INFORME EJECUTIVO

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

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

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

OBSERVACIONES:

Las principales observaciones realizadas están referidas a:

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

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

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