INFORME EJECUTIVO

Lugar y fecha de emisión	Ciudad Autónoma de Buenos Aires, Septiembre de 2019.
Código del Proyecto	10.18.03
Denominación	Agencia de Sistemas de Información
Tipo	Relevamiento
Período examinado	2018
Objeto:	Plan de Contingencia e infraestructura primaria y redundante de los *Data Centers* que dan soporte a los sistemas Core de CABA
Jurisdicción:	21 – Jefatura de Gabinete de Ministros
Unidad Ejecutora	682 – Dirección General de Infraestructura 1 – *Data Center*
Objetivo	Revisión de Continuidad Operacional de los Sistemas *Core* de la CABA
Alcance	Analizar la seguridad física, lógica y continuidad operativa y formal de la Arquitectura de Servicios y los Sistemas de la CABA.
Desarrollo de tareas	Las tareas de auditoría se desarrollaron desde de enero a junio de 2019
Aclaraciones previas	**Introducción.** Las cada vez mayores exigencias de los centros de cómputo en materia de seguridad y prevención, sumado a la abundancia de conectividad ha llevado a un proceso de concentración de procesamiento en sitios muy sofisticados, que han ido absorbiendo a los centros de cómputo descentralizados sectoriales más pequeños. Esto ha reducido los costos de procesamiento debido al beneficio de la escala, ya que es más barato tener pocos centros de cómputos que tener muchos. Los centros de cómputo deben cumplir muchos requisitos y, en consecuencia, son costosos de instalar y mantener. Asimismo, los grandes centros de cómputo con la ayuda de la robotización generan importantes ahorros de personal a la vez que aseguran mejor rendimiento y seguridad. Los informes de la AGCBA impulsaron este cambio y el GCBA ha evolucionado mucho en este sentido. En los comienzos de la AGCBA eran muy pocos los sistemas que se procesaban en la

entonces Dirección General de Sistemas de la Información (DGSinf). La mayoría de ellos eran procesados sectorialmente o en servicios a cargo de proveedores externos al GCBA. En la actualidad se procesan casi todos los sistemas con exclusión de los sistemas de recaudación y los sistemas de la gestión administrativa como presupuesto y compras, y otros de menor importancia. La ASInf ha ido incorporando el procesamiento de los sistemas de educación, documentales, de la salud y otros. Esto, asimismo, facilita la integración de la información y es un elemento formador de un mejor ambiente de control.

El riesgo de tener una gran concentración de procesamiento en pocos sitios está relacionado con la suspensión del servicio por algún hecho grave en ellos ya que impacta sobre muchos aplicativos. Es por ello que se han desarrollado métodos y técnicas para mitigar estos hipotéticos eventos no deseados en los que diferentes actores pautan lineamientos y acuerdos para su estructuración. El marco de control COBIT (Ver anexo) asigna un ciclo de gestión específico a este tema. El marco COBIT utiliza las pautas de la norma ISO 22301 relativas a la continuidad de la operación. Para algunos aspectos como la seguridad física la normativa TIER (Ver anexo) ofrece un marco específico. Este informe trata sobre ese tópico: ¿qué tan maduro es el modelo de gestión de riesgo para el tratamiento de la continuidad del procesamiento en la ASInf y el GCBA?

Antecedentes de la ASInf.

En el mes de abril del año 2008, la Legislatura de la Ciudad Autónoma de Buenos Aires sanciona la Ley 2.689 mediante la cual se crea la Agencia de Sistemas de Información. Dentro de la misma, en el artículo 3°, se enuncian principios rectores como el de "Promover la estandarización de los bienes informáticos, equipos, recursos, sistemas y programas a ser utilizados por el Poder Ejecutivo", así como "…el desarrollo, modernización y economía administrativa integral, en las dependencias y entidades de la administración pública, a fin de que los recursos y los procedimientos técnicos sean aprovechados y aplicados con criterios de transparencia, eficacia, eficiencia y austeridad".[1]

Dentro de la misma ley, en el artículo 4, se definen las funciones del ente, "a) Definir y establecer la política gubernamental en materia de Sistemas de Información y el uso de medios electrónicos para la gestión, dictando normas técnicas, metodologías de gestión de

[1] Ley 2.689 - http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley2689.html

proyectos y desarrollo de software y estándares en materia de Tecnologías de Información y Telecomunicaciones a ser aplicadas en consonancia con estándares internacionales, que garanticen la interoperabilidad y accesibilidad de los servicios electrónicos del Poder Ejecutivo"

En el año 2013, ASinf confeccionó un Marco Normativo de Tecnología de Información, publicado en la Resolución N° 177 (con complementarias posteriores), con el objetivo de promover la estandarización de los bienes informáticos, equipos, recursos, sistemas y programas a ser utilizados por el Poder Ejecutivo.[2]

El Marco Normativo de Tecnología de Información está conformado por Políticas con alcance sobre las actividades relacionadas directa o indirectamente con la utilización de recursos de Tecnología de Información y comunicación dentro del Gobierno de la Ciudad Autónoma de Buenos Aires. Por ello, toda organización dependiente del Poder Ejecutivo del Gobierno de la Ciudad Autónoma de Buenos Aires debe implementarlo.

Organización de la ASInf.

La ASInf está estructurada con cuatro Direcciones Generales, una Coordinación General de Servicios[3] y una Unidad de Auditoria Interna.

Las Direcciones Generales son Seguridad Informática, Infraestructura, Técnica y Legal, Integración de Sistemas. Esta auditoria involucra a las dos primeras[4].

Acciones de la ASInf.

Los sistemas procesados en la ASInf son administrados con diferentes modelos de gestión según los casos. Algunos son procesados y administrados por las áreas descentralizadas.

La ASInf posee un proceso estructurado de copias de respaldo que abarca todos los aplicativos e información. Efectúan pruebas genéricas de recupero de la información, pero no realizan informes ni actas formales en los que expliquen los objetivos y los resultados.

[2] Resolución N°177/ASInf/13 - https://www.buenosaires.gob.ar/sites/gcaba/files/rs-2013-177--asinf_4.pdf

[3] Anexo de la Resolución Nº 224/ASINF/2018 - https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJGGC-ASINF-224-18-ANX.pdf

[4] Ver Anexo Organigrama Otras áreas.

	Los acuerdos de niveles de servicio no están formalizados salvo excepciones. Los accesos a los ambientes de trabajo (Producción, QA, Prueba, Homologación) se enmarcan en las políticas de la Agencia y los accesos de usuarios en custodia se basan en el estándar de puesta en producción. La ASInf no administra todas las redes del GCBA ya que hay cuatro dependencias que lo hacen por sí. (Tránsito, AGIP, Seguridad y SBASE) No se han hecho análisis de criticidad de los nodos de las redes aunque disponen de redundancia en sus niveles más importantes. No disponen de un plan de contingencia de redes. La seguridad física cuenta con elementos redundantes para mitigar los riesgos en ambas sedes. La ASInf en el año 2017 confeccionó un plan de recuperación de desastre para el centro de cómputos de situado en Independencia 635, sede de la ASInf. La estrategia de recuperación consistía en trasladar los aplicativos críticos al data center secundario en la sede de Parque Patricios (Uspallata 3160, CABA) estableciendo un esquema de replicación entre ambos sitios. **<u>Los Planes de la ASInf con relación a contingencia.</u>** Se planea pasar de un esquema estático a uno dinámico. Actualmente Uspallata es el centro de cómputos alternativo al de Independencia. Si un aplicativo crítico dejase de operar se requeriría de un cierto tiempo para recuperar la operación en Uspallata. Con el uso dinámico de los equipos, si deja de operar cualquiera de los dos centros de cómputo, el otro podría sostener la operación con una performance un poco más baja. Esto aprovecharía mejor la capacidad de procesamiento ya que todos los equipos soportarían al mismo, así como a la continuidad que funcionaría bajo un esquema ininterrumpido (*non stop*) Este objetivo cuenta con aprobación y presupuesto para el año 2019.
Conclusiones	La ASInf ha confeccionado planes y prevenciones que mitigan los riesgos tecnológicos usuales como los cortes de energía, incendio, accesos indebidos a los centros de cómputo y otros. Cuenta con una política de copias de respaldo y equipos para el recupero de los sistemas en caso de caídas. Asimismo se encuentra embarcada en un plan para que el procesamiento se efectúe en sincronía entre los centros de cómputo de Independencia y Uspallata que permitirá reducir la probabilidad de una interrupción indeseada de los servicios de procesamiento, ya que esta solución mantendría el servicio, aún en el caso de salida de operaciones de uno de los dos centros de

	cómputo. Sin embargo esto se aplica solamente a todo lo que procesa la ASInf que excluye toda la información financiera y de la recaudación entre otros. La ASInf ha sido prescindente en cuanto a tomar recaudos con esta parte de la información a pesar de que le ley le asigna responsabilidad por la totalidad de la información del GCBA. Este mismo concepto es extensible a las redes de datos, en las que algunas redes se encuentran fuera de la órbita de la ASInf. Subsisten asimismo aspectos organizacionales que, de adecuarse, mejorarían el ambiente de control, como la independencia del área de seguridad del área técnica y su subordinación a un área no técnica de mayor nivel político, así como también la designación de la responsabilidad política por la contingencia de la información, su procesamiento y disponibilidad para la toma de decisiones, a un nivel adecuado. No se ha normado la política relativa a la contingencia, y, aunque hay otras que constituyen insumos o partes de la misma, muchas de ellas no se han implementado ni siquiera en la ASInf. Es un ejemplo de esto la falta de designación de los propietarios de la información. El propietario de la información es rol clave en el tratamiento de la seguridad, los perfiles de accesos, y otros, y su designación dejaría en claro que las áreas tecnológicas custodian la información bajo el mandato del dueño del dato. Tampoco se ejecutó un proceso sistemático de evaluación de riesgos, la evaluación de impacto fue incompleta y no se clasificaron los activos informáticos. En cuanto a aspectos formales, los proyectos se informan de un modo carente de precisión a la ciudadanía en la ley de presupuesto. Internamente se carece de planos de redes de datos y de documentación adecuada de las pruebas de recupero de información. Por lo antedicho el plan de contingencia existente resulta incompleto, por su alcance limitado a la información procesada en la ASInf, por la no inclusión de hipótesis de riesgo amplias, por la falta de participación del nivel político requerido y la falta de ejecución o la ejecución incompleta de ciclos de gestión necesarios para el mismo.

Principales Debilidades	Deber de informar falto de precisión. La planificación del área de infraestructura no describe con precisión lo que se va a hacer en el año 2018. Las descripciones de los años 2017, 2018 y 2019[5] no proporcionan metas acerca de cuantas redes se van a incorporar, cuantos incidentes calculan atender, cuál va a ser el crecimiento del parque informático, qué herramientas van a ser actualizadas, qué objetivos responden a lo que se efectúa habitualmente y qué objetivos apuntan a cambios para la mejora de los servicios, como por ejemplo el cambio de complementación en el procesamiento entre los centros de cómputo de Independencia y Uspallata. Así se cumple parcialmente la ley 70 que requiere de presupuestos por programa, con objetivos y metas definidos. Llamativamente, la planificación interna cuenta con esta información que no se provee a la ciudadanía. Alcance incompleto en el tratamiento de la seguridad de la información. La ASI no interviene en materia de continuidad del servicio, la seguridad de los accesos en custodia, la seguridad física y otros, en los centros de cómputo del GCBA que operan por fuera de su organización. Su acción se limita a la promulgación de normas sin facilitar, controlar ni obligar a su cumplimiento a las áreas de sistemas externas[6] lo que incumple el mandato de la ley que le impone responsabilidad por la totalidad de la información del poder ejecutivo del GCBA. Más aún, existen áreas de seguridad descentralizadas, como la de la AGIP, no subordinadas a la ASInf que no reportan a esta lo que resulta contrario al mandato de la ley y a principios de la buena organización como la unidad de mando. La ASInf no administra la totalidad de las redes del GCBA. Existen redes en el GCBA que están fuera de la administración de la ASInf y, en consecuencia, también le es ajena la responsabilidad por lo que sucede en ellas en materia tecnológica y de seguridad. Esto también contradice el mandato de la ley de creación de la ASInf que

[5] El texto en el que se describe lo que se va a efectuar en el año con los fondos asignados es exactamente el mismo en los tres años, a pesar de que el presupuesto del área de infraestructura del año 2019 es 250% mayor al presupuesto del año 2018 no se agrega nada diferente al del año anterior.

[6] La ley impone, entre otras, la función de Administrar la operación, mantenimiento y soporte de los sistemas y la infraestructura tecnológica del Poder Ejecutivo, redes y centros de datos, asegurando un estricto marco de seguridad para todas las áreas y sistemas; impulsando y desarrollando por sí o por terceros sistemas de información. La ley no le proveyó a la ASI herramientas para el ejercicio de su autoridad como la capacidad de remover y designar a los responsables de sistemas de acuerdo con la autoridad del área respectiva tal como lo poseen otros órganos rectores, algo que podría salvarse con un decreto.

	le otorga mandato por la totalidad de la infraestructura. Las redes no administradas por la ASInf no existen por delegación de funciones sino porque pre existieron a la creación de la Agencia. El área de Seguridad no guarda independencia de las áreas técnicas. El área de seguridad es una Dirección General dentro de la ASInf dependiente del responsable ejecutivo de la misma. La independencia de la Seguridad es un elemento formador del ambiente de control que la dimensión del GCBA justifica plenamente[7]. Falta de un responsable de la contingencia al nivel requerido. No hay un responsable por la contingencia de la información del máximo nivel de la organización tal como lo requiere la normativa. La responsabilidad por la continuidad del servicio debe recaer en el principal de la organización, que en el caso del GCBA podría ser el Jefe de Gabinete de Ministros que se encargaría de las decisiones estratégicas, como el presupuesto y la definición general del apetito al riesgo y delegaría en niveles inferiores el tratamiento de las decisiones instrumentales tecnológicas, sociales y organizacionales, reservándose la ratificación o rectificación final de las mismas. Falta de ejecución sistemática del proceso de evaluación de riesgos. No se ejecuta el proceso de evaluación de riesgos de forma sistemática y amplia. Tampoco se ha efectuado una revisión de riesgos tecnológicos en línea con lo requerido por la norma interna PO0201. Falta de un plan de contingencia y de recuperación de desastre completo. El plan de contingencia de la ASInf no parte de las hipótesis de riesgo generales, para abordarlas y mitigarlas sino que se limita a una estrategia de recuperación de procesos considerados críticos por la ASInf en el que no intervinieron para su determinación los propietarios de la información sino referentes técnicos. Tampoco se cuenta con un plan de recuperación de desastre completo que defina las acciones, los actores, los recursos y la forma de recuperación del estado inicial del servicio. El plan existente no contempla las comunicaciones. Este plan asimismo no incluye la información que se procesa fuera de la ASInf o sea, toda la información económica y

[7] La ASInf podría resolver la cuestión de la dependencia efectuando una avocación de la función que quedaría a cargo de un área superior, como la Jefatura de Gabinete de Ministros. Esta debilidad ya fue mencionada en informes anteriores.

	financiera así como tampoco la referida a la recaudación y la deuda pública por citar algunos ejemplos. Tampoco alcanza a algunos servicios que se han implementado en la nube. Propietarios de la Información (*Data owner*) sin designar. No se han definido los dueños del dato o propietarios de la información en línea con lo requerido por la norma interna PO0401 Responsabilidades sobre la información. Estas designaciones constituyen una pieza clave en al armado de la seguridad ya que asignan responsabilidades sobre funcionarios no técnicos, cuya falta genera un vacío organizacional. [8] Clasificación de los activos informáticos. No se efectuó una clasificación de los activos informáticos en línea con lo requerido por la norma interna PO0201 - Política de Análisis de Riesgos Tecnológicos. Tampoco se realizó la clasificación de los activos de información en línea con lo requerido por la norma interna PO0402-Política de clasificación de la información. La clasificación de la información es un insumo del proceso de evaluación de riesgos. Falta de planificación y trazabilidad de las pruebas de recupero. Las pruebas de recupero de datos no fueron planificadas formalmente, no siguieron un protocolo, no se documentaron adecuadamente y no participaron los interesados como seguridad, auditoria y el propietario de la información. En consecuencia se cumple de manera incompleta con la norma interna PO0701-Política de copias de resguardo y recuperación[9]. Tampoco se han incluido en los planes para el año 2019 pruebas de recupero de datos que permitirían comprobar y asegurar la capacidad de recuperación y los tiempos necesarios para la misma. Documentación de las redes.

[8] En efecto, existe la creencia de que la responsabilidad por la información digitalizada recae sobre el área tecnológica, pero esta cumple solo un rol como custodio de la misma. El usuario designado como propietario de la información es el responsable por la integridad de la misma y debe conocer y autorizar el acceso y uso, dentro y fuera del Organismo; entendiendo también los riesgos y problemas potenciales a los que está expuesta y actuando en consecuencia para minimizar el grado de exposición de la misma. El propietario del dato es el mandante y el custodio, el mandatario.

[9] Los trabajos de recuperación realizados por necesidad no reemplazan a las pruebas que tienen finalidades específicas que deben explicitarse en la planificación y que se documentan luego de ejecutadas, requisitos que no se aplican a restauración de archivos y sistemas ejecutados por otros motivos.

	No disponen de documentación de red completa en los siguientes ítems: Mapas de red lógicos. Topología de la red. Inventario de redes. Inventario de dispositivos de comunicaciones. Inventario de dispositivos de seguridad. Relaciones con los respectivos acuerdos de nivel de servicio (SLA). Identificación de puntos críticos y estadísticas sobre los puntos críticos. De este modo incumple la norma interna PO0703-Política de seguridad en redes. <u>Áreas que manejan su política de implementación.</u> Hay áreas como Salud que administran los ambientes de manera directa a través de las áreas de sistemas descentralizadas sin que esto haya sido aprobado por el propietario de la información lo que incumple la norma interna PO0901 - Política de Separación de Ambientes y su anexo Política de Control de Cambios.