevas Instalaciones”, dictado del 24/7/2000 al 28/7/2000 en la Escuela de Ciencias Informáticas (ECI) de la Facultad de Ciencias Exactas y Naturales de la UBA por el Dr. Manuel Medina de la Universidad Politécnica de Cataluña, Barcelona.

- Manual de COBIT.

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.

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 del área.
- Se efectuaron verificaciones “in situ” de la Instalación del equipamiento informático y de las comunicaciones.
- Se verificó la documentación de los sistemas.
- Se efectuó el análisis de la documentación provista por el área.

III.- LIMITACIONES AL ALCANCE:

Los siguientes factores limitaron la tarea de auditoria:
Documentación incompleta debida a la respuesta fuera de término a la nota dirigida a la Dirección General de Sistemas para la Salud (en adelante DGSIS) con fecha 18 de marzo de 2003 AGCBA nro 638/03 y su reiteración del 20 de mayo de 2003 AGCBA nro 0194/03. -
Diferencias entre la estructura formal y la real.-

Carencia de normas y procedimientos escritos.-

IV.- ACLARACIONES PREVIAS:

El Departamento de Sistemas del SAME depende de la Dirección General de Sistemas de Información de Salud (DGSIS) la cual forma parte de la Secretaria de Salud desde noviembre del 2001. Anteriormente constituía una de las dependencias del SAME. Tiene una antigüedad de cinco años.
Dispone de una dotación de cuatro personas que tienen, entre otras tareas, la de brindar soporte al usuario, desarrollar y mantener los sistemas informáticos y de comunicación digital, excluidos los sistemas de comunicación de voz.
El SAME posee un parque de cincuenta computadoras personales que se encuentran distribuidas de la siguiente forma:

- El Departamento de Sistemas cuenta de dos computadores personales. Estas computadoras son utilizadas para desarrollar el Sistema de Administración de Emergencias.
    - El área administrativa tiene asignadas 33 máquinas personales (PC) de las cuales 2 no se encuentran conectadas en la red.
- El área operativa dispone de 17 computadoras personales distribuidas del siguiente modo:
    - 4 Fueron prestadas al Hospital Rivadavia.
    - 2 Fueron prestadas al Hospital Vélez Sarsfield.
    - 2 Se encuentran destinadas al desarrollo del sistema de Administración de Emergencias.
    - 4 Son utilizadas para capacitar a los futuros operadores del sistema de Administración de Emergencias de estos 2 serán utilizadas como Server, en las que residirá el sistema de Administración de Emergencias según lo manifestado por el personal del área.
    - 1 Fue facilitada en forma temporaria al personal de Auditoria General de la Ciudad de Buenos Aires.
    - 1 Se encuentra en la Dirección.

- Un equipo que es utilizado actualmente en el sector operativo para las pruebas del sistema de Administración de Emergencias.

El área operativa del SAME cuenta con 1 Switch de 16 bocas para interconectar el equipamiento mencionado.
En el área administrativa la comunicación de datos se efectúa a través de los siguientes dispositivos:

- 1 Hub de 8 bocas
- 1 Hub de 16 bocas
- 1 Hub de 24 bocas
- 1 Pachera
- 1 Router Cisco 800 con TDU

El equipamiento es utilizado con software local (herramientas de oficina) ya que prácticamente no hay software específico para las tareas del área.

Se encuentra demorada la implementación, que estaba prevista inicialmente para Abril de 2003, de un aplicativo desarrollado por la DGSIS (Dirección General de Sistemas para la Salud) para la administración de emergencias.

V -OBSERVACIONES:

1-Observaciones Generales.

1.1-No se encuentran informatizadas las funciones principales del SAME.

El SAME posee equipamiento y una red de comunicación de información interna que se encuentran subutilizados ya que prácticamente no hay sistemas específicos instalados en la dependencia a pesar de que el Departamento de Sistemas tiene cinco años de existencia y que estos desarrollos constituyen parte de sus tareas y funciones.
El SAME cuenta con una red interna de 50 PC, 33 de las cuales se encuentran en la administración. La mayoría de los equipos están intercomunicados. Es especialmente llamativa la falta de soporte informático a la logística, la administración y el registro de las emergencias que constituyen la esencia del organismo. Esto afecta la eficiencia y la agilidad en la operación en un área donde la rapidez y la oportunidad son factores críticos.

1.2-Evaluación económica para el procesamiento de datos.

No se encuentra justificada la decisión de la DGSIS de distribuir procesamiento instalando un centro de cómputos en el SAME.
La constitución de numerosos centros de cómputos a nivel de Dirección General es antieconómica ya que implica la necesidad de dotar de medidas de seguridad y edilicias especiales en cada locación, generar y operar procedimientos redundantes, mantener equipos duplicados, y otros que se evitarían con el procesamiento centralizado, el que resulta posible dada la existencia de suficiente capacidad de interconexión en el ámbito de la Ciudad de Buenos Aires.

1.3-Las herramientas utilizadas en el desarrollo no se encuadran dentro de una política informática.

Las herramientas utilizadas son del tipo “software libre”, o sea software que es de libre disponibilidad y acceso. Esta decisión no se encuentra respaldada por un estudio que la justifique ya que si bien el software de este tipo es generalmente gratuito, no lo es la capacitación, su mantenimiento y soporte.
El uso de este tipo de herramientas no facilita la integración de los sistemas así como tampoco de la información resultando de dudosa conveniencia. Resulta poco recomendable su uso sin que la misma constituya una política del área previa evaluación de las ventajas de su utilización, en especial para un proyecto crítico como la Administración de Emergencias de SAME.

1.4-Nuevo Sistema para emergencias de Same.

El nuevo sistema informático **Registro de Atención Médica de Emergencias**, cuya implantación se ha retrasado (estaba prevista para mayo de 2003 según lo manifestado por la DGSIS) no fue desarrollado con una adecuada metodología. En consecuencia carece de elementos fundamentales para un desarrollo de esta envergadura y criticidad, y se incumplió con las etapas claves de las buenas prácticas en la materia.
En efecto, no se dispone de un plan conformado formalmente, el diseño no fue aprobado por el área usuaria (la que tampoco participó en su especificación), no se prevé su integración con otras aplicaciones, ni mecanismos para el mantenimiento de la continuidad de la operación, y carece de documentación, entre otros aspectos claves.

1.5-Organización.

No se encuentra organizada el área para la futura operación del Sistema mencionado precedentemente.
El área de sistemas actual no se encuentra totalmente formalizada y no hay normas y procedimientos esenciales para su operación así como tampoco está definido quién las ejecutará. Estas normas están referidas a seguridad, continuidad, operación, mantenimiento, contingencia y soporte entre otros.

1.6-Comunicaciones del Sistema para emergencias.

El Sistema de comunicación utilizado para la asignación de las emergencias a las ambulancias es ineficiente y obsoleto.
El sistema actual carece de integración y desaprovecha las posibilidades de la tecnología. El procedimiento actual requiere de intercambio manual de información escrita, tareas redundantes y consultas verbales para la asignación del móvil. Esto provoca ineficiencia y pérdidas de tiempo que pueden demorar la respuesta de este servicio crítico. En la actualidad la tecnología disponible permite la interccomunicación digital y a través de ella la localización del móvil y la asignación automática, semiautomática o manual del mismo en función de criterios predeterminados en el sistema. Disponen de este tipo de dispositivos firmas de taxis de la ciudad.

1.7-Fallas en la continuidad del Sistema de grabación.

No existen mecanismos que aseguren la continuidad de los sistemas de grabación de voz, debido a que el mismo se puede discontinuar por múltiples factores, como por ejemplo fallas en la central, problemas en equipo de aire acondicionado que generan fallas en la central, problemas en el suministro de energía eléctrica y otros.
La importancia de este sistema radica en que constituye la prueba más importante para la reconstrucción de la comunicación en caso de que sea requerido legalmente.

1.8-Reportes de la Central Telefónica.

Existe una subutilización de esta información, que no es emitida y revisada sistemáticamente.
La central telefónica genera en forma automática reportes estadísticos y / o de seguimiento de llamados. Su análisis permitiría conocer la cantidad de llamadas perdidas, el tiempo promedio de espera y otras variables que permitirían evaluar la eficiencia del servicio del centro de llamados.

1.9 Mesa de Entrada

Se utilizan desarrollos propios para cubrir funciones que son provistas a nivel central sin que se justifique la razón de esta superposición.

- La mesa de entrada utiliza un sistema de desarrollo propio para el registro y seguimiento de expedientes. (Sistema que no es confiable por su inestabilidad e inconsistencia en la información que almacena).
- Hay usuarios del organismo que utilizan un correo interno ubicado en el Departamento de Sistematización de Datos.

Actualmente el Gobierno de la Ciudad Autónoma de Buenos Aires cuenta con el sistema SUME (Sistema Único de Mesa de Entrada) implementado sobre la red MAN, a la cual tienen acceso todos los organismos pertenecientes a la ciudad y también provee del servicio de correo centralizado. La dirección de Sistemas de Salud informó que el servicio prestado por la DGSI no es satisfactorio ya que restringe en exceso el otorgamiento de cuentas.

Esta situación nos lleva a tener duplicado servidores, estructuras de soporte y otros elementos innecesariamente, aumentando de esta manera los costos de los servicios.

1.10 Falta de una página web.

El SAME no cuenta con información en la WEB del Gobierno de la Ciudad de Buenos Aires. La falta de información en la Web impide la divulgación por ese medio de los servicios que el organismo brinda a la comunidad, su alcance, modalidad y forma de acceso al mismo.
Por otra parte existe una página no oficial SAME que no se encuentra disponible y que posee referencias personales.

2-Organización y personal.

2.1-Estructura de la Organización.

Se constató la existencia de una estructura real que difiere de la estructura formal. En dicho departamento se encuentran desarrollando tareas dos personas que no han sido nombradas formalmente para las funciones que actualmente desempeñan.
Esta situación trae como consecuencia que los agentes no tengan definidas funciones y responsabilidades formales lo que hace que sus obligaciones no tengan un alcance preciso para las tareas que ejecutan y el área en la que se desempeñan.

2.2-Plan de capacitación de los agentes.

No hay una política de capacitación de los agentes que tienen a su cargo la administración y desarrollo de las aplicaciones y de la red.
Los sistemas y las redes van creciendo en complejidad sin el adecuado nivel de entrenamiento de sus responsables, al tiempo que continuamente se producen cambios tecnológicos que obligan a una actualización permanente.
La falta de capacitación puede afectar la implementación de mejoras y actualizaciones en la red y los sistemas, y reducir el aprovechamiento de las tecnologías informáticas.

2.3-Condiciones ambientales y laborales.

Las condiciones ambientales y laborales del departamento de informatización de datos no son las apropiadas.
El personal desarrolla sus tareas en el lugar destinado al archivo de planillones, (registros manuales de atención médica con ambulancia). El espacio es reducido y falto de limpieza (Es un área de paso que siempre se encuentra abierta). A esto se le suma el constante ruido producido por los vehículos que circulan sobre la autopista 25 de Mayo la cual se encuentra a nivel y a unos pocos metros de la ventana de dicha oficina. Esto afecta negativamente el rendimiento del personal.

3-Hardware y software.

3.1-Equipamiento Informático.

No se lleva un control adecuado del equipamiento informático existente.

- No se dispone de un inventario detallado del parque informático, lo que ocasiona el desconocimiento de la configuración de los equipos y por consiguiente la imposibilidad de determinar alteraciones y/o faltantes en los mismos.

- No se halló el registro formal del movimiento del equipamiento informático que fue transferido en calidad de préstamo a los hospitales (6 equipos).

Esto implica la falta de control formal sobre el movimiento de bienes lo que evidencia ineficiencia en el resguardo y control de los activos de la ciudad.

3.2-Control del Software Instalado.

No se lleva el inventario y el control del software instalado sobre los equipos de computación.
La falta de registro del software instalado implica la imposibilidad de su adecuado resguardo y protección. Asimismo implica el riesgo de que se ingresen virus por instalación de programas infectados o que se afecte la estabilidad por la utilización de software inapropiado.

4-Red de comunicaciones.

4.1-Documentación.

No se dispone de un mapa lógico y el mapa físico de la red de comunicación de datos es incompleto (inespecificidad de tipo de cableado, cantidad de líneas, cantidad y tipo de bocas identificación precisa de cada dispositivo y otros) lo que implica la imposibilidad de conocer la forma de operar detallada de la misma y el flujo de la información entre sus nodos. Esto dificulta el mantenimiento, la detección y solución de problemas. Asimismo dificulta el análisis y la evaluación de posibles ampliaciones futuras.

4.2-Arquitectura.

La red interna no dispone de un equipo con mayor jerarquía que el resto, arquitectura cliente servidor, lo que limita la administración de la seguridad, la adecuada administración de recursos y la operación de la red de acuerdo a buenas prácticas y las reglas del arte en la materia.

5-Seguridad Física

5.1-Plan de contingencia, plan de evacuación y plan de recuperación de desastre.

No existe un Plan de Contingencia que indique las acciones y procedimientos que garanticen la continuidad de los servicios de procesamiento de datos frente a situaciones imprevistas y de desastre. Tampoco se dispone el plan que permita retornar al servicio normal luego de la contingencia. (Plan de recuperación de desastre).
Asimismo, se carece de un Plan de Evacuación y de sus prácticas periódicas.
Si se produjera un desastre, la falta de planificación reflejada en la carencia de estos planes pone en riesgo las vidas humanas, la información y la continuidad de los procesos.

5.2-Salidas, luces y señalización de Emergencia.

El escape en casos de emergencia se encuentra mal indicado y obstruido. Esto implica el riesgo de vida para las personas que trabajan en el edificio.

- Se pudo constatar que las tres salidas de emergencia ubicadas en el primero y en el segundo piso no poseen el mecanismo de apertura apropiado, aberturas de pánico, y se encuentran cerradas con llave y provistas de rejas. Estas salidas desembocan por medio de una escalera a la cochera del edificio en la cual el escape se dificulta por la presencia de los móviles de la dependencia.

- Dos de las tres salidas utilizan una escalera exterior la que se encuentra en muy mal estado por falta de mantenimiento, por medio de la misma se arriba a un patio interior el cual se encuentra obstruido con diferentes elementos, no permitiéndose así el paso hacia puerta de la cochera previamente mencionada. Por último esta puerta se encuentra cerrada por medio de un pasador ubicado del lado de adentro de la cochera, siendo imposible su abertura desde el patio interno.
- Actualmente, no existe señalización ni luces de emergencia que conduzcan a las salidas de emergencia del edificio, y por las razones anteriormente mencionadas las mismas no pueden ser utilizadas.

5.3-Elementos de seguridad del edificio.

Se comprobó la falta de elementos de seguridad.
En el caso de que se inicie un incendio se corre el riesgo de no poder controlarlo por no contar con los medios de seguridad suficientes como por ejemplo algunos matafuegos, mangueras y otros. También se constató que algunos de los matafuegos existentes estaban descargados.

5.4-Red eléctrica.

No existe una red eléctrica que alimente en forma exclusiva la totalidad de la red de datos.
La misma red eléctrica es utilizada para los datos y para artefactos de uso cotidiano (calentadores, estufas de cuarzo, etc.); consecuentemente, se generan picos de tensión y recalentamiento de la línea por sobrecarga.
Esto incrementa el riesgo de incendios y de caídas en la red e interrupción en las tareas de procesamiento, con pérdida de información y de tiempo por parte de los usuarios de la red por suspensión del servicio.

5.5-Gas Halón.

Se pudo constatar la existencia de una instalación para combatir incendios basado en gas Halón. Los agentes del organismo manifestaron que desconocían su existencia y modus operandi.
La comunidad científica mundial determinó que dicho gas destruye la capa de ozono de la atmósfera en proporciones alarmantes con graves consecuencias para la humanidad. Patrocinado por la ONU, en 1987 se firmó el Protocolo de Montreal, acuerdo en el cual se prohibió la fabricación de gas halón desde enero de 1994.

5.6-Resguardo de las Planillas de Registro de Atención Médica de Emergencias.

Las planillas de registro de atención médica de emergencias se almacenan en el ambiente contiguo a la cocina. Junto a los estantes con papel sobresale la presencia de una instalación precaria de gas.
Está situación incrementa el riesgo de incendios por la gran cantidad de papel depositado en ese lugar.

5.7-Instalación de gas natural.

La instalación de gas antes mencionada no cumple con las especificaciones técnicas establecidas por ENARGAS ya que utiliza cañería de cobre exterior, no permitida en tramos largos.
El incumplimiento de estas normas y especificaciones incurren en un aumento del riesgo de incendio, con posible perdida de vidas, activos e información.

5.8-Fuente alternativa de energía.

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

6-Seguridad Lógica.

6.1-Altas de Usuarios.

No hay procedimientos 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.
La falta de un procedimiento de alta de usuarios perjudica gravemente a la seguridad y confiabilidad de la información de los sistemas.

6.2-Bajas de Usuarios.

No existe un procedimiento de baja de usuarios.
Esto puede implicar que usuarios que dejan de pertenecer a la institución ingresen a los sistemas de información y provoquen daños o tengan acceso a información privada. Asimismo implica el riesgo de que otro usuario utilice la clave del agente dado de baja con lo que se habilita el repudio de todo lo actuado.

6.3-Perfiles de Usuarios.

No existen procedimientos para la definición de perfiles de usuarios.
Esto impide que se pueda definir con precisión el alcance del accionar del nuevo usuario en el momento de solicitar el alta, lo que afecta el control sobre los accesos y la seguridad de la información.

6.4-Bloqueo por Intentos de Acceso Fallidos.

No existen procedimientos de bloqueo de usuarios por intentos fallidos de acceso a la red y a los sistemas.
La falta de un procedimiento de bloqueo de usuarios por intentos fallidos incrementa la vulnerabilidad de los sistemas, posibilitando el ingreso de usuarios no autorizados.

El ingreso de usuarios no autorizados puede incurrir en daños, pérdida, destrucción o divulgación de información crítica.

6.5-Seguimiento de la Actividad de la Red e Intentos de Acceso Fallidos.

No se halló evidencia de que se efectúe un adecuado seguimiento, sistemático y rutinario, de la actividad de la red ni de los intentos de acceso fallidos a la red.
Lo observado incrementa el riesgo de intrusiones a los equipos y a la información administrada en los mismos.

6.6-División de Funciones.

No hay división de funciones ni control por oposición entre la administración de la seguridad, desarrollo de sistemas y las eventuales tareas de mantenimiento.
Esto implica que todas las responsabilidades sobre la administración de los aplicativos recaen sobre la misma área.
Esta concentración de funciones atenta contra la integridad y confiabilidad de los datos.

6.7-Ambientes de Desarrollo y de Producción.

No hay separación lógica de ambientes ni organizativa entre las funciones de desarrollo de sistemas y producción.
La buena práctica aconseja generar al menos un entorno de desarrollo separado del ambiente de producción, de modo que las modificaciones a los programas puedan compilarse y probarse con un conjunto coherente de datos antes de su traslado al entorno productivo. Esto minimiza el riesgo de problemas emergentes de cambios en el sistema, al mismo tiempo que impide que los desarrolladores accedan a los datos y demás elementos de producción.
La falta de una adecuada segregación de los ambientes mencionados constituye una falla grave de la seguridad, ya que los desarrolladores estarían en condiciones de modificar la información real de los sistemas debido a que disponen de acceso a los datos y conocen con detalle el funcionamiento de la aplicación.

6.8-Requerimientos de modificaciones e innovaciones a los sistemas.

No se ha obtenido evidencia de la existencia de procedimientos que establezcan los pasos a seguir por los usuarios para la solicitud de modificaciones correctivas e incorporación de nuevas funciones a los sistemas.
La ausencia de normas repercute en una disminución de la eficiencia en el mantenimiento y desarrollo de los sistemas, generando un obstáculo para estimar plazos de ejecución, asignar adecuadamente recursos y aprovechar las ventajas de una correcta planificación.

6.9-No existen políticas ni procedimientos de back-up.

No existe una política ni los procedimientos formales para la ejecución de los back up's. Esto implica la ausencia de pasos que especifiquen la acción a seguir,

frecuencia, responsabilidades, y otros que apunten a una correcta ejecución y definición de la responsabilidad en esta tarea. La ausencia de procedimientos de back-up aumenta el riesgo de pérdida de la información en caso de desperfectos o de desastre. Asimismo se demora el retorno del servicio y se requiere de mayor cantidad de horas hombre para su recuperación.

6.10-Falta de ejecución de copias de respaldo.

Los back-up realizados por el organismo son deficientes, incompletos y esporádicos, por consiguiente no brindan garantías en caso de un desastre. El riesgo es el mismo que se señala en el punto anterior.

6.11-Falta de copia de respaldo en sede externa.

El único back up que se realiza en forma sistemática, correspondiente a las cintas con las grabaciones de la voz por computadora, no cuenta con un juego back-up alternativo guardado en sede externa. Esto implica el mismo riesgo señalado en los puntos anteriores.

6.12-Prueba de recupero de datos.

No existe un procedimiento formal de pruebas de recupero de back-up. Asimismo las mismas tampoco se ejecutan de modo informal.
Esto implica el riesgo de no poder efectuar el recupero por fallas no detectadas en las copias de respaldo.

7-Sistema de Registro de Atención Médica de Emergencias.

7.1-Seguridad en el Acceso a los Módulos del Sistema.

Las medidas de seguridad desarrolladas para acceder a los diferentes módulos del sistema por parte de los usuarios son deficientes.
La implementación de perfiles de usuarios por medio de la dirección IP, Internet Protocol, para controlar el acceso a los módulos del sistema es deficiente ya que esta dirección es un atributo del puesto de trabajo y no del usuario, por consiguiente si un usuario cambiase de máquina o la dirección IP de la misma, podría estar accediendo a módulos que no le correspondan.
La ausencia de un control eficiente en el ingreso de los usuarios a los módulos del sistema aumenta el riesgo de pérdida, alteración y revelación de información privada.

7.2-Capacitación de los Usuarios.

Al momento de la verificación y a punto de ser implementado el sistema de registro de atención médica, no fue posible constatar que los agentes involucrados hubieran recibido suficiente capacitación específica en el sistema, necesaria para poder operar el mismo.
La ausencia de capacitación de los usuarios del sistema pone en riesgo la operabilidad del mismo, existiendo la posibilidad de que se afecte directamente la

calidad del servicio prestado. En efecto la capacitación específica para la operación del sistema no es sistemática, no se lleva un registro de usuarios capacitados, no se los califica, y no se efectúa una comprobación de que la capacitación resultó adecuada.

7.3-Modalidad de Implantación del Sistema.

La modalidad elegida consiste en discontinuar el uso de las planillas de registro de atención médica y comenzar a utilizar el sistema informático para tal fin en forma simultánea, no es la más adecuada por la importancia del sistema.
Cualquier falla en el sistema informático imposibilitaría seguir prestando el servicio de atención de emergencias médicas de no contar con un tipo de registro alternativo.

VI-RECOMENDACIONES

1-Aspectos Generales

1.1-Informatizar las principales funciones del SAME brindando apoyatura informática tanto a la administración como a la operación del área.

1.2-Justificar económicamente la decisión y definir el nivel al que se realizará el procesamiento así como también el resto de las tareas necesarias para una adecuada operación.

1.3-Utilizar herramientas de desarrollo y de base encuadradas en una política común para el ámbito del GCBA.

1.4-Incorporar una metodología para el desarrollo de sistemas moderna y eficaz que permita planificar adecuadamente los proyectos.

1.5-Es indispensable definir con claridad la organización para los sistemas de la salud del GCBA. Actualmente no está definido el nivel organizacional en el que se efectuará el procesamiento, el soporte, la mesa de ayuda, la administración de la seguridad, el desarrollo de sistemas, la implementación, la administración de los datos, de las redes, el mantenimiento de equipos y dispositivos de comunicación y otros. Sin este requisito es muy difícil alcanzar resultados satisfactorios en un área de naturaleza compleja como la informática. Esta organización debe definirse considerando el aprovechamiento de la escala que posibilita la dimensión de los servicios que deben prestarse.

1.7-Eliminar las diferentes causas de suspensiones en el sistema de grabación con un plan que paulatinamente permita alcanzar un nivel de riesgo razonable.

1.8-Analizar los reportes disponibles en la central telefónica y definir cuales se emitirán de modo sistemático, produciendo información de control del servicio de call center. Definir asimismo quién recibirá y analizará dicha información y a quién informará acerca de los desvíos y tendencias que surjan de la misma.

1.9-Evaluar y eliminar las superposiciones innecesarias en los servicios.

1.10-Incorporar a la Web de GCBA la información del SAME y gestionar la eliminación del sitio no oficial.

2-Organización y personal.

2.1-Actualizar la estructura organizacional del Departamento de Sistematización de la Información.

2.2-Realizar un plan de capacitación para personal involucrado en el desarrollo, mantenimiento y administración de las aplicaciones y las redes de modo que el mismo se actualice y desarrolle en función de la actividad que debe desarrollar.

2.3-Trasladar al personal a una oficina apropiada para las tareas que desempeñan.

3-Hardware y software.

3.1-Realizar un inventario detallado de los equipos informáticos incluyendo ubicación características, número de serie y otros. Evaluar la ejecución de este control a través de la red de comunicación con software "ad hoc". De adoptarse una solución de este tipo se deberá evaluar el nivel organizacional en el que la misma debe instalarse de forma que la inversión que esta implica se encuentre debidamente aprovechada.

3.2-Controlar estrictamente el software instalado en los equipos de computación.
Este control se puede efectuar a través del software que se instale para la administración de los recursos. El software del equipo administrador puede definir políticas mediante las que se limita la instalación de software indeseable en los equipos bajo su dominio. No se debe permitir que los usuarios instalen software. Esta función debe ser ejecutada centralizadamente desde el nivel que se defina. Se deberá realizar asimismo una revisión del software instalado, removiendo el software que no corresponda por cuestiones de trabajo o legales.

4-Red de comunicaciones.

4.1-Confeccionar el mapa lógico y físico de la red de comunicaciones.

4.2-Incorporar un servidor que permita administrar los recursos físicos, la seguridad y el software de la red.

5-Seguridad Física

5.1-Confeccionar un plan de contingencia y de recupero de desastre apropiado que contemple la posibilidad de tener que abandonar el edificio y operar desde otra sede. En este plan deben incluirse todas las funciones críticas, como el traslado del número de llamada a otra central, el uso de equipos de voz

alternativos, la ubicación de los operadores en otra locación, la operación de los sistemas en la locación alternativa y otros. Este plan debe probarse luego de ser confeccionado.
Asimismo se deberá preparar un plan de evacuación y desarrollar practicas periódicas. Para esta tarea se puede contar con la colaboración de la Dirección General de Defensa Civil.

5.2-Acondicionar y señalizar las salidas de emergencias para que puedan ser utilizadas en caso de emergencia. Capacitar al personal para su uso adecuado en caso de ser necesario.

5.3-Controlar el estado y completar los medios de seguridad faltantes en el edificio.

5.4-Instalar una red eléctrica estabilizada para datos independiente de la red de uso general.

5.5-Realizar una inspección de la instalación de gas Halón determinando si deberá ser reemplazado por otro gas extinguidor de incendios. Capacitar al personal en su modo operación y establecer las normas de seguridad correspondientes. Consultar a la DGDC para la toma de esta decisión.

5.6-Trasladar las planillas de registro de atención médica de emergencia a un lugar seguro para su resguardo, minimizando el riesgo de incendio.

5.7-Regularizar la instalación de gas en la sede.

5.8-Dotar a la instalación de una fuente alternativa de energía.

6-Seguridad Lógica.

6.1-Establecer un procedimiento que detalle los pasos necesarios por parte de los agentes para solicitar el alta como usuario a la red y a los sistemas de información.

6.2-Establecer un procedimiento para dar de baja usuarios. Asimismo establecer los controles pertinentes en conjunto con el área de personal para impedir el acceso a la red y a los sistemas de información por parte usuarios que dejen de pertenecer al organismo.

6.3-Formalizar el procedimiento para la definición de los perfiles de usuarios que precisen los accesos a la información y a los recursos adecuados para cada función. Es necesaria la definición de dueño de datos, clasificación de la información, determinación de necesidad por función y otros.

6.4-Establecer un procedimiento de bloqueo automático a partir de los tres intentos de acceso fallidos a los sistemas de información.

6.5-Confeccionar los procedimientos para el seguimiento de la actividad de la red e intentos de acceso fallidos. Evaluar la incorporación de software para la ejecución de esta función. Definir a qué nivel será efectuada y dentro de qué estructura.

6.6-Realizar una adecuada división de funciones y asignar las responsabilidades concordantemente.

6.7-Separar los ambientes de Desarrollo y Producción. Formalizar los procedimientos para la implantación de nuevas versiones de software en el ambiente de producción.

6.8-Establecer procedimientos para la adecuada respuesta a los requerimientos de modificaciones correctivas e incorporación de funciones nuevas a los sistemas.

6.9-Formalizar un procedimiento de back-up central y sistemático que prevenga adecuadamente del riesgo de perdida de información.

6.10-Ejecutar copias de respaldo sistemáticamente para reducir el riesgo de perdida de información.

6.11-Definir dentro del procedimiento y ejecutar una copia de respaldo adicional efectuando su guarda en sede externa.

6.12- Definir el procedimiento y ejecutar las pruebas de recupero de datos al menos una vez al año.

7-Sistema de Registro de Atención Médica de Emergencias.

7.1-Implementar un método confiable para controlar el acceso de los usuarios a los módulos del sistema.

7.2-Reforzar y asegurar una adecuada capacitación en el uso del sistema a todos los agentes involucrados, evaluando el nivel de aptitud y captación de los contenidos de los cursos de cada uno de ellos.

7.3-Se recomienda mantener el uso de las planillas de registración de emergencias médicas primero en paralelo, de ser posible, y luego para situaciones de contingencia.

VII-CONCLUSIONES

El nivel de servicio informático y de utilización de la red de comunicación de datos en el SAME es bajo según se desprende de las observaciones del presente informe. Por otra parte el nivel de riesgo debido a debilidades en la seguridad de la información y protección de activos informáticos es alto (Criterio de la SIGEN ver Alcance).

Se carece de una estrategia para el desarrollo informático del Sistema de Salud del GCBA que contemple políticas informáticas y administrativas centrales y un modelo de gestión claramente definido así como también de planes formales que aporten una razonable solución a las necesidades existentes en el área.

No se aprovecha la escala ni las comunicaciones existentes. No existe estandarización de las herramientas de desarrollo de aplicativos ni del software de base.

Se debe procurar la integración de la información minimizando las redundancias. Como ejemplo mencionaremos que toda la estadística generada hoy con importante esfuerzo debería ser un subproducto de los sistemas con los que se administra esta información. Esto no solo mejoraría la eficiencia y la oportunidad de la misma sino que también incrementaría la confiabilidad de los informes generados en un adecuado marco de control.

Se deben integrar las diferentes aplicaciones de la órbita de la salud entre sí y con los restantes sistemas de la administración del GCBA, como 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 mayor aprovechamiento de los recursos. A manera de ejemplo mencionaremos la necesidad de que el Sistema para la Administración de Emergencias interactúe con las guardias de los hospitales que van a recibir a los accidentados y estas a su vez con el resto de los servicios hospitalarios.

Resulta necesario evaluar las novedades tecnológicas existentes en el mercado de forma de aprovechar las ventajas y oportunidades que ofrece la tecnología cuando se encuentren justificadas. Resulta paradójico que existan compañías de taxis con sistemas de asignación digitales automáticos y el SAME ni siquiera haya considerado la posibilidad de su utilización.

Se encuentran asimismo en estado precario los mecanismos de seguridad físicos y lógicos. El SAME debe trabajar en forma integrada con otros sectores del GCBA para una eficiente resolución. A modo de ejemplo citaremos que la Dirección de Defensa Civil puede colaborar con el plan de evacuación y su puesta en práctica. Del mismo modo otras áreas especializadas del Gobierno pueden colaborar para el trabajo que es necesario llevar a cabo.

Por último se deberá atender a la situación coyuntural en forma inmediata procurando cubrir los aspectos más importantes referidos a la seguridad, continuidad de los servicios informáticos, y las mejoras cuya incorporación resulte justificada hasta la concreción de soluciones más ambiciosas.

Asimismo se deberá priorizar el apoyo informático al área operativa del SAME ya que la misma se encuentra totalmente carente de dichos servicios a pesar de que constituye la esencia de la Dirección.