AUDITORIA GENERAL
DE LA CIUDAD DE BUENOS AIRES

Informe Final de Auditoría

Con Informe Ejecutivo

Proyecto Nº 10.21.03

AGENCIA DE SISTEMAS

Auditoría de Sistemas

Período 2020

Buenos Aires, Mayo 2022

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

JEAN JAURES 216- CIUDAD DE BUENOS AIRES

Presidente

Dra. Mariana Inés GAGLIARDI

Auditores Generales

Dr. Juan José CALANDRI

Dr. Pablo CLUSELLAS

Cdra. Mariela Giselle COLETTA

Lic. María Raquel HERRERO

Dr. Daniel Agustín PRESTI

Dr. Lisandro Mariano TESZKIEWICZ

Nombre del Proyecto	Agencia de Sistemas de Información.
Número de proyecto	10.21.03
Organismo Auditado	Agencia de Sistemas de Información.
Tipo de Auditoría	Sistemas.
Período bajo examen	2020
Jurisdic./ Programa / Inciso	Jurisdicción 21 - Jefatura de Gabinete - Unidad ejecutora 8056 - Agencia Sistemas de Información.
Supervisor	Mg. Hernán García
Objeto	Agencia de Sistemas de Información.
Objetivo	Evaluar la eficacia de la gestión de las comunicaciones y operaciones.
Alcance	Analizar el cumplimiento de la gestión de las comunicaciones y operaciones establecidas en el Marco Normativo Tecnológico vigente en el GCABA.

Las tareas de auditoría comenzaron en el mes de abril del año 2021.

FECHA APROBACIÓN DEL INFORME: 19 DE MAYO DE 2022

APROBADO POR: UNANIMIDAD

INFORME EJECUTIVO

Lugar y fecha de emisión	Ciudad Autónoma de Buenos Aires, Mayo 2022
Código de Proyecto	10.21.03
Denominación del Proyecto	Agencia de Sistemas de Información.
Tipo de Auditoría	Sistemas.
Dirección General	Dirección General Sistemas de Información.
Período bajo examen	2020
Objeto de la Auditoría	Agencia de Sistemas de Información.
Objetivo de la Auditoría	Evaluar la eficacia de la gestión de las comunicaciones y operaciones.
Alcance	Analizar el cumplimiento de la gestión de las comunicaciones y operaciones establecidas en el Marco Normativo Tecnológico vigente en el GCABA.
Limitaciones al Alcance	Sin limitaciones.
Observaciones Relevantes	1) Alinear, Planificar y Organizar - APO01 • Gestionar el marco de gestión de I&T ✓ **Dependencia jerárquica de la Dirección General Seguridad Informática respecto de la Dirección Ejecutiva de la Agencia de Sistemas de Información. La configuración funcional y jerárquica actual de la estructura organizativa no favorece el control interno de los sistemas de comunicaciones y operaciones.** 2) Alinear, Planificar y Organizar - APO07 • Gestionar los recursos humanos

- ✓ **Falta de actualización en el dictado de cursos de concientización a usuarios para la Prevención de Software Malicioso, uso de Correo Electrónico y uso responsable de Internet. La carencia del dictado de cursos de actualización limita los conocimientos específicos, habilidades y competencias del recurso humano.**

Descripción de las observaciones vinculadas a los sistemas y aplicativos de gestión de comunicaciones y operaciones.

3) Alinear, Planificar y Organizar - APO12

- Gestionar el riesgo
  - ✓ **No exhibe documentación vinculada con la gestión del riesgo en los sistemas. Definición del apetito al riesgo aceptado, niveles de tolerancia, métricas, probabilidad de ocurrencia de los eventos y magnitud de la pérdida. Elaboración de informes, frecuencia y los responsables de la implementación de las acciones correctivas. Evaluar los riesgos en los sistemas permite definir, analizar y aceptar un determinado nivel de pérdidas de información.**

4) Construir, adquirir e implementar - BAI03

- Gestionar la identificación y construcción de soluciones
  - ✓ **No presenta documentación respaldatoria para la planificación en los sistemas asociados a las comunicaciones y operaciones, a corto, mediano y largo plazo. Tampoco respecto de las modificaciones en curso y terminadas. La carencia de planificación en los sistemas atenta contra su capacidad y disponibilidad.**

5) Construir, adquirir e implementar - BAI06

- Gestionar los cambios de TI
  - ✓ **No expone documentos que definan un modelo de control de cambios en los sistemas que gestionan las comunicaciones y operaciones. Falta de metodología, solicitud, evaluación,**

	priorización, procesos de control, aceptación y versionados de los cambios. Es necesario mitigar el riesgo de los cambios a realizar para lograr sistemas estables que conserven la integridad de la información que administran. 6) Construir, adquirir e implementar - BAI08 • Gestionar el conocimiento ✓ **La identificación, contextualización y clasificación de la información permite disponer y compartir el conocimiento relevante para los procesos del organismo. Carencia de manuales, diagramas entidad-relación y estudios de factibilidad de los proyectos de desarrollo de los sistemas.** 7) Construir, adquirir e implementar - BAI09 • Gestionar los activos ✓ **No se presenta documentación que garantice que se efectuó la gestión de los activos vinculados a los sistemas de comunicaciones y operaciones, cuyo objetivo es asegurar aquellos que son críticos para planificar la demanda de capacidad y disponibilidad. Es necesario identificar y registrar los activos actuales, priorizar los críticos, optimizar su valor y gestionar las licencias. La falta de ejecución del proceso pone en riesgo el adecuado funcionamiento de los mencionados sistemas.** 8) Entregar, dar servicio y soporte - DSS01 • Gestionar las operaciones ✓ **No adjunta documentación que ratifique la ejecución de procedimientos operativos de los sistemas a cargo del monitoreo de la infraestructura de TI, el medioambiente y la gestión de las instalaciones operativas. Los mencionados aseguran la continuidad de los servicios asociados a las comunicaciones y operaciones. La gestión de los servicios de TI propios y de terceros permite detectar los**

desvíos e implementar las acciones correctivas necesarias para cumplir con la planificación establecida.

9) Entregar, dar servicio y soporte - DSS02

- Gestionar las peticiones y los incidentes de servicio

✓ **No consta la definición e implementación de un proceso de administración de peticiones e incidentes por fallos en los sistemas ligados con las comunicaciones y operaciones. Debe establecerse un esquema de clasificación y petición que incluya el registro, priorización, aprobación, resolución, seguimiento e informe de incidentes. La falta del proceso atenta contra la productividad, no minimiza los incidentes y favorece las interrupciones en los servicios asociados.**

10) Entregar, dar servicio y soporte - DSS05

- Gestionar los servicios de seguridad

✓ **No se detallan procesos de gestión de seguridad en los sistemas para proteger la conectividad, red, dispositivos de punto final, vulnerabilidades y los ataques por parte de software malicioso. Es indispensable controlar los sistemas asociados a las comunicaciones y operaciones y evaluar el impacto ocasionado en la seguridad de la información para garantizar la continuidad y disponibilidad del servicio.**

11) Entregar, dar servicio y soporte - DSS06

- Gestionar los controles de procesos de negocio

✓ **No se expone un proceso de gestión de roles, responsabilidades, privilegios para el acceso y niveles de autoridad en los sistemas de comunicaciones y operaciones. El incumplimiento en la utilización del mencionado proceso no garantiza que la información administrada sea íntegra, completa, válida, precisa, segura y oportuna.**

12) Monitorizar, evaluar y valorar - MEA01

	• Gestionar la supervisión del rendimiento y la conformidad ✓ **No consta el uso de un enfoque de supervisión del rendimiento y la conformidad en los sistemas de comunicaciones y operaciones. No se expusieron procesos de recopilación de datos, proyección de objetivos de rendimiento, conformidad, análisis e implementación de acciones correctivas. Las acciones mencionadas promueven el incremento en el rendimiento y la obtención de las metas planificadas.**
Conclusión / Dictamen	La Agencia de Sistemas de Información, como órgano rector en Tecnologías de la Información y promotor de políticas gubernamentales en materia de Sistemas de Información, administra la infraestructura informática de todas las dependencias del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires. Por tal motivo, los programas de capacitación deben ser revisados de manera regular. La gestión de riesgos relacionados con IT fija los niveles de tolerancia y pérdidas de información que el gobierno de tecnología está dispuesto a asumir. Permite equilibrar los costos, beneficios y riesgos dentro del organismo. Evaluar los incidentes, interrupciones y pérdidas para proponer acciones correctivas y minimizar los daños. ASInf provee servicios de TI al GCABA, por ello las soluciones a través de servicios digitales deben ser ágiles, progresivas y escalables, que permitan planificar la expansión de su capacidad y disponibilidad a mediano plazo. Es imprescindible medir los cambios solicitados con emergencia respecto del total de cambios cuyo objetivo es plantear las acciones correctivas necesarias para minimizar los primeros mencionados. Es oportuno evaluar el costo-beneficio de los activos de TI, principalmente aquellos críticos. Analizar la conveniencia de su actualización o el recambio tecnológico y contrastarlo con el ciclo de vida planificado, desde su adquisición hasta su baja. La mejora continua en los servicios puede ser aplicada mediante el análisis minucioso de los incidentes manifestados.

	El seguimiento, la producción de informes, la definición de métricas y la evaluación de las posibles causas de problemas recurrentes, aportan los datos necesarios para generar eficacia en los servicios de comunicaciones y operaciones. La gestión de controles de los procesos no sólo debe aplicarse al flujo de información generado en el organismo, sino también a los datos que ingresan desde otros entes del GCABA y de los proveedores de servicios de TI externalizados. Es beneficioso que la evaluación y el monitoreo de los mencionados controles se ejecute regularmente. Es conveniente, en el próximo presupuesto, asignar recursos destinados a mejorar y adecuar el Plan de Contingencia y Recuperación de Desastres, además de agregar las aplicaciones que actualmente no se encuentren incluidos. Se sugiere incrementar la cantidad de métricas e indicadores utilizados para evaluar el Gobierno y la Gestión de TI. También, intensificar los procedimientos de monitoreo y la implementación de acciones correctivas que permitirán el cumplimiento de los objetivos planteados garantizando el nivel de cobertura de los servicios tecnológicos provistos. Las tareas de auditoría desarrolladas en campo culminaron en el mes de noviembre del año 2021.
Palabras Claves	Agencia, Sistemas, ASInf, comunicaciones, operaciones.

INFORME FINAL DE AUDITORÍA
"AGENCIA DE SISTEMAS DE INFORMACIÓN"
PROYECTO N° 5.20.05

DESTINATARIO

Señor
Vicepresidente 1°
Legislatura de la Ciudad Autónoma de Buenos Aires
Lic. Emmanuel Ferrario
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 Infraestructura de la Agencia de Sistemas de Información con el objeto detallado en el apartado siguiente.

OBJETO DE AUDITORIA

I. Agencia de Sistemas de Información.

OBJETIVO DE LA AUDITORIA

II. Evaluar la eficacia de la gestión de las comunicaciones y operaciones.

ALCANCE DEL EXAMEN

III. Analizar el cumplimiento de la gestión de las comunicaciones y operaciones establecidas en el Marco Normativo Tecnológico vigente en el GCABA.

Marco Normativo

Se utilizará el siguiente marco normativo:

Normas Básicas de Auditoría Externa de la AGCBA y las Normas Básicas de Auditoría de Sistemas de la AGCBA, la ley 70, ley 325 y complementarias.

Marco de Referencia COBIT® 2019 (Control Objectives for Information and Related Technology). Capítulo Buenos Aires.

Las normas y recomendaciones establecidas por ASInf (Resolución N°177/ASInf/13 y ampliaciones).[1]

Procedimientos realizados

Se cursó nota a la Agencia de Sistemas de Información (ASInf) para dar inicio al proyecto de auditoría.

Búsqueda en los sitios oficiales del GCABA relacionada con el objeto de auditoría.

Se solicitó por nota la información asociada con la organización, normativa y el presupuesto.

Respecto de los recursos humanos, se requirieron los perfiles técnicos, cursos de capacitación realizados y procesos utilizados por cada área.

Se solicitaron los informes de auditoría, relevamientos y/o seguimientos realizados en los últimos tres años.

Se requirió el mapa físico y lógico de la red y los dispositivos relacionados con las comunicaciones y operaciones. Los servicios de tecnología recibidos por ASInf y los brindados por proveedores externos.

Se solicitó documentación e información de los sistemas vinculados a las comunicaciones y operaciones. Además, especificaciones de la metodología, entornos de desarrollo y los procesos de gestión de riesgos.

Se mantuvieron contactos telefónicos y por videoconferencia con la finalidad de evacuar las dudas respecto de la información solicitada a la Dirección de Infraestructura (DGIASInf), Dirección General Técnica, Administrativa y Legal,

[1] Resolución N°177/ASInf/13. Obtenido el 6 de noviembre del año 2013 en: https://n9.cl/12dwx [Accedido el 6/5/21]

la Gerencia Operativa de Legales y Recursos Humanos y la Gerencia Operativa de Infraestructura.

Se cursaron correos a la Dirección General Integración de Sistemas para solicitar respuesta respecto de los sistemas y aplicativos vinculados a las comunicaciones y operaciones. Se reiteró la solicitud de pedido de información.

Se cursaron correos a la Dirección General Seguridad Informática para solicitar respuesta respecto del software malicioso, las políticas de uso de correo electrónico y política de uso de internet.

Se verificó la normativa vigente relativa al objeto de esta auditoría y su cumplimiento.

Reformulación de las fechas del Plan Operativo. Se inició el examen de la información durante el mes de junio.

Se evaluó el cumplimiento del objetivo de la auditoría dentro del Marco Normativo de Tecnología vigente según la Resolución N°177/ASInf/13.

Se verificó la eficacia de la gestión de las comunicaciones y operaciones por parte de ASInf.

Entrevistas con los responsables en las áreas físicas relacionadas con la gestión de las comunicaciones y operaciones.

Visitas a los centros de datos de ASInf ubicados en Av. Independencia y la calle Uspallata, con la finalidad de verificar la seguridad física y la infraestructura tecnológica.

IV. LIMITACIONES AL ALCANCE

Sin limitaciones.

V. ACLARACIONES PREVIAS

Jurisdicción y Presupuesto

La sanción del presupuesto 2020, otorgó a la Agencia de Sistemas de Información, mediante la Jurisdicción 21, Unidad Ejecutora 2051, $ 1.408.380.207, mientras que para la Dirección General de Infraestructura se distribuyeron créditos por $ 715.630.291. (ANEXO I).[2]

El Plan Plurianual de Inversiones Públicas 2020-2022 asignó a la Agencia de Sistemas de información una inversión total de $ 732.786.819 y para el año

[2] Anexo I - Distribución Administrativa de Créditos - Presupuesto 2020. Obtenido el año 2020 en: https://n9.cl/aj8en [Accedido el 11/5/21]

2020 de $ 270.609.245. Para la Dirección General de Infraestructura, una inversión total de $ 453.352.678, con inversiones para el año 2020 de $ 149.609.245 (ANEXO II).[3]

Según las Planillas Anexas del Presupuesto 2020, para Organismos Descentralizados, Entes Autarquicos y Organos de Control, la Composición del Gasto por Jurisdicción, y Carácter Económico para la Agencia de Sistemas de Información, se otorgaron Gastos Corrientes por $ 1.418.615.462 y Gastos de Capital por $ 333.412.245, totalizando $ 1.752.027.707. (ANEXO III).[4]

El Presupuesto Financiero asignado a la Dirección de Infraestructura, por un total de $ 715.630.291, anteriormente mencionado, se compone de $ 155.310.815 para Gastos en Personal, $ 616.100 para Bienes de Consumo, $ 458.750.376 para Servicios no personales y $ 100.953.000 para Bienes de uso. (ANEXO IV).[5]

Normativa

En el año 2008, mediante la ley 2689, sancionada por la Legislatura de la Ciudad Autónoma de Buenos Aires, se crea la Agencia de Sistemas de Información.[6] Entre sus objetivos se encuentra la promoción de la estandarización de los bienes informáticos, equipos, recursos y sistemas utilizados por el Poder Ejecutivo. También, el desarrollo y la modernización de las dependencias y entidades de la administración pública de la Ciudad Autónoma de Buenos Aires.

En el año 2009, se sancionó la Ley N° 3304, Ley de Modernización de la Administración Pública.[7] El objetivo perseguía la implementación de un proceso de modernización administrativa en el Gobierno de la Ciudad Autónoma de Buenos Aires.

El Ministerio de Modernización, mediante la Resolución Nº 190, en el año 2012, reconocía la necesidad de profundizar el Plan de Modernización, por ello

[3] Anexo II - Plan Plurianual de Inversiones Públicas 2020-2022. Obtenido el año 2020 en: https://n9.cl/j3kkz [Accedido el 11/5/21]

[4] Anexo III - Presupuesto 2020. Distribución Administrativa de Créditos. Obtenido el año 2020 en: https://n9.cl/o2a9a [Accedido el 11/5/21]

[5] Presupuesto 2020 - Jurisdicción 21. Jefatura de Gabinete de Ministros. Obtenido el año 2020 en: https://n9.cl/b4j1f [Accedido el 14/6/21]

[6] Ley 2689 - Creación de la Agencia de Sistemas de Información. Obtenido el 17 de abril del año 2008 en: https://n9.cl/5b2c7 [Accedido el 11/5/21]

[7] Ley 3304 - Ley de Modernización de la Administración Pública. Obtenido el año 2009 en: https://n9.cl/8uesr [Accedido el 12/5/21]

aprobó la utilización del Formulario Único de Requerimientos (FUR) y el Instructivo para el Proceso de Gestión de Demanda. [8]

Durante el año 2013, mediante la Resolución N° 18 [9] de la Agencia de Sistemas de Información, se modifica su estructura organizativa. Define las principales acciones para cada cargo y los nombramientos para las gerencias y subgerencias operativas.

A través de la Resolución Nº 224/2018,[10] ASInf modifica nuevamente su organigrama y define sus responsabilidades primarias. (ANEXO V).

La página del Gobierno de la Ciudad Autónoma de Buenos Aires refleja la estructura organizativa vigente de la Agencia de Sistemas de Información acorde con la resolución recién mencionada.[11]

Dirección General de Infraestructura

La Dirección General de Infraestructura forma parte de la estructura organizativa de ASInf. Está a cargo de la administración y gestión de los recursos que componen la infraestructura tecnológica del GCABA. El director, los gerentes y subgerentes operativos, fueron nombrados y formalizados mediante resoluciones emitidas por ASInf en los años 2013, 2015, 2016 y 2017.

En la citada web, se destacan sus misiones y funciones:

- “Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios a los recursos de infraestructura de TI del G.C.A.B.A”
- “Establecer los controles que deberán realizarse en el proceso de cambios de software de aplicación, software de base, información e infraestructura tecnológica de los ambientes, de manera de asegurar su integridad y minimizar el riesgo de pérdida de información, accesos no autorizados o falta de disponibilidad del servicio”

[8] Res N° 190/MMGC/12. Obtenido el 11 de mayo del año 2012 en: https://n9.cl/5jua [Accedido el 12/5/21]

[9] Resolución Nº 18/ASInf/2013. Obtenido el 6 de febrero del año 2013 en: https://n9.cl/4gr6f [Accedido el 12/5/21]

[10] Anexo de la Resolución Nº 224/ASInf/2018. Obtenido el 18 de diciembre del año 2018 en: https://n9.cl/760m [Accedido el 12/5/21]

[11] Organigrama ASInf vigente. Obtenido el año 2021 en: https://n9.cl/mu0zt [Accedido el 12/5/21]

- "Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del G.C.A.B.A"

La Resolución Nº 224/ASInf/2018 describe responsabilidades primarias como la administración y el control de los sistemas de comunicaciones, supervisión y operación de los servicios de las redes del GCABA.

Asimismo, el procesamiento de los sistemas de información y el mantenimiento operativo de la infraestructura de soporte de hardware y software. La definición de los estándares de las plataformas, operación de sus redes y los sistemas de las arquitecturas tecnológicas del GCABA.

Entre sus principales objetivos se distingue la gestión de los recursos de infraestructura de tecnología, la adecuada administración de los sistemas de comunicaciones y el aseguramiento de la integridad y disponibilidad de la información del GCABA.

La comunicación desde la Dirección General de Infraestructura hacia las Gerencias Operativas es coordinada a través de reuniones semanales. A su vez, las Gerencias Operativas articulan cada semana, reuniones con sus respectivos agentes, en las que también participa la DGIASInf.

Todas las solicitudes y requerimientos ingresan a la Dirección General de Infraestructura mediante el Ecosistema SADE (Sistema de Administración de Documentos Electrónicos),[12] desde allí se evalúa el pedido, se genera un ticket y se deriva a la Gerencia Operativa correspondiente según el requerimiento recibido.

Las vías de comunicación utilizadas dentro de la Dirección General son el Ecosistema SADE, correo electrónico oficial, teléfonos celulares corporativos del GCABA y los teléfonos de línea con sus respectivos internos.

La DGIASInf está compuesta por cuatro Gerencias y nueve Subgerencias Operativas, totalizando un plantel aproximado de ciento noventa personas.

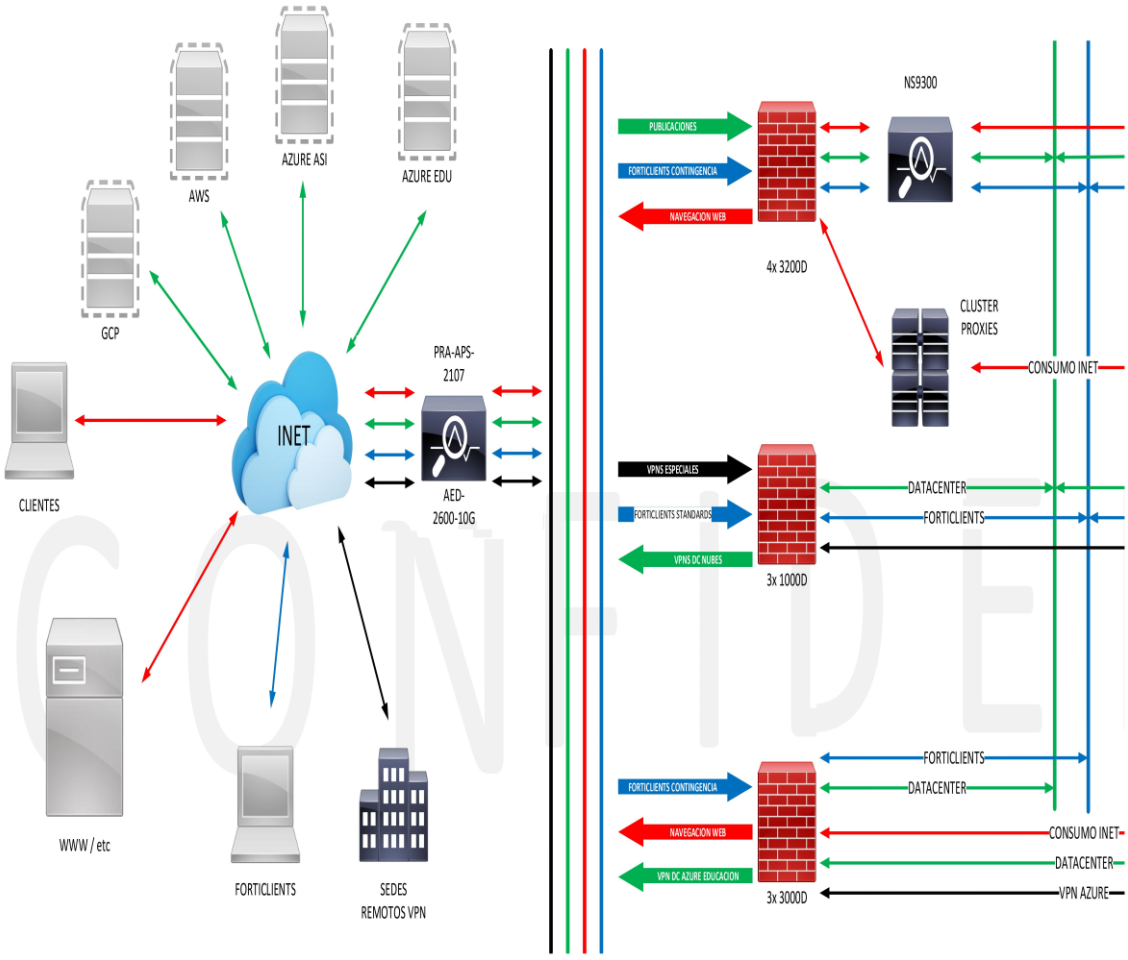
La planta permanente está conformada por ciento seis agentes, además, treinta y cuatro realizan tareas a través de locaciones de servicios y otros en planta transitoria.

El 40 % del total del plantel posee estudios con orientación técnica, de los cuales el 23% adquirió un título profesional.

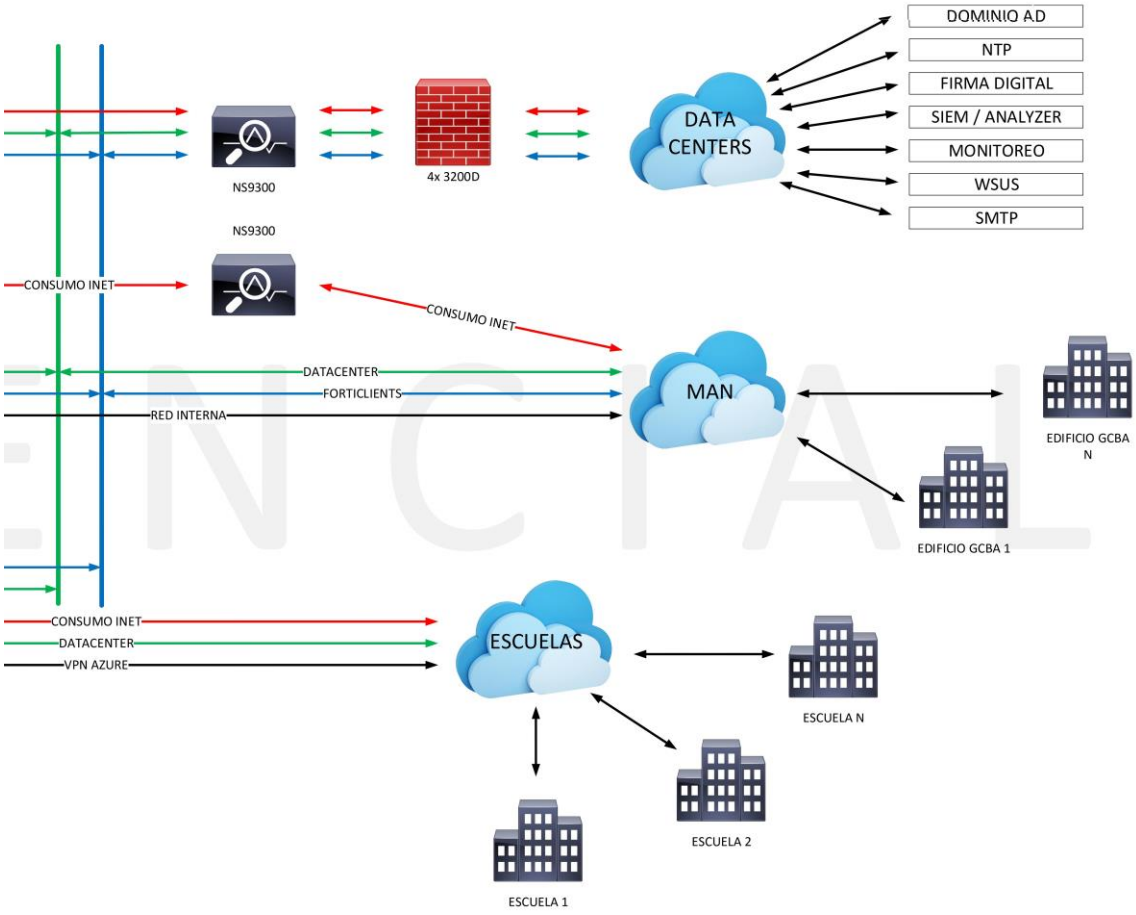
[12] Decreto Nº 196/11. Expediente electrónico. SADE. Obtenido el 28 de marzo del año 2011 en: https://n9.cl/r51f [Accedido el 28/5/21]

Mapa físico del GCABA

La siguiente imagen describe el diagrama general de arquitectura de seguridad informática del GCABA.



Fuente: ASInf



Fuente: ASInf

Servicios provistos por ASInf

La Agencia de Sistemas de información provee conexión a la red MAN a las diferentes reparticiones del GCABA mediante los siguientes enlaces primarios:

Enlace Primario	Número de reparticiones conectadas
4G MOVISTAR	2
FIBERCORP	67
GPON[13]	1008
GPON SAME	1
L2L METROTEL	2
LITEBEAM[14]	11
LTE[15]	5
NANOSTATION[16]	1
P2P[17]	95
TASA[18]	366
UTP MAN	1
WIMAX[19]	1

[13] GPON (Gigabit - Capable Pasive Optic Network, en español Red de Fibra Óptica Pasiva con Capacidad de Gigabit) es una tecnología que permite acceder al usuario al sistema de telecomunicaciones a través de un cableado de fibra óptica.

[14] LITEBEAM es un dispositivo de telecomunicaciones que permite establecer la conectividad inalámbrica direccional, ya sea punto a punto o multipunto.

[15] LTE es un tipo de tecnología de transmisión de datos de banda ancha inalámbrica con disponibilidad de acceso constante a internet para teléfonos móviles y dispositivos portátiles.

[16] Nanostation es una tecnología que permite una conexión de banda ancha exterior, de bajo costo y alta performance.

[17] P2P permite a los usuarios de internet conectarse entre sí y compartir archivos que están dentro de sus ordenadores.

[18] TASA (Telefónica de Argentina), es el acceso MPLS.

[19] WiMAX (Worldwide Interoperability for Microwave Access, en español Interoperabilidad Mundial para Acceso por Microondas), es un método de transmisión de datos con tecnología de ondas de radio con frecuencias de 2,5 a 5,8 GHz.

Enlace Primario	Número de reparticiones conectadas
Total	**1560**

Del total de las reparticiones conectadas mediante un enlace primario, aproximadamente el 12 % además posee un enlace de backup.

Servicios contratados a terceros

Los servicios contratados a terceros, relacionados con la gestión de las comunicaciones y operaciones, vigentes o acordados durante el año 2020 son los siguientes:

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor contrato ($)
Mantenimiento Routers	Trans	8056-0263-OC20	23/1/20	12	23/1/21	29.609.616
Prorroga OC Mantenimiento Routers de acceso	Trans	8056-0431-OC21	2/2/21	2	2/4/21	4.934.936
Prorroga OC Mantenimiento Routers de acceso	Trans	8056-1785-OC21	11/3/21	3	3/7/21	7.402.404

Fuente: ASInf

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor contrato ($)
Mantenimiento FO - Renglón 1 y 2	Acertis	8056-13196-OC20	24/12/20	12	24/12/21	61.717.740
Mantenimiento FO - Renglón 3 y 4	Trans UT	8056-13197-OC20	24/12/20	12	24/12/21	59.220.000

Fuente: ASInf

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor Contrato ($)
Servicio de mantenimiento integral LTE	Trans Industrias Electrónicas SA - Systemnet SA - Unión Transitoria	8056-5801-OC20	1/6/20	12	1/6/21	57.495.000

Fuente: ASInf

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor Contrato ($)
Provisión, instalación y configuración equipos GPON	Intellihelp	8056-9979-OC19	2/7/19	24	2/7/21	9.046.000

Fuente: ASInf

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor Contrato ($)
Mantenimiento de centrales Telefónicas Unify	Unify Communications S.A.	8056-15687-OC19	30/9/19	12	30/9/20	5.875.704
Mantenimiento de centrales Telefónicas Unify Hipath edificios CABA	Unify Communications S.A.	8056-17492-OC19	31/10/19	12	31/10/20	5.032.800
Mantenimiento de centrales Telefónicas Unify	Unify Communications S.A.	8056-10875-OC20	20/10/20	12	20/10/21	9.480.000
Mantenimiento de centrales telefónicas Unify Hipath edificios CABA	Unify Communications S.A.	8056-12411-OC20	25/11/20	12	25/11/21	7.183.908
OCA de Licencias de uso mensual de Telefonía IP	Unify Communications S.A.	8056-0125-OC20	25/11/20	12	25/11/21	34.347.468

Fuente: ASInf

Descripción	Proveedor	Orden de compra	Fecha de inicio	Duración (meses)	Fecha de fin	Valor Contrato ($)
Servicio Mantenimiento Nodos de la Red MAN	Trans UT	8056-13320-OC20	15/12/20	12	15/12/21	18.018.600

Fuente: ASInf

La siguiente tabla detalla los proveedores externos que brindan servicios de mantenimiento a los centros de datos, acceso y conectividad.

Descripción	Proveedor
Servicio de mantenimiento integral de centros de datos de ASInf	Aceco TI Argentina S.A.
Servicios de conectividad por tecnología 4G	Telefónica Móviles Argentina S.A.
Servicios de conectividad por cable modem	Telecom
Servicios de enlaces de acceso y transporte IP/MPLS[20]	Telefónica Móviles Argentina S.A.

Fuente: ASInf

Evaluación y clasificación de áreas críticas

ASInf incluye dentro de la clasificación de áreas críticas tanto a los centros de procesamiento de datos como a los centros de almacenamiento de copias de resguardo, los cuales contengan información del GCABA, ya sean propios o de terceros.

La Agencia de Sistemas de Información posee dos centros de datos, ubicados en la Av. Independencia 635 y en la calle Uspallata 3160, CABA. Ambos están protegidos por sensores biométricos, motivo por el cual el acceso está restringido sólo al personal autorizado o, para casos de accesos eventuales por parte de proveedores, se ingresa acompañado por personal autorizado de ASInf firmando la bitácora de ingreso correspondiente.

[20] MPLS (Multiprotocol Label Switching, en español Conmutación de Etiquetas Multiprotocolo), es una técnica de transferencia de datos, un estándar de transmisión de datos bajo diferentes etiquetas.

Además, en el hall de acceso a los edificios, existe una custodia con personal de vigilancia durante las 24 horas, complementado por un circuito cerrado compuesto por cámaras de video.

Ambos centros se encuentran protegidos por sistemas contra incendios, por UPS[21] y generadores.

Infraestructura del centro de datos - Av. Independencia

El ingreso al edificio está controlado por cámaras y personal de vigilancia. La Dirección de Infraestructura de ASInf es la responsable del centro de datos, al cual se accede mediante control biométrico por huella digital, se registra en la bitácora de ingreso y en el log de auditoría del sistema.

Posee luces de emergencia, piso técnico y UPS, la cual permite una autonomía aproximada de 50 minutos, variable según la carga conectada. Está dotado de controles y alarmas para temperatura y humedad, detectores de humo, flores regadoras y un sistema de extinción de fuegos FM 200[22] con un tanque principal y local. Los procesos de evacuación del edificio están a cargo de la Dirección General Técnica, Administrativa y Legal (DGTALINF).

El grupo electrógeno de 300 kva posee un tanque auxiliar de alimentación que permite doce horas de autonomía sin reponer combustible, variable según la carga conectada.

El sistema de refrigeración está conformado por dos equipos en tándem funcionando al 50% de su capacidad, dándose cobertura mutuamente en caso de ocurrencia de eventos indeseados. El mantenimiento es brindado a través de un contrato con una empresa externa que provee tareas preventivas y por demanda.

Los procesos que se llevan a cabo en el centro de datos de Av. Independencia, ante un evento indeseado, pueden demorar dos horas en dar continuidad a las operaciones en el centro de datos de la calle Uspallata.

[21] UPS (Uninterruptible Power Supply, en español, Sistemas de Alimentación Ininterrumpida), son dispositivos que proveen energía a los dispositivos conectados durante un tiempo determinado ante un corte en el suministro eléctrico.

[22] FM 200 es un sistema de protección contra incendios que suprime todo principio de incendio, se destaca por no utilizar agua en su accionar.

Respecto de las mejoras realizadas, se amplió la capacidad de las llaves eléctricas de 160 Amper a 250 Amper. Se realizó la limpieza del piso técnico y se implementó un sistema de monitoreo eléctrico para todo el edificio, no sólo para el centro de datos.

Dentro del sector de almacenamiento, se acondicionaron las puertas de ingreso y sus luminarias.

Actualmente, se encuentra con procesos de mejoras y reingeniería mediante la instalación de una nueva central de incendios dotada de un sistema de monitoreo con notificaciones a través de distintas plataformas, software gráfico y generación de informes de estado.

Está proyectado implementar un tablero redundante con la finalidad de proveer respaldo ante eventos indeseados en el mismo. También, mejorar el espacio físico, eliminar algunos pasillos y ampliar el sistema de refrigeración actual. (ANEXO VI - Fotos Independencia).

Infraestructura del centro de datos - Uspallata

El acceso al edificio por parte del personal que desarrolla tareas diarias es habilitado mediante un control biométrico por huella digital y controlado por personal de vigilancia, el cual está presente las 24 horas y es complementado por un circuito de cámaras. Las visitas y los proveedores eventuales sólo acceden con personal autorizado a ese efecto, ingresando a través de un detector y exponiendo sus objetos a un escáner.

El edificio de última generación posee un centro de datos ubicado en el subsuelo, con cámaras de vigilancia y acceso mediante un dispositivo por huella digital. Los eventos eléctricos indeseados con suspensión del servicio son subsanados por la provisión eléctrica de un sistema de UPS con una autonomía aproximada de 2 horas. El mantenimiento y control de los mismos es realizado mensualmente. Para los casos en los que se requiera mayor cobertura de tiempo, existen grupos electrógenos de alta capacidad.

El centro de datos posee en su interior una sala cofre. Su acceso es controlado por huella digital y su interior es monitoreado por cámaras de vigilancia.

Respecto de las mejoras implementadas, la central de incendios del centro de datos fue interconectada con la central de incendios del edificio. Se realizó el confinamiento de pasillo frío[23] para la zona 2, la que actualmente provee servicios de contingencia para la Administración Gubernamental de Ingresos Públicos (AGIP). En el pasillo frío de la zona 1 se efectuó el recambio del piso técnico, instalando baldosas perforadas, las cuales favorecen la recirculación del aire optimizando el sistema de refrigeración.

También se realizó el tendido de fibra óptica desde la sala de ingreso del proveedor del servicio hasta el interior del centro de datos. De esta manera se eleva la redundancia y se mejora la conectividad del GCABA.

La intendencia, quien está a cargo de las UPS y las baterías que proveen energía al centro de datos, elevó su nivel de control y disminuyó los tiempos entre pruebas a un período semestral.

Con el objetivo de certificar la sala cofre, se efectuaron pruebas de estanqueidad.

Se proyectan acciones de reingeniería para concluir el confinamiento iniciado para el pasillo frío de la zona 2 del centro de datos. También, instalar baldosas perforadas y elevar el nivel de conectividad a través del tendido de fibra óptica con interconexión con la zona 1 para permitir incrementar el nivel de provisión de servicios a AGIP. (ANEXO VI - Fotos Uspallata).

Plan de Recuperación de Desastres

El Plan de Recuperación ante Desastres (DRP), vigente desde el año 2017, está conformado por:

- Identificación de procesos de negocio
- Análisis de Impacto en el Negocio
- Informe de Relevamiento y Situación Actual
- Estrategia de Recuperación
- Esquema General

[23] El pasillo frío es un confinamiento, un área creada dentro de los centros de datos con la finalidad de obtener una temperatura óptima, evitar la condensación, la carga electrostática, elevar el rendimiento energético y la capacidad de refrigeración de la zona.

- Plan de Administración del Desastre
- Plan de Recuperación
- Plan de Restauración
- Esquema detallado de uso
- Esquema de Prueba
- Esquema de Mantenimiento
- Template Prueba

Procedimiento para el resguardo de la información

ASInf cuenta con procedimientos para el respaldo de servidores virtuales, servidores físicos y base de datos.

Para el respaldo de servidores virtuales se utiliza el software "Veeam Backup & Replication".[24] Los diversos tiempos de almacenamiento de la información están definidos en las políticas de ASInf y su depuración se realiza mediante procesos internos.

Para el caso de respaldo de servidores físicos, es necesario que el propietario de los datos genere una solicitud a través del NOC[25] (https://noc-mesa.buenosaires.gob.ar) indicando los horarios, archivos o directorios incluidos y excluidos, etc. Los diferentes tiempos de retención están establecidos en las políticas de la Agencia de Sistemas de información según su clasificación.

El respaldo de las bases de datos se realiza automáticamente en el servidor donde se encuentre la base de datos a respaldar.

Procedimiento para tareas de restauración

El procedimiento para tareas de restauración debe ser generado mediante una solicitud a través del NOC (https://noc-mesa.buenosaires.gob.ar) especificando:

- Nombre y la dirección IP del servidor

[24] Veeam Backup & Replication es una aplicación de respaldo de información utilizada para entornos virtuales, la cual permite verificar automáticamente la recuperación de la información almacenada.

[25] NOC - Instructivo del centro de operaciones de red. Obtenido en el año 2009 en: https://n9.cl/yc03q [Accedido el 16/6/21]

- Fecha del backup solicitado
- Tipo de restauración:
    1) Completa. Debe indicarse si el servidor virtual es sobreescrito o si el mismo es conservado.
    2) Nivel de archivos. Se debe indicar la ruta completa del ítem a restaurar, si debe ser sobreescrito o conservado.
    3) Nombre de la base de datos. Debe especificarse si el servidor virtual debe ser sobreescrito o si el mismo debe ser conservado.
    4) Esquema de la base de datos. Se debe establecer si el servidor virtual es sobreescrito o es conservado.

Las características del respaldo de la información establecidas son:

1. Información que se resguarda:
    a. Servidores virtuales
        - La totalidad del servidor virtual.
    b. Servidores físicos
        - Archivos de directorios compartidos.
        - Archivos de sistema.
        - Dumps[26] de bases de datos.
        - La información total correspondiente a la base de datos.

2. El tiempo de guarda definido es:
    a. Veeam
        - Copia de seguridad diaria, se ejecutan una vez al día y tienen una retención de 30 días.
        - Copia de seguridad mensual, consiste en la copia a cinta del total de la información correspondiente a los datos del último día del mes. La retención de la información tiene un período de 2 años (24 meses).
        - Copia de seguridad anual, consiste en la copia a cinta del total de la información correspondiente a los datos del último día del año. La retención de la información se realiza durante 10 años (120 meses).
    b. ISP[27]

[26] Dump: permite realizar copias de seguridad de la base de datos con el objetivo de proteger la información.

[27] ISP es un software que permite crear copias de seguridad en forma manual o automática, almacenar en un disco local y cargar en un servidor remoto o en la nube.

- Copia de seguridad diaria, se ejecutan una vez al día y son retenidas durante 30 días.
- Copias de seguridad mensuales, se ejecutan el primer día o durante el primer fin de semana del mes. Son almacenadas durante 2 años (24 meses).
- Copias de seguridad anual, ejecutadas el primer día o durante el primer fin de semana del mes. Son resguardadas durante 10 años (120 meses).

c. ZDL[28]

- Copia de seguridad diaria, se ejecutan una vez al día y se almacenan durante 65 días.
- Copias de seguridad mensual, se ejecutan el primer fin de semana del mes y son conservadas durante 5 años (60 meses).

3. Tamaño estimado de las copias de seguridad (expresados en TeraBytes)

Software	TB
Veeam	730
ISP	1750
ZDL	20

4. Software utilizado
   - Veeam Backup & Replication
   - IBM Spectrum Protect[29]
   - Export Datapump[30] (copias de seguridad lógica)
   - RMAN[31] (Copias de seguridad física). Este último es soportado con el software de Oracle ZDLRA[32]

[28] ZDL (Zero Data Loss, en español Sin Pérdida de Datos) permite proteger las bases de datos y proporcionar las copias de seguridad en tiempo real desde la memoria del sistema.

[29] IBM Spectrum Protect es una plataforma que permite la protección de los datos mediante un único punto de control y posibilita la administración para el respaldo y la recuperación de la información.

[30] Export Datapump es un software de servidor utilizado para mover información entre las bases de datos Oracle.

5. Tipo de ejecución de las tareas de las copias de seguridad
   a. Veeam
      - Las copias de seguridad se realizan en forma automática en los horarios establecidos.
      - Perfiles de usuario autorizados a realizarlos.
   b. ISP
      - Todas las copias de seguridad se ejecutan en forma programada.
      - Perfiles de usuario autorizados a realizarlos.
   c. ZDL
      - Todas las copias de seguridad se efectúan de manera programada.
      - Perfiles de usuario autorizados a realizarlos.

6. Ubicación del repositorio de guarda
   a. Veeam
      - Las copias de seguridad diarias son almacenadas en repositorios a discos del tipo HDD[33] y SSD,[34] los cuales se encuentran asociados a sus respectivos servidores.
         - ✓ Dentro del repositorio ubicado en Av. Independencia 635, CABA, se utiliza el servidor Veeam Repository.[35]
         - ✓ Dentro del repositorio ubicado en la calle Uspallata 3160, CABA, se utiliza el servidor Veeam Repository.
      - Las copias de seguridad ejecutadas en forma mensual y anual se almacenan en cajas ignífugas.

[31] RMAN (Recovery Manager, en español Gestor de Recuperación) es un administrador que provee un servicio de alta disponibilidad para la realización y recuperación de copias de seguridad para bases de datos Oracle.

[32] ZDLRA (Zero Data Loss Recovery Appliance, en español Dispositivo de Recuperación sin Pérdida de Datos) es una plataforma informática de Oracle compuesta por hardware y software cuyo objetivo es el respaldo y la recuperación de la base sin pérdida de datos.

[33] HDD (Hard Drive Disk, en español Disco Duro) es un tipo de disco integrado por componentes mecánicos que sirve para almacenar los datos en forma permanente, los cuales no se borran cuando la unidad carece de alimentación por energía eléctrica.

[34] SSD (Solid State Drive, en español Unidad de Estado Sólido), es un disco que almacena los datos en microchips con memorias flash interconectadas entre sí.

[35] Veeam Repository (en español Repositorio Veeam) es la ubicación de almacenamiento donde la aplicación Veeam Backup & Replication conserva los archivos de respaldo.

- Sólo los perfiles de usuario autorizados pueden acceder.

b. ISP
   - Las copias de seguridad diarias son almacenadas en repositorios a discos dentro del servidor, las que luego son migradas a cinta.
   - Las copias de seguridad realizadas en forma mensual y anual son almacenadas en cajas ignífugas.
   - Solamente los perfiles de usuario autorizados poseen acceso.

c. ZDL
   - Las copias de seguridad realizadas en forma diaria son almacenadas en repositorios a discos que se encuentran dentro del dispositivo.
   - Las copias de seguridad ejecutadas mensual y anualmente son almacenadas en cajas ignífugas.
   - Únicamente los perfiles de usuario autorizados poseen acceso.

7. Tipos de copias de seguridad (completo, incremental y/o diferencial)
   a. Veeam
      Realizado mediante el método de “Forever Forward Incremental Backup”, basado en la creación de un respaldo inicial total seguido de una cadena de respaldos incrementales.
   b. ISP
      Ejecutado a través de la metodología “Incremental Forever”, consistente en la creación de una copia de seguridad con la totalidad de los datos y luego el incremento del almacenamiento con los datos a partir de la copia inicial.
   c. ZDL
      Utilizando el método “Incremental Forever”, se crea una copia de seguridad inicial elaborada con la totalidad de los datos existentes y posteriormente se incrementa el almacenamiento con los nuevos datos.

8. Pruebas de restauración
   Una vez al mes se realizan las pruebas de restauración para el entorno de servidores físicos y para el entorno virtual. Actualmente se están tomando como pruebas de restauración las mismas solicitudes

realizadas a través del NOC, identificadas por fecha, solicitante, tipo y ubicación.

Política de Prevención de Software Malicioso

Basado en la política PO0704 “Política de Prevención de Software Malicioso”, Resolución N°177/ASInf/13, la Agencia de Sistemas de Información provee a todos los usuarios del GCABA, un antivirus/antimalware de última generación.

Actualmente, la solución implementada a través de la Licitación Pública N° 8056-1899-LPU19, es Sophos, tramitada mediante el expediente EX-2019-37347246-GCABA-ASInf.[36]

La solución permite contar con un sistema liviano, pero con la prevención que brinda un antivirus tradicional y amenazas de día cero. Todos los equipos incorporados al directorio activo de la CABA tienen instalado el antivirus corporativo.

La cobertura de la solución alcanza a equipos Windows, Mac, Linux y servidores. Las actualizaciones son automáticas, pudiendo ejecutar un parche de forma centralizada, si así se requiriera.

El correo electrónico corporativo está montado principalmente sobre Office365,[37] con los controles de seguridad de la misma plataforma (incluido el control de Spam, limpieza de virus y controles de log’s),[38] adicionalmente y en la misma forma, hay tres mil cuentas en la plataforma G Suite[39].

Política de uso de Correo Electrónico

La Resolución N°177/ASInf/13 también define la PO0706 - “Política de uso de Correo Electrónico”, la misma establece la solicitud y el otorgamiento de los correos electrónicos de manera descentralizada, en las Direcciones Generales Técnicas, Administrativas y Legales de cada organismo.

[36] EX-2019-37347246-GCABA-ASInf. Obtenido el 19 de diciembre del año 2019 en: https://n9.cl/ix36j [Accedido el 28/5/21]

[37] Office365 es una herramienta informática que permite crear, acceder y compartir entre sus usuarios, documentos en línea, con los formatos definidos por la empresa Microsoft.

[38] Log es el almacenamiento del historial secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular.

[39] G Suite es un conjunto de herramientas informáticas para oficina con servicios en la nube cuya finalidad es mejorar la productividad de las tareas a realizar.

El filtrado de contenido de la navegación se realiza por medio de proxys dedicados.[40] El tipo de filtrado realizado y su prohibición está aplicado a sitios de contenidos pornográficos, maliciosos y de juegos y apuestas. El monitoreo del tráfico se realiza por medio de un correlacionador de log's,[41] y solo se dan alertas al momento de detectar un archivo o ejecución de código malicioso.

Política de uso de Internet

La PO0707 - "Política de Uso de Internet", definida en la Resolución N°177/ASInf/13, especifica las prohibiciones dentro del uso de internet tales como obtener acceso no autorizado, descargas de archivos de video o voz que no sean para fines laborales, acciones que comprometan la seguridad de los servidores del GCABA, etc. También detalla la responsabilidad de los usuarios en el ingreso a los sitios de internet y del respeto de las leyes en la administración de la información.[42]

Capacitación a usuarios finales

El GCABA cuenta con el Instituto Superior de la Carrera (ISC), encargado del dictado de cursos a los distintos escalafones de la carrera administrativa, como así también del seguimiento de los efectuados por cada agente.

Durante la pandemia, habiéndose suspendido la presencialidad, se han seguido dictando cursos en forma virtual.

Asimismo, la Dirección de Infraestructura de ASInf aclara que ante la necesidad de adquisición de un nuevo software o hardware, el cual requiera capacitación específica, se efectúa la contratación de la misma para los encargados de poner la operación activa.

Respecto de la capacitación a usuarios finales, la Dirección General de Seguridad Informática indica que no se dictaron cursos de concientización sobre la Prevención de Software Malicioso, uso de Correo Electrónico y de Internet desde el año 2018.

[40] Es un dispositivo informático el cual actúa como intermediario en las conexiones de un cliente y un servidor de destino. Permite filtrar, gestionar o almacenar los paquetes de datos que se envían, utilizado especialmente para internet.

[41] Permite la centralización y sincronización de todos los dispositivos, gestionando los eventos recibidos y generando alertas en la recepción de log´s de infraestructura y aplicaciones.

[42] Ley Nacional N° 11723, Ley de Protección de Datos Personales (Ley del GCABA N° 1845 y Ley Nacional N° 25326).

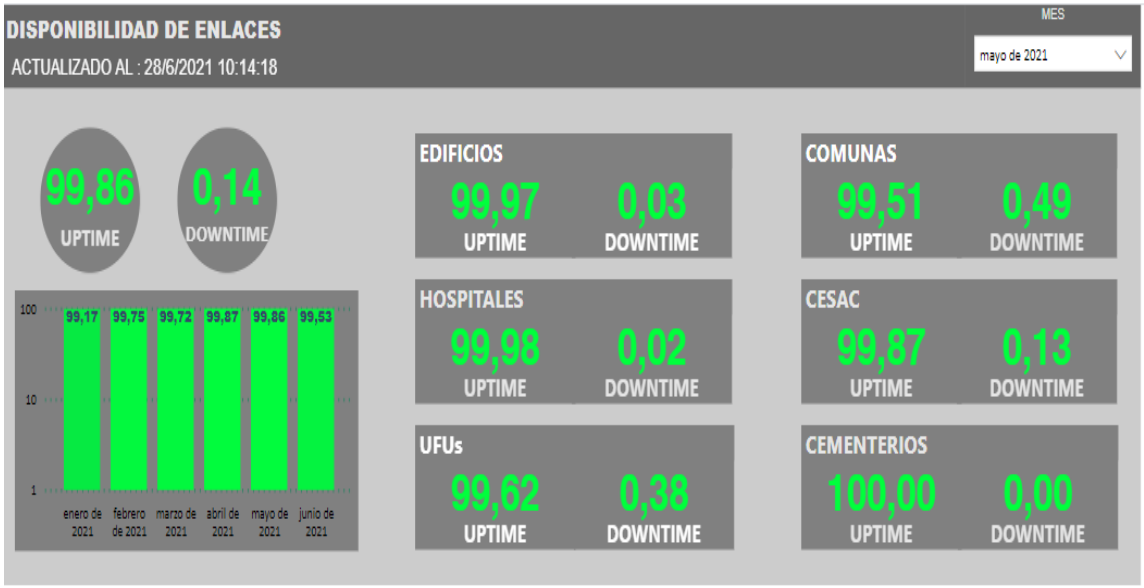
Gobierno, Gestión y Monitoreo de TI

Es necesario definir objetivos de gobierno, de gestión y establecer indicadores para su medición. Los procesos de gobierno y gestión deben dar cobertura a las metas organizacionales de ASInf, por tal motivo, su monitorización permanente exige la implementación de las acciones correctivas ante la detección de desvíos.

ASInf, a partir del año 2021, ha comenzado a utilizar métricas relacionadas con el Gobierno, la Gestión y el Monitoreo de las tecnologías.

Algunas métricas tales como los Indicadores Mensuales de Conectividad, están vigentes desde enero del año 2021, y los Indicadores de Cumplimiento de SLA de Incidentes Críticos [43], utilizados desde febrero del mismo año.

La siguiente imagen pertenece a los Indicadores Mensuales de Conectividad en hospitales, comunas, CeSac (Centros de Salud y Acción Comunitaria) y otros, correspondientes al mes de mayo del año 2021.



Fuente: ASInf

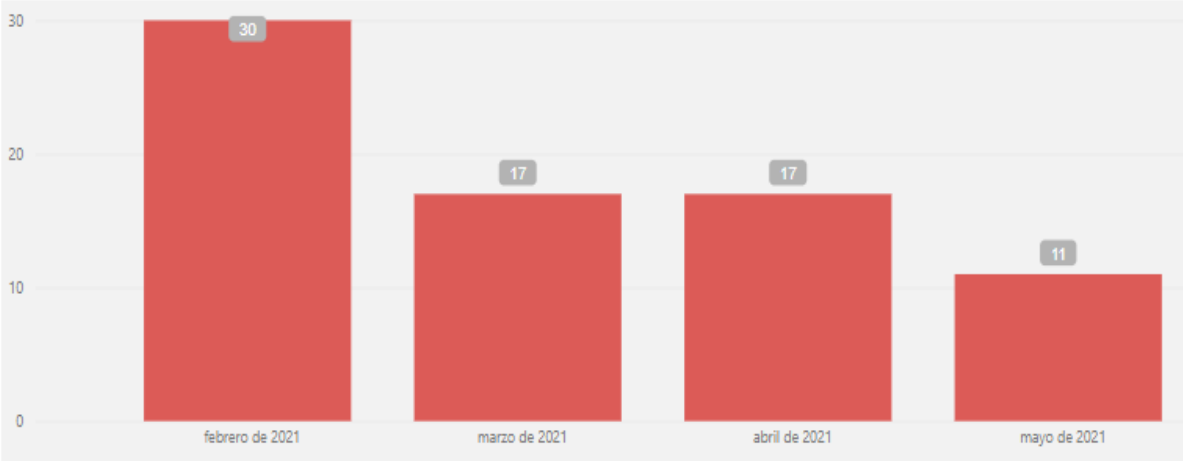
[43] SLA Service Level Agreement, (en español, Acuerdo de Nivel de Servicio), es un acuerdo firmado entre el proveedor de un servicio y el cliente. El objetivo es establecer el nivel del servicio y sus parámetros, tales como los plazos de entrega, responsables, tiempos de respuesta, tipo de soporte técnico, etc.

La próxima tabla describe los indicadores de conectividad utilizados y su detalle:

Nombre del Indicador	Detalle
Incidentes Prioridad 1 - SLA 6 hs	Cumplimiento del SLA de Incidente de Prioridad 1
Generales - Uptime	Tiempo en el que el enlace se encuentra disponible
Generales - Downtime	Tiempo en el que el enlace no se encuentra disponible
Edificios - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
Edificios - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles
Comunas - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
Comunas - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles
Cementerios - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
Cementerios - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles
Hospitales - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
Hospitales - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles
UFUs - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
UFUs - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles
CESACs - Uptime	Promedio de tiempo en el que los enlaces se encuentran disponibles
CESACs - Downtime	Promedio de tiempo en el que los enlaces no se encuentran disponibles

Fuente: ASInf

El siguiente gráfico muestra el Indicador de Cumplimiento de SLA de Incidentes Críticos, clasificado mediante tickets y el promedio de días abierto para los meses de febrero, marzo, abril y mayo del año 2021.



CATEGORIA	SUBCATEGORIA	#
REDES	ENLACE ASI	10
REDES	ENLACE LTE	1
Total		**11**

ITEM	#TICKETS	SLA OK	SLA VENCIDO	PROMEDIO DIAS ABIERTO
FIBRA OPTICA	7	7		2,02
CONFIGURACION DE EQUIPO	2		2	3,32
REINICIO DE EQUIPO	1	1		0,09
RELEVAMIENTO	1		1	14,15
Total	**11**	**8**	**3**	**3,18**

Fuente: ASInf

Nombre del Indicador	Detalle
SLA Incidentes Críticos	Cumplimento de SLA de incidentes críticos en el mes

VI. OBSERVACIONES

Cumplimiento del Marco de Referencia COBIT 2019

1) Alinear, Planificar y Organizar - APO01

- Gestionar el marco de gestión de I&T

✓ **Dependencia jerárquica de la Dirección General Seguridad Informática respecto de la Dirección Ejecutiva de la Agencia de Sistemas de Información. La configuración funcional y jerárquica actual de la**

estructura organizativa no favorece el control interno de los sistemas de comunicaciones y operaciones.

2) Alinear, Planificar y Organizar - APO07

- Gestionar los recursos humanos

✓ **Falta de actualización en el dictado de cursos de concientización a usuarios para la Prevención de Software Malicioso, uso de Correo Electrónico y uso responsable de Internet. La carencia del dictado de cursos de actualización limita los conocimientos específicos, habilidades y competencias del recurso humano.**

Descripción de las observaciones vinculadas a los sistemas y aplicativos de gestión de comunicaciones y operaciones.

3) Alinear, Planificar y Organizar - APO12

- Gestionar el riesgo

✓ **No exhibe documentación vinculada con la gestión del riesgo en los sistemas. Definición del apetito al riesgo aceptado, niveles de tolerancia, métricas, probabilidad de ocurrencia de los eventos y magnitud de la pérdida. Elaboración de informes, frecuencia y los responsables de la implementación de las acciones correctivas. Evaluar los riesgos en los sistemas permite definir, analizar y aceptar un determinado nivel de pérdidas de información.**

4) Construir, adquirir e implementar - BAI03

- Gestionar la identificación y construcción de soluciones

✓ **No presenta documentación respaldatoria para la planificación en los sistemas asociados a las comunicaciones y operaciones, a corto, mediano y largo plazo. Tampoco respecto de las modificaciones en curso y terminadas. La carencia de planificación en**

los sistemas atenta contra su capacidad y disponibilidad.

5) Construir, adquirir e implementar - BAI06

- Gestionar los cambios de TI

✓ **No expone documentos que definan un modelo de control de cambios en los sistemas que gestionan las comunicaciones y operaciones. Falta de metodología, solicitud, evaluación, priorización, procesos de control, aceptación y versionados de los cambios. Es necesario mitigar el riesgo de los cambios a realizar para lograr sistemas estables que conserven la integridad de la información que administran.**

6) Construir, adquirir e implementar - BAI08

- Gestionar el conocimiento

✓ **La identificación, contextualización y clasificación de la información permite disponer y compartir el conocimiento relevante para los procesos del organismo. Carencia de manuales, diagramas entidad-relación y estudios de factibilidad de los proyectos de desarrollo de los sistemas.**

7) Construir, adquirir e implementar - BAI09

- Gestionar los activos

✓ **No se presenta documentación que garantice que se efectuó la gestión de los activos vinculados a los sistemas de comunicaciones y operaciones, cuyo objetivo es asegurar aquellos que son críticos para planificar la demanda de capacidad y disponibilidad. Es necesario identificar y registrar los activos actuales, priorizar los críticos, optimizar su valor y gestionar las licencias. La falta de ejecución del proceso pone en riesgo el adecuado funcionamiento de los mencionados sistemas.**

8) Entregar, dar servicio y soporte - DSS01

- Gestionar las operaciones
  - ✓ **No adjunta documentación que ratifique la ejecución de procedimientos operativos de los sistemas a cargo del monitoreo de la infraestructura de TI, el medioambiente y la gestión de las instalaciones operativas. Los mencionados aseguran la continuidad de los servicios asociados a las comunicaciones y operaciones. La gestión de los servicios de TI propios y de terceros permite detectar los desvíos e implementar las acciones correctivas necesarias para cumplir con la planificación establecida.**

9) Entregar, dar servicio y soporte - DSS02

- Gestionar las peticiones y los incidentes de servicio
  - ✓ **No consta la definición e implementación de un proceso de administración de peticiones e incidentes por fallos en los sistemas ligados con las comunicaciones y operaciones. Debe establecerse un esquema de clasificación y petición que incluya el registro, priorización, aprobación, resolución, seguimiento e informe de incidentes. La falta del proceso atenta contra la productividad, no minimiza los incidentes y favorece las interrupciones en los servicios asociados.**

10) Entregar, dar servicio y soporte - DSS05

- Gestionar los servicios de seguridad
  - ✓ **No se detallan procesos de gestión de seguridad en los sistemas para proteger la conectividad, red, dispositivos de punto final, vulnerabilidades y los ataques por parte de software malicioso. Es indispensable controlar los sistemas asociados a las comunicaciones y operaciones y evaluar el impacto ocasionado en la seguridad de la información para garantizar la continuidad y disponibilidad del servicio.**

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

11) Entregar, dar servicio y soporte - DSS06

- Gestionar los controles de procesos de negocio
  - ✓ **No se expone un proceso de gestión de roles, responsabilidades, privilegios para el acceso y niveles de autoridad en los sistemas de comunicaciones y operaciones. El incumplimiento en la utilización del mencionado proceso no garantiza que la información administrada sea íntegra, completa, válida, precisa, segura y oportuna.**

12) Monitorizar, evaluar y valorar - MEA01

- Gestionar la supervisión del rendimiento y la conformidad
  - ✓ **No consta el uso de un enfoque de supervisión del rendimiento y la conformidad en los sistemas de comunicaciones y operaciones. No se expusieron procesos de recopilación de datos, proyección de objetivos de rendimiento, conformidad, análisis e implementación de acciones correctivas. Las acciones mencionadas promueven el incremento en el rendimiento y la obtención de las metas planificadas.**

VII. RECOMENDACIONES

1) Alinear, Planificar y Organizar - APO01

- Gestionar el marco de gestión de I&T
  - ✓ Es conveniente definir e implementar una estructura organizativa que permita a la Dirección General Seguridad Informática accionar de manera independiente del organismo e implementar las acciones correctivas para lograr la consecución de sus responsabilidades primarias**.**

2) Alinear, Planificar y Organizar - APO07

- Gestionar los recursos humanos

- ✓ Se recomienda identificar las habilidades y competencias del personal, así como las necesidades de capacitación en el uso de sistemas y tecnologías para incrementar los beneficios obtenidos en el dictado de cursos. La finalidad es mitigar los riesgos existentes en la ejecución de acciones que permitan el acceso no autorizado a datos sensibles.

Descripción de las observaciones vinculadas a los sistemas y aplicativos de gestión de comunicaciones y operaciones.

3) Alinear, Planificar y Organizar - APO12

- Gestionar el riesgo
  - ✓ Implementar un modelo de recolección, clasificación y análisis de datos vinculados con los riesgos tecnológicos que evidencie los riesgos existentes, impactos y posibles pérdidas.

4) Construir, adquirir e implementar - BAI03

- Gestionar la identificación y construcción de soluciones
  - ✓ Identificar y construir soluciones de alto nivel que cubran los servicios de comunicaciones y operaciones que brinda ASInf al GCABA. Evaluar la tecnología, procesos y los flujos de trabajo que garanticen la alineación de la estrategia y la arquitectura establecida por el organismo.

5) Construir, adquirir e implementar - BAI06

- Gestionar los cambios de TI
  - ✓ Gestionar los cambios requiere de un modelo que contemple el registro, priorización, clasificación, evaluación, autorización, planificación y programación. Considerar el impacto generado por los cambios y analizar el efecto causado por la integración de los cambios pedidos. Los cambios solicitados en los sistemas deben ser versionados, al ser registrados es adecuado considerar parámetros tales como la fecha de recepción del cambio, el error asociado, descripción del cambio propuesto, motivo, propósito, y si se

conoce, los recursos estimados y elementos de la configuración que requieren modificación. En la gestión y seguimiento del cambio, es indispensable incluir el estado (aceptado o rechazado), motivo del rechazo, fecha, evaluación preliminar, su prioridad, las acciones de retroceso, recursos asignados, fecha y plan de implementación, cronograma, evaluación final y su fecha de cierre.

6) Construir, adquirir e implementar - BAI08

- Gestionar el conocimiento
  - ✓ Reconocer, clasificar, estructurar y contextualizar la información, de forma que permita ser utilizada para la toma de decisiones del gobierno y la gestión de TI. La información recopilada exige la validación de su fuente. La transformación de información en conocimiento requiere de un proceso de valoración de la importancia, confiabilidad, integridad, precisión y vigencia. Identificar los usuarios potenciales del conocimiento técnico y planificar su transferencia.

7) Construir, adquirir e implementar - BAI09

- Gestionar los activos
  - ✓ Instaurar un proceso de identificación y registro de los activos actuales, propios o de terceros controlados por ASInf, reconociendo aquellos que son críticos y su capacidad para proveer los servicios. Planificar la resiliencia de los activos críticos, monitorear su rendimiento e implementar un plan de mantenimiento preventivo.

8) Entregar, dar servicio y soporte - DSS01

- Gestionar las operaciones
  - ✓ Implementar procedimientos operativos que midan los rendimientos de los servicios internos provistos y sus incidentes. Asimismo, evaluar el nivel de los servicios tercerizados de TI respecto de los SLA firmados. Monitorear la infraestructura y los eventos asociados no deseados, registrando, clasificando y distinguiendo aquellos con

menores impactos respecto de los eventos significativos con consecuencias en los servicios críticos.

9) Entregar, dar servicio y soporte - DSS02

- Gestionar las peticiones y los incidentes de servicio
  - ✓ Definir un modelo de atención de incidentes de servicios que contenga el registro, clasificación, priorización y escalamiento. Considerar el tipo y categoría para efectuar y documentar un análisis de las tendencias. Investigar y diagnosticar los síntomas que generan los incidentes, posibles causas, asignar su solución y actualizar su estado y posterior cierre.

10) Entregar, dar servicio y soporte - DSS05

- Gestionar los servicios de seguridad
  - ✓ Es esencial que el organismo y el GCABA, todos sus servicios e instalaciones, cuenten con medidas preventivas, detectivas y correctivas. La instalación, activación, actualización, concientización y capacitación del recurso humano para su uso minimizarán el impacto por incidentes y vulnerabilidades en la seguridad. La gestión del acceso físico y lógico a los activos de TI, la identidad del usuario, la seguridad de la conectividad y de la red pueden garantizar la confiabilidad, integridad, disponibilidad y privacidad de los datos administrados.

11) Entregar, dar servicio y soporte - DSS06

- Gestionar los controles de procesos de negocio
  - ✓ Alinear las tareas de control de los procesos vinculados a los servicios de TI con los objetivos de ASInf. Verificar el procesamiento de los datos, su integridad y validez, origen, roles, responsabilidades y autorización de accesos. La asignación de roles para las tareas críticas debe respetar una clara segregación de las funciones.

12) Monitorizar, evaluar y valorar - MEA01

- Gestionar la supervisión del rendimiento y la conformidad
  - ✓ Es fundamental proyectar objetivos de rendimiento y conformidad en los servicios de TI, recopilar y procesar los datos obtenidos para priorizar aquellos vinculados con los procesos críticos. Establecer un modelo con metas y métricas, las cuales sean relevantes y alcanzables en tiempos determinados. Informar en forma periódica el nivel de desvío del rendimiento y plantear los plazos estimados para la ejecución de acciones correctivas y su seguimiento.

VIII. CONCLUSIONES

La Agencia de Sistemas de Información, como órgano rector en Tecnologías de la Información y promotor de políticas gubernamentales en materia de Sistemas de Información, administra la infraestructura informática de todas las dependencias del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires. Por tal motivo, los programas de capacitación deben ser revisados de manera regular.

La gestión de riesgos relacionados con TI fija los niveles de tolerancia y pérdidas de información que el gobierno de tecnología está dispuesto a asumir. Permite equilibrar los costos, beneficios y riesgos dentro del organismo. Evaluar los incidentes, interrupciones y pérdidas para proponer acciones correctivas y minimizar los daños.

ASInf provee servicios de TI al GCABA, por ello las soluciones a través de servicios digitales deben ser ágiles, progresivas y escalables, que permitan planificar la expansión de su capacidad y disponibilidad a mediano plazo.

Es imprescindible medir los cambios solicitados con emergencia respecto del total de cambios cuyo objetivo es plantear las acciones correctivas necesarias para minimizar los primeros mencionados.

Es oportuno evaluar el costo-beneficio de los activos de TI, principalmente aquellos críticos. Analizar la conveniencia de su actualización o el recambio tecnológico y contrastarlo con el ciclo de vida planificado, desde su adquisición hasta su baja.

La mejora continua en los servicios puede ser aplicada mediante el análisis minucioso de los incidentes manifestados. El seguimiento, la producción de informes, la definición de métricas y la evaluación de las posibles causas de

problemas recurrentes, aportan los datos necesarios para generar eficacia en los servicios de comunicaciones y operaciones.

La gestión de controles de los procesos no sólo debe aplicarse al flujo de información generado en el organismo, sino también a los datos que ingresan desde otros entes del GCABA y de los proveedores de servicios de TI externalizados. Es beneficioso que la evaluación y el monitoreo de los mencionados controles se ejecute regularmente.

Es conveniente, en el próximo presupuesto, asignar recursos destinados a mejorar y adecuar el Plan de Contingencia y Recuperación de Desastres, además de agregar las aplicaciones que actualmente no se encuentren incluidos.

Se sugiere incrementar la cantidad de métricas e indicadores utilizados para evaluar el Gobierno y la Gestión de TI. También, intensificar los procedimientos de monitoreo y la implementación de acciones correctivas que permitirán el cumplimiento de los objetivos planteados garantizando el nivel de cobertura de los servicios tecnológicos provistos.

Las tareas de auditoría desarrolladas en campo culminaron en el mes de noviembre del año 2021.

ANEXO I

Presupuesto 2020 - Distribución de Créditos

Jur.	SubJ.	Ent.	U.E.	Descripción	Crédito Sanción
21	0	0	2.051	AGENCIA DE SISTEMAS DE INFORMACION	1.406.380.207

Presupuesto 2020 - Distribución de Créditos

Jur.	SubJ.	Ent.	U.E.	Descripción	Crédito Sanción
21	0	270	662	DIR.GRAL. DE INFRAESTRUCTURA	715.630.291

ANEXO II

PLAN PLURIANUAL DE INVERSIONES PUBLICAS 2020-2022

(en pesos)

Jur Og UE Pg. Sg. Py. Ac. Ob. FF	Denominación	Inversión Total	Inversiones			Posteriores
			Anteriores	2020	2021	2022	
270	AGENCIA SISTEMAS DE INFORMACION	732.786.819	462.177.574	270.609.245	0	0	0
682	DIR.GRAL. DE INFRAESTRUCTURA	453.352.678	303.743.433	149.609.245	0	0	0
96	INFRAESTRUCTURA INFORMATICA	453.352.678	303.743.433	149.609.245	0	0	0
1	DATA CENTER	227.624.106	183.208.411	44.415.695	0	0	0
0 52 11	DATA CENTER	227.624.106	183.208.411	44.415.695	0	0	0

ANEXO III

Organismos Descentralizados, Entes Autarquicos y Organos de Control
Composición del Gasto por Jurisdicción, y Carácter Económico
(En Pesos)

CARACTER ECONOMICO / JURISDICCION/ENTIDAD	GASTOS CORRIENTES	GASTOS DE CAPITAL	TOTAL
AGENCIA SISTEMAS DE INFORMACION	1.418.615.462	333.412.245	1.752.027.707

ANEXO IV

DESCRIPCIÓN DEL PROGRAMA AÑO 2020

Jurisdicción/Entidad AGENCIA SISTEMAS DE INFORMACION
Programa N° 96.INFRAESTRUCTURA INFORMATICA

UNIDAD RESPONSABLE: DIR.GRAL. DE INFRAESTRUCTURA

DESCRIPCIÓN:

Este programa tiene como finalidad administrar, mantener y expandir los sistemas de comunicaciones y sistemas informáticos, bajo la órbita del GCABA, para garantizar una elevada disponibilidad y confiabilidad de los mismos.

El objetivo es brindar una disponibilidad 7x24 de todos los sistemas de gobierno y la seguridad física de la información.

Para lograrlo se cuenta con una plataforma de software y hardware, una mesa de ayuda, brinda soporte técnico a usuarios internos y externos a la ASI, una plataforma de monitoreo y un equipo de técnicos que administran, dan soporte técnico y monitorean la red MAN de GCBA, la red BA Wifi (Wifi Público gratuito), la red WLAN GCBA (Red Wifi Corporativa), el servicio de correo y el acceso de los usuarios del GCABA.

- Puesta en valor - Ampliación del Backbone de Red.
- Puesta en valor - Ampliación Capacidades Datacenter
- Puesta en valor - Extensión WIFI edificios GCBA.
- Nuevos Servidores para procesamiento.
- Nueva librería de respaldos.
- Renovación tecnológica de los balanceadores de carga.
- Nuevos servidores de Storage para ampliar la capacidad de almacenamiento.
- Nuevo UPS (180 KVA) para Centro de cómputos.

DESCRIPCIÓN DEL PROGRAMA AÑO 2020

Jurisdicción/Entidad AGENCIA SISTEMAS DE INFORMACION
Programa N° 96.INFRAESTRUCTURA INFORMATICA

UNIDAD RESPONSABLE: DIR.GRAL. DE INFRAESTRUCTURA

DESCRIPCIÓN:

- Telefonía IP.
- Activos de red.
- Control de acceso y presentismo.
- Cableado Cat. 6
- Ampliación red CABA reparticiones conectadas a la MAN.
- Ampliación Cobertura WIMAX:
- Potenciales Ahorros de costo de enlaces.
- Recambio tecnológico con reemplazo de Access Point de red Wireless.
- Nuevo servicio de impresión en edificios GCBA.
- Proyecto nuevo edificio Ministerio de Hábitat en Edificio Elefante Blanco.
- Proyecto Polo Educativo María Elena Walsh.
- Proyecto Corrientes Peatonal.
- Proyecto Parque de la Estación.

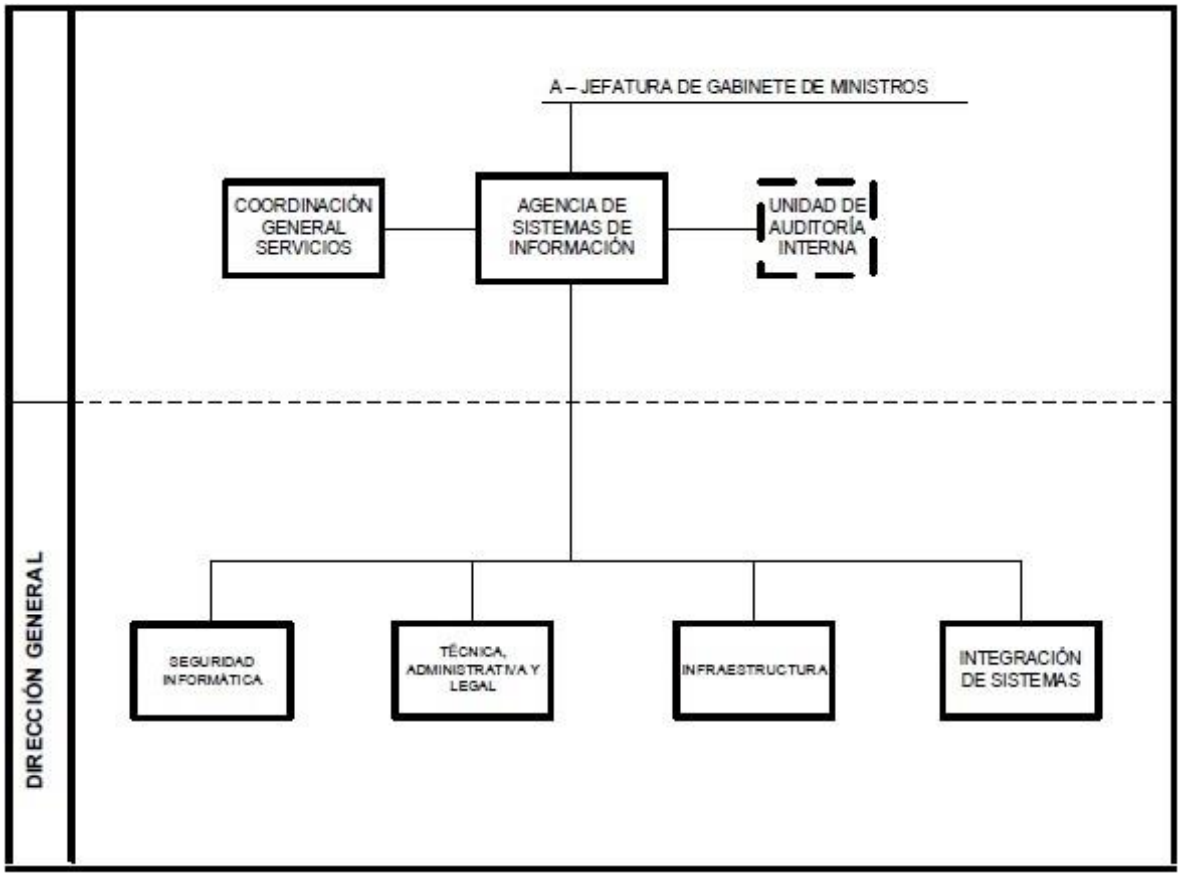
Unidad Ejecutora: DIR.GRAL. DE INFRAESTRUCTURA
Jurisdicción: 21.JEFATURA DE GABINETE DE MINISTROS
Finalidad: Administración Gubernamental
Función: Dirección ejecutiva

PRESUPUESTO FINANCIERO	
Inciso Principal	**IMPORTE**
Gastos en personal	**155.310.815**
Personal Permanente	85.801.840
Personal Transitorio	64.625.751
Asignaciones familiares	217.713
Asistencia social al personal	2.305.369
Gabinete de autoridades superiores	2.360.142
Bienes de consumo	**616.100**
Productos alimenticios, agropecuarios y forestales	143.000
Textiles y vestuario	244.400
Pulpa,papel, cartón y sus productos	28.600
Productos químicos, combustibles y lubricantes	14.300
Productos metálicos	28.600
Otros bienes de consumo	157.200
Servicios no personales	**458.750.376**
Servicios básicos	7.960.372
Mantenimiento, reparación y limpieza	119.200.950
Servicios profesionales, técnicos y operativos	16.858.164
Servicios Especializados, Comerciales y Financieros	314.380.890
Pasajes, viáticos y movilidad	350.000
Bienes de uso	**100.953.000**
Maquinaria y equipo	94.453.000
Activos intangibles	6.500.000
TOTAL	**715.630.291**

Fuente: ASInf

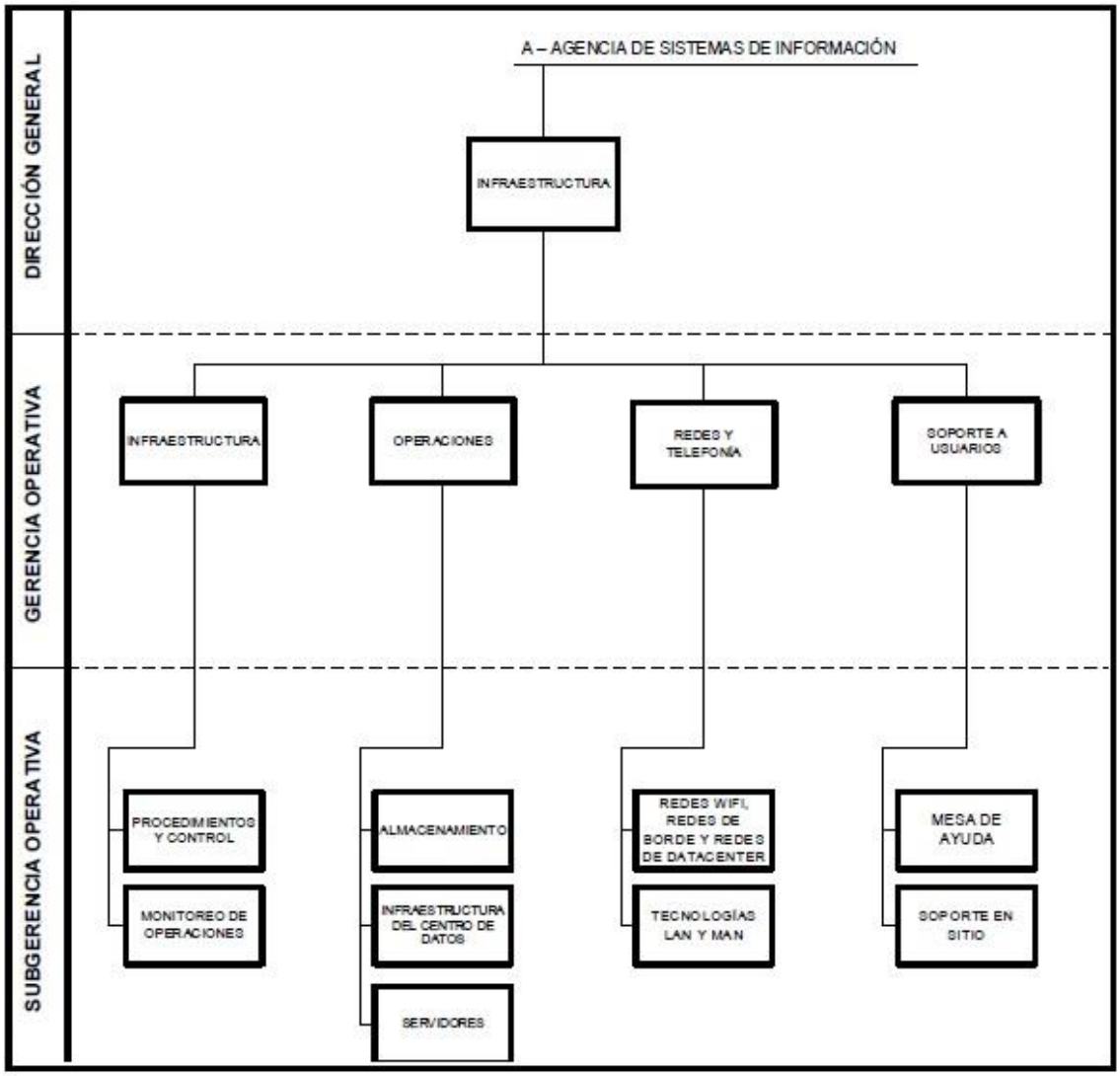
ANEXO V

Organigrama de la Agencia de Sistemas de Información



Fuente: ASInf

Organigrama de la Dirección General de Infraestructura



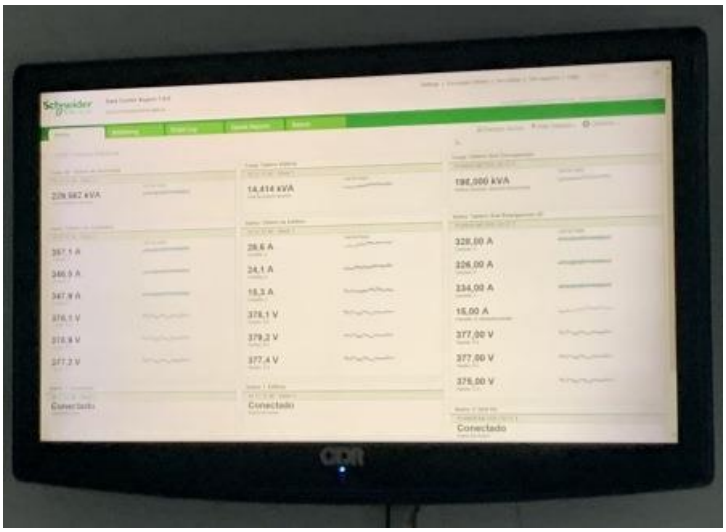
Fuente: ASInf

ANEXO VI

Fotos Independencia

Panel del sistema central de seguridad contra incendios.

Sistema de monitoreo eléctrico.



Fotos Uspallata

Piso técnico perforado y confinamiento de pasillo frío.

Sistema de extinción de incendio ubicado en el sector de cocheras.