AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

INFORME FINAL DE AUDITORIA

Con Informe Ejecutivo

Proyecto Nº 10.18.03

AGENCIA DE SISTEMAS DE INFORMACIÓN (ASI)

Auditoría de Relevamiento

Período 2017

Buenos Aires, Agosto 2019

AUDITORÍA GENERAL DE LA CIUDAD DE BUENOS AIRES

Av. Jean Jaurés 216 Ciudad Autónoma de Buenos Aires

Presidente

Lic. Cecilia Segura Rattagan

Auditores Generales:

Cdra. Mariela Coletta

Ing. Facundo Del Gaiso

Dr. Jorge Garayalde

Lic. María Raquel Herrero

Cdor. Vicente Rodriguez

Lic. Hugo Vasques

Código de Proyecto: 10.18.03

Nombre del Proyecto Auditoría: Agencia de Sistemas de Información

Tipo: Relevamiento

Organismo auditado: Agencia de Sistemas de Información

Objeto: Plan de Contingencias y la infraestructura primaria y redundante de los *Data Centers* que dan soporte a los sistemas Core de CABA

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.

Jurisdicción / Unidad Ejecutora: 21 – Jefatura de Gabinete de Ministros, 682 – Dirección General de Infraestructura 1 – *Data Center*

Período a auditar: 2018

Supervisores: Ing. José Recasens y Lic. Héctor S. Zancada

FECHA DE APROBACIÓN DEL INFORME: 18 DE SEPTIEMBRE DE 2019

APROBADO POR: UNANIMIDAD

RESOLUCIÓN AGC Nº: 262/19

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.

INFORME FINAL DE AUDITORÍA
"AGENCIA DE SISTEMAS DE INFORMACIÓN"
PROYECTO N° 10.18.03

DESTINATARIO

Señor
Presidente
Legislatura Ciudad Autónoma de Buenos Aires
Sr. Diego César Santilli
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 Sistemas en el ámbito de la Dirección General de Tecnología Educativa con el objeto detallado en el apartado siguiente.

I-OBJETO DE AUDITORIA

Plan de Contingencias y la infraestructura primaria y redundante de los *Data Centers* que dan soporte a los sistemas *Core* de CABA

II-OBJETIVO DE LA AUDITORIA

Revisión de Continuidad Operacional de los Sistemas *Core* de la CABA

III-ALCANCE DEL EXAMEN

Analizar la seguridad física, lógica y continuidad operativa y formal de la Arquitectura de Servicios y los Sistemas de la CABA

Marco Normativo:

Se utilizó el siguiente marco normativo:
Normas Básicas de Auditoria Externa de la AGCBA y las Normas Básicas de Auditoria de Sistemas de la AGCBA, la ley 70, ley 325 y complementarias.

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

Supletoriamente se utilizaron:
Norma ISO 22301.
Las normas y recomendaciones de seguridad establecidas por la ASI (Ex DGEySI), como las resoluciones ASINF-177-2013 y ASINF-239-2014.

Procedimientos realizados.

Se envió Nota solicitando información relacionada con la auditoría planificada respecto de los sistemas, los principales resguardos y la organización del área.

Se envió Nota solicitando información ampliatoria con relación al alcance de las funciones, servicios y otros.

Se efectuaron entrevistas con:

- Director General de Infraestructura de la ASInf
    - Gerente Operativo de Redes y Telefonía.
    - Gerente Operativo de Operaciones.
        - Subgerente Infraestructura de Data Center
            - Supervisor de Mantenimiento.
- Director General de Seguridad Informática.
- Sub Gerente de Procedimientos y Control.

Se verificó in situ el Data Center de Independencia 635, su subsuelo y entorno junto con el personal del área.

Se verificó in situ el Data Center de Uspallata 3160, su subsuelo y entorno junto con el personal del área.

Se revisó el marco organizacional de la seguridad y la contingencia.

Se participó de una prueba de verificación de enrutado automático dinámico de redes a nivel de nodo central.

Se analizó el plan de contingencia de procesamiento de Data Center Activo – Pasivo.

Se revisó el plan 2017-2019 de la ley de presupuesto relacionado con la continuidad del servicio y su adecuación a la ley 70 (Presupuesto por programa).

Se analizó la documentación interna de los planes de la ASInf.

Se analizó el alcance de los servicios de la ASInf en función del mandato de la ley de creación y su relación con las áreas receptoras del servicio.

Se revisó la formalización y alcance de los acuerdos de niveles del servicio prestado por la ASInf.

Se revisó el rol de los actores en el tratamiento de la contingencia y su metodología.

Se revisó el procedimiento de copias de respaldo, su alcance, secuencia y revisiones.

Se revisó la planificación, el alcance y la documentación de las pruebas de recuperación de las copias de respaldo.

Se revisó la documentación de redes existente en función de la normativa interna e internacional.

Se revisaron los inventarios de hardware y software.

Se revisaron los procedimientos existentes.

Las tareas de auditoría se efectuaron entre Enero y Mayo de 2019.

El organismo auditado no remitió descargo al informe Preliminar enviado.

IV – 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?

Jean Jaures 220 - C1215ACD - Ciudad Autónoma de Buenos Aires - Tel. 3754-3700

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".[10]

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 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"

Mediante el Decreto N° 1.036/GCABA/08, se estableció que la adquisición, contratación y licenciamientos de bienes y servicios informáticos deben contar con la conformidad de la Agencia de Sistemas de Información (ASInf).[11]

En el año 2009, el mismo órgano sanciona la Ley 3.304, Ley de Modernización de la Administración Pública, con el objetivo de implementar un proceso de modernización administrativa en el Gobierno de la Ciudad Autónoma de Buenos Aires.[12]

En el año 2012 mediante la Resolución Nº 190 del Ministerio de Modernización, se aprueba el Formulario Único de Requerimientos (FUR) y el Instructivo para el Proceso de Gestión de Demanda.[13]

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

[11] Decreto N° 1.036/GCABA/08 - https://ar.vlex.com/vid/decreto-n-42103517

[12] Ley 3.304 - http://www2.cedom.gob.ar/es/legislacion/normas/leyes/anexos/al3304.html

[13] Resolución N° 190/MMGC/12 - https://webcache.googleusercontent.com/search?q=cache:fDLbAgdX1rsJ:https://mibuenosairesweb.go

El Formulario Único de Requerimientos tiene por finalidad la solicitud de servicios tecnológicos a la ASInf. El proceso de Gestión de Demanda tiene como objetivo que los programas, herramientas, compra de equipos, y metodologías de gestión de procesos y tecnologías sean tramitados de acuerdo a las Políticas y Programas del GCABA que les son aplicables.

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.[14]

En el año 2014, la administración gubernamental reconocía mediante el Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Data Center que "el desarrollo de aplicaciones sucede en un entorno tecnológico caracterizado por su diversidad y constante transformación. Las diferentes plataformas, sistemas operativos, servidores de aplicaciones y de bases de datos, la variedad de lenguajes de desarrollo y la evolución de las tecnologías de integración, ofrecen mejoras y ventajas demandadas por los desarrolladores quienes esperan con ellas brindar mejores servicios a los Usuarios de dichas aplicaciones. Esta situación plantea también un desafío para los Arquitectos y los Administradores de Sistemas, quienes en caso de no haber tomado las decisiones adecuadas, enfrentarían el riesgo de encontrarse en el futuro lidiando con un conjunto heterogéneo de sistemas y aplicaciones"[15]

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.

---

b.ar/sites/default/files/uccop/comunicaciones/anexos/Resol%2520190%2520-%2520MModernizacion-2012-Texto.pdf+&cd=1&hl=es&ct=clnk&gl=ar

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

[15] ES0101 – Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Data Center https://www.buenosaires.gob.ar/sites/gcaba/files/estandar_arquitectura_asi.pdf

Dentro de cada una de las mencionadas Políticas se detalla el objetivo, alcance y contenido para lograr la interoperabilidad y seguridad de los sistemas, como así también la ejecución del Plan Integral de Tecnologías de la información y de las Comunicaciones.

ASinf, en el año 2014, definió junto con el Marco Normativo de Tecnología de la Información, el Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Data Center (ES0101).[16] También implementó el Estándar de Desarrollo de la Agencia de Sistemas de Información[17] y se reglamentó el Proceso de Control de Cambios en Software de Aplicación provisto por Organismos C0901.[18] El objetivo de los documentos es definir los requerimientos que un desarrollo debe cumplir en relación con las tecnologías adoptadas por la ASInf, como así también la interacción con los proveedores de software en cuanto a entregables, seguimiento de errores, control de cambios, etc.

En el año 2015 y mediante la Resolución N° 239/ASInf/15[19], acorde con los avances tecnológicos y las necesidades, se ampliaron políticas, guías y estándares.

El Formulario Único de Requerimientos y el Proceso de Gestión de Demanda fueron ratificados en el año 2016 mediante la Resolución N° 134 de ASINF.[20]

El Marco Normativo de Tecnología de Información, como se expresa en la Resolución ASInf 177 del año 2013, son lineamientos teóricos a seguir por los organismos dependientes del Poder Ejecutivo de la Ciudad.

[16] Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Data Center https://www.buenosaires.gob.ar/sites/gcaba/files/estandar_arquitectura_asi.pdf

[17] Estándar de Desarrollo - https://www.buenosaires.gob.ar/sites/gcaba/files/estandar_desarrollo_asi.pdf

[18] PC0901 - Proceso de control de cambios en software de aplicación provisto por Organismos - https://www.buenosaires.gob.ar/sites/gcaba/files/pc0901_-_proceso_de_control_de_cambios_para_organismos_0_0.pdf

[19] Resolución N° 239/ASInf/15 - https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-ASINF-ASINF-239-14.-ANX.pdf

[20] Resolución N° 134/ASInf/16 - https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJGGC-ASINF-134-16-ANX.pdf

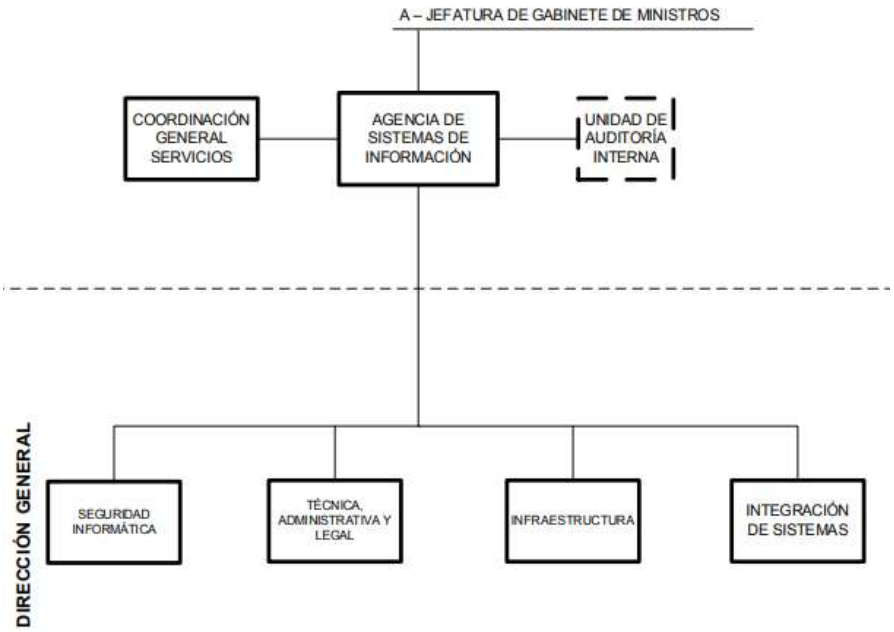
Organización de la ASInf

La ASInf está estructurada con cuatro Direcciones Generales, una Coordinación General de Servicios[21] y una Unidad de Auditoria Interna.

Las Direcciones Generales son:

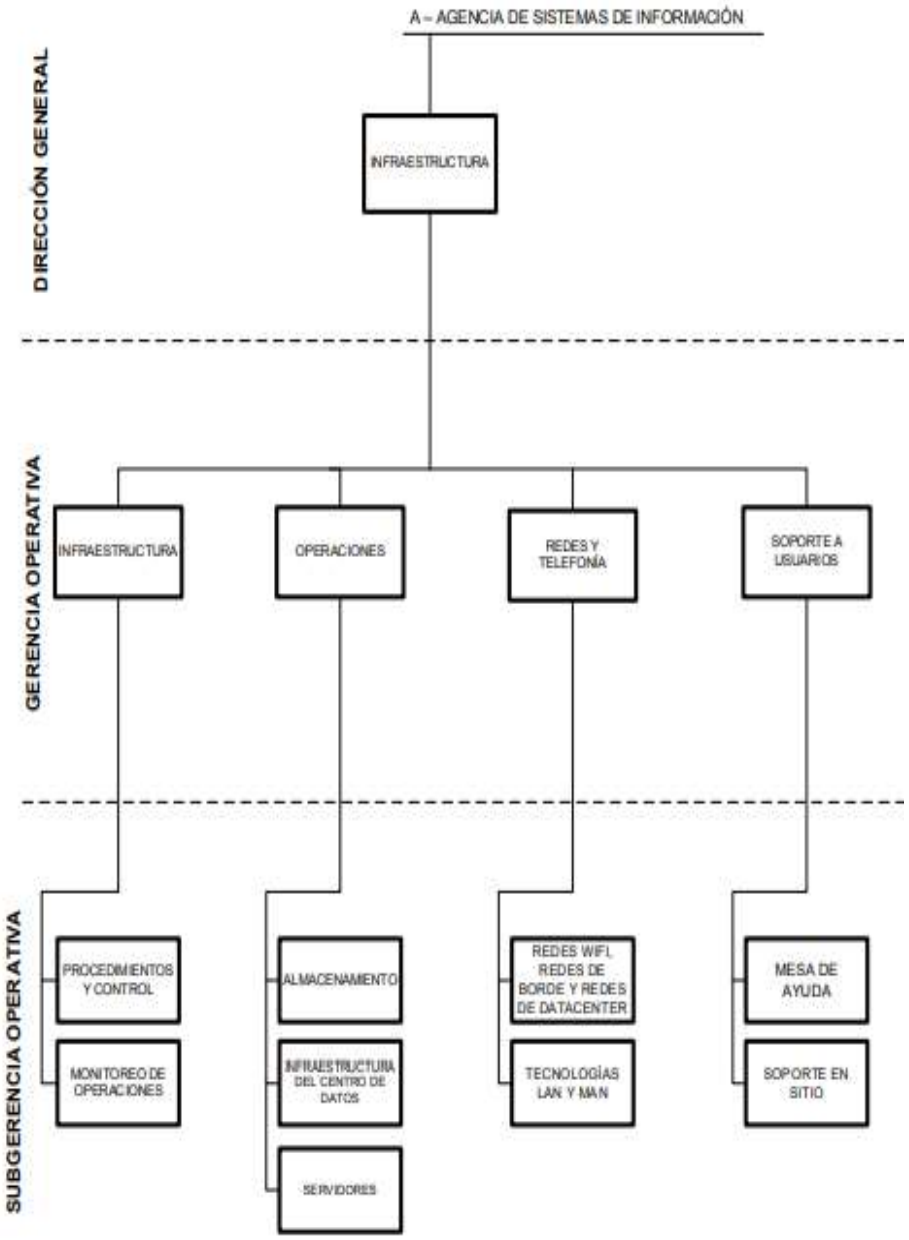
- Seguridad Informática.
- Infraestructura.
- Técnica y Legal. (Ver estructura en anexo)
- Integración de Sistemas. (Ver estructura en anexo)

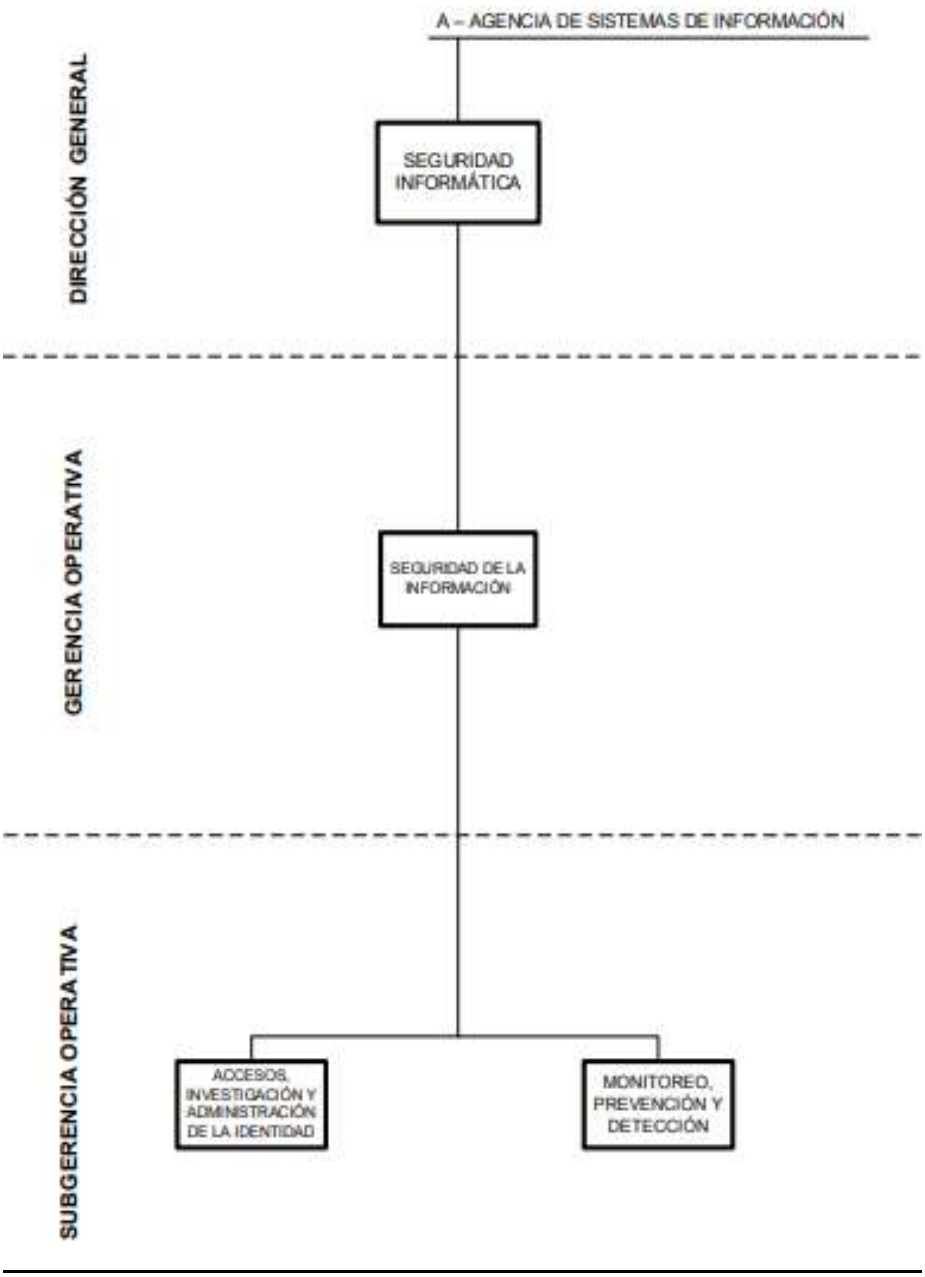
Esta auditoria involucra a las dos primeras[22].



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

[22] Ver Anexo Organigrama Otras áreas.




A – AGENCIA DE SISTEMAS DE INFORMACIÓN
DIRECCIÓN GENERAL
SEGURIDAD INFORMÁTICA
GERENCIA OPERATIVA
SEGURIDAD DE LA INFORMACIÓN
SUBGERENCIA OPERATIVA
ACCESOS, INVESTIGACIÓN Y ADMINISTRACIÓN DE LA IDENTIDAD
MONITOREO, PREVENCIÓN Y DETECCIÓN

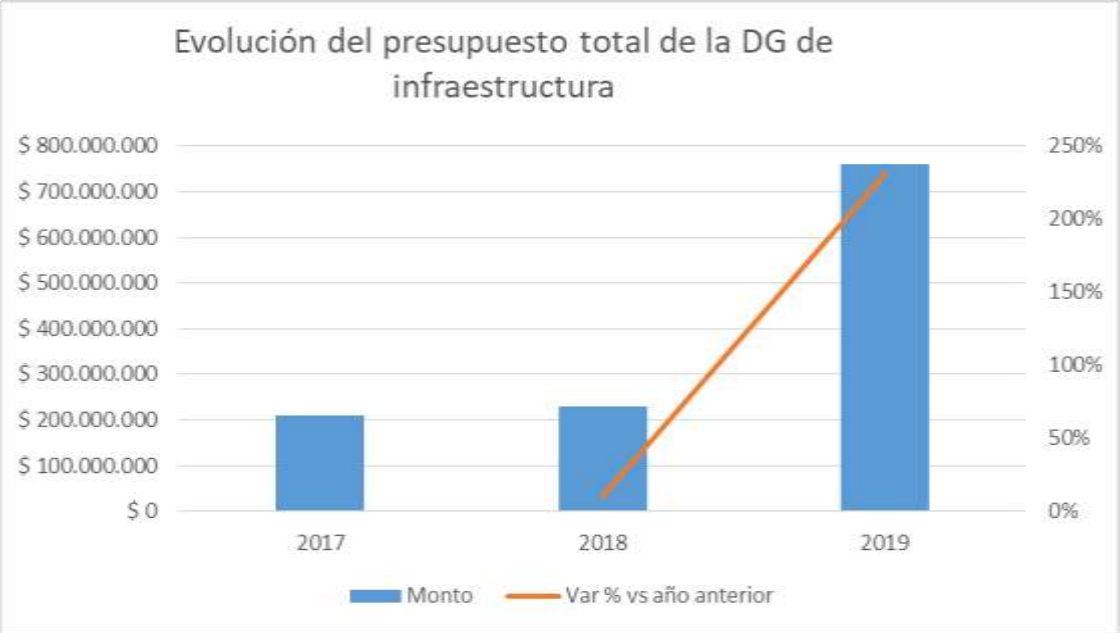
Presupuesto de la ASInf[23]

Evolución del presupuesto total de la ASInf En pesos			
Año	2017	2018	2019
Monto	$ 467.686.658	$ 719.656.551	$ 1.345.344.758
Var % vs año anterior		54%	87%

Evolución del presupuesto total de la DG de infraestructura			
Año	2017	2018	2019
Monto	$ 208.782.936	$ 230.089.821	$ 760.685.069
Var % vs año anterior		10%	231%

Evolución del presupuesto de la inversión en la ASInf			
Año	2017	2018	2019
Monto	$ 202.333.703	$ 126.773.888	$ 619.206.513
Var % vs año anterior		-37%	388%

[23] Fuente: Cuenta de Inversión 2017/2018, página del Gobierno de la Ciudad de Buenos Aires. http://www.buenosaires.gob.ar/economiayfinanzas/contaduria/informacion-contable/cuentas-anuales-de-inversion



La descripción presupuestaria de la ASInf en el presupuesto 2017 estuvo planteada como un plan 2017/2019 con ejes en:

- Más conectividad para facilitar el acceso de los servicios al ciudadano.
- Mejorar la calidad de los trámites de Gobierno Electrónico.
- Incorporar nuevos servicios.

- Desarrollar más aplicaciones móviles.

En el programa presupuestario del año 2018 se planteó:

- Coordinar el desarrollo informático con las dependencias del ejecutivo,
- Mantener los logros del área de integración.
- Mantener y expandir la infraestructura tendiendo a una mayor homogeneidad.

La descripción del programa presupuestario de Infraestructura enunció las funciones del área como mantener los sistemas de comunicaciones y proveer infraestructura informática, asesorar respecto de ello, elaborar políticas, efectuar el soporte del centro de llamadas y la red social, mantener el sitio de internet, coordinar y dirigir la mesa de ayuda, coordinar la implementación de mantenimiento de sistemas garantizando operación 7x24 y elaborar planes de capacitación y entrenamiento.

Con relación a los planes de contingencia manifestaba:

"Participar en el diseño y elaboración de planes de contingencia y recuperación destinados a resolver problemas graves de salida de servicio de los sistemas y redes de operación. Ejecutar dichos planes de contingencia y recuperación[24]."

Continuidad de los servicios y seguridad según la ley de creación.

La ley de creación de la ASInf (LEY Nº 2689/08 CABA) le asigna la responsabilidad por la seguridad de la información y los recursos tecnológicos ya que establece que debe asegurar un estricto marco de seguridad para todas las áreas y sistemas y definir lineamientos de normas en cuanto a calidad y de seguridad para todo el Poder ejecutivo.

Se establece (Resolución Nº 224/ASINF/2018) que la Dirección de Seguridad Informática debe intervenir en las definiciones de los esquemas de seguridad, planes de contingencia y administrar y controlar los procedimientos de seguridad lógica.

[24] La descripción del presupuesto del programa de infraestructura de la cuenta de inversión es exactamente la misma para los años 2017,2018, y 2019 a pesar de que los fondos asignados variaron, especialmente del año 2018 al 2019.

Por su parte la Subgerencia Operativa Accesos, Investigación y Administración de la Identidad tiene como responsabilidad mantener y actualizar la plataforma de seguridad de la información implementada. Y, por último la Subgerencia Operativa Monitoreo, Prevención Y Detección debe administrar un sistema de alertas tempranas de incidentes de seguridad informática e implementar un sistema de escalamiento de los mismos. Por último debe implementar y controlar los procesos que garanticen el nivel de seguridad requerido para el pasaje a producción de las aplicaciones

Estándares de la Agencia de Sistemas de Información

La Agencia de Sistemas de Información (ASInf), desarrolla sus tareas en base a estándares y procesos implementados por la propia Agencia de Sistemas de Información[25]. Estos estándares están formalizados y comunicados y son de aplicación en todo el ámbito del poder ejecutivo.

Se han confeccionado guías sobre diferentes temas pero no se incluyó la política para la continuidad de los servicios que aún se encuentra sin confeccionar. Sin embargo estas políticas incluyeron muchos tópicos que son insumos del plan de continuidad de la operación, como la designación del propietario de la información, la clasificación de los activos tecnológicos y de la información, la definición de los roles y otros. También incluyó pautas para componentes que son piezas del plan de continuidad como la realización de copias de respaldo, el tratamiento de los incidentes y la arquitectura del Data Center. Sin embargo no se alcanzó a construir un procedimiento para instrumentar la guía para el tratamiento sistemático y periódico de los riesgos, así como tampoco un manual de procedimientos acabado que oriente el accionar de los ciclos de tecnología. Los procedimientos existentes son piezas dispersas sin solución de continuidad y sin formalizar[26].

Como ejemplo de políticas internas formalizadas y publicadas y de cumplimiento obligatorio relacionadas con este trabajo de auditoría mencionaremos:

[25] Estándares ASI https://www.buenosaires.gob.ar/jefaturadegabinete/agenciadesistemas/estandares

[26] Sería positivo referenciar los procedimientos a las políticas, darles el mismo orden, conformarlos en un cuerpo y aprobarlos.

Evaluación y tratamiento de riesgos

Tiene como objetivo identificar, cuantificar, y priorizar los riesgos de seguridad a los que se encuentra sometido el GCABA, definiendo cuáles deben ser las vías para determinar si serán aceptados, transferidos o mitigados.

PO0201-Política análisis de riesgos tecnológicos (pág. 20) Definir y establecer los requisitos para la realización de evaluaciones de riesgos tecnológicos y la administración de los mismos dentro del ámbito del GCABA.

La ASInf no ejecuta un proceso de evaluación de riesgos sistemático y formal.

Gestión de activos de Información

Procura alcanzar y mantener una adecuada protección de los activos, estableciendo roles y responsabilidades para la clasificación y tratamiento de los mismos. Cada Organismo clasificará la información de acuerdo a los criterios que establece el GCABA en sus políticas, contando para ello con la asistencia del Área de Seguridad Informática.

PO0401-Política de responsabilidades sobre la información (pág. 28) Establece los roles y responsabilidades de actuación, los actores que custodian, administran y salvaguardan de la información, así como los que autorizan el acceso; a través de una correcta asignación y una adecuada segregación de funciones.

PO0402-Política de clasificación de la información (pág. 34) Establece los criterios que se deben considerar para clasificar la información a fin de poder definir el nivel de criticidad de la misma y adoptar las medidas de protección y tratamiento adecuadas.

La ASInf no ha efectuado la clasificación de los activos y de la información.

Seguridad física y del entorno

Procura impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información del GCABA.

PO0601-Política de seguridad física (pág. 40) Define las pautas generales de seguridad física que permitan asegurar la integridad de los recursos informáticos utilizados para el procesamiento, transmisión y resguardo de la información.

Hay importantes medidas de seguridad física que se describirán más adelante.

Gestión de las comunicaciones y operaciones

Busca garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, implementando y manteniendo un nivel de seguridad adecuado en la provisión de servicios y detectando las actividades de procesamiento de información no autorizadas.

PO0701-Política de copias de resguardo y recuperación Establece los lineamientos para la generación, prueba y administración de copias de resguardo periódicas de la información, como así también los criterios básicos para su recuperación.

La ASInf. Dispone de procedimientos de copias de respaldo, y software semiautomático con las que realiza la tarea de copiado y restauración. El proceso es revisado anualmente por auditoría interna. Efectúan pruebas de recupero de información pero las mismas no están planificadas, protocolizadas y documentadas adecuadamente.

PO0704-Política de prevención de software malicioso (pág. 74) Establece los requerimientos que deben cumplir todos los equipos de procesamiento centralizado y estaciones de trabajo conectados a la red de comunicaciones del GCABA, de forma de garantizar la detección y eliminación de software malicioso (virus informáticos, troyanos, gusanos, malware en general; incluyendo código móvil), minimizando el riesgo de infección y propagación de los mismos.

Desarrollan una política de prevención centralizada que distribuye la salvaguarda en los diferentes ámbitos.

Control de accesos

Procura controlar los accesos a la información sobre la base de los requerimientos de seguridad y de los objetivos definidos por el GCABA. Los accesos serán otorgados sobre los principios de “mínimo privilegio” y “necesidad de conocer”, aplicables a cada usuario.

PO0805-Política de administración de usuarios GCABA (pág. 113) Establece los lineamientos que permitan asegurar una adecuada administración de los usuarios del GCABA.

PO0806-Política de administración de usuarios en custodia (pág. 120) Establece las medidas de control para la utilización de usuarios en custodia, de manera que los mismos sean utilizados solo en situaciones de emergencia que lo ameriten.

PO0807-Política de administración de contraseñas (pág. 125) Asegura una adecuada administración (generación, modificación, utilización y almacenamiento) de las contraseñas de los usuarios del GCABA.

La ASInf no ha designado a los propietarios de la información que tienen un rol clave en estos procesos.

Adquisición, desarrollo y mantenimiento de sistemas de información

PO0901-Política de separación de ambientes de TI (Res. ASINF 177/13 - pág. 145)

Establece los lineamientos y las pautas generales para garantizar una adecuada separación de ambientes de procesamiento de la información del GCABA, definiendo las características de los ambientes y asegurando una apropiada segregación de funciones y limitaciones de acceso.

La mayoría de las áreas de desarrollo han adoptado estas prácticas. Sin embargo hay áreas que incumplen con la norma como salud, que administra su aplicativo sin que el propietario haya aceptado formalmente el riesgo implícito en esta acción.

Gestión de incidentes de seguridad de la información

Busca asegurar que se aplique un proceso de mejora continua para la gestión de los incidentes de seguridad de la información, garantizando que los eventos sean registrados y comunicados de forma correcta y oportuna.

PO1001-Política de respuesta ante incidentes de TI (Resolución ASINF 177/13 - pág. 158) Establece lineamientos que permitan corregir con la máxima celeridad posible, las consecuencias y efectos negativos de los incidentes de los servicios de TI, a fin de minimizar su impacto.

Se cuenta con un procedimiento y con un esquema de nivel de servicio no formalizado que se describe más adelante con mayor detalle.

Gestión de la continuidad de las actividades

Guías para desarrollar e implementar planes de continuidad que aseguren la reanudación oportuna de las operaciones esenciales. Contrarrestar las interrupciones de las operaciones y proteger los procesos críticos del GCABA.

A la fecha, el presente dominio no posee documentos asociados.

El procesamiento en la ASInf y el GCBA

El procesamiento en la ASInf está a cargo de la Gerencia Operativa de Operaciones, de la que dependen cuatro áreas de trabajo que se ocupan de las Bases de Datos, los Servidores, los Sistemas Operativos, y las copias de respaldo y el almacenamiento (*Back up y Storage*).

En la ASInf no se procesan todos los Sistemas del GCBA ni se almacena toda la información del Poder Ejecutivo.

Los principales sistemas que se procesan en la ASInf son los denominados críticos en el Plan de Contingencia formulado en 2017 y revisado en 2018.

Estos son:

- SIAL (Sistema Integral de Administración de Recursos Humanos y Liquidación de Haberes)
- SADE (Sistema de Administración de Documentos Electrónicos)
- SIGEHOS (Sistema de Gestión Hospitalaria)
- PIG – BA (Plataforma Integral de Gestión)
- SAP (Seguimiento y gestión de Reclamos Ingresados por SUACI)
- Páginas Web (Sitio Web del GCBA)
- Boletín Oficial
- Mapas - USIG (Unidad de Sistemas de Información Geográfica)
- MiBA (MI Buenos Aires MiBA, plataforma interactiva con el ciudadano)
- SUACI (Sistema Único de Atención Ciudadana)

Algunos de ellos no sólo son críticos por si, sino también por los sistemas con los que interactúan que dejan de funcionar total o parcialmente si ellos no lo hacen, como Mapas Usig y SADE.

El resto de la información es procesada en otros centros de cómputo o en la nube. Los centros de cómputo importantes fuera de la ASInf existentes en la jurisdicción del Poder Ejecutivo son:

- UAIF (Unidad de Administración Información Financiera)
- Ministerio de Seguridad
- AGIP (Agencia de Ingresos Públicos)

- AGC (Agencia Gubernamental de Control)
- Transporte

Hay otros centros de cómputos menores como por ejemplo en la Sindicatura, en Educación y en Salud. También hay áreas que llevan información en la nube como IVC (Instituto de la Vivienda de la Ciudad), BsAs desde adentro, Potenciate, CRM (*call center*), SAME (Sistema de Atención Médica de Emergencias) CUCC (Centro Único de Coordinación y Control). Se ha planificado trasladar el procesamiento de AGC y UAIF a Uspallata, como parte de un proceso de centralización de procesamiento.

En la ASInf se procesa bajo dos modalidades diferentes:

- En equipos provistos por la ASInf que es la modalidad más utilizada.
- En equipos de terceras áreas.

Por ejemplo el TSJ (Tribunal Superior de Justicia) tiene un equipo con una versión reducida de SADE que se encuentra instalado en la ASInf (*hosteo)* aprovechando su infraestructura pero sin los servicios usuales. Esta se encarga de efectuar las copias de respaldo solamente.

Sistemas de Gestión y ambientes tecnológicos.

Los sistemas procesados en la ASInf son administrados con diferentes modelos de gestión según los casos. Por ejemplo los sistemas de Salud, DGAI y el IVC son administrados por la Dirección de Sistemas del Área respectiva, para lo cual acceden a todos los ambientes según sus requerimientos. Además no todas las aplicaciones utilizan el mismo ambiente operativo ni la misma base de datos. Hay aplicaciones con Postgres (Ver Anexo software utilizado por la ASInf) como SUACI, con Oracle (Ver Anexo software utilizado por la ASInf), como SADE y con My SQL como algunas partes del Sistema de Salud.

El proceso de copias de respaldo.

El área de Almacenamiento (*Back up y Storage*) se encarga de las copias de respaldo. Estas abarcan la totalidad de la información que se procesa en el *Data Center* de Independencia y de Uspallata. Se excluye toda la información que se procesa en *Data centers* externos a la ASInf y en la nube.

Hay algunas áreas que utilizan los *Data centers* de la ASInf pero administran sus propios copias de respaldo (*back ups)* como el IVC y la DGAI. En el caso

de salud, si bien esta área se encarga de administrar su aplicativo, delega en la ASInf la ejecución de las copias de respaldo. Otro caso particular es el de la Sindicatura que procesa parte de su información en los equipos de la ASInf y otra parte localmente. La ASInf se encarga de las copias de la información almacenada en equipos virtuales situados en la ASInf y la Sindicatura se encarga de los respaldos de los aplicativos situados en su área.

Actualmente Independencia es el sitio principal y Uspallata el alternativo. Hay aproximadamente 2600 máquinas virtuales en Independencia y 100 en Uspallata. La arquitectura es Activo – Pasivo. Si hubiera una falla que impidiera efectuar el procesamiento en Independencia se debería realizar el traslado a Uspallata con las acciones incluidas en el plan de contingencia, por lo que habría un retraso que variaría con la complejidad de lo que se traslade y algunos factores como el nivel de compresión que, cuanto mayor, más demora la restauración.

Marco organizacional.

Poseen una política (guía para todo el GCBA) de copias de respaldo, que se encuentra formalizada por la resolución ASINF 177 del 2013 y revisada en el 2014. Posteriormente no sufrió actualizaciones.

Disponen de un procedimiento de copias de respaldo que detalla las acciones para su ejecución así como también para el recupero de los datos. Incluye el tratamiento a dar cuando se recibe un aplicativo con información acumulada. Ningún procedimiento está aprobado y comunicado formalmente, aunque se encuentran disponibles para su consulta en la web interna.

La metodología de las copias de respaldo es la descripta en la resolución ASInf 177:

- Diaria incremental, con rotación mensual.
- Completo *(Full)* semanal con rotación mensual.
- Completo *(Full)* mensual con rotación anual.
- Completo *(Full)* Anual con rotación cada 10 años.

Las copias de respaldo mensuales y anuales de Independencia se conservan en formato cinta en las dos cajas ignífugas de Uspallata. No se efectúan pruebas de recupero de las copias de la caja ignífuga. El recupero de esta información suele ser complejo ya que la misma está guardada en el formato y

con la herramienta propia de cada época. En el caso de que fuera necesario su recupero, se recurriría al proveedor para ello, en el caso de que no se dispusiera del herramental necesario.

Tecnología del respaldo.

Utilizan dispositivos VEEAM (Ver anexo) para todo lo que está bajo la configuración de VM (*Virtual Machine*). Poseen dos servidores VEEAM en Independencia y otros dos en Uspallata. Efectúa las copias de respaldo de equipos virtuales y físicos.

Disponen además del producto *Zero Data Loss* (Cero Pérdida de Datos) específicamente para la base de datos Oracle. Las Bases de Datos Oracle están instaladas en 2 equipos Exadata (Servidor para Bases de Datos Oracle) en Independencia y otros dos en Uspallata. El equipo de Independencia copia las transacciones en el de Uspallata con un retraso máximo de aproximadamente 30 minutos. También el SADE tiene una solución integrada al *Storage* (Almacenador) que genera una copia con un mecanismo de recupero rápido (*snap shoot*) cada hora acotando la ventana de riesgo de pérdida de información.

Los dispositivos VEEAM tienen un alto grado de automatismo aunque requieren de adecuaciones en su configuración a medida que se incrementa el volumen de las copias por el paso del tiempo. También se debe configurar el nivel de compresión que, cuando es mayor, aprovecha mejor el dispositivo de almacenamiento y cuando es menor acelera la operatoria de recuperación.

Las copias se realizan primero en disco y luego en cinta. El producto administra automáticamente el ciclo de vida de las cintas.

Alcance del respaldo.

Se efectúan copias de todos los ambientes (Producción, QA (*Quality Assurance)*, Homologación, Prueba) y de todos los fuentes administrados a través del GIT (herramienta para la administración del versionado) y del mismo GIT. También se efectúan copias de todos los *logs* de los *back ups* ya que estos están en una VM, y están alcanzados por el proceso de back up. Los períodos de guarda son los generales ya descriptos.

Acuerdos de niveles de servicio para las copias de respaldo.

Se ha efectuado un acuerdo de nivel de servicio con la SECLYT(Secretaría Legal y Técnica). No hay otros acuerdos de niveles de servicio.

Utilizan las pautas establecidas para la mesa de ayuda para la evaluación de los resultados ante incidentes. Con ellas se efectúa una categorización y se les asigna un tiempo de resolución en función de la prioridad. Efectúan estadísticas y análisis mensuales de los mismos.

Recuperos.

Efectúan pruebas genéricas de recupero de la información, pero no realizan informes ni actas formales en los que expliquen los objetivos y los resultados. En estas pruebas no participa ni auditoría interna ni los responsables de los aplicativos ni los usuarios. No se confeccionan actas de las mismas. No efectúan recuperos de información antigua almacenada en las jaulas cofre.

Accesos a los ambientes de trabajo (Producción, QA, Prueba, Homologación).

Los accesos de usuarios en custodia se basan en el estándar de puesta en producción. Cuando necesitan que a un agente se le asigne un permiso determinado, se solicita por TK(*Ticket*) y la Dirección General de Seguridad informática lo otorga si el solicitante lo justifica. Se enmarcan en las políticas de la Agencia.

Las comunicaciones de datos.

Están a cargo de la **Gerencia Operativa de Redes y Telefonía de la ASInf.**

No administra todas las redes del GCBA ya que hay cuatro dependencias que lo hacen por sí.

- Tránsito. Disponen de una interconexión con la misma. Es una red de fibra propia de la repartición.
- AGIP. Le proveen fibra para accesos a los Centros de Atención y Gestión Ciudadana, (Ex CGP) y otros por lo que funcionan como proveedores. La AGIP mantiene algunos enlaces redundantes propios.
- Seguridad (Policía). Proveen enlaces para las comisarías y también funcionan como proveedores.

- SBASE (Subterráneos de Buenos Aires Sociedad del Estado) Sus redes se están sumando a la red Man.

Organización interna.

Dependen de la Dirección General de Infraestructura. Tiene organizada el área en dos subgerencias y un liderazgo.

- Subgerencia de Redes. Cuenta con 3 sectores.
    - Infraestructura que se encarga de las instalaciones externas e internas.
    - Incidentes que se encarga de la resolución de los tickets de mesa de ayuda. Cubren el intervalo de tiempo de 8 a 20 hs con personal propio y el horario nocturno con un servicio tercerizado.
    - Proyectos que efectúa las proyecciones a futuro.
- Subgerencia de WI FI y Data center. Atiende todo lo concerniente a WI FI Público e interno y todo lo relativo a la infraestructura de redes de los data center.
- Liderazgo de telefonía. Se encarga de las comunicaciones de voz.

Monitoreo.

Utilizan el software PRTG para el monitoreo de la red.

Topología.

La red tiene un primer anillo de 6 nodos[27] con equipamiento de 100 Gb cada uno. Estos se comunican con 21 nodos satélites que poseen enlaces redundantes y que se pueden reemplazar uno por otro, generando enrutamiento por otras vías alternativas si se pierde algún vínculo. Estos se enlazan con las locaciones finales que son unas 1500. No todos tienen redundancia, pero si los principales: a los Centros de Atención y Gestión Vecinal (exCGP) y a los hospitales llegan dos vínculos, uno de enlace de fibra propio y otro de Telefónica y a las escuelas llegan dos enlaces también uno de fibra provisto por la ASInf y otro de Fibertel.

[27] Las seis dependencias donde se encuentran los equipos principales son: ASinf (Independencia 635), SAME, CCPP, CUCC, Teatro General San Martín, DICOM. Estos constituyen el Back bone de la red Man.

En los niveles más importantes como el primer nivel de nodos (*back bone*) y el segundo hay redundancia de vínculo en todos los nodos. Si se deja de funcionar un dispositivo o si se corta algún vínculo se en ruta la comunicación. En el enlace final hay redundancia en la mayoría de las locaciones pero no en todas. No se analizó la topología y otros aspectos desde la contingencia. La topología de la acometida y los dispositivos de comunicación de la ASInf, por ejemplo, es única y un problema serio físico podría afectar toda la redundancia existente.

Contingencia.

No disponen de un plan de contingencia. Han solicitado a la firma proveedora Trans que lo confeccione. Realizan pruebas para verificar funcionamiento y para constatar que se produce en rutado alternativo cuando falla algún vínculo sin producir documentación probatoria[28]. No han efectuado análisis de riesgo según la metodología del mismo (hipótesis, impacto, opciones de mitigación etc).

Niveles de servicio.

Los acuerdos de niveles de servicio con los proveedores están incluidos en las condiciones de los pliegos.

Han efectuado un acuerdo de nivel de servicio con el área de educación. No poseen otros acuerdos de niveles de servicio firmados. Utilizan el cuadro con los niveles de servicio pautados y se sacan estadísticas con los mismos. Si alguna área no está satisfecha con él puede pedir otro nivel de atención.

Documentación.

No cuentan con un inventario técnico completo que informe qué equipamiento administran, en qué locaciones se encuentra, y cómo se lo identifica. Cuentan con inventarios parciales de los edificios importantes y de los Ruteadores principales de la red Man. No disponen de un mapa físico completo de la red aunque sí poseen mapas o esquemas parciales. (Ver ejemplos en anexo)

Poseen un inventario parcial de ductos. Realizaron un acuerdo para colocar ductos cada vez que se hace un excavado de forma de extender los ductos para datos en toda la ciudad.

[28] Con excepción de la prueba presenciada por los auditores de la AGCBA que fue documentada.

Disponen de un mapa lógico de la parte principal de la red. No de todas las locaciones atendidas que son más de 1500.

Revisiones.

No se efectúa una revisión sistemática de la seguridad en las redes cada año. Si se revisan algunos aspectos como la longitud de la clave que utilizan los administradores y otros.

Los Planes de la ASInf con relación a contingencia.

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 la aprobación y el presupuesto para el año 2019.

También se planea que Uspallata procese AGC y UAIF en un proyecto de consolidación de procesamiento que también cuenta con aprobación y presupuesto.

Seguridad física.

Infraestructura Data Center de Independencia 635.

Disponen de UPS (Uninterrupted Power System) que, en caso de suspensión del servicio eléctrico, permiten continuar operando durante 50 minutos. Los generadores, extienden el tiempo de servicio a 20 horas, lo que a su vez se prolonga indefinidamente siempre que se pueda proveer combustible. El grupo electrógeno genera 250 KVA y abastece a todo el edificio. Las UPS y el generador son revisados periódicamente.

Para la prevención de incendios, tienen detectores de humo, flores regadoras, matafuegos de anhídrido carbónico, tanques de FM 200, cada elemento para

las diferentes zonas del Data Center. No cuentan con tanques alternativos de gas inhibidor del fuego como sí lo dispone el edificio de Uspallata.

El piso de la sala es técnico. El sistema de refrigeración está duplicado. Hay cámaras que son vigiladas por el personal de seguridad. El cableado es ignífugo.

Han implementado un sistema de control de accesos biométrico en base a la huella digital. El procedimiento de autorización de accesos está escrito y publicado en la intranet, pero no fue aprobado mediante acto administrativo. Este procedimiento habilita el acceso de manera selectiva según la función a los diferentes sectores.

Existen procedimientos escritos para situaciones de emergencia.

Disponen de una caja ignifuga para las copias de respaldo que, además se guardan en sede externa.

Auditoría interna ha efectuado revisiones de la seguridad física del área.

Infraestructura del Centro de Cómputos de Uspallata.

Se ingresa al edificio mediante registro del documento de identidad y se otorga tarjeta magnética para atravesar los molinetes.

El edificio posee monitores que controlan el acceso a servidores, *datacenter* y caja cofre mediante cámaras a cargo de la vigilancia, así como también otras áreas del edificio. Para acceder al mismo se debe efectuar una registración e identificación previa de la huella digital ya que el acceso se controla con dicha tecnología. La vigilancia del edificio está presente las 24 hs. El centro de cómputos no funciona actualmente en el horario nocturno.

En caso de suspensión del servicio eléctrico posee UPS que son controladas mensualmente y que permiten mantener en funcionamiento la infraestructura tecnológica de servidores y de comunicaciones durante 2 horas hasta el arranque de los grupos electrógenos que son de gran porte y se encuentran en el subsuelo, en la misma planta del sector cocheras. Todos estos mecanismos se disparan automáticamente. Al sector de ups y de generadores se accede también mediante dispositivo de huella digital. En todos los casos, en cada acceso, se encuentran cámaras que registran las entradas y salidas. Las puertas poseen dispositivos de seguridad y son anti incendio. Para acceder se deben atravesar dos áreas la primera con la que se accede a la jaula

atravesando la cual se accede al área de servidores. Las instalaciones internas cuentan con piso técnico antiestático elevado.

Posee una sala cofre, ubicada en área separada pero contigua al *Data Center*, cuyo ingreso, al igual que las otras áreas, requiere de la huella digital autorizada y es vigilada mediante cámaras.

Los extinguidores de área, de gran dimensión, se ubican en la planta de cocheras en el sector opuesto a los grupos electrógenos. Utilizan gas permitido (no halón) y el sistema está duplicado.

Toda la instalación eléctrica está construida con materiales ignífugos.

Poseen equipos de refrigeración duplicados con administración sectorizada dentro de la sala.

El sitio posee un importante espacio aún no utilizado.

Según las manifestaciones del auditado, el *Data Center* no puede ser certificado con TIER 3 porque para ello sería necesario recibir alimentación eléctrica desde 2 (dos) proveedores distintos, Edesur y Edenor. Por ley vigente en el territorio argentino, es imposible desarrollar dicha acción, ya que el territorio de suministro está geográficamente delimitado y no hay superposición de servicio.

Ver fotos en anexo Sitio Uspallata.

Plan de recuperación de desastre.

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.

Se definieron las aplicaciones críticas mencionadas anteriormente[29].

La criticidad por las diferentes dimensiones fue evaluada mediante una encuesta a los referentes técnicos de cada sistema.

[29] SIAL, SADE,SIGEHOS, PIG – BA Gestión, SAP, Páginas Web, Boletín Oficial, Mapas – USIG, MiBA, SUACI.

En base a ello se confeccionaron los siguientes documentos:

- • Esquema General
- • Plan de Administración del Desastre
- • Plan de Recuperación
- • Plan de Restauración
- • Esquema Detallado de Uso
- • Esquema de Mantenimiento
- • Esquema de Prueba
- • Anexo de Contactos
- • Manuales de restauración.

El plan se basó en los siguientes supuestos:

- Se ejecutaría si se interrumpe el servicio en forma total de las aplicaciones SADE, SUACI, SIAL, BA Gestión, SIGEHOS y Páginas de buenosaires.gob.ar.
- El centro alternativo no se vio afectado y se encuentra accesible.
- El personal a cargo para ejecutar las tareas definidas en el DRP se encuentra disponible.

Para mayor detalle ver anexo Plan de Recuperación de Desastre.

Acuerdos de niveles de servicio.

La mesa de ayuda cuenta con un cuadro de pautas para la medición y evaluación del nivel de servicio que no está aprobado pero si publicado. Establece el resultado a través de indicadores en función de esta pauta.

Prioridad	Descripción	Tiempo de atención	Tiempo de resolución
Prioridad 1	Impacto a aplicación o servicio crítico. Sin acceso todos los usuarios	30´	6 hs
Prioridad 2	Impacto a una funcionalidad de aplicación. Sin acceso todos los usuarios	30´	8 hs
Prioridad 3	Impacto a una funcionalidad de aplicaron, sin acceso a un grupo de usuarios	1Hs	10 hs
Prioridad 4	Incidente menor que no interrumpe la normal operativa - sin acceso grupo de usuarios	1Hs	48 hs
Prioridad 5	Afecta a un usuario	2HS	72 hs

Si bien no constituye un acuerdo completo para el tratamiento de incidentes es un estadio intermedio que la ASInf podría formalizar de oficio. Por su parte, los usuarios podrían solicitar cambios específicos en caso de que se justificasen.

Para el tratamiento de los incidentes cuenta con un procedimiento no formalizado.

V DEBILIDADES

1-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[30] 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

[30] 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.

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.

2-Alcance incompleto en el tratamiento de la seguridad de la información.

La ASInf 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[31] 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.

3-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 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.

4-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

[31] 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.

un elemento formador del ambiente de control que la dimensión del GCBA justifica plenamente[32].

5-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.

6-Falta de normativa interna para la contingencia.

Las normas internas de la ASInf resoluciones 177/ASINF/2013 y 239/ASINF/2014 no incluyeron la política relativa al plan de contingencia y continuidad de los servicios informáticos por lo que el GCBA carece del marco interno para encuadrar las acciones al respecto. Asimismo las normas no son revisadas periódicamente para su adaptación a los cambios careciéndose de un proceso protocolizado.

7-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.

8-Evaluación de impacto incompleta.

La evaluación de impacto realizada con los sistemas críticos no incluyó a los sistemas que se procesan fuera de la ASInf y fue realizada por los referentes técnicos de los mismos, siendo que debió realizarla el propietario de la información o algún referente de las áreas usuarias no técnicas. Esta evaluación constituye otro de los insumos del análisis de riesgo y es requerido por la norma interna PO0201 - Política de Análisis de Riesgos Tecnológicos. La evaluación del impacto económico asociado a la probabilidad de ocurrencia genera un indicador de la inversión más conveniente para los diferentes

[32] 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.

incidentes potenciales mediante el cálculo de la esperanza matemática de la misma.

9-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 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.

10-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. [33]

11-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.

[33] 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.

12-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[34]. 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.

13-Copias de recupero de años anteriores.

Las copias de respaldo de años anteriores no son sometidas a pruebas de recuperación. Esto implica el riesgo de que en caso de que fuese necesaria su recuperación la misma podría dificultarse o ser de imposible realización. El propietario de la información, una vez designado, debe definir si asume el riesgo de no poder recuperar información resguardada con formatos y sistemas antiguos o si requiere que se verifique el recupero de dichos resguardos con las herramientas en que fueron realizados o si prefiere que las antiguas copias de respaldo se conviertan a los formatos actuales de los sistemas de recupero en uso.

14-Falta de formalización de los acuerdos de niveles de servicio.

No se han formalizado acuerdos formales de nivel de servicio entre la ASInf y los organismos que reciben sus servicios con la excepción de unas pocas excepciones puntuales. Los acuerdos de nivel de servicio son un componente que condiciona las políticas de recupero y seguridad.

15-Asignación de perfiles sin intervención de Propietario de la información.

La asignación de los usuarios a los perfiles de los aplicativos se realiza a solicitud del administrador del sistema que no cuenta con designación formal mientras que la asignación de perfiles a los usuarios en custodia se efectúa a solicitud del Director General del área respectiva. En ambos casos no interviene el propietario de la información por lo que se incumplen las normas internas PO0809 - Política de Administración de Accesos a Recursos de

[34] 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 recuperos ejecutados por otros motivos.

Infraestructura de TI y PO0808 - Política de Administración de Accesos a Software de Aplicación.

16-Documentación de las redes.

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.

17-Areas que manejan su política de implementación.

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.

18-Defectos formales en los procedimientos.

Los procedimientos en la ASInf tienen defectos formales lo que disminuye su estructuración, efectividad y claridad.

- No se encuentran formalizados[35].
- No se revisan periódicamente[36] en forma sistemática ni se cuenta con la trazabilidad de dichas revisiones.
- La operación, el control y la decisión no están bien explicitados y diferenciados en algunos casos.

[35] Las Políticas que se encuentran formalizadas no son procedimientos sino guías para su confección aunque en algunos casos se asemejan a estos.

[36] Esto también es válido para las políticas.

- Hay procedimientos que contienen nombres de agentes.
- No están agrupados en un manual que facilite su consulta y revisión.

19-Falta de independencia de la mesa de ayuda.

La mesa de ayuda no es independiente de las áreas que controla. Mesa de ayuda depende de la DG de infraestructura cuyas áreas son controladas con la información que produce la primera[37]. Si mantuviera una mayor independencia mejoraría el ambiente de control.

VI 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 subredes 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.

[37] Sería interesante que el software de mesa de ayuda y la metodología para medir el servicio fueran únicos dentro del GCBA de modo de poder generar indicadores y efectuar comparaciones de los diferentes resultados homogéneas y centralizadas.

Jean Jaures 220 - C1215ACD - Ciudad Autónoma de Buenos Aires - Tel. 3754-3700

No se ha normado la política relativa a la contingencia, y, aunque se encuentran normadas 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 el rol de las áreas tecnológicas es de mero custodio de la información. 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.

ANEXOS

Anexo COBIT

"COBIT es el único marco de gestión que se ocupa de todo el ciclo de vida de la inversión en TI. El marco soporta el logro de los objetivos de negocio por parte de TI, asegura el alineamiento de TI con el negocio, y mejora la eficiencia y la eficacia de las TI"[38].

Cobit detalla una base de construcción sobre pilares fundamentales y destaca que “las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI”, “proporciona estructuras organizacionales que faciliten la implementación de estrategias y metas” y “asegura que los inversionistas y accionistas logran un debido cuidado estandarizado para la mitigación de los riesgos de TI”

COBIT posee 4 Dominios, que contienen 44 procesos, a su vez, cada uno de ellos puede estar afectado de manera Primaria o Secundaria en sus Aspectos de Gobierno, Criterios de la Información y Recursos de TI.

Dentro de los Aspectos de Gobierno se puede encontrar: Alineación Estratégica, Valor Agregado, Administración de Recursos, Administración de Riesgos, y Administración de Desempeño.

Los Criterios de la Información están compuestos por: Eficacia, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento, y Confiabilidad.

Finalmente, los Recursos de TI se pueden definir como: Aplicaciones, Información, Infraestructura y Personas.

“COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son: Planear y Organizar (PO), proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS). Adquirir e Implementar (AI), proporciona las soluciones y las pasa para convertirlas en servicios. Entregar y Dar Soporte (DS), recibe las soluciones y las hace utilizables por los usuarios finales. Monitorear y Evaluar (ME), monitorear todos los procesos para asegurar que se sigue la dirección provista.”[39]

[38] COBIT- http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/La-traduccion-de-COBIT-4-1-al-espanol-hace-las-Practicas-Internacionales-mas-accesibles.aspx

[39] COBIT 4.1 - https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf

Anexo TIER

El estándar Tier es una norma que describe los criterios para diferenciar cuatro clasificaciones de topología de infraestructura del sitio, basada en los crecientes niveles de los componentes de capacidad redundantes y vías de distribución.

Las Clasificaciones Tier fueron creadas para describir la infraestructura requerida a nivel de sitio para sostener operaciones de centros de datos, no las características de sistemas o subsistemas individuales.

Esta norma se basa en el hecho de que los centros de datos dependen de las operaciones exitosas e integradas de varios subsistemas de infraestructuras de sitios separados, cuyo número depende de las tecnologías individuales.

Se ha tomado el nivel Tier III: Centro de datos Concurrentemente Mantenible.

Requisitos fundamentales:

- Un centro de datos Concurrentemente Mantenible tiene componentes de capacidad redundantes y múltiples vías de distribución que sirven a los equipos de TI. Solamente una vía de distribución es requerida para servir a los equipos TI en cualquier momento.

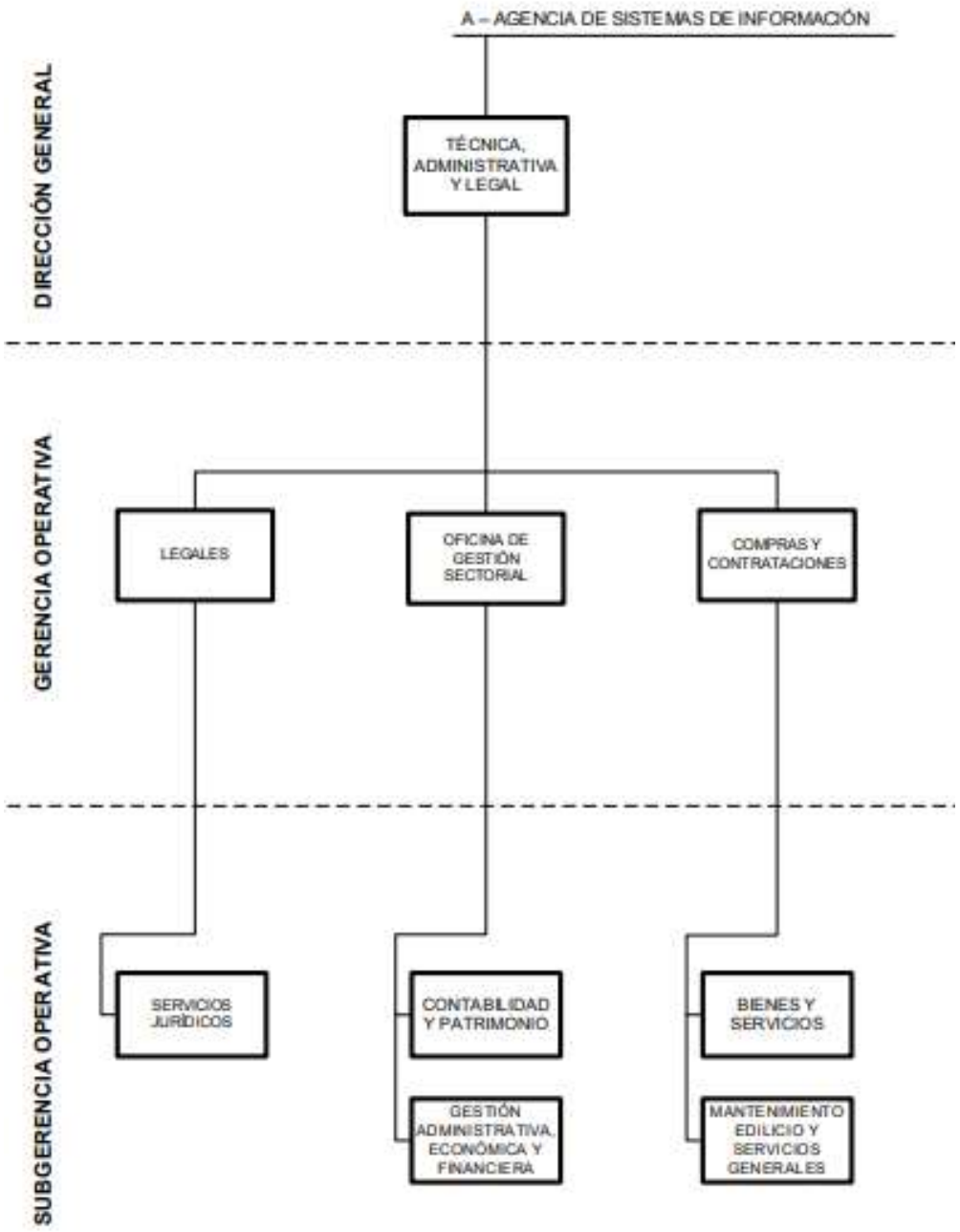
- Todo equipamiento de TI está energizado doblemente, como se define en la Versión 2.0 en la Especificación de Tolerancia por Falla en la Alimentación.

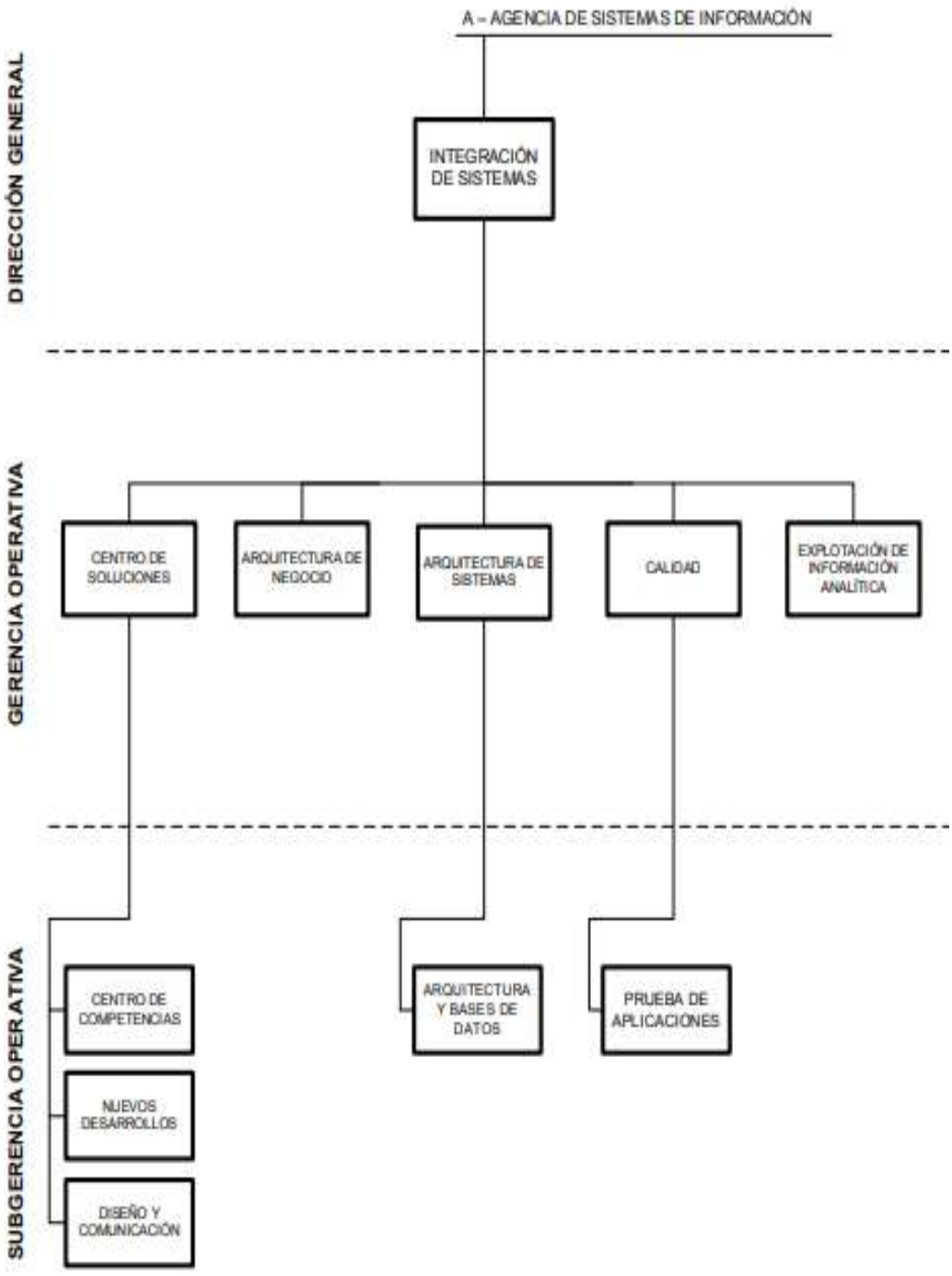
- Doce horas de almacenamiento de combustible en el sitio para una capacidad “N”.

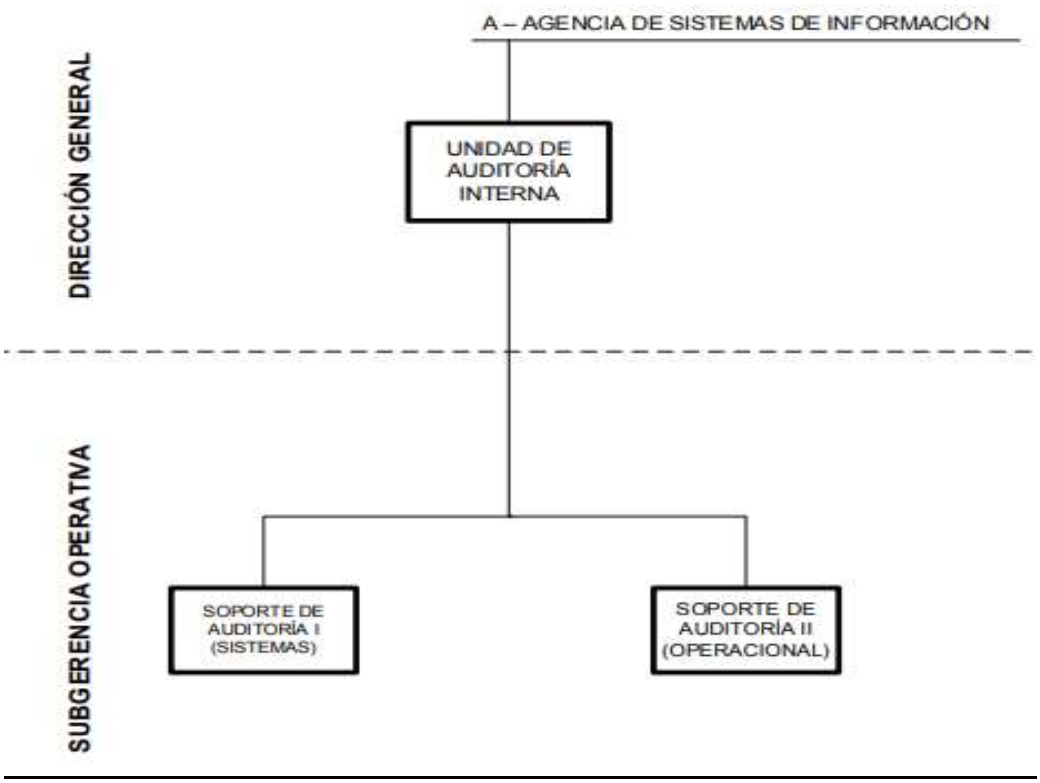
ANEXO ISO 22301 para la Gestión de la Continuidad del Servicio

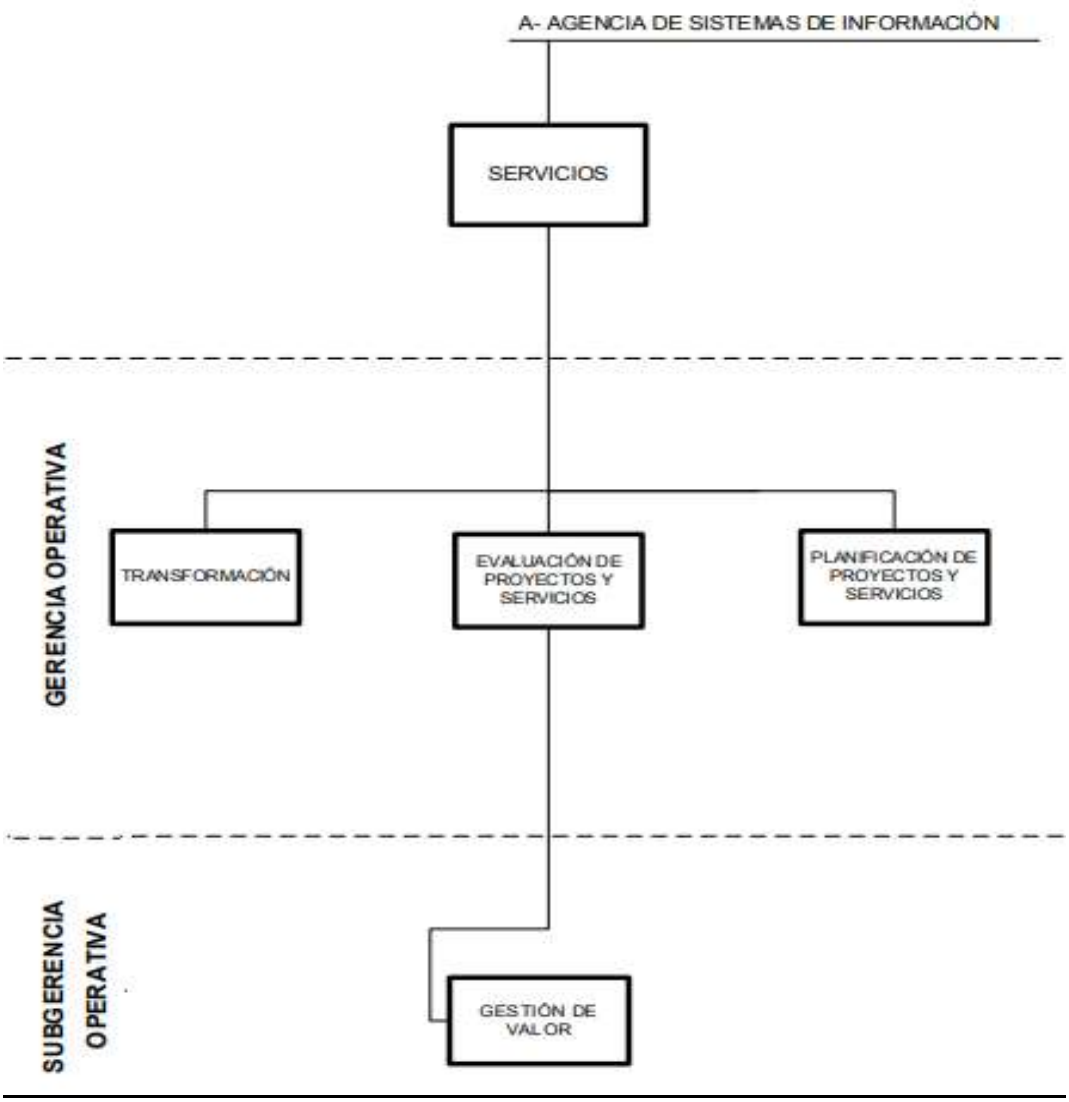
Es una norma internacional de gestión de continuidad de servicio, creada con el objetivo de responder la demanda internacional. Proporciona una base común de entendimiento, desarrollo e implantación de continuidad de negocio, que identifica los fundamentos y establece el proceso, los principios y la terminología de gestión de continuidad de negocio. Proporciona a las organizaciones un marco de trabajo para asegurar la continuidad del servicio en circunstancias inesperadas.

Anexo Organigrama Otras áreas.









Anexo Responsabilidades y acciones de la Dirección General Seguridad Informática

Descripción de Responsabilidades Primarias

Elaborar y/o aprobar las pautas, políticas y normas de seguridad física y lógica de sistemas, equipos informáticos, datos y comunicaciones del Gobierno de la Ciudad Autónoma de Buenos Aires.

Intervenir en las definiciones de los esquemas de seguridad del software, datos y comunicaciones, de los programas de prevención y control de seguridad, y de

los planes de contingencia. Definir, implementar y administrar la Identidad de los usuarios del Gobierno de la Ciudad Autónoma de Buenos Aires.

Administrar la infraestructura de firma digital del Gobierno de la Ciudad Autónoma de Buenos Aires. Administrar y controlar la operatividad de los sitios de internet, el servicio de correo electrónico y el servicio de acceso a internet.

Administrar y controlar los procedimientos de seguridad lógica de acceso a los componentes del software de base y aplicativo de los servidores bajo responsabilidad de la Agencia de Sistemas de Información. Definir los mecanismos de monitoreo, alarmas, y monitorear los sistemas y las redes de comunicaciones para detectar intentos de acceso no autorizados al software aplicativo, y a los datos almacenados en los servidores bajo la responsabilidad de la Agencia de Sistemas de Información.

Participar en la capacitación de usuarios con el objetivo de entrenar, informar y concientizar en materia de seguridad informática.

Gerencia Operativa Seguridad de la Información

Descripción de Acciones

Definir e implementar el software relacionado con el análisis de riesgo y pruebas de vulnerabilidad de los servidores, aplicativos y sistemas bajo la responsabilidad de la Agencia de Sistemas de Información.

Definir e implementar el software relacionado con la detección en tiempo real de ataques, intentos de acceso no autorizado a las redes, telecomunicaciones, aplicativos, datos y servidores bajo la responsabilidad de la Agencia de Sistemas de Información.

Garantizar el nivel de seguridad requerido para el pasaje a producción de las aplicaciones que se encuentren bajo responsabilidad de la Agencia de Sistemas de Información.

Definir las políticas de seguridad de aplicación en la Ciudad Autónoma de Buenos Aires. Analizar y generar informes de los incidentes o ataques con elevadas posibilidades de éxito que pudieran afectar la prestación de servicios y elevarlos al Director General.

Investigar, analizar y definir las pautas de seguridad informática en los proyectos del Gobierno de la Ciudad Autónoma de Buenos Aires que involucre la utilización de tecnologías de la información. Definir y administrar el software para contener y resguardar la identidad de los usuarios del Gobierno de la Ciudad Autónoma de Buenos Aires.

Definir y administrar el esquema de autenticación y autorización de los usuarios a los recursos de tecnologías de la información del Gobierno de la Ciudad Autónoma de Buenos Aires.

Asistir al Director General en la planificación de las capacitaciones en materia de seguridad informática.

Asistir al Director General en la elaboración, implementación y ejecución de proyectos relacionados con la asistencia al ciudadano en temas de seguridad de la información

Asistir al Director General en la elaboración de políticas y normas de seguridad física y lógica de sistemas, equipos informáticos, datos y comunicaciones del Gobierno de la Ciudad Autónoma de Buenos Aires.

Subgerencia Operativa Accesos, Investigación y Administración de la Identidad

Descripción de Acciones Administrar los accesos a la información, las redes y aplicaciones del Gobierno de la Ciudad Autónoma de Buenos Aires.

Administrar y autorizar los accesos remotos a la red del Gobierno de la Ciudad Autónoma de Buenos Aires. Administrar la seguridad de las estaciones de trabajo del Gobierno de la Ciudad Autónoma de Buenos Aires.

Administrar la solución de antispam y las pautas de seguridad del correo corporativo del Gobierno de la Ciudad Autónoma de Buenos Aires.

Administrar la identidad de los usuarios del Gobierno de la Ciudad Autónoma de Buenos Aires. Administrar, controlar y aplicar las políticas de seguridad en estaciones de trabajo y servidores.

Supervisar la implementación de la autenticación de los usuarios a los recursos de comunicación e informáticos de la red del Gobierno de la Ciudad Autónoma de Buenos Aires. Mantener y actualizar la plataforma de seguridad de la información implementada.

Subgerencia Operativa Monitoreo, Prevención Y Detección

Descripción de Acciones

Instalar, configurar y operar un sistema de monitoreo para relacionar los eventos que proveen los equipos de seguridad. Administrar un sistema de alertas tempranas de incidentes de seguridad informática e implementar un

sistema de escalamiento de los mismos. Instalar, configurar y operar el hardware y el software de los equipos que se utilicen para realizar análisis y test de penetración de aplicaciones web, aplicaciones móviles y activos de red.

Implementar y controlar los procesos que garanticen el nivel de seguridad requerido para el pasaje a producción de las aplicaciones que se encuentren bajo responsabilidad de la Agencia de Sistemas de Información.

Capacitar a los desarrolladores en lo referente a la programación segura e implementar capacitaciones sobre herramientas de detección de vulnerabilidades. Configurar y administrar los equipos de seguridad para la prevención de intrusiones y vulnerabilidades.

Implementar y administrar un sistema de antivirus y antispyware en las estaciones de trabajo del Gobierno de la Ciudad Autónoma de Buenos Aires y en los servidores bajo responsabilidad de la Agencia de Sistemas de Información.

Mantener actualizado los firmwares, firmas de detección y sistemas operativos de los activos de seguridad bajo la responsabilidad de la Gerencia Operativa. Realizar los análisis de seguridad en búsqueda de las causas de un ataque informático detectado o reportado.

Anexo Plan de Recuperación de Desastre.

Se enumeran a continuación los documentos del procedimiento de DRP Plan de Recuperación de desastre:

1.1.1 Identificación de procesos de negocio

1.2.1 - Informe Resultados BIA

1.3.1 - Informe Entendimiento Situación Actual Aplicaciones

1.4.1 - Estrategia de Recuperación

2.1.1 Esquema General

2.1.2 Plan de Administración del Desastre

2.1.3 Plan de Recuperación

2.1.4 Plan de Restauración

2.1.5 Esquema detallado de uso

2.2.1 Esquema de Prueba

2.2.2 Esquema de Mantenimiento

2.2.3 Template Prueba

1.1 Identificación de procesos del negocio.
1.2 Objetivo
La identificación de procesos de negocio tiene como objetivo definir el alcance, identificando los procesos sobre los cuales se pretende desarrollar las estrategias de continuidad.
1.3 Procesos por aplicación
1.2.1 Análisis de Impacto en el Negocio (BIA Business Impact analysis)

1. Resumen ejecutivo

En un entorno de negocios y de tecnología en constante cambio y cada vez más complejo, interrupciones no planificadas pueden dar lugar a pérdidas financieras y no financieras importantes.

Para desarrollar un plan de continuidad de negocio eficaz, el primer paso es entender la organización a través de un Análisis de Impacto al Negocio (BIA). El mismo es un proceso de análisis de los procesos y los efectos que una interrupción del negocio podría tener sobre ellos. El BIA es un documento que identifica y da prioridad a las actividades críticas referentes a la continuidad del servicio por parte de la organización.

2. Desarrollo

2.1. Objetivo

El objetivo de este informe es documentar la información reunida de los distintos Key User acerca de los procesos críticos del Gobierno de la Ciudad de Buenos Aires (GCBA) mediante la documentación de su importancia en relación con las operaciones en curso y los recursos informáticos necesarios para recuperar un mínimo de sus funciones

2.2. Metodología de trabajo

Se efectuaron una serie de encuestas en las diferentes aplicaciones críticas por la agencia de información

2.3. Conclusiones BIA

Los aspectos principales tenidos en cuenta para el desarrollo del BIA, son los siguientes:

1. Identificación y descripción de las funciones principales de los servicios.

2. Cómo impacta la contingencia en la disponibilidad del servicio.

3. Cuánto tiempo puede operarse si determinados servicios se ven afectada por una contingencia.

2.3.1 Informe de Relevamiento y Situación Actual

1 Objetivo.

El presente documento tiene como objetivo documentar la situación actual referente a las aplicaciones identificadas como críticas por la ASInf.

2 Detalle del relevamiento

2.1 SIAL

2.2 SADE

2.3 SIGEHOS

2.4 PIG – BA Gestión

2.5 SAP

2.6 Páginas Web

2.7 Boletín Oficial

2.8 Mapas - USIG

2.9 MiBA

2.10 SUACI

3 Entendimiento de Networking.

La infraestructura de red del Gobierno de la Ciudad De Buenos Aires se encuentra formada por los siguientes componentes principales:

• Red MAN (Backbone): Anillo de fibra óptica que interconecta todos los nodos de la red del Gobierno de la Ciudad de Buenos Aires. Todos los hospitales, ministerios, escuelas y demás organismos se encuentran conectados a esta red para el uso de los servicios a través del Nodo ASInf.

• Nodo ASI: Nodo principal del BACKBONE en el cual se encuentra la conexión con el Data Center de la Agencia de sistemas de información mediante el cual

pasa todo el tráfico de los usuarios para el consumo de los servicios y aplicaciones internas.

• Firewalls Internet: Firewalls de salida a internet para los usuarios dentro de la red.

• Router BGP: Routers de borde con salida a internet de proveedores TASA, IPLAN y CABASE.

• F5 Load Balancer: Balanceador de carga para tráfico entrante a los Data Center.

4. Estrategia de Recuperación

1 Objetivo

El presente documento tiene como objetivo identificar y detallar la estrategia de recuperación establecida por la Agencia de Sistemas de Información (ASI) del Gobierno de la Ciudad de Buenos Aires para el presente plan de contingencia.

En el mismo se detallarán los siguientes puntos:

• Arquitectura de sitios de contingencia

• Componentes de infraestructura

• Componentes de telecomunicaciones

• Réplicas entre sitios

2 Estrategia de recuperación.

La estrategia de recuperación consiste en tener un data center secundario en la sede de Parque Patricios (Uspallata 3160, CABA) con infraestructura de soporte para las aplicaciones identificadas como críticas que se encuentran hosteadas en el data center de la ASINF (Av. Independencia 635, CABA), estableciendo un esquema de replicación entre ambos sitios y en caso de una contingencia trasladar las operaciones al sitio secundario.

2.1 Telecomunicaciones

2.2 Equipos principales de procesamiento y almacenamiento de información

Soporte aplicaciones y virtualización:

Storage y Base de datos

2.3 Esquema de Replicación

Los sitios de procesamiento contarán con un esquema de replicación online entre los componentes que se mencionan a continuación:

• Réplica entre centros de cómputo (8 pelos de fibra dedicados)
• Réplica entre redes SAN (8 pelos de fibra dedicados)

• Réplica entre equipos de Oracle Exadata utilizando Oracle Dataguard (Por red SAN)

• Réplica entre motores mySQL y PostgreSQL

• Réplica entre vCenters (por red de Data Center)

3 Anexo Infraestructura de Parque Patricios.

3.1 Servidores

Hpe bladesystem c7000 enclosure

Hpe proliant bl460c gen9

3.2 Almacenamiento y Storage

Configuración hitachi vsp g1000:

Configuración de software 11

Configuración oracle exadata

3.3 Plataforma de Red

Equipos de acceso

Equipos de data center

4. Esquema General del Plan.

4.1 Objetivo

Realizar el Plan de Recuperación ante Desastres (DRP) de los Sitios de Procesamiento soporte de las aplicaciones identificadas como críticas en alta disponibilidad de la ASInf. Actualmente, se cuenta con dos sitios de procesamiento, detallados a continuación:

• Sitio de Procesamiento Principal: Av. Independencia 635 – Ciudad Autónoma de Buenos Aires, Argentina.

• Sitio de Procesamiento Alternativo: Uspallata 3160 – Ciudad Autónoma de Buenos Aires, Argentina.

El DRP cubre la ocurrencia de un desastre que afecte en su totalidad las aplicaciones SADE, SIGEHOS, SIAL, SUACI, BA Gestión y las Páginas de buenos aires.gob.ar, alterando la normal prestación del servicio informático.

El DRP consiste en organizar las decisiones necesarias a ser tomadas por el personal, en caso que se presente una contingencia en alguna de las aplicaciones anteriormente mencionadas.

4.2 Alcance

El Plan de Recuperación ante Desastres (DRP) de los Sitios de Procesamiento, contempla las tareas que se deberán realizar para garantizar el restablecimiento de la operación total de las aplicaciones críticas en caso de ocurrencia de un siniestro. Se definió como PDC Centro de procesamiento principal al de Av. Independencia 635 y como RDC Recovery Data Center al correspondiente a Uspallata 3160

El DRP contempla las actividades a desarrollar por las áreas IT de la ASInf en caso de una contingencia. Asimismo, y en función de la estrategia de recuperación elegida por la ASInf, las aplicaciones que han sido definidas como críticas para la continuidad de los servicios y que serán contemplados en el Plan se listan a continuación:

4.3 Premisas y limitaciones

El presente Plan de Recuperación ante Desastres fue diseñado y documentado por EY bajo las siguientes premisas y limitantes de la ASInf:

• La ASInf definió responsables técnicos y funcionales por aplicación con el fin de proveer información y procedimientos de recuperación técnica.

• Los mismos fueron los encargados de proveer los pasos de resolución de los problemas.

• Dicha información fue tomada como válida y confiable en la documentación de los planes de remediación. EY no realizó validación de integridad de la información suministrada.

• La ASInf definió que el DRP alcance a las aplicaciones críticas SADE, SIAL, SUACI, SIGEHOS, BA Gestión y Páginas Web Buenosaires.gob.ar.

• EY solo realizará pruebas del DRP sobre las siguientes aplicaciones a pedido de la ASInf:

- SADE
- SIAL

• SUACI

• SIGEHOS

• BA Gestión

• Páginas Web

• EY no realizará pruebas de performance sobre enlaces y dispositivos de comunicación de forma tal de garantizar que los mismos puedan soportar la carga adicional tanto en la prueba como en una eventual futura contingencia.

• Antes del cierre de cada documento técnico referente a la recuperación se solicitó conformidad respecto de cada responsable de área respecto de la integridad y claridad de los contenidos.

4.4 Documentos

Los documentos que conforman el DRP son los siguientes:

• Esquema General

• Plan de Administración del Desastre

• Plan de Recuperación • Plan de Restauración

• Esquema Detallado de Uso

• Esquema de Mantenimiento

• Esquema de Prueba

• Anexo de Contactos

• Manuales de restauración y orden de encendido

4.5 Estrategia de Recuperación

4.6 Supuestos

A continuación, se detallan los supuestos sobre los cuales se elaboró el DRP de los Sitios de Procesamiento:

• El plan de DRP se desarrollará bajo el hipotético escenario de interrupción total del servicio de las aplicaciones SADE, SUACI, SIAL, BA Gestión, SIGEHOS y Páginas de buenosaires.gob.ar.

• Solo las aplicaciones de un Sitio de Procesamiento han sido inhabilitadas por el evento, no ocurriendo un desastre en los dos Sitios de Procesamiento al mismo tiempo.

• El RDC no ha sido afectado y se encuentra accesible.

• Contar con personal calificado disponible para ejecutar las tareas definidas en el DRP.

• El mantenimiento y actualización del plan será realizado periódicamente para asegurar la ejecución del mismo, siendo llevada a cabo dicha tarea por responsables que el propio organismo se encargará de designar.

• Haber implementado el plan de capacitación necesario para el personal involucrado.

• Haber realizado la prueba integral del presente plan.

4.7 Aplicación general de los documentos del DRP

4.7.1 Visión general del Plan

4.8 Responsabilidad de los equipos de trabajo y sectores

4.9 Descripción de los equipos de trabajo

4.10 Organización del DRP de los Sitios de Procesamiento

5. Plan de Administración del Desastre

5.1 Esquema de Respuesta ante Emergencias

5.1.1 Oportunidad de Aplicación

5.1.2 Introducción

5.1.3 Equipo de respuesta

El equipo de Respuesta será el encargado de coordinar las medidas operativas de emergencia necesarias según el tipo de siniestro o falla técnica significativa ocurrida.

5.1.4 Fallas Técnicas significativas (caída parcial)

Estos tipos de caídas hacen referencia a aquellas fallas que puedan afectar al correcto funcionamiento de las aplicaciones que se encuentran bajo el alcance del plan, las mismas pueden corresponder a fallas técnicas o desastres ocasionales

6.1. Esquema de Notificación

Se encuentra perfectamente definido los pasos y procedimientos correspondientes al esquema de notificación, líderes y equipo de dirección estratégica.

6.2. Esquema de notificación

6.3 Esquema de Evaluación inicial del daño

El propósito de la evaluación inicial del daño es determinar la indisponibilidad de las instalaciones o interrupción de las aplicaciones críticas en alta disponibilidad del negocio.

6.3.1 Esquema de Evaluación inicial del daño – oportunidad de aplicación

6.4 Esquema de Declaración del desastre

El propósito del Esquema de Declaración del Desastre es definir los pasos a seguir para realizar la declaración del desastre o falla presentada y así efectivizar la activación del DRP

6.4.1 Esquema de Declaración del Desastre

7.1. Plan de Recuperación

7.1. Esquema de recuperación técnica

71.1. Esquema de recuperación técnica – Diagrama de aplicación

7.1.2. Descripción del esquema de recuperación técnica

El Plan de Recuperación Técnica desarrollado tiene por objeto detallar los procedimientos a seguir en el Sitio de Procesamiento ante la declaración de un desastre. El objetivo principal de la ASInf es recuperar la operatoria de las Aplicaciones críticas ya sea en forma aislada como así también integrada asumiendo que el resto de las integraciones satélites, dispositivos de comunicación e infraestructura de soporte funcionan correctamente.

7.2. Estrategia de recuperación técnica

Siniestro o falla técnica significativa que afecte al PDC donde reside el equipamiento e infraestructura de soporte de las aplicaciones críticas del negocio de la ASInf

7.3. Procedimiento de recuperación técnica general

7.4. Documentación de recuperación y restauración técnica

Se listan los documentos que forman parte del “Anexo I - Documentos Orden de Encendido”, los cuales contienen los procedimientos para recuperar las aplicaciones incluidas dentro del alcance, considerando la estrategia de recuperación establecida previamente.

En cada uno de los documentos, se detalla:

- Descripción de la contingencia
- Supuestos y premisas a tener en cuenta
- Explicación paso a paso para realizar la recuperación

8.1. Plan de Restauración del Sitio Original

1.1. Esquema de restauración

8.1.1. Esquema de restauración - oportunidad de aplicación

8.1.2. Objetivo

El Plan de Restauración desarrollado tiene por objeto detallar los procedimientos a seguir para restablecer la operación en el Sitio de Procesamiento Principal (PDC) afectado por un siniestro que ocasione el traslado de la operación de la/las aplicaciones críticas del PDC al RDC, con el objetivo de:

• Restablecer la capacidad de procesamiento del equipamiento y la infraestructura de soporte de las aplicaciones críticas del negocio definidas por la ASInf.

Para cumplir con este objetivo, se han identificado dos tareas:

• Procedimientos de Evaluación Final del Daño. • Procedimientos de Restauración del equipamiento del PDC.

8.1.3. Procedimiento de evaluación final del daño

La evaluación final del daño será llevada a cabo con el objeto de analizar las causas del siniestro o la falla técnica significativa, determinar las medidas preventivas necesarias, los recursos a ser reparados y/o reemplazados y el tiempo de recuperación del Sitio de Procesamiento afectado. Definiendo tareas y responsables en cada caso.

8.1.4. Procedimiento de restauración del sitio de procesamiento original

Las acciones a ejecutar para la recuperación de las operaciones en el sitio contingente

8.1.5 Esquema Detallado de uso del DRP

1. Esquema detallado del uso del DRP.

1.1 Objetivo

El Esquema detallado del uso del DRP tiene como objetivo describir los recursos de la ASInf implicados y los documentos del Plan de Recuperación ante Desastres (DRP) a ser utilizados frente a la ocurrencia de un problema o incidente acontecido en la Agencia de Sistemas de Información (ASInf).

En este esquema se detallan, paso por paso, las tareas a realizar por cada recurso en el momento que le corresponda conforme se va analizando el evento, haciendo uso de aquellos documentos del DRP que en cada tarea le sirvan de apoyo.

1.2 Esquema de uso del DRP

Este esquema incluirá la descripción de Actividad, Responsable, Descripción y Documento

1.2.1 Esquema de Prueba

2.1 Objetivo

El Esquema de Prueba tiene como objetivo describir las estrategias de prueba del Plan de Recuperación ante Desastres (DRP). Estas deberán ser utilizadas por la ASInf para asegurar la efectividad y validez del Plan.

2.2 Responsabilidades

Los Responsables del DRP tendrán que:

• Realizar la coordinación y ejecución de las pruebas del Plan de Recuperación ante Desastres (DRP). • Evaluar la necesidad de algún tipo de cambio en las estrategias de prueba definidas en este esquema, teniendo en cuenta las necesidades de la ASInf y los cambios realizados en los diferentes esquemas a través del tiempo. • Documentar los resultados tras ejecutar las Pruebas de forma pertinente en la documentación del DRP.

Los Equipos de Trabajo y cada miembro de la ASInf que se encuentre involucrado en la Prueba del Plan tendrá la responsabilidad de:

• Canalizar, mediante los Responsables del DRP el Mantenimiento y todo problema que haya surgido durante la ejecución del Plan, así como también la solución que se le dio al problema. • Indicar soluciones dadas a los problemas surgidos al ejecutar el Plan.

2.3 Objetivos de las Pruebas

Los objetivos de probar el Plan de Recuperación ante Desastres (DRP) son los siguientes:

• Asegurar la efectividad del DRP.

• Detectar fortalezas y debilidades del DRP e identificar oportunidades para mejorarlo.

• Familiarizar al personal de la ASInf con el DRP en su totalidad.

Los objetivos mencionados son generales y abarcan a todos los esquemas incluidos en el Plan. Para la realización de la prueba de un Esquema o Procedimiento en particular se deben definir objetivos específicos

2.4 Alcance y periodicidad de las Pruebas

El Plan de Recuperación ante Desastres (DRP) debe ser sometido a pruebas para cumplir con los objetivos definidos.

Resulta fundamental definir el alcance y periodicidad de las pruebas a realizar:

• El alcance de la prueba de un esquema está dado por el grado de cobertura que tendrá la prueba. Es decir, si la prueba cubrirá todos los aplicativos contemplados en el DRP o no; es por ello que esta puede ser integral o parcial.

• La periodicidad de la prueba de un Esquema indica cada cuánto tiempo se tiene que llevar a cabo la prueba (anualmente, semestralmente, etc.)

2.5 Enfoque de las Pruebas

El enfoque mínimo de pruebas a llevarse a cabo por la ASInf será el siguiente:

• Se deberá realizar como mínimo una prueba integral anualmente.

• La prueba de contemplar el corte programado de las operatoria de las Aplicaciones críticas en el sitio de procesamiento principal y el recupero de su

operatoria en el otro sitio de procesamiento, que funcionará como sitio de procesamiento alternativo.

• Los resultados de la prueba deberán ser documentados y anexados a los procedimientos del Plan de Recuperación de Desastres.

2.6 Esquema de Mantenimiento

2.6.1 Importancia del documento

Para lograr que la recuperación de la operatoria sea viable, precisa y adecuada, el Plan de Recuperación ante Desastres (DRP) debe mantenerse actualizado. Para ello, se debe contar con el esfuerzo continuo de todo el personal de la ASInf de modo tal que cualquier cambio que pueda afectarlo sea reflejado y documentado adecuadamente.

2.6.2 Responsabilidad

El mantenimiento del DRP se encuentra a cargo de Responsables, que se encuentran indicados en el Anexo de Contactos:

• Un responsable del DRP para el PDC (Primary Data Center) (Ver Anexo de Contactos).

• Un responsable del DRP para el RDC (Recovery Data Center) (Ver Anexo de Contactos).

Los Responsables del Mantenimiento del DRP deberán asegurar que los responsables asignados para la actualización de las diferentes partes del DRP efectúen esta tarea correctamente y con la periodicidad definida.

2.6.3 Objetivos y responsabilidades de los responsables del Mantenimiento

Están indicadas en un cuadro descriptivo

2.6.4 Objetivos y responsabilidades de los Equipos de Trabajo respecto al mantenimiento

Están indicadas en un cuadro descriptivo

2.6.5 CONSIDERACIONES GENERALES DE MANTENIMIENTO

2.6.6 Distribución de las actualizaciones del DRP

Indica los responsables que deberán recibirlas

2..6.7 Comunicación de las actualizaciones

Indica el procedimiento para efectuar las comunicaciones

2.6.8. Procedimiento de mantenimiento del DRP

3.1 Evaluación de riesgos y funciones críticas de negocio

Las siguientes áreas deben participar en la reunión semestral de riesgos (o de frecuencia a definir por el Equipo de Dirección Estratégica) a efectos de evaluar los riesgos potenciales a los que se encuentra expuesta la ASInf, desde el punto de vista de sus funciones:

• Responsable del DRP.

• Gestión operativa aplicaciones.

• Gestión de la infraestructura.

• Service Desk.

• Disponibilidad y performance.

3.2 Mantenimiento de Planes

Incluye un cuadro indicando:

Esquema, Detalle, Frecuencia, Procedimiento y Responsable

3.3 Template de Prueba DRP

1. Introducción
2. Descripción de la prueba
    - 2.1 Fecha y lugar de la prueba
    - 2.1 Objetivos
    - 2.2 Alcance
3. Características generales del Ambiente de Prueba
4. Participantes en la prueba
5. Plan de Prueba
6. Descripción detallada de la estrategia del plan de pruebas

6.1 Traslado de ambiente a probar de PDC a RDC

6.1.1. Tareas previas a la realización de la prueba

6.1.2. Tareas de simulación de bajada de servicio

6.1.3. Tareas para traslado del ambiente a probar de PDC a RDC y subida del ambiente en el destino

6.2. Fallback de ambiente a probar de origen a destino

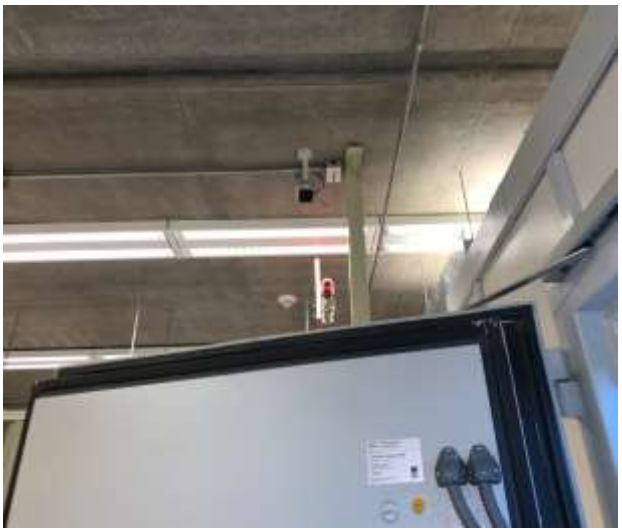
6.2.1. Tareas de simulación de bajada de servicio

6.2.2. Tareas para traslado (Fallback) ambiente a probar de PDC a RDC y subida del ambiente en destino

6.2.3. Tareas de verificación del correcto funcionamiento del sistema productivo original incluyendo los cambios realizados por la prueba

ANEXO FOTOS

Acceso a servidores, *data center* y caja cofre, está monitoreado por cámaras, acceso con huella digital y vigilancia del edificio 24 horas.



Las puertas poseen dispositivos de seguridad y son anti incendio.

Extinguidores de área ubicados en la planta de cocheras en el sector opuesto a los grupos electrógenos.

Jean Jaures 220 - C1215ACD - Ciudad Autónoma de Buenos Aires - Tel. 3754-3700

Anexo: Software o servicios que utiliza la Agencia de Sistemas de Información:

Software o Servicio:	Descripción:
Vmware vsphere esxi Hypervisor	Es una plataforma de virtualización a nivel de centro de datos. Está compuesto por un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software *hipervisor* y los servicios y servidores que permiten la interacción con el software de gestión y administración y las máquinas virtuales
Vmware Vcenter Management	Es un software de administración de servidores que suministra una plataforma centralizada para administrar los entornos de VMware v Sphere, lo que le permite automatizar y suministrar una infraestructura virtual en la nube híbrida.
VMware Site Recovery Manager Orchestration	VMware Site Recovery Manager es un software de automatización que se integra con una tecnología de replicación subyacente para proporcionar administración basada en políticas, pruebas no disruptivas y orquestación automatizada de planes de recuperación.
VMware Replication Manager Orchestration	VMware v Sphere Replication es una extensión de VMware vCenter Server que proporciona replicación y recuperación de máquinas virtuales basadas en hipervisores. Después de configurar la infraestructura de replicación, se pueden elegir las máquinas virtuales que se replicarán en un punto objetivo de recuperación diferente (RPO).

Jean Jaures 220 - C1215ACD - Ciudad Autónoma de Buenos Aires - Tel. 3754-3700

VMware Vrealize Operation Management	Se basa en una plataforma resistente con escalabilidad horizontal, diseñada para proporcionar información operativa detallada, que permite automatizar la gestión de las aplicaciones y la infraestructura en entornos virtuales, físicos y en la nube.
Turbonomic Management	Determina las demandas de recursos en tiempo real de las máquinas virtuales, contenedores, almacenamiento y servicios de bases de datos en la nube.
Redhat Linux OS	Sistema operativo que sirve de base a las aplicaciones actuales, y se puede implementar en equipos sin sistema operativo, en entornos virtuales, en contenedores y en entornos de nube.
Oracle Enterprise Database	Base de datos para aplicaciones de misión crítica,
Mysql Database	Es un sistema de gestión de bases de datos relacionales de código abierto y de libre acceso que utiliza el lenguaje de consulta estructurado (SQL).
Mariadb Database	MariaDB es un derivado del sistema de gestión de bases de datos relacionales MySQL, con soporte comercial. Es software libre y de código abierto.
Windows Server OS	Sistema operativo diseñado para servidores de la firma Microsoft.

Openshift Platform Private Container Cloud Platform	OpenShift es una familia de software de contenedores desarrollada por Red Hat.
Cloudform Cloud Orchestration	Plataforma de gestión para la nube híbrida y abierta.
Ansible Orchestration	Plataforma de software libre para configurar y administrar computadoras.
Oracle Enterprise Manager Management	Software para Administrar las bases de datos de Oracle,
ELK Elastic Search Kibana	Es un conjunto de herramientas de código abierto para la administración de registros, la monitorización, consolidación y análisis de logs generados en múltiples servidores.
Veeam Aivailability Suite Backup	Producto que Gestiona todas las cargas virtuales, físicas y cloud y la recuperación de servicios IT, aplicaciones y datos.
Veeam One Management	Software para visibilizar y administrar el entorno de IT, incluidas las cargas virtuales y las físicas y cloud.
IBM Spectrum Management	Es un producto de respaldo y recuperación, que se puede utilizar con almacenamiento físico, virtual o en la nube, proporciona replicación de sitios múltiples y gestión de recuperación ante desastres.

HDS Device Manage Management	Se utiliza para monitorear los subsistemas de almacenamiento conectados a los servidores.
HDS Storage Navigator Management	Administrador de dispositivos a través de una red TCP/IP (TCP: protocolo de control de transmisión. IP: protocolo de Internet). Varios sistemas de almacenamiento de datos pueden ser gestionados por un cliente de administración. Administrador de dispositivos: Storage Navigator debe configurarse para cada sistema de almacenamiento.
HDS Storage Advisor Management	Es una solución de administración de infraestructura que unifica el aprovisionamiento de almacenamiento, la protección de datos y la administración de almacenamiento. Simplifica la administración de los centros de datos a gran escala al proporcionar servicios de software más inteligentes y es extensible para proporcionar una mejor capacidad de programación y un mejor control.
Mongo DB Database	Es un sistema de base de datos No SQL, está orientado a documentos de código abierto, es una base de datos adecuada para su uso en producción y con múltiples funcionalidades.

SQL Server Database	Es un sistema de gestión de bases de datos relacionales (RDBMS) de Microsoft, de manejo de bases de datos relacionales que permite programar en entornos híbridos ya sea de forma local o en la nube de Microsoft.
Apache Tomcat Java Platform	Tomcat es un contenedor de servlets que se utiliza en la Referencia oficial desarrollado con Java, pudiendo funcionar en cualquier sistema operativo con su máquina virtual java correspondiente, siendo un servidor Web con soporte de servlets y JSPs.
Apache WebServer WbServer	Servidor Web multiplataforma de fuente abierta.
F5 LTM Load Balancer	F5 LTM Es un módulo ofrecido en plataforma BIG-IP De F5. Siendo este un Proxy completo, lo que le permite aumentar las conexiones del lado del servidor y del cliente. Toma decisiones sobre el equilibrio de la carga en cuanto a disponibilidad, rendimiento y persistencia.

Schneider DCIM Datacenter Infraestructure Manager	Sftware de monitoreo de la infraestructura del Data center y otras locaciones IT
Pentaho Ops BI	Pentaho, es un software de inteligencia empresarial que proporciona integración de datos. Servicios OLAP (procesamiento analítico en línea, informes, paneles de información, extracción de datos y capacidades de extracción**.)**
Grafana Monitoring	Grafana es un software de código abierto, permite la visualización y el formato de datos métricos. Permite crear cuadros de mando y gráficos a partir de múltiples fuentes, incluidas bases de datos de series de tiempo.
Prometheus Monitoring	Prometheus es un software de código abierto, que almacena los datos como series de tiempo, flujos de valores con marcas de tiempo que pertenecen a la misma métrica y al mismo conjunto de dimensiones. Además de las series temporales almacenadas, puede generar series temporales derivadas como resultado de consultas.

Anexo Ejemplos de Diagramas de Sistemas y Aplicaciones que administra la ASInf con sus respectivos esquemas.

SIAL

El Sistema Integrado de Administración y Liquidación (SIAL), es utilizado en el proceso de administración y liquidación de haberes, su arquitectura se encuentra definida por los siguientes componentes:

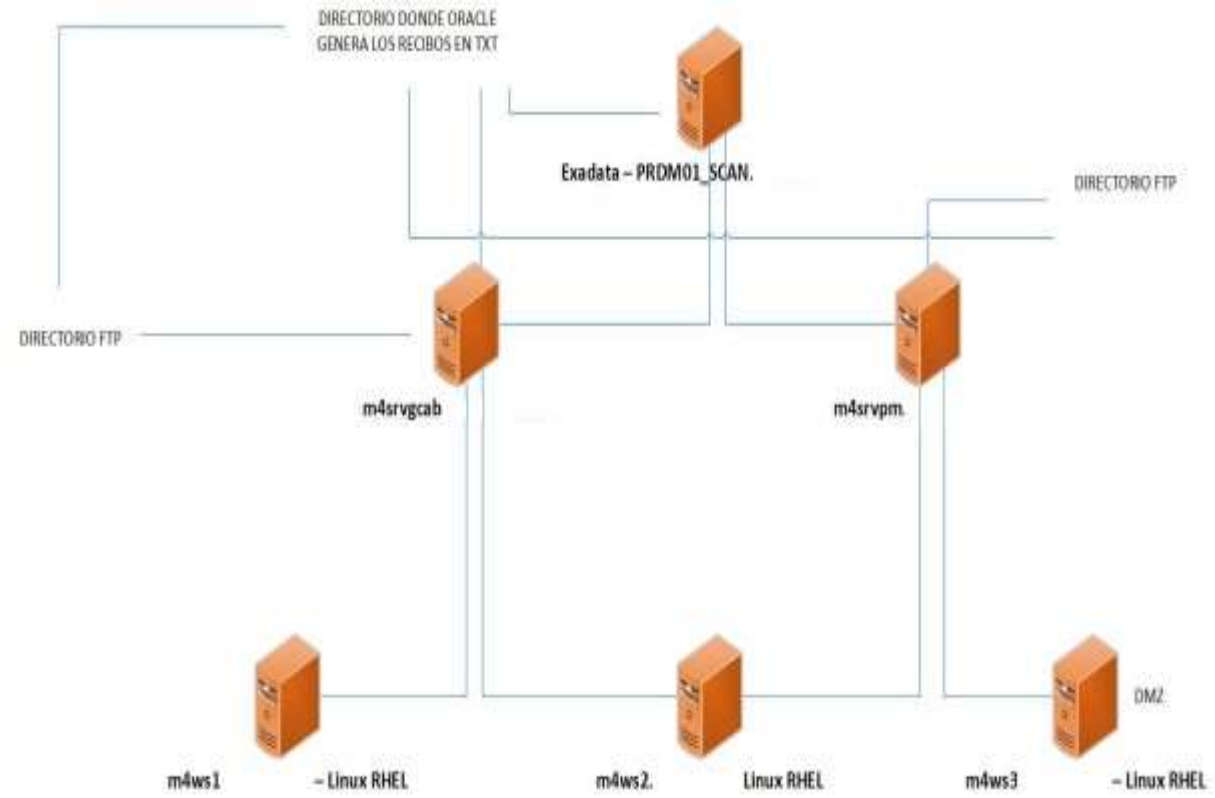
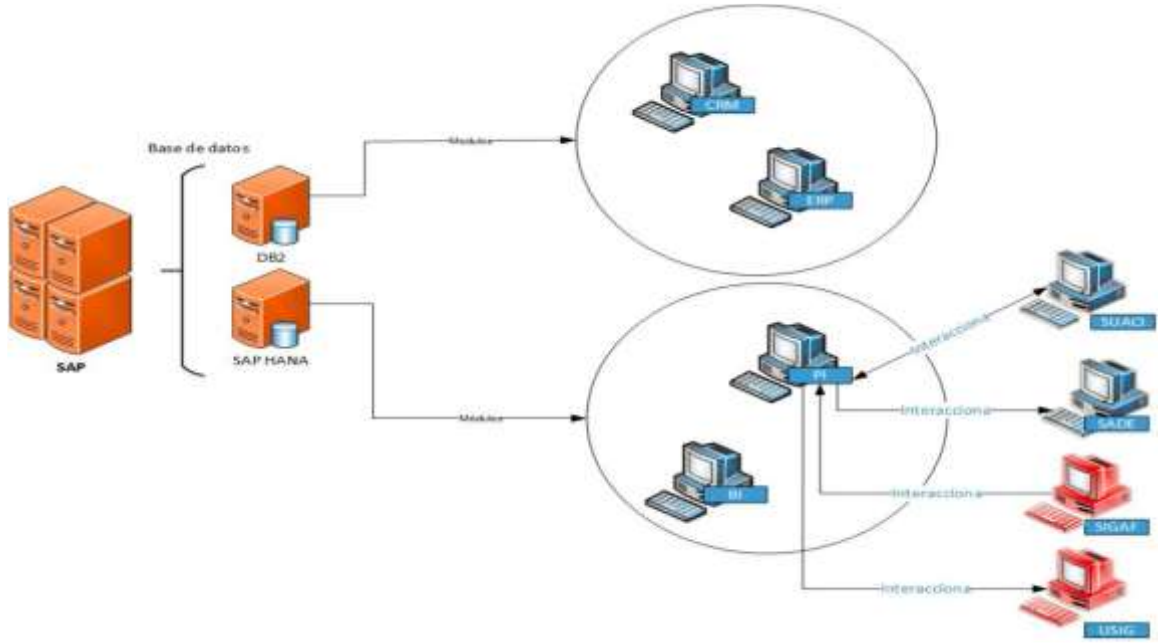


Diagrama de servidores y servicios de SIAL –

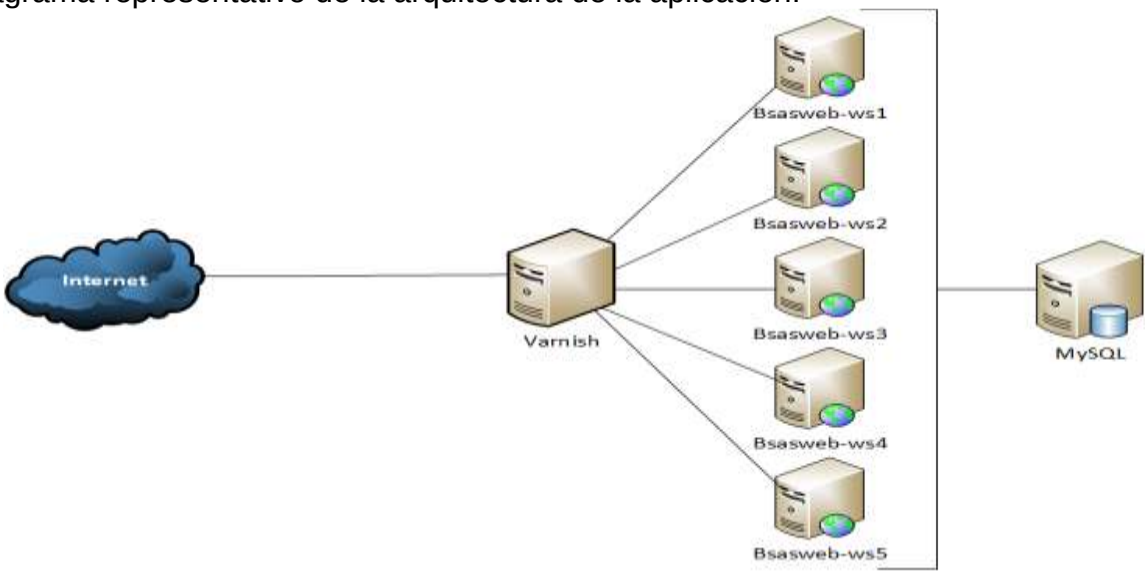
SAP

La ASInf cuenta con una implementación de la herramienta SAP con los módulos CRM, ERP, PI y BI. Su funcionalidad principal es dar seguimiento y gestión a los reclamos ingresados en el aplicativo por medio de la aplicación SUACI.



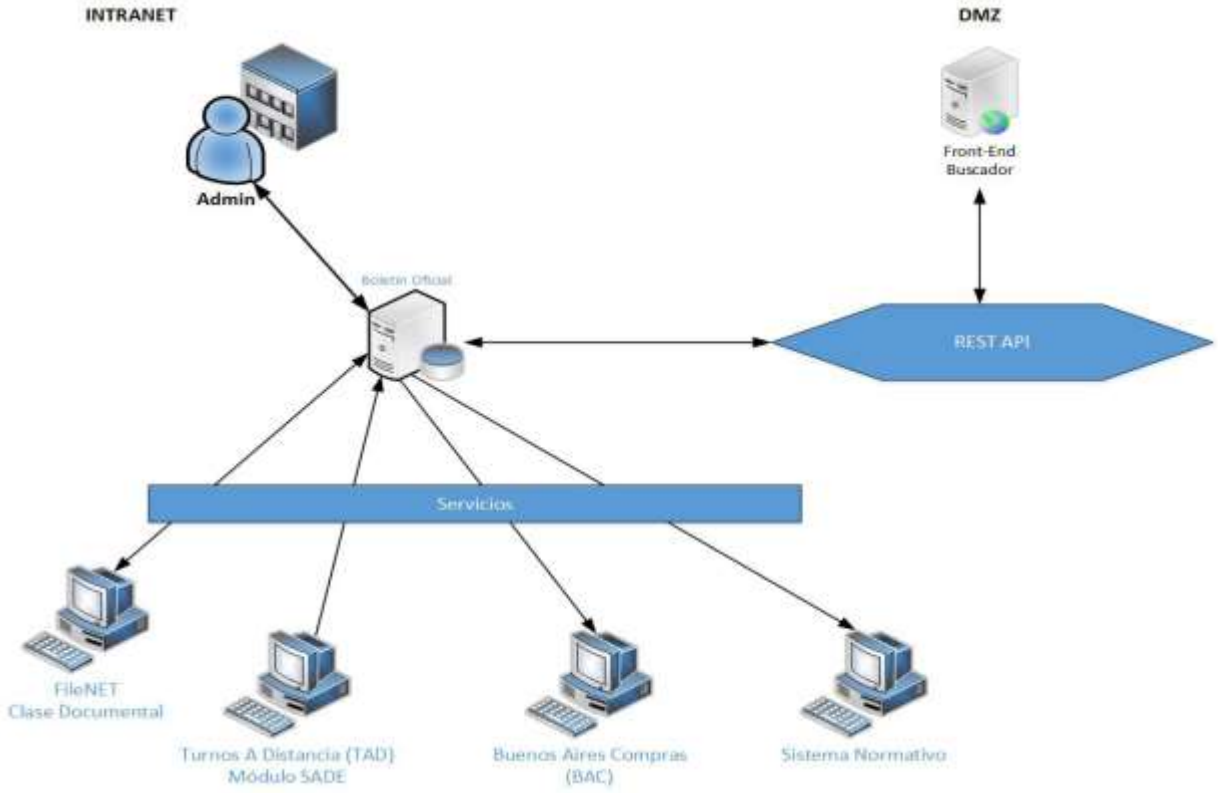
Páginas Web

Las páginas web de buenos aires corresponden a todas las páginas mediante las cuales se brindan servicios hacia los ciudadanos. En conjunto con las aplicaciones miBA y SUACI son el frente visible hacia el ciudadano para todo tipo de trámites, reclamos, gestión de turnos y solicitudes de servicios. A continuación se muestra un diagrama representativo de la arquitectura de la aplicación:



Boletín Oficial

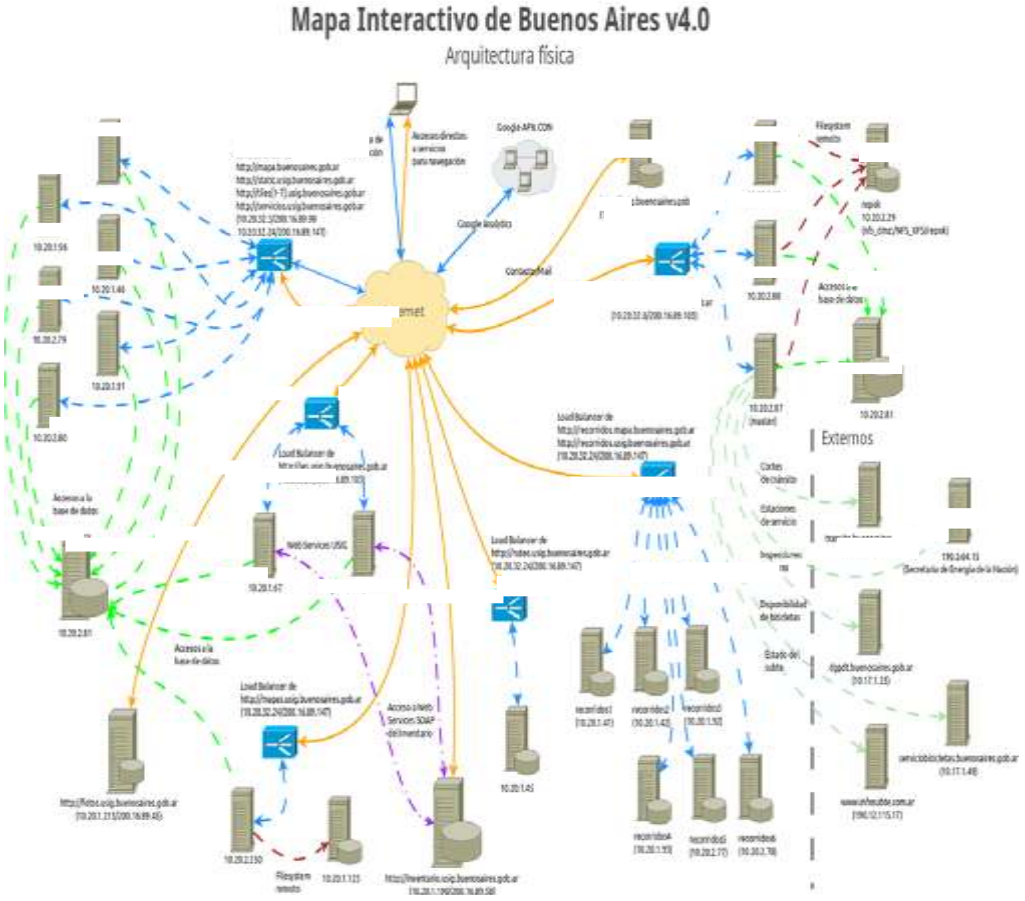
La aplicación de Boletín Oficial gestiona las comunicaciones oficiales que son incluidas dentro del Boletín Oficial con una frecuencia diaria.



Mapas – USIG

Aplicación de mapas que ofrece al usuario la visualización de información geográfica a través de un conjunto de herramientas que permiten seleccionar las capas de información, la escala de visualización, medición de distancias, selección de polígonos, consulta de información, y otros.

A continuación se muestra un diagrama de todas las interacciones que posee la misma:



Arquitectura Física de Servicios–

SUACI

El Sistema Único de Atención al Ciudadano (SUACI) es el sistema mediante el cual los ciudadanos pueden realizar reclamos y consultas referidos al espacio público y hacer un seguimiento de dicho reclamo hasta su finalización. Entre las categorías de reclamos y solicitudes disponibles se encuentran: Alumbrado, ordenamiento del espacio público, seguridad, arbolado y espacios verdes, calles y veredas, pluviales, limpieza y recolección, entre otros.
A continuación se muestra un diagrama de los componentes principales de la arquitectura de la aplicación y sus interacciones:

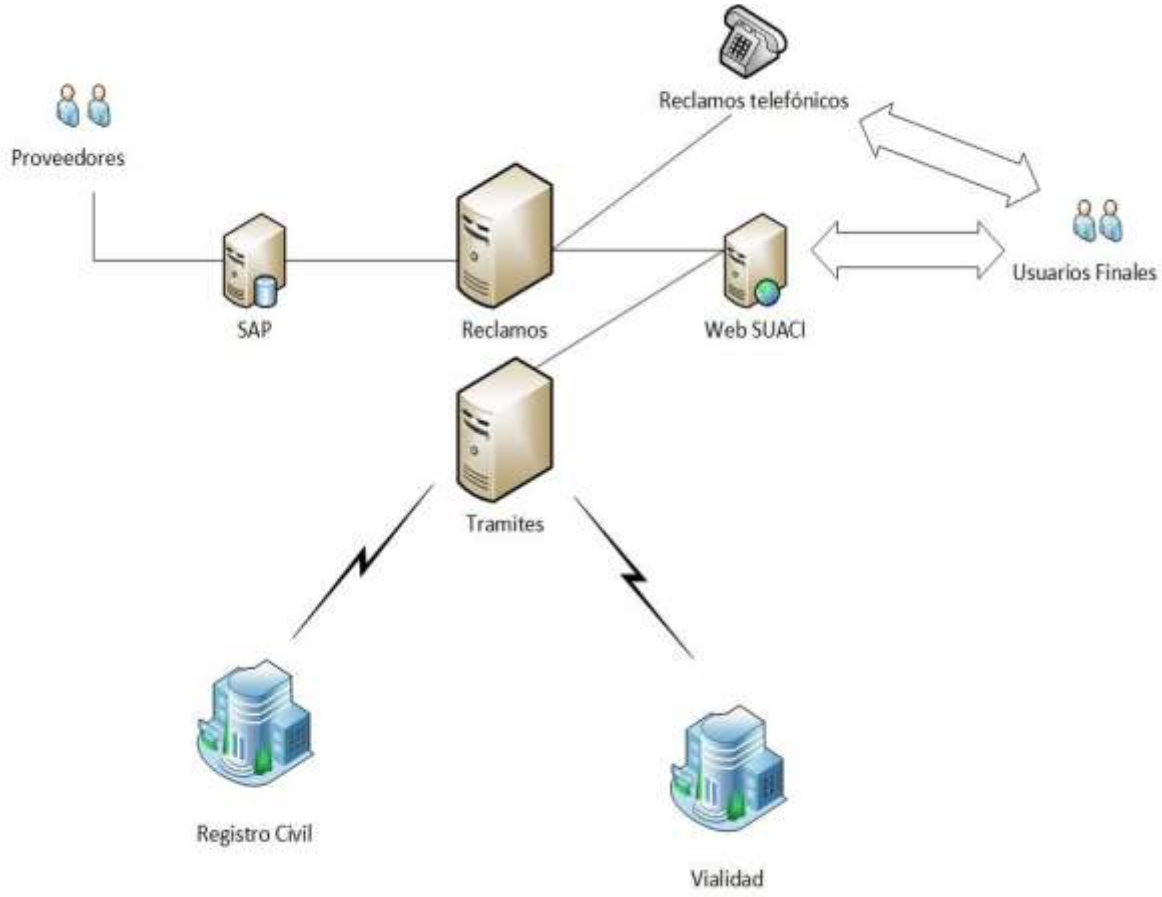
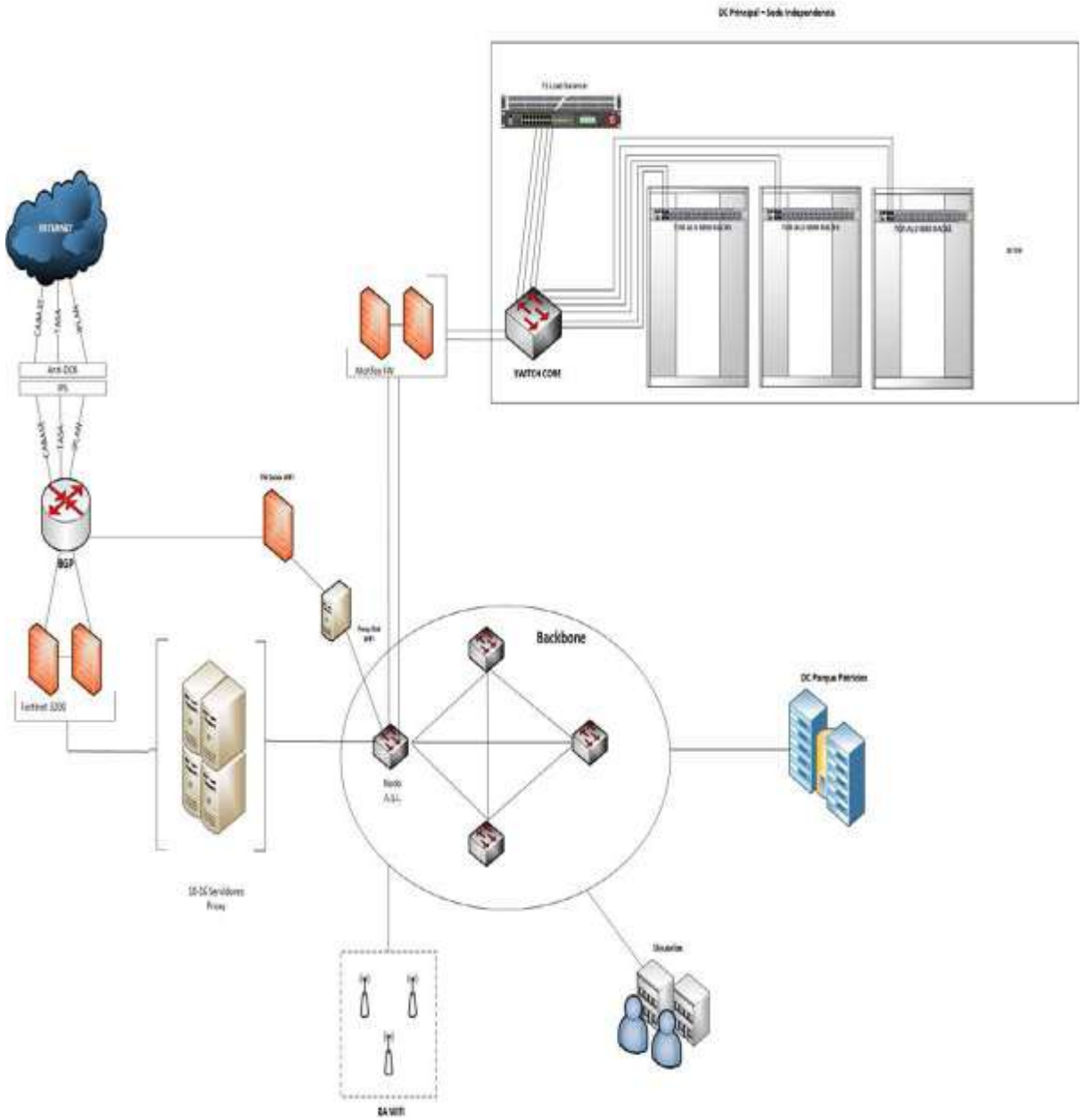


Diagrama de entendimiento e interacciones

Anexo esquemas red MAN

Esquema de red correspondiente a la ciudad de buenos aires identificando sus componentes principales, enlaces y servicios:



Arquitectura Conectividad entre Datacenter

Cada Datacenter (Independencia y Uspallata) está compuesto de un Fabric Nexus ACI
Ambos fabric están conectados entre si, en L2, en el estilo dual site mediante fibra oscura dedicada, troncales doble acometida.