UNIVERSIDAD NACIONAL DE SAN MARTÍN

ESCUELA DE POLÍTICA Y GOBIERNO

Maestría en Auditoría Gubernamental

Promoción 2018 - 2019

Nombre y Apellido: **Hernán Darío García**

Título de la Tesis: **"Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires"**

Director: Lic. Jorge Nunes

Buenos Aires, diciembre de 2020

Índice

Introducción

El gobierno de la Ciudad Autónoma de Buenos Aires a través del Plan de Modernización y de la Agencia de Sistemas de Información (ASInf) ha generado un conjunto de instrumentos para la estandarización, el desarrollo y la adquisición de nuevas tecnologías. En el mes de abril del año 2008, la Legislatura de la Ciudad Autónoma de Buenos Aires sanciona la ley 2689 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 proyectos y desarrollo de software y estándares en materia de Tecnologías de Información (TI) y Telecomunicaciones a ser aplicadas en consonancia con estándares internacionales, que garanticen la interoperabilidad y accesibilidad de los servicios electrónicos del Poder Ejecutivo".[1] Mediante el Decreto N° 1036/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).[2]

En el año 2009, el mismo órgano sanciona la ley 3304, 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.[3]

[1] Ley 2689. Obtenido el 17 de Abril de 2008 en la Word Wide Web: https://n9.cl/5b2c7 [Accedido el 22/5/20]

[2] Decreto N° 1036/GCABA/08. Obtenido el 27 de Agosto de 2008 en la Word Wide Web: https://n9.cl/h8z6 [Accedido el 22/5/20]

[3] Ley 3304. Obtenido el 7 de Enero de 2010 en la Word Wide Web: https://n9.cl/zy8e [Accedido el 22/5/20]

En el Anexo I de dicha ley se detallan los Objetivos Generales y Específicos del Plan de Modernización de la Administración Pública del Gobierno de la Ciudad de Buenos Aires. En el Artículo 2°, en los Objetivos Específicos, se destaca la necesidad de mejorar la gestión pública, promover e introducir el uso de nuevas Tecnologías de Información y Comunicación, además de la profesionalización y jerarquización de los recursos humanos. En el Capítulo III, titulado Del Gobierno Electrónico y nuevas Tecnologías de la Información y Comunicación, se describe la Sede Electrónica, Firma Electrónica y Digital, la Digitalización de procesos administrativos y Seguridad Informática.

Lo más destacado se expresa en el punto 6.5, Interoperabilidad. En el mismo se reconoce la necesidad de "Mejorar los sistemas de información y comunicación del Gobierno de la Ciudad de Buenos Aires, con el fin de evitar duplicaciones, inconsistencias en la actualización y normalizar la definición y el tratamiento de la información común". Así también, las actividades necesarias para el cumplimiento del objetivo "Definir los estándares tecnológicos para la interoperabilidad entre sistemas de información, para la interacción entre organismos de la Administración Pública de la Ciudad y entre éstos y los ciudadanos en la presentación electrónica de documentos"[3]

Las acciones implementadas por la dirección del GCABA (Gobierno de la Ciudad Autónoma de Buenos Aires) tienen como objetivo la implementación de un Plan de Modernización mediante la actualización de toda la infraestructura tecnológica y la capacitación de los recursos humanos. 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.[4]

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 el

[4] Res N° 190/MMGC/12. Obtenido el 11 de Mayo de 2012 en la Word Wide Web: https://n9.cl/5jua [Accedido el 15/5/19]

objetivo de promover la estandarización de los bienes informáticos, equipos, recursos, sistemas y programas a ser utilizados por el Poder Ejecutivo.[5]

En el año 2014, la administración gubernamental reconoció mediante el Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Centro de Datos que "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" [6]

Las autoridades del Ministerio de Modernización evidenciaron que ha ocurrido una actualización tecnológica en algunos ministerios dependientes del Poder Ejecutivo, pero que la misma se ha dado sin una mirada integral y de largo plazo. Reconocen que sin la existencia de un órgano rector que defina el camino a seguir, los esfuerzos sólo aportarán mejoras aisladas pudiendo no ser integrales. De allí se desprende con lógico razonamiento, que quizás algunas direcciones hayan contratado servicios de proveedores externos cuando podrían haberse obtenido desde algún organismo de esa especialidad perteneciente al GCABA. Las acciones de gobierno ratificaban los esfuerzos tendientes a centralizar la administración de los recursos tecnológicos. El Poder Ejecutivo reconoce que no es conveniente que cada organismo desarrolle un plan basado en sus propios estándares. Las necesidades de infraestructura y manejo de información de cada organismo varían notablemente. Los atributos de la información, confidencialidad, integridad, disponibilidad y privacidad, deben cumplir los requisitos mínimos según las misiones y funciones asignadas a cada ente en cuestión.

El Marco Normativo de Tecnología de Información está conformado por Políticas con alcance sobre las actividades relacionadas directa o indirectamente con la utilización de los 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. Dentro de cada una de las mencionadas Políticas se detalla el

[5] Res N°177/ASInf/13. Obtenido el 6 de Noviembre de 2013 en la Word Wide Web: https://n9.cl/12dwx [Accedido el 15/5/19]

[6] ES0101. Obtenido el 22 de Junio de 2015 en https://n9.cl/5i05 [Accedido el 15/5/19]

objetivo, alcance y contenido para lograr la interoperabilidad y seguridad de los sistemas y la ejecución del Plan Integral de Tecnologías de la información y Comunicaciones.

ASInf, en el año 2014, definió junto con el Marco Normativo de Tecnología de la Información, el Estándar de Desarrollo de la Agencia de Sistemas de Información[7] y se reglamentó el Proceso de Control de Cambios en Software de Aplicación provisto por Organismos PC0901.[8] 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. Cabe destacar que la adecuada gestión de la información y la correcta implementación de la infraestructura tecnológica proveen al ciudadano un servicio transparente, eficiente y seguro. Se define como Infraestructura Tecnológica a los sistemas operativos, software de base de datos, dispositivos de redes, seguridad informática, gestión de los accesos a los recursos, plataforma de comunicaciones y el entorno ambiental de los mismos. Es importante destacar que el perfil de necesidades de cada organismo y de cada uno de sus usuarios es muy diferente. Por lo cual la estandarización de la información es crucial. En el año 2015 y mediante la Resolución N° 239/ASInf/15[9], acorde con los avances tecnológicos y las necesidades, se ampliaron las políticas, guías y estándares.

Habrá casos en que la ASInf no pueda cubrir el pedido de servicio tecnológico de un organismo por falta de infraestructura, recurso humano, tiempo o capacitación. En esos casos, la resolución define que ASInf prestará el apoyo técnico necesario para llevar adelante el proceso de contratación de un proveedor externo para satisfacer dicho pedido, cumpliendo con las políticas vigentes en el Marco Normativo de Tecnología. 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.[10] En el año 2019

[7] Estándar de Desarrollo (año 2014). Obtenido el 30 de Diciembre de 2014 en la Word Wide Web: https://n9.cl/9qh9 [Accedido el 15/5/19]

[8] PC0901. Obtenido el 30 de Diciembre de 2014 en la Word Wide Web: https://n9.cl/jlw3 [Accedido el 15/5/19]

[9] Res N° 239/ASInf/15. Obtenido el 12 de Enero de 2015 en la Word Wide Web: https://n9.cl/ivc1 [Accedido el 15/5/19]

[10] Res N° 134/ASInf/16. Obtenido el 29 de Agosto 2016 en la Word Wide Web: https://n9.cl/xwhg [Accedido el 16/5/19]

se publicó una actualización del Estándar de Desarrollo.[11] El Marco Normativo de Tecnología de Información, como se expresa en la Resolución ASInf 177 del año 2013, son lineamientos teóricos y de normativa genérica, a seguir por los organismos dependientes del Poder Ejecutivo de la Ciudad. Por ello, a juicio profesional, sostengo que es conveniente seguir avanzando con una estrategia tecnológica superadora. Para lograrlo es necesario reformular el Marco Normativo de Tecnología de Información del Gobierno de la Ciudad Autónoma de Buenos Aires. Es importante tener en cuenta que cada organismo dependiente del Poder Ejecutivo de la Ciudad puede considerarse único. Esta aseveración viene dada porque cada organismo posee una estructura, tamaño, complejidad, necesidades y recursos que le son propios, únicos.

El problema posee tres aristas. Los dos actores involucrados, ASInf y los entes que requieren sus servicios y el Formulario único de requerimientos que actúa como canal de comunicación entre ambos. También en ciertas oportunidades los servicios podrían ser solicitados a través de la mesa de ayuda.

En el caso de los organismos más complejos, poseen recursos humanos propios capacitados y específicos en el área de sistemas, los cuales podrían procesar y definir de manera más adecuada cuáles son sus necesidades tecnológicas. En los organismos más pequeños, algunos, poseen escasos recursos humanos y quizás generalizando, no tan capacitados tecnológicamente. Cada ente debe completar el Formulario único de requerimientos para solicitar los servicios a ASInf. El mencionado formulario no posee el detalle técnico suficiente para solicitar un servicio específico. Y por último, ASInf, recibe el Formulario único de requerimientos del ente, posiblemente con errores u omisiones motivados en el escaso conocimiento técnico de quienes lo completan o no logran completarlo con la especificidad requerida.

El problema podría agravarse con la estructura organizativa vigente en ASInf, ya que permite llevar a cabo cambios que quizás no estén en línea con los objetivos estratégicos del organismo. En esos casos las responsabilidades de dichas acciones estarían difusas por la carencia de la separación funcional entre el gobierno y la gestión de TI. Este flujo degradado de información tecnológica atenta directamente a los principios de economía, eficiencia y eficacia que requiere la gestión pública.

[11] Estándar de Desarrollo (año 2019). Obtenido el 1 de Abril de 2019 en la Word Wide Web: https://n9.cl/2ywv6 [Accedido el 16/5/19]

Por lo antes mencionado, en mi opinión, la situación planteada actualmente mediante el Marco Normativo de Tecnología sería insuficiente, porque si bien ambos colaborarían con la estandarización y gestión en el manejo de la información, no permitirían el análisis profundo de las necesidades tecnológicas actuales de cada organismo ni aportarían las soluciones necesarias. Asimismo, en la estructura organizativa vigente en ASInf no existe la separación funcional entre la gobernanza y la gestión de la tecnología, lo que provoca una asignación difusa de la responsabilidad para definir los lineamientos estratégicos de tecnología y su gestión. Dicha situación podría empeorar para los casos en los que los agentes de cada organismo posean desconocimientos técnicos o ignoren las necesidades tecnológicas de medio y largo plazo. Cabe destacar la existencia de otros centros de procesamiento y almacenamiento dependientes del Poder Ejecutivo, ubicados fuera de la órbita de ASInf.

Por dicho motivo, desde el Control Interno del organismo, considero importante repensar la estrategia del Gobierno de Tecnología de ASInf. Se plantea como objetivo general elaborar un nuevo Marco Tecnológico de Referencia para el GCABA, el cual estaría basado en COBIT 5 (Control Objectives for Information and related Technology),[12] y complementado mediante ITIL v3 (Information Technology Infrastructure Library)[13], lo que permitiría gestionar la información de manera eficiente. El Marco Normativo de Tecnología vigente sería reemplazado en un contexto de trabajo tecnológico integrado. Permitiría la implementación de los principios de COBIT 5 para satisfacer las necesidades de las partes interesadas, cubrir los requisitos tecnológicos del GCABA de extremo a extremo, aplicar un marco de referencia único integrado, posibilitar un enfoque holístico y separar el gobierno de la gestión. Para lograr dicha propuesta se plantean tres objetivos específicos. El primero, expuesto en el capítulo 1, analizar los instrumentos de evaluación y estandarización tecnológica generados por el Gobierno de la Ciudad Autónoma de Buenos Aires. El segundo objetivo es determinar las normas técnicas a utilizar por los organismos de la Ciudad Autónoma de Buenos Aires, formulado en el capítulo 2. Y el tercer objetivo, implementado desde el capítulo 3 al 10, es proponer un Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires. Concluiré con la elaboración de un nuevo formulario de requerimientos de servicios que subsane los problemas señalados anteriormente.

[12] COBIT 5. Obtenido el año 2009 en la Word Wide Web: https://n9.cl/4qy9 [Accedido el 15/5/19]

[13] ITIL v3. Obtenido el año 2007 en la Word Wide Web: https://n9.cl/lgxs [Accedido el 15/5/19]

Capítulo 1 - Análisis del marco tecnológico vigente del GCABA

Antecedentes del marco

En la introducción de esta tesis se destacaba que en la estructura organizativa vigente en ASInf no existe la separación funcional entre la gobernanza y la gestión de la tecnología, trayendo como consecuencias, una asignación difusa de la responsabilidad para definir los lineamientos estratégicos tecnológicos y su gestión. Hablar de gestión tecnológica sin antes hablar de su gobierno es como construir una casa sobre un terreno desconocido. Las probabilidades que la casa siga en pie durante años son muy bajas. El Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires no puede tener gestión si previamente no tiene gobierno tecnológico y menos aún, quedar librado a la suerte. Las ideas previas para los antecedentes del marco demandan contextualizar y dimensionar los componentes del marco para establecer el impacto, como, dónde, cuando, por qué y a quienes afectarán los vacíos o carencias de un marco de tecnología.

Los actores involucrados son todos los ciudadanos usuarios de los servicios provistos por ASInf, directamente o a través de un ente del GCABA. La interrupción de los servicios entregados impediría la atención en hospitales, renovación de licencias de conducir, el pedido de ambulancias, denuncias de un robo o el cobro de sueldos de los empleados, todos del GCABA, sólo por mencionar algunos casos. El impacto causado en la vida de los ciudadanos usuarios es significativo.

La tecnología y la capacitación que poseen los usuarios no es un tema menor, los dispositivos y servicios con los que acceden forman un eslabón de una larga cadena que soporta amenazas y posee vulnerabilidades. Existe interacción de algunas bases de datos de la Ciudad con la Nación. Sin reglas claras de gobierno de tecnología, datos sensibles quedan expuestos y carecen de confidencialidad. ASInf forma parte del Gobierno de la Ciudad Autónoma de Buenos Aires, compuesto por agentes con relación laboral permanente o transitoria, algunos de ellos con responsabilidades en la decisión de los lineamientos tecnológicos. En algunos casos, el vínculo laboral con los agentes podría durar cuatro años o aún menos, por ser tentados al cambio en un mercado externo tecnológico muy competitivo.

El gobierno de TI establece inversiones a mediano y largo plazo, afectadas por el reemplazo de los responsables en llevarlas a cabo.

El Estado, posee un alto nivel de formalización, pero al no ser total, los responsables jerárquicos definen estrategias tecnológicas, a veces sin ser documentadas, que ante el reemplazo del agente quedan truncas y las inversiones no son llevadas a término o sólo se hacen parcialmente. Esto se traduce, como mínimo, en una gestión de recursos públicos poco eficiente.

La dimensión del Gobierno de la Ciudad Autónoma de Buenos Aires no es comparable con una empresa privada, por su dimensión y diversidad de servicios. El GCABA debe gestionar los recursos públicos de forma eficiente, no prioriza el retorno en la inversión y crea valor con el objetivo de maximizar la inclusión y el desarrollo social, minimizar los riesgos y optimizar los recursos para suministrar servicios a través de tecnologías innovadoras. El nivel de formalización exigido a los proveedores del GCABA es mayor al solicitado en empresas privadas. La provisión de servicios de TI de ASInf es gratuita, y en algunos casos como el servicio de internet en lugares públicos, compite con empresas privadas. El nivel de seguridad, calidad, continuidad y disponibilidad de los servicios es alto, sobre todo para servicios urgentes. La demanda de aplicaciones por parte de los ciudadanos es significativa. El número, diversidad y evolución tecnológica de los servicios ofrecidos exige una eficiente gestión y comunicación de los conocimientos. Por último, la disparidad de peticiones de desarrollos, accesos, cambios y soluciones a eventos y problemas requiere de una administración eficiente. Los antecedentes del marco también requieren exponer los conocimientos, investigaciones y experiencias obtenidas hasta la actualidad para poder establecer y priorizar la dirección y los lineamientos tecnológicos logrados a nivel mundial. En el año 2008 la Legislatura de la Ciudad Autónoma de Buenos Aires sancionaba la creación de la Agencia de Sistemas de Información. Para lograr una mirada general, se analiza el contexto internacional desde la creación de ASInf a la actualidad.

En el año 2010, se realizó una investigación para evaluar la madurez en el uso de TI en el sector público en Tanzania. Este documento está basado en los 15 (quince) procesos más importantes del marco COBIT en cinco sectores públicos con un formato comparable de un estudio similar hecho en Australia. El resultado indica que algunos procesos de TI han obtenido un nivel de madurez bajo, pero muy importante para el proceso de toma de decisiones y monitoreo de TI en el ambiente estudiado. Además,

indica que la madurez es relativamente menor en las organizaciones con mecanismos de gobierno de TI menos establecidos. En comparación con las organizaciones del sector público de Australia, como país desarrollado, el patrón de madurez de la gobernanza de TI resultó ser relativamente más bajo en todos los procesos de TI estudiados. Los resultados también manifestaron que no hay una comunicación formal de procedimientos y existe un alto grado de confianza en el conocimiento de las personas, por lo tanto, es probable que los errores ocurran. Estos hallazgos, cuando se interpolan con un estudio reciente sobre el estado de gobernanza de TI en este entorno, indican que tener más mecanismos de gobierno de TI probablemente conducirá a un mayor nivel de madurez. En algunos casos, incluso una madurez relativamente baja en los procesos, resultaron ser muy importantes para la toma de decisiones de TI. Los procesos en Australia están relativamente bien definidos con procedimientos estandarizados y documentados en contraste con el caso de un país en desarrollo como Tanzania.[14]

En el año 2011 se presentó una investigación que tuvo como objetivo explorar los motivos, obstáculos, desafíos y resultados en la implementación de ISO 27001 en organizaciones en Arabia Saudita. Los resultados definieron al proceso de identificación de los activos de una organización como el principal obstáculo. Cuando se preguntó si la falta de experiencia del equipo de implementación fue un obstáculo, el 50% de los participantes contestó que era un obstáculo secundario, mientras que el 37,5% afirmó que fue el principal obstáculo. Ante la consulta sobre la resistencia al cambio de los empleados, el 37,5% indicó que era un obstáculo significativo, otro 37,5% que era un obstáculo secundario y el 25% especificó que no era aplicable. En el caso de la participación de la alta dirección en el proyecto, el 50% reveló que la falta de participación de la dirección fue un obstáculo secundario, mientras que el 37,5% indicó que no fue relevante. El 62,5%, dijo que la razón principal para adoptar la norma ISO 27001 fue la seguridad y ningún entrevistado indicó que el objetivo era la certificación solicitada por el cliente o un socio.[15]

[14] IT Governance Maturity in the Public Sector Organizations in a Developing Country. Obtenido en Septiembre de 2010 en la Word Wide Web: https://n9.cl/uxxq [Accedido el 12/8/20]

[15] Australian Information Security Management Conference. Obtenido el 1 de Enero de 2011 en la Word Wide Web: https://n9.cl/trovx [Accedido el 14/8/20]

En el sector bancario de India, el cual debe cumplir las Normas de Basilea III, que impone al banco la adopción del marco para gestionar los riesgos, se implementó COBIT 5 como marco de gobernanza. Las conclusiones del estudio destacan algunos conceptos como la gran dependencia actual de la tecnología de la información y la necesaria separación del gobierno de TI respecto del gobierno de la empresa. La gestión de la innovación mediante tecnologías y nuevos productos en el dominio de TI es fundamental para lograr los objetivos corporativos del banco. También lo es la coherencia en los servicios de TI, la transparencia con las partes interesadas y la minimización de los costos en infraestructura al utilizar computación en la nube. También destaca la cobertura que brinda COBIT 5 al sector bancario en gobernanza forense evitando la ocurrencia de fraudes cibernéticos.[16]

La Universidad de Queensland, Australia, publicó una investigación realizada a ciento diez encuestados sobre el uso de ITIL, nivel de progreso en la implementación, tipo, tamaño de la organización y su personal de TI. La conclusión fue que las grandes organizaciones están liderando la implementación. Las empresas del sector privado están más avanzadas en la implementación de ITIL que las organizaciones del sector público. Menos de un tercio de los encuestados también están implementando COBIT, y para estas organizaciones, el progreso de ITIL está más avanzado que la implementación de COBIT. Los factores más críticos para la implementación exitosa de ITIL fueron el compromiso de la alta dirección. Los problemas relacionados con los clientes, consultores externos y la tecnología no se consideraron importantes. Se destacaron los problemas del personal de TI, su capacidad para adaptarse a los cambios, su calidad y capacitación. Contrariamente a la opinión defendida por consultores y revistas para profesionales, COBIT no se está adoptando ampliamente junto con ITIL, y cuando se implementa COBIT, generalmente está precedido por ITIL.[17]

En Colombia, durante el año 2015, se realizó una investigación sobre el contexto de la evolución de las organizaciones en la implementación de prácticas de Gobierno de

[16] Mapping of BASEL III and COBIT 5 framework in Banking Sector of India. Obtenido en Junio de 2013 en la Word Wide Web: https://n9.cl/qjpw [Accedido el 12/8/20]

[17] University of Southern Queensland. Implementation of IT Infrastructure Library (ITIL) in Australia. Obtenido el 2 de Julio de 2013 en la Word Wide Web: https://n9.cl/1qge [Accedido el 12/8/20]

TI[18]. El objetivo era determinar el grado de reconocimiento del concepto de Gobierno de TI dentro de las organizaciones, el alcance y desarrollo de las TI como parte estratégica del negocio. Los resultados expusieron que el 75,3% de los encuestados manifestó estar aplicando prácticas formales de Gobierno de TI; y de éstos, el 24,2% indicó que la implementación se encuentra en proceso. Del 24,7% que manifestó no tener implementadas prácticas de Gobierno de TI, el 58,6%, señaló como causa el desconocimiento del concepto. También fueron señalados la falta de recursos y el no reconocimiento de la contribución de TI a la organización. En el mismo año, en una entrevista, Javier Peris, experto en Gobierno de TI, decía "Entendiendo al negocio como un paciente, Gestionar las tecnologías es recetar lo que pide el paciente, mientras que Gobernar las tecnologías es recetar lo que necesita el paciente".[19]

En tres organizaciones bancarias del sector público brasileño se evaluaron las capacidades de los procesos del dominio de gobernanza de COBIT 5, basada en el enfoque ISO/IEC 15504[20]. El principal beneficio percibido fue el análisis detallado de la ejecución del proceso analizado, dando resultados sobre el logro o no de sus metas y la producción de los resultados requeridos. COBIT 5 ha sido implementado en diversas industrias, estatales o privadas, algunas como la Armada de Indonesia para respaldar su sistema de defensa marina[21]. El gobierno de la ciudad de Bandung, Indonesia, como agencia gubernamental, aplicó ITIL v3 a la transición, operación y la capacidad del servicio de TI. Los resultados permitieron evaluar y medir la situación actual, logrando ubicarse en el nivel 1.[22] También en Bandung, se realizó la evaluación del sistema de información en el Servicio de Salud Pública usando el marco de COBIT 5. Las conclusiones definieron que la gestión de TI es un proceso que cumple su propósito. La

[18] Asociación Colombiana de Ingenieros de Sistemas. Obtenido el 14 de Septiembre de 2015 en la Word Wide Web: https://n9.cl/izjrb [Accedido el 2/9/20]

[19] ¿ITIL o COBIT? Javier Peris. Obtenido el 22 de Septiembre de 2015 en la Word Wide Web: https://n9.cl/171y [Accedido el 12/8/20]

[20] Benchmarking of COBIT 5 PAM Assessments Performed in Brazilian Public Sector Banking Organizations. Obtenido el 24 de Agosto de 2015 en World Wide Web en https://n9.cl/c3ts7 [Accedido el 13/8/20]

[21] International Journal of Applied Engineering. Obtenido el año 2017 en World Wide Web en https://n9.cl/ungbv [Accedido el 13/8/20]

[22] Journal of Information Systems Engineering and Business Intelligence. Obtenido en Octubre de 2016 en la Word Wide Web: https://n9.cl/du8t [Accedido el 13/8/20]

administración de presupuestos y costos se ubica en el nivel 3, siendo un proceso gestionado y la gestión de solicitudes e incidentes en nivel 2, implementado.[23]

En una investigación realizada en la ciudad de Johannesburgo se propuso identificar los marcos, la integración de TI y las metodologías que se adoptan al implementar la gobernanza de TI en las entidades públicas en Sudáfrica. También los desafíos de implementación de la gobernanza de TI y los factores de falla que contribuyen a la experiencia de las entidades públicas en Sudáfrica. Asimismo, reconocer los éxitos de la gobernanza de TI y los factores que contribuyen al éxito dentro de la ciudad de Johannesburgo. Los resultados establecieron que el principal éxito de la implementación de la gobernanza de TI dentro de la ciudad de Johannesburgo fue que ha contribuido al cumplimiento de los requisitos legales y reglamentarios al aumentar la utilización de TI para mejorar los procesos comerciales. Más de la mitad de los encuestados indicaron que la implementación del gobierno de TI tuvo un impacto significativo. El éxito se atribuyó a factores organizacionales, liderazgo, entorno de TI, asignación adecuada de recursos, gestión correcta del proyecto y una conveniente comunicación. Sin embargo, en menor grado, hubo sentimientos de que la implementación de la gobernanza de TI tuvo un bajo impacto, atribuidos a desafíos institucionales, de liderazgo, fallas en la gestión de proyectos, desafíos de recursos humanos, financieros y desafíos externos.[24] En la actualidad, universidades internacionales como GTI4U[25] desarrollan investigaciones en el gobierno de TI, fomentando el desarrollo desde el ámbito académico para ser aplicado en el ambiente laboral. Promueven líneas de investigación tales como el análisis y planificación estratégica de las TI, madurez y buenas prácticas del gobierno tecnológico o el modelo de transformación digital.

La elección de las investigaciones para definir los antecedentes del marco fue direccionada intencionalmente hacia países que no cuenten con experiencia y trayectoria

[23] Evaluation of Patient Information System in Public Health Service Using the COBIT 5 Framework. Trianto. Obtenido el año 2018 en World Wide Web en https://n9.cl/cgmax [Accedido el 13/8/20]

[24] Information Technology Governance challenges facing the public sector in South Africa. Wits Business School. Obtenido el año 2017 en la Word Wide Web: https://n9.cl/vw1b [Accedido el 14/8/20]

[25] GTI4U. Obtenido el año 2019 en la Word Wide Web: http://www.gti4u.es/ [Accedido el 13/8/20]

en desarrollos de marcos tecnológicos con el objetivo de sentar una mínima base similar para el análisis y la proyección de la implementación de TI en el GCABA.

Interpretando las anteriores investigaciones, se puede establecer una base para el razonamiento y definir una dirección de desarrollo para la tesis. Los anteriores reportes, en la mayoría de los casos muestran que la implementación de un marco de trabajo ofrece mayor seguridad, calidad, gestión y cumplimiento de los requisitos legales. También incrementa la transparencia con las partes interesadas, favorece la toma de decisiones y el monitoreo de TI, facilita el cumplimiento de logros y metas y promueve la necesidad de separar el gobierno de TI del gobierno de la empresa. Se destaca la implementación de un sólo marco internacional de TI, no se verifica la instalación de un estándar que defina la gobernanza y otro marco que establezca la gestión de TI. Más aún, hay casos de implementación de estándares como ITIL para gestionar las TI con proyecciones de establecer la gobernanza mediante COBIT en el futuro.

No se distingue la capacitación para usuarios y equipos a cargo de la implementación de los marcos de trabajo como un componente importante que garantice el funcionamiento del estándar. Tampoco la documentación de los procesos, manuales de desarrollo, instalación y usuario. El desarrollo de tecnologías innovadoras no se proyecta a futuro, ni se menciona como un factor importante la comunicación formal de los procedimientos. Pero, en general, existe un incremento en el uso de TI a nivel mundial, al igual que en GCABA, con un alto porcentaje de uso en el sector público y la concientización de la necesidad de implementar TI para cumplir con la visión organizacional.

Por los motivos expresados, propongo elaborar un Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires aplicando el estándar internacional COBIT 5 para definir los lineamientos del gobierno de TI y complementar su desarrollo con ITIL v3 para la gestión de la tecnología. A través de ambas implementaciones se cubrirían todos los requerimientos de TI y vacíos recién mencionados. El marco tendría limitaciones temporales por la evolución tecnológica, el incremento y la diversidad de los servicios de TI que no asegurarían su vigencia con el paso del tiempo. Se examina la Agencia de Sistemas de Información desde la macro, se exploran los servicios brindados, su estructura organizacional y las políticas que componen el Marco Normativo de Tecnología de la Información definido.

Marco tecnológico de la Agencia de Sistemas de Información

La información obtenida para comenzar el análisis del actual marco tecnológico de ASInf proviene de fuentes primarias y secundarias, éstas últimas obtenidas de artículos, libros y publicaciones en internet. Las fuentes primarias provienen de ASInf, mediante el análisis de documentos, entrevistas con el personal, estudios de campo con visitas a las instalaciones de la agencia y por medio de correspondencia electrónica con los ejecutivos de la organización. Estos últimos, obtenidos en tareas que he desarrollado a través de la Auditoría General de la Ciudad de Buenos Aires. Las tareas realizadas y sus papeles de trabajo constan en los informes.[26]

Misiones y funciones de ASInf

Por medio de la ley 2689[1] se crea la Agencia de Sistemas de Información. Es constituida como una entidad autárquica para su administración funcional, financiera y administrativa, en el ámbito de la Jefatura de Gabinete de Ministros de la Ciudad Autónoma de Buenos Aires. En su normativa se describen sus misiones, en el año 2010, se modificaron las misiones y funciones de la Dirección General de Desarrollo de Sistemas mediante la Resolución N° 97/ASINF/10.[27]

Organigrama de la Agencia de Sistemas de Información

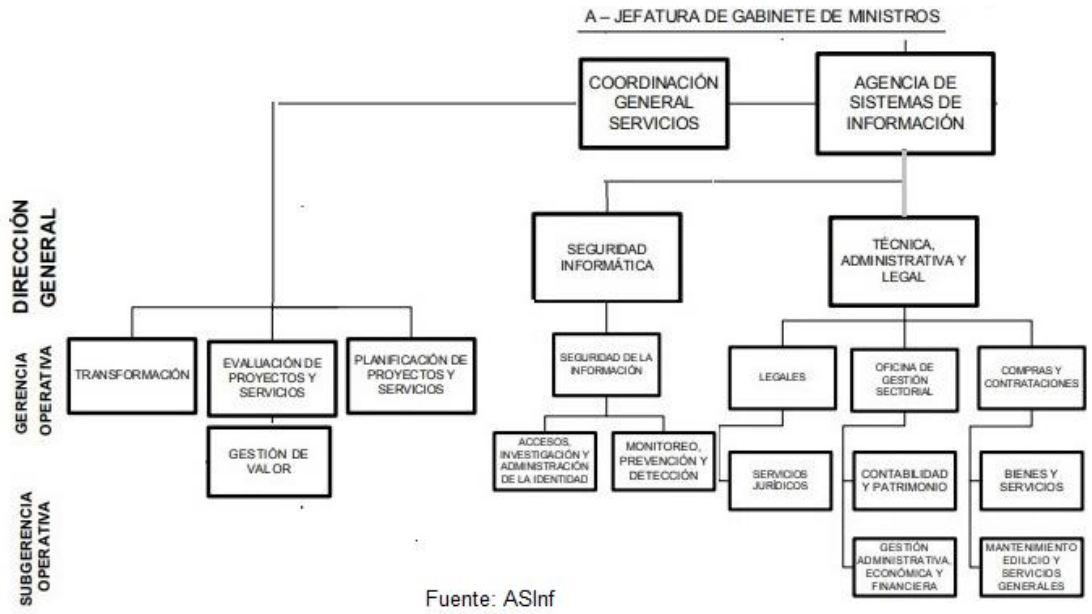
ASInf desarrolla sus tareas basadas en estándares y procesos implementados por la Agencia de Sistemas de Información.[28] La Agencia tiene como objetivo organizar y coordinar con todas las dependencias del Poder Ejecutivo la infraestructura informática de telecomunicaciones y de sistemas de información, dotando a la Ciudad de un plan autosuficiente de gobierno electrónico que permita el acceso del ciudadano por medios electrónicos y telefónicos a los servicios de información. La ley 2689[1] facultó a ASInf como órgano rector en tecnologías, por lo tanto define y establece las políticas gubernamentales en materia de sistemas de información. Las dos imágenes siguientes

[26] AGCBA. Obtenido el año 2019 en la Word Wide Web: http://www.agcba.gov.ar/web/ [Accedido el 15/5/19]

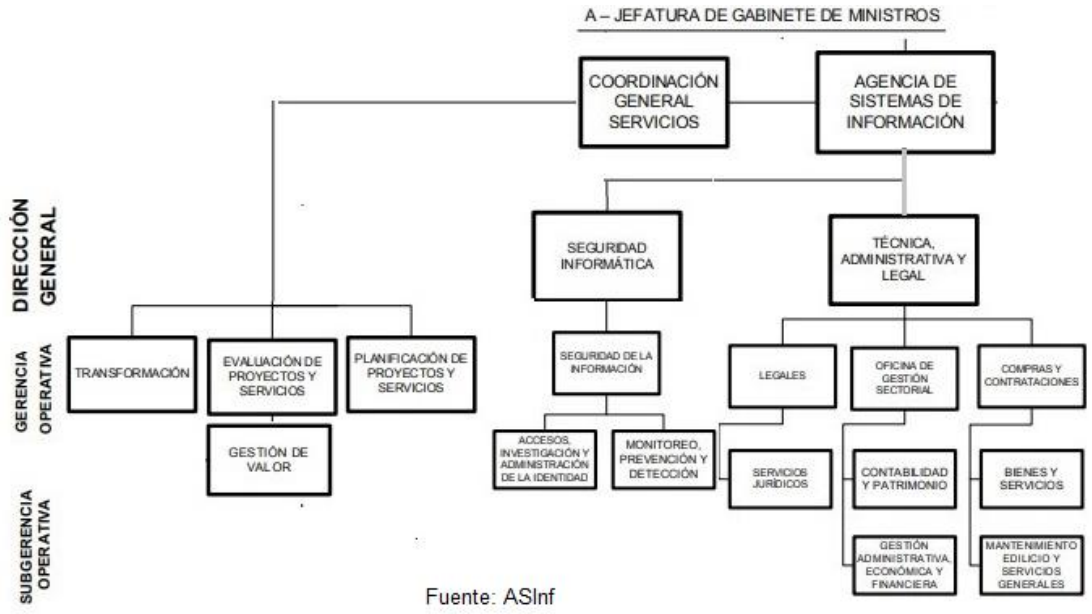
[27] Resolución N° 97/ASINF/10. Obtenido el 4 de junio de 2010 en la Word Wide Web: https://n9.cl/bhnax [Accedido el 15/5/19]

[28] Estándares ASI. Obtenido el Obtenido el 30 de Diciembre de 2014 en la Word Wide Web: https://n9.cl/crgm [Accedido el 15/5/19]

conforman la *figura 1, Organigrama de ASInf* según la Resolución Nº 224/ASINF/2018[29]



Fuente: ASInf



Fuente: ASInf

Descripción de los sistemas

Las acciones del Gobierno de la Ciudad Autónoma de Buenos Aires pretenden colaborar en la gestión y transparencia con el ciudadano. ASInf diseña, desarrolla y administra sistemas propios y de terceros. No todos los sistemas del GCABA son

[29] Anexo de la Resolución Nº 224/ASINF/2018.Obtenido el 18 de Diciembre de 2018 en la Word Wide Web: https://n9.cl/760m [Accedido el 16/5/19]

procesados ni almacenados en la infraestructura de ASInf. La Gerencia Operativa de Operaciones gestiona sistemas operativos, bases de datos, servidores, almacenamiento y copias de respaldo. El procesamiento más utilizado es mediante equipos provistos por la agencia, aunque también existe el procesamiento mediante equipos en otras reparticiones. En ASInf se administran aquellos sistemas considerados críticos, los cuales deben adecuarse a los objetivos estratégicos planteados por el GCABA.

Los sistemas son: **USIG** (Sistema de Ubicación Geográfica), **SIGEHOS** (Sistema de Gestión Hospitalaria), **SIAL** (Sistema de liquidación de haberes de empleados GCABA), **SAP** (Seguimiento y Gestión de Reclamos Ingresados por SUACI), **SADE** (Sistema de Administración de Documentos Electrónicos), **Boletín Oficial** (medio de publicidad de los actos de Gobierno), **Páginas Web** (Sitio Web del GCABA), **PIG-BA** (Plataforma Integral de Gestión de la Ciudad), **MiBA** (Plataforma interactiva de trámites con el ciudadano) y **SUACI** (Sistema Único de Atención Ciudadana). Algunos sistemas no sólo poseen criticidad por sí mismos sino por la interacción parcial o total con otros sistemas. Además, existen otros centros de procesamiento y almacenamiento dependientes del Poder Ejecutivo, ubicados fuera de la órbita de ASInf. Los más importantes son: **Ministerio de Desarrollo Urbano y Transporte, Ministerio de Seguridad, AGC** (Agencia Gubernamental de Control), **AGIP** (Agencia Gubernamental de Ingresos Públicos) y **UAIF** (Unidad de Administración Información Financiera).

La Agencia de Sistemas de Información diseña, desarrolla y administra sistemas propios y de terceros. Desde diversas áreas intentan agilizar las necesidades de información y trámites, ofreciendo servicios mediante los sistemas:

- **SIGAF** (Sistema de Gestión y Administración Financiera)
- **GEDO** (Generador de Documentos Oficiales)
- **RER** (Sistema de conexión de red de trenes)
- **SIR** (Sistema Integral de Recaudación)
- **SGE** (Sistema de Gestión Escolar)
- **BAstrap** (Restablecer los sitios y páginas web del GCABA)
- **GIT** (Gestión Integral Tributaria)
- **BAC** (Buenos Aires Compra)
- **Garantía BA** (Sistemas de Garantías de Alquiler para viviendas)

- **Consorcio Participativo** (Sistema de gestión para consorcios)
- **SIDIAU** (Sistema Informático de Infraestructura y Arquitectura)
- **TAD** (Sistema de Trámites a Distancia)
- **INFOAGIP** (Sistema de consultas de estados y vencimientos)
- **BA-Csirt** (Sistema de prevención de riesgos en redes sociales)
- **Sistema Público APRA** (Certificados de Aptitud Ambiental)
- **Ascensores Registrados** (Registro de elevadores)
- **Sistema de Gestión de Calidad** (Sistema público de salud)
- **Trabajo BA** (Sistema público de ofrecimiento y búsqueda laboral)
- **RAT** (Registro de Artefactos Térmicos)
- **Sistema de Relevamiento de Actividades Comerciales**
- **Sistema de eventos de Alerta Meteorológica**
- **Sistema de Administración de Información Ambiental**
- **Sistema de Seguimiento vehicular** (Monitoreo de unidades)
- **Tablero de Comando de comunicaciones** (Emergencias para SAME)
- **Sistema de consulta de Planos Históricos digitalizados**
- **Mapas embebidos Temáticos** (discapacidad, ciclovías, etc.)
- **Sistema de Guardia de Auxilio** (Gestión de emergencia)
- **Cargador de Ovitrampas** (Control y organismos intervinientes)
- **Sistema de Espacios Verdes** (Gestión de espacios verdes)
- **Sistema de Fotos de Fachada** (Gestión fotográfica de fachadas)
- **Recorridos de transporte público** (transporte público)
- **Sistema de Liquidación de Sueldos** (liquidación de sueldos)
- **SIGA** (Sistema de Seguimiento de Actuaciones)
- **CCOO** (Sistema de Comunicaciones Oficiales)

Aplicaciones Móviles

Las aplicaciones móviles soportadas por ASInf y su detalle son:

- **BA Taxi–Pasajeros** (Permite a pasajeros solicitar un taxi)
- **BA Subte** (Permite ver el estado del subte en tiempo real)
- **BA Cómo Llego** (Medios de transporte en la Caba)
- **BA EcoBici** (Información de ciclovías y estaciones de bicicleta)

- **BA Wifi** (Puntos de conectividad a la red de Wifi de la Ciudad)
- **BA 147** (Realizar solicitudes al GCABA)
- **BA Medios** (Escuchar Radio Ciudad AM 1110, FM 92.7 y La 2x4)
- **BA Denuncia Vial** (Denunciar vehículos mal estacionados)
- **BA Ferias** (Ver productos en ferias y mercados de la Caba)
- **BA Móvil** (Conocer el estado del tránsito en tiempo real)
- **BA Turismo** (Actividades Culturales)
- **BA Taxi - Conductor (Seguridad y servicio para taxistas)**
- **BA Cultural** (Actividades Culturales en Caba)
- **BAFICI** (Información del Festival Internacional de Cine)
- **BA Mascotas** (Información asociada a mascotas)

Software o Servicio utilizado por ASInf

A continuación se describe cada software o servicio utilizado actualmente por ASInf para brindar servicios a los ciudadanos. La datos de la próxima *tabla 1*, *Software o Servicio utilizado por ASInf*, fueron obtenidos del Informe AGCBA 10.18.03.[31]

Software o Servicio	Descripción
Vmware vSphere esxi Hypervisor	Es una plataforma de virtualización a nivel de centro de datos compuesta por un sistema operativo autónomo.
Vmware vCenter Management	Es un software de administración de servidores que suministra una plataforma centralizada para administrar los entornos.
VMware Site Recovery Manager Orchestration	Es software de automatización integrado para proporcionar administración basada en políticas de planes de recuperación.
VMware vSphere Replication	Es una extensión de VMware vCenter Server, permite la elección de las máquinas virtuales y crea una copia.
VMware vRealize Operation Management	Es un sistema que ofrece optimización continua de los recursos de TI y gestiona el rendimiento.
Turbonomic Management	Es un software que garantiza automáticamente el rendimiento de las aplicaciones para que funcionen de forma ininterrumpida.
Redhat Linux OS	Sistema operativo que sirve de base a las aplicaciones actuales, se puede implementar en equipos sin sistemas operativos.
Oracle Enterprise Database	Es un sistema de gestión de base de datos que permite ser usado en cualquier plataforma, almacena y recupera en forma rápida.
Mysql Database	Es un sistema de gestión de bases de datos relacionales de código abierto y de libre acceso.
Mariadb Database	MariaDB es un derivado del sistema de gestión de bases de datos relacionales MySQL, compatible con gran cantidad de lenguajes.
Windows Server OS	Permite a un equipo manejar funciones de red, servidor de impresión, controlador de dominio, servidor web y de archivos.

Software o Servicio	Descripción
Openshift Platform Private Container Cloud Platform	Es una plataforma empresarial de aplicaciones con operaciones automatizadas integrales, de código abierto y multifacética.
Cloudform Cloud Orchestration	Permite crear, actualizar y administrar los recursos de la nube y sus componentes de software como una sola unidad.
Ansible Orchestration	Plataforma de software libre para configurar y administrar computadoras de manera automatizada evitando tareas repetitivas.
Oracle Enterprise Manager Management	Es un conjunto de herramientas basadas en la web para administrar software y hardware.
ELK ElasticSearch Kibana	Es un conjunto de herramientas de código abierto para recolectar, cargar, buscar y visualizar información en tiempo real.
Veeam Availability Suite Backup	Gestiona de forma intuitiva el almacenamiento físico, en la nube y brinda disponibilidad y recuperación de los servicios de TI.
Veeam One Management	Es un software para visibilizar y administrar el entorno de TI. Monitorea la infraestructura y resuelve de forma automatizada.
IBM Spectrum Management	Es un producto de respaldo y recuperación que se puede utilizar con almacenamiento físico o virtual.
HDS Device Manage Management	Software utilizado para unificar, simplificar y monitorear los subsistemas de almacenamiento conectados a los servidores.
HDS Storage Navigator Management	Es un software que permite gestionar, habilitar y optimizar los sistemas de almacenamiento individuales.
HDS Storage Advisor Management	Es una solución de administración de infraestructura que unifica las soluciones de almacenamiento y la protección de datos.
MongoDB Database	Es un sistema de gestión de bases de datos de código abierto que utiliza un modelo que admite datos en distintos formatos.
SQL Server Database	Es un sistema de gestión de bases de datos relacionales que permite programar en entornos híbridos ya sea de forma local o en la nube.
Apache Tomcat Java Platform	Es un servidor web para aplicaciones, desarrollado por Java, con código abierto que funciona en cualquier sistema operativo.
Apache WebServer	Es un servidor web multiplataforma de código abierto que almacena, procesa y entrega las páginas web a los usuarios.
F5 LTM Load Balancer	Es un módulo que permite aumentar las conexiones del lado del servidor y del cliente.
Schneider DCIM Datacenter	Es un software que brinda a los operadores de centros de datos, la capacidad de ejecutar operaciones eficientes en la infraestructura.
Pentaho Ops BI	Es un software de inteligencia empresarial que proporciona integración de los datos, provee información y extracción de datos.
Grafana Monitoring	Es un software de código abierto que permite la visualización, monitoreo y análisis de datos.
Prometheus Monitoring	Es una aplicación de software utilizada para la supervisión y los alertas de eventos en los servicios.

Fuente: AGCBA

Servicios internos y externos provistos por ASInf

Los servicios que brinda ASInf actualmente son los siguientes:

- Desarrollo, mantenimiento y actualización de sistemas y aplicaciones.
- Desarrollo, gestión, mantenimiento y actualización de bases de datos.
- Provisión, mantenimiento y actualización de internet.
- Actualización y mantenimiento del correo de los entes del GCABA.
- Generación de copia de respaldo de las bases de datos.
- Instalación y actualización de herramientas informáticas del GCABA.
- Instalación y actualización de hardware y software del GCABA.
- Instalación y actualización de videoconferencia para el GCABA.
- Instalación y actualización de antivirus en equipamiento del GCABA.
- Gestión presencial y remota de hardware, software, internet e impresión.
- Creación de puntos de red para el GCABA.
- Gestión, almacenamiento, custodia, traslado y recuperación de información del GCABA.
- Gestión de hardware y software en los centros de cómputos propios o de terceros proveedores del GCABA.
- Contingencia por cortes de suministro de energía o catástrofe.
- Suministro y prevención de la red inalámbrica, fibra óptica, telefonía y comunicaciones del GCABA.
- Gestión y mantenimiento de Wifi público y privado del GCABA.
- Conexión de proveedores a redes, enlaces del GCABA.
- Provisión de puntos de presencia de Wifi en eventos GCABA.
- Gestión de infraestructura para la implementación de firma digital.
- Administración de los servidores.
- Gestión del almacenamiento de datos centralizados del GCABA.
- Gestión y mantenimiento de la red LAN y MAN del GCABA.
- Registración de incidentes de los servicios del GCABA.
- Provisión de soporte a incidentes de los servicios del GCABA.

Procesos desarrollados en ASInf

Los procesos desarrollados por las Direcciones Generales, Gerencias Operativas y Subgerencias Operativas de ASInf fueron relevados por la Dirección General de Sistemas de Información de la Auditoría General de la Ciudad de Buenos Aires

(AGCBA). La tarea fue desarrollada mediante una Auditoría de Relevamiento, con número de proyecto 10.10.01[30], realizada en el mes de mayo del año 2011 y reflejada en los papeles de trabajo. Luego, mediante la ya mencionada Resolución Nº 224/ASInf/2018[29], se implementaron cambios en la estructura organizacional de ASInf. Durante los años 2018 y 2019, la Dirección General de Sistemas de Información de la AGCBA, mediante una Auditoría de Relevamiento, proyecto 10.18.03, se relevaron algunos procesos de la estructura de ASInf.[31]

Marco normativo vigente en la Agencia de Sistemas de Información

Con el objetivo de promover la estandarización de los bienes informáticos, equipos, recursos, sistemas y programas a ser utilizados por el Poder Ejecutivo, en el año 2013, ASInf confeccionó un Marco Normativo de Tecnología de Información, publicado en la Resolución N° 177.[5] En dicha resolución se catalogan los documentos que conforman el marco y se enumeran cada uno de ellos, siendo la base para la gestión segura de las actividades relacionadas con la tecnología de información. Se deja constancia que las políticas deben ser interpretadas en el marco de lo dispuesto por la ley 104/98[32] de Acceso a la Información y la ley 1845/05 de Protección de Datos Personales[33] y sus modificatorias. El Marco Normativo de Tecnología de Información fue desarrollado partiendo de la base de 2 (dos) normas internacionales complementarias.

A dicha conclusión se arriba por la documentación analizada, en la cual se implementa un Sistema de Gestión de la Seguridad de la Información enfocado a procesos. A lo largo del Ciclo de Vida Continuo se Planifica, Hace, Verifica y Actúa. Una de las normas recién mencionadas es ISO/IEC 27001, la cual permite el

[30] AGCBA. Proyecto 10.10.01. Obtenido en Mayo de 2011 en la Word Wide Web: https://n9.cl/akxb [Accedido el 20/5/19]

[31] AGCBA. Proyecto 10.18.03. Obtenido el 3 de Agosto de 2017 en la Word Wide Web: https://n9.cl/akxb [Accedido el 20/5/19]

[32] Ley 104/98. Obtenido el 19 de Noviembre de 1998 en la Word Wide Web https://n9.cl/mz7yd [Accedido el 25/5/19]

[33] Ley 1845/05 y modificatorias. Obtenido el 17 de Agosto de 2007 en la Word Wide Web: https://n9.cl/hs9r [Accedido el 25/5/19]

aseguramiento de la confidencialidad, integridad de los datos, privacidad de la información y la de los sistemas que la procesan.[34]

La otra norma utilizada es ISO 17799, la cual ofrece una estructura para identificar e implementar soluciones a los riesgos asociados a la gestión de la seguridad de la información en una organización.[35] El Marco Normativo de Tecnología de ASInf [5] comparte desde su página 3 hasta la 7, los dominios con la norma ISO 17799 desde los cuales se implementan las políticas. Los dominios son los siguientes: Política de seguridad de la información, Gestión de activos, Seguridad de los recursos humanos, Seguridad física y ambiental, Gestión de las comunicaciones y operaciones, Control de acceso, Adquisición, desarrollo y mantenimiento de sistemas de información, Gestión, de incidentes de seguridad de la información, Gestión de la continuidad del negocio y el Cumplimiento.

La diferencia entre el Marco Normativo de Tecnología de ASInf y la norma ISO 17799 v2005, es que el primero además agrega una política de Evaluación y Tratamiento de Riesgos. En las versiones posteriores al año 2005 fue incluida. Si se analiza la complementariedad de las 2 (dos) normas, se puede sintetizar que "ISO 17799 e ISO 27001, juntas proporcionan un conjunto de mejores prácticas y un estándar de certificación para la seguridad de la información. La norma ISO 17799 proporciona recomendaciones de mejores prácticas para iniciar, implementar o mantener sistemas de gestión de seguridad de la información. La segunda norma, ISO 27001, especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que sea compatible con las mejores prácticas descritas en la norma ISO 17799.[36] ISO 27001 contiene requisitos para establecer un Sistema de Gestión de Seguridad de la información, es un estándar certificable. Si una organización va a obtener la certificación, los mencionados requisitos "deben" ser cumplidos obligatoriamente. La norma ISO 17799 proporciona recomendaciones de mejores prácticas que para ser implementadas adecuadamente, se aconseja que "deberían" ser cumplidas. Por ello ambas palabras, "deben" y "deberían" denotan distintos niveles de

[34] ISO 27001. Obtenido el año 2013 en la Word Wide Web: https://n9.cl/tetg [Accedido el 26/6/19]

[35] ISO 17799. Obtenido el año 2005 en la Word Wide Web: https://n9.cl/4gyw [Accedido el 26/6/19]

[36] ISO 17799. Obtenido el 2 de Octubre de 2006 en la Word Wide Web: https://n9.cl/ej00v [Accedido el 22/5/20]

obligación de cumplimiento. El Marco Normativo de Tecnología de Información diseñado por ASInf parte de la base de la implementación de un sistema de seguridad de la información que preserva la confidencialidad, integridad, disponibilidad y privacidad, compartido por ambas normas.

Marco regulatorio vigente de tecnología para el GCABA

El marco regulatorio vigente de tecnología para el GCABA debe ser cumplido por los entes del GCABA y sus proveedores externos. Está compuesto por políticas[5] como el Estándar de Desarrollo (año 2014)[7] y el PC0901 (Proceso de control de cambios en software de aplicación)[8] y el Anexo Resolución Nº 239-ASInf/15.[9]

Impacto por la implementación de la tecnología

Con el objetivo de medir los esfuerzos según los recursos destinados y el impacto generado por el Plan de Modernización, se evalúan algunos casos testigos. Se pretende evaluar si la dirección proyectada está en línea con el plan de modernización. El primer caso elegido, de forma azarosa, es el Sistema de Inscripción en Línea del GCABA. Es un sistema web del Ministerio de Educación para la preinscripción de aspirantes a ingresar a las escuelas públicas de gestión estatal de la Ciudad, se accede ingresando en la web del GCABA o mediante un correo electrónico de cualquier proveedor. Durante fines del año 2013, el sistema estaba planteado como un desarrollo que debía superar varios desafíos. Los mayores eran facilitar su utilización para los habitantes de los barrios vulnerables, por falta de comprensión, acceso a internet o recursos informáticos, estarían limitados en su uso. Los informes realizados por la Defensoría del Pueblo[37] y por la Auditoría General de la Ciudad de Buenos Aires[38] expresan que el sistema en sus comienzos, año 2014, carecía de eficiencia y estaba afectado por errores de diseño.

En años subsiguientes, ambos órganos de control manifiestan algunas falencias, “subsisten en el área auditada imperfecciones organizativas, y un exceso en la concentración de funciones”, “el sistema mejoró parcialmente la eficiencia, y la

[37] Defensoría del Pueblo. Obtenido el mes de Abril de 2014 en la Word Wide Web: https://n9.cl/u4ia [Accedido el 26/6/19]

[38] Auditoría General de la Ciudad de Buenos Aires. Obtenido en Diciembre de 2018 en la Word Wide Web: https://n9.cl/959f [Accedido el 26/6/19]

transparencia ya que incorporó información y despersonalizó en gran medida el proceso. También mejoró parcialmente la auditabilidad y la trazabilidad de decisiones críticas como por ejemplo la asignación manual de las vacantes e incorporó información digitalizada antes no disponible como la demanda, ahora pasible de análisis con herramientas informáticas"

El segundo caso a evaluar es el informe realizado por la Auditoría General de la Ciudad de Buenos Aires del teléfono 0800 - Número Único de la Ciudad Autónoma de Buenos Aires.[39] El GCABA a través de la Dirección General de Atención Ciudadana dependiente de la Subsecretaría de Atención Ciudadana implementó el Call Center de la Ciudad de Buenos Aires para contar con un número breve de fácil memorización (147). Desarrolló el acceso vía web y vía correo (sistema SUACI) para facilitar el contacto con el ciudadano. Antes de la implementación, la gran mayoría de los servicios eran presenciales, incluso la solicitud de turnos. Durante el año 2008 se recibieron catorce tipos de llamadas, y en el año 2009 se incrementaron a veintidós. Cabe aclarar que los tipos de llamadas están asociados a los servicios brindados por el GCABA al ciudadano. Servicios como poda de árboles, residuos en vía pública, turnos, información de trámites y otros. En el año 2009 se atendieron un millón cuatrocientas veintiocho mil llamadas. En ambos casos mencionados, las acciones implementadas mediante el Plan de Modernización en capacitación de los recursos humanos y la actualización de la infraestructura tecnológica producen un impacto positivo al ciudadano.

Objetivos estratégicos

Los objetivos estratégicos de ASInf, anteriormente mencionados, fueron definidos en la ley 2689.[1]

Formulario único de requerimientos

Según la Resolución Nº 190/MMGC/12[4], 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, compras de

[39] 0800 Número Único. Obtenido en Mayo de 2012 en la Word Wide Web: https://n9.cl/odwjv [Accedido el 26/6/19]

equipos, metodologías de gestión de procesos y tecnologías sean tramitados según las Políticas y Programas del GCABA.

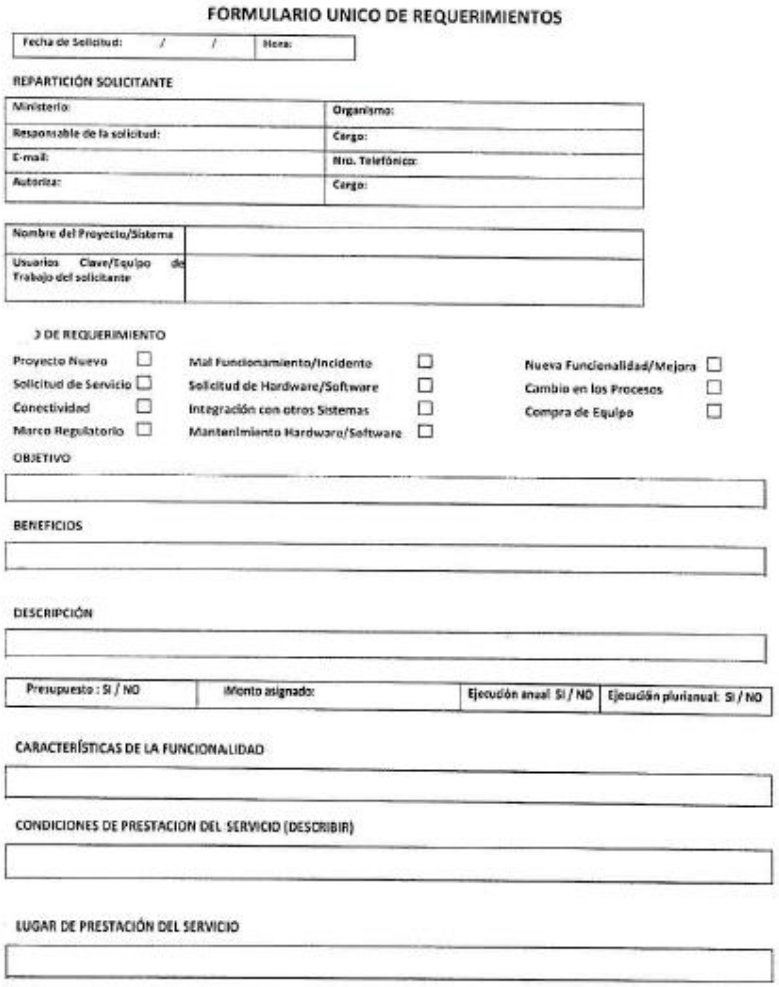
La resolución también expresa que el formulario está disponible para ser completado por el solicitante en intranet http://intranet.buenosaires.gob.ar/. Es necesario haber sido dado de alta en el sistema SADE (Sistema de Administración de Documentos Electrónicos)[40] para poder ingresar mediante usuario y clave. Caso contrario el formulario puede ser enviado por correo a requerimientos-ASI@buenosaires.gob.ar. También detalla que el requerimiento es analizado por ASInf y de ser necesario se gestionará una reunión para profundizar el requerimiento. La resolución es emitida por el Ministerio de Modernización del GCABA. El canal de comunicación, en principio unidireccional, podría recibir una mirada favorable si se establece como un primer contacto para el inicio de un servicio o proyecto, solicitado desde una repartición hacia ASInf.

Es importante destacar, que no siempre desde la repartición el agente encargado de realizar el pedido posee la capacitación para definir las especificaciones técnicas. El Formulario único de requerimientos no es sólo para agregar, solicitar o modificar un servicio existente, sino también para desarrollar un nuevo proyecto, según define la resolución. Dicha declaración invita a pensar si el proyecto solicitado ya fue desarrollado, si hay uno similar en funcionamiento en otra repartición, y lo más importante, si el proyecto o sistema a desarrollar está alineado estratégicamente con los objetivos de ASInf. También debe analizarse si aporta valor al organismo y si satisface a las partes interesadas.

En el año 2008 se crea ASInf y un año más tarde comienza la implementación de la Ley de Modernización de la Administración Pública. En el 2013 se define el Marco Normativo de Tecnología, el cual sigue vigente, pero con modificaciones en los años 2014, 2015, 2016 y 2019. Dichas modificaciones no fueron menores, ya que modificaron organigramas, funciones en ASInf y en el GCABA. Pero lo más destacado fueron los cambios en los objetivos estratégicos del GCABA, las necesidades de los ciudadanos, los servicios brindados, la tecnología usada y los estándares internacionales. Por estos motivos, creo conveniente redefinir un Nuevo Marco

[40] Decreto Nº 196/11. Expediente electrónico. SADE. Obtenido el 28 de Marzo de 2011 en la Word Wide Web: https://n9.cl/r51f [Accedido el 7/3/19]

Tecnológico que considere los recursos existentes. De igual modo, se evalúa la estructura, políticas vigentes y la reutilización de los recursos. La siguiente *figura 2* es el *Formulario único de requerimientos vigente.*



FORMULARIO UNICO DE REQUERIMIENTOS

Fecha de Solicitud: / /	Hora:

REPARTICIÓN SOLICITANTE

Ministerio:	Organismo:
Responsable de la solicitud:	Cargo:
E-mail:	Nro. Telefónico:
Autoriza:	Cargo:

Nombre del Proyecto/Sistema	
Usuarios Clave/Equipo de Trabajo del solicitante	

) DE REQUERIMIENTO

Proyecto Nuevo ☐	Mal Funcionamiento/Incidente ☐	Nueva Funcionalidad/Mejora ☐
Solicitud de Servicio ☐	Solicitud de Hardware/Software ☐	Cambio en los Procesos ☐
Conectividad ☐	Integración con otros Sistemas ☐	Compra de Equipo ☐
Marco Regulatorio ☐	Mantenimiento Hardware/Software ☐	

OBJETIVO

BENEFICIOS

DESCRIPCIÓN

Presupuesto : SI / NO	Monto asignado:	Ejecución anual SI / NO	Ejecución plurianual: SI / NO

CARACTERÍSTICAS DE LA FUNCIONALIDAD

CONDICIONES DE PRESTACION DEL SERVICIO (DESCRIBIR)

LUGAR DE PRESTACIÓN DEL SERVICIO

Fuente: ASInf

Capítulo 2 - Normas técnicas internacionales

En el segundo capítulo se evalúan los estándares internacionales, sus principios, estructuras, limitaciones, utilidad, ventajas y desventajas. Se analizan ISO/IEC 27001, ISO/IEC 17799, PMBOK v6 (Project Management Body of Knowledge),[41] ITIL v3 y COBIT 5.

Es importante conocer, destacar y comparar los principales marcos, normas y estándares internacionales, para poder concluir y elegir entre ellos el más adecuado según la necesidad a cubrir. Se describen y estudian las estructuras de algunos estándares internacionales, sus ventajas, desventajas y las comparaciones pertinentes. Cada marco fue diseñado para dar distinta cobertura y profundidad en diversos tipos y tamaños organizacionales. Luego de analizar cada marco, se define cual es el estándar internacional adecuado para cubrir los objetivos del Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires.

ISO/IEC 27001

Fue publicado por la ISO[42] y por la IEC en el año 2005. Es una norma mediante la cual se especifican los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en una organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en la norma son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.[43] Para preservar la seguridad de la información, es indispensable proteger su confidencialidad, que es la propiedad que posee la información mediante la cual se pretende garantizar el acceso sólo a las personas autorizadas. La integridad que es una de las dimensiones de la calidad de los datos respecto de la exactitud, completitud de la información y sus métodos de proceso, cuya pérdida impacta en la privacidad y la disponibilidad que es el

[41] PMBOK. Obtenido el 6 de Setiembre de 2017 en la Word Wide Web: www.pmi.org [Accedido el 27/7/19]

[42] International Organization for Standardization. Obtenido en el año 2005 en la Word Wide Web: https://n9.cl/ydcgc [Accedido el 27/7/19]

[43] ISO/IEC 27001. Obtenido el año 2005 en la Word Wide Web: https://n9.cl/tetg [Accedido el 27/7/19]

acceso y uso de la información y los sistemas asociados a las personas u organismos autorizados en el momento requerido.

Mediante la norma ISO/IEC 27001 versión 2013 es posible implementar un SGSI (Sistema de Gestión de la Seguridad de la Información), que mediante los elementos o fases definidas, es posible proteger la información. Para implementar un SGSI basado en el estándar internacional ISO/IEC 27001, se debe utilizar el Ciclo de Vida Continuo, PHVA (por sus siglas), que está conformado por cuatro fases: Planificar (definir el SGSI, los parámetros asociados a la organización, negocio, infraestructura tecnológica, ubicación geográfica y sus activos), Hacer (implementar el SGSI, definir e identificar las acciones a desarrollar, recursos, responsabilidades y las prioridades vigentes en el plan de gestión de riesgos en el SGSI), Verificar (revisar el SGSI, ejecutar procedimientos para monitorear y revisar errores en los resultados generados en el procesamiento de la información e incidentes de seguridad) y Actuar (mejorar el SGSI, accionar correctiva y preventivamente).

La documentación para implementar un SGSI con Enfoque a Procesos es:

- Política y objetivos de seguridad (compromiso documentado por la dirección de la organización respecto de la seguridad de la información)
- Alcance del SGSI (áreas de la organización incluidas en el SGSI)
- Procedimientos y mecanismos de control que soportan al SGSI (son los procedimientos mediante los cuales se regula el funcionamiento de la organización)
- Enfoque de evaluación de riesgos (criterios de aceptación de riesgos, evaluación de vulnerabilidades, amenazas e impactos en los activos de información)
- Informe resultante de la evaluación del riesgo (resultados obtenidos luego de aplicar la metodología)
- Plan de tratamiento de los riesgos (escrito mediante el cual se definen las acciones a implementar de acuerdo con los resultados de la evaluación del riesgo)
- Procedimientos documentados (acciones para implementar la planificación y el control de los procesos de seguridad de la información)

- Registros (evidencias documentadas con la conformidad por el funcionamiento eficaz del SGSI)

- Declaración de aplicabilidad de la Arquitectura Orientada a Servicios, SOA (documento con los controles de evaluación y gestión del riesgo del SGSI)

- Procedimiento de gestión de toda la documentación del SGSI (son los procesos aplicados al control, actualización, seguimiento y almacenamiento)

Las actividades más destacadas que se deben desarrollar para implementar un SGSI son: participación activa de la dirección, alcance del SGSI y la política de seguridad, inventario de todos los activos de información, metodología de evaluación del riesgo, identificación de amenazas, vulnerabilidades e impactos, análisis y evaluación de riesgos, selección de controles para el tratamiento de riesgos, aprobación por parte de la dirección del riesgo residual, declaración de aplicabilidad, plan de tratamiento de riesgos y la implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo. La implementación de ISO/IEC 27001 permite minimizar el riesgo de pérdidas de información, establece una metodología para gestionar la seguridad de la información, continúa las operaciones de las organizaciones, incrementa la motivación de sus agentes, reduce los costos, aumenta la eficiencia y garantiza el cumplimiento legal.

ISO/IEC 17799

En el año 1995, el Instituto de Estándares Británicos, publicó el primer estándar de seguridad, denominado BS 7799. La segunda versión con la implementación de mejoras fue presentada durante el año 1998, presentada como un estándar nacional certificable. IRAM, en el documento publicado el 28 de junio del año 2002, Norma IRAM, Código de práctica para la administración de la seguridad de la información, acepta y aclara: “Este código de práctica puede ser considerado como un punto de partida para el desarrollo de lineamientos específicos aplicables a cada organización. No todos los lineamientos y controles de este código de práctica resultarán aplicables. Más aún, es probable que deban agregarse controles que no están incluidos en este

documento. Ante esta situación puede resultar útil retener referencias cruzadas que faciliten la realización de pruebas de cumplimiento por parte de auditores y socios"[44]

Los atributos de confidencialidad, integridad, disponibilidad y privacidad de la seguridad de la información antes mencionada, en ISO/IEC 17799 también son pilares fundamentales para la estructura. Actualmente la norma ISO/IEC 17799 también es llamada ISO 27002. ISO/IEC 17799 versión 2005 se basa en una estructura piramidal y expone la clasificación de la seguridad en cuatro tipos: organizativa, lógica, física y legal. La Norma ISO/IEC 17799 establece diez dominios de control que abarcan la gran mayoría de la Gestión de la Seguridad de la Información:

- Políticas de seguridad: establece que deben estar documentadas las políticas de seguridad y los procedimientos internos de la organización.
- Aspectos organizativos: toda organización debe contar con un marco formal de seguridad y definir la responsabilidad en los equipos de seguridad.
- Clasificación y control de activos: evalúa los recursos de la información según el análisis de riesgos y la gestión de incidentes según el nivel de confidencialidad.
- Seguridad ligada al personal: capacita e informa a los empleados respecto de la seguridad, confidencialidad y gestión de los activos de información.
- Seguridad física y del entorno: identifica las áreas y establece controles a los recursos afectados a la información.
- Gestión de comunicaciones y operaciones: define procesos y sistemas íntegros que permitan administrar la infraestructura tecnológica y la seguridad.
- Control de accesos: define procesos documentados con asignación de responsabilidades y monitorea el acceso a los recursos de información.
- Desarrollo y mantenimiento de sistemas: define procedimientos que aseguren la calidad y seguridad de los sistemas implementados en la organización.
- Gestión de continuidad del negocio: el sistema de administración en caso de contingencias, contiene procedimientos de recuperación y pruebas.
- Cumplimiento o conformidad de la legislación: respetando la legislación vigente, la organización establece y hace cumplir los contratos acordados.

[44] Norma IRAM. Obtenido el 28 de junio del año 2002 en la Word Wide Web: https://n9.cl/awhv [Accedido el 27/6/19]

De los dominios recién mencionados, se desprenden objetivos de control de la norma asociados a la evaluación de los riesgos.

1. Política de seguridad

    1.1 Política de seguridad de la información: la gerencia define la seguridad.

2. Organización de la Seguridad de la Información

    2.1 Organización interna: foro gerencial define la seguridad de la información.

    2.2 Grupos externos: designa a un propietario para cada recurso de información.

3. Gestión de Activos

    3.1 Responsabilidades sobre los activos: protección de recursos y procesos.

    3.2 Clasificación de la Información: asegura la protección a los recursos.

4. Seguridad de Recursos Humanos

    4.1 Antes del empleo: ingresos autorizados por ingresos físicos y lógicos.

    4.2 Durante el desempeño de funciones: otorga acceso físico y lógico a terceros.

5. Seguridad Física y Ambiental

    5.1 Áreas seguras: impide daños y accesos no autorizados a la empresa.

    5.2 Equipo de seguridad: área de recepción con personal y medios de control.

6. Gestión de las Comunicaciones y Operaciones

    6.1 Procedimientos y responsabilidades operacionales: establece procedimientos que garanticen el correcto funcionamiento de las instalaciones.

    6.3 Planeación y aceptación del sistema: minimiza el riesgo del sistema.

    6.4 Protección contra el código malicioso: previene el software malicioso.

    6.5 Respaldo o Back-Up: realiza copias de resguardo de la información.

    6.6 Gestión de seguridad de la red: controla la protección de los servicios.

    6.7 Gestión de medios: protege los activos y medios de almacenamiento.

    6.8 Intercambio de información: regula acuerdos de uso de la información.

    6.10 Monitoreo: detecta accesos no autorizados y registra incidentes.

7. Control de Acceso

    7.1 Requerimiento del negocio para el control del acceso.

    7.2 Gestión de acceso del usuario: impide el acceso no autorizado.

    7.3 Responsabilidades del usuario: capacita a usuarios en seguridad.

7.4 Control de acceso a la red: supervisa el acceso a los servicios de red.

7.5 Control del acceso al sistema operativo: bloquea accesos no autorizados.

7.6 Control de acceso a la aplicación e información: bloquea y limita el acceso.

7.7 Computación y trabajo remoto: garantiza el acceso remoto seguro.

8. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

8.1 Requerimientos de seguridad de los sistemas de información: garantiza los requerimientos de seguridad, planes de reanudación y seguridad en aplicaciones.

8.2 Procesamiento correcto en las aplicaciones: valida los datos de entrada, autentica mensajes y valida los datos de salida.

8.3 Controles criptográficos: técnicas criptográficas aseguran la información.

8.4 Seguridad de los archivos del sistema: supervisa el acceso a los archivos.

8.5 Seguridad en los procesos de desarrollo y soporte: controla los proyectos.

9. Gestión de un incidente en la Seguridad de la Información

9.1 Reporte de eventos y debilidades de la seguridad: registra los incidentes.

9.2 Gestión de incidentes y mejoras en seguridad: resuelve las amenazas.

10. Gestión de la Continuidad del Negocio

10.1 Aspectos de la seguridad de la información en la gestión de la continuidad del Negocio: evalúa los riesgos e identifica eventos que generen interrupciones.

11. Cumplimiento

11.1 Cumplimiento de los requerimientos legales: cumple las leyes, reglamentos, estatutos, normas y contratos de los requisitos de seguridad.

11.2 Cumplimiento de políticas, estándares de seguridad y técnico: asegura sistemas compatibles con las políticas y estándares de seguridad.

11.3 Consideraciones de auditoría de los sistemas de información: implementa el proceso de auditoría mediante controles sobre los sistemas de operaciones.

La implementación de ISO/IEC 17799 permite el aumento de la seguridad de los sistemas de información, proporciona un incremento de la imagen de la empresa y mejora la trazabilidad brindando auditorias de seguridad más confiables.

Además, eleva el nivel de confianza de los socios y clientes, minimiza el daño por responsabilidad civil, mejora la planificación y administración de la seguridad, permite alianzas comerciales más seguras y perfecciona la continuidad del negocio.

Ventajas y Desventajas de ISO con COBIT/ITIL (desarrollado al final del capítulo)

- Ventajas: incrementa la calidad y la productividad, ofrece resultados visibles en el corto plazo, funciona para pequeñas y grandes empresas, mejora los procesos de distribución y producción de los productos. Además, concentra los procesos organizativos y procedimientos competitivos, minimiza los costos por incremento del consumo y mejora la adaptación de los procesos a los avances tecnológicos.

- Desventajas: la implementación requiere de tiempo e inversión, en empresas familiares su aceptación es resistida, exige un proceso de cambio en toda la empresa y eleva el riesgo de eliminar la interdependencia entre departamentos.

PMBOK v6

La versión 6 del PMBOK está dividida en tres partes. La primera parte incluye los Fundamentos para la Dirección de Proyectos. Describe los proyectos, su dirección y el entorno sobre el cual se desarrollan. Luego se detalla el rol del director del proyecto.

Allí se desarrollan las competencias necesarias del director del proyecto asociado con el Marco de desarrollo de competencias del director del proyecto. Se destacan tres habilidades profesionales tales como la dirección técnica de proyectos (son las habilidades, conocimientos y comportamientos asociados con la dirección de programas y proyectos), Liderazgo (habilidades y comportamientos que permiten guiar, motivar y dirigir al equipo para cumplir los objetivos de la organización) y la Gestión Estratégica y de Negocios (conocimientos de la organización y su industria, que posibilita mejorar el desempeño).

Se explica la necesidad de integrar el proyecto, su contexto y coordinación de los procesos y actividades de dirección, cada uno con sus entradas, salidas, herramientas y técnicas.

Se establecen diez Áreas de Conocimiento, si bien están interrelacionadas, se analizan de forma unitaria, son las siguientes:

- Gestión de la Integración del Proyecto: son los procesos para identificar, y coordinar las actividades en los Grupos de Procesos de la Dirección de Proyectos.
- Gestión del Alcance del Proyecto: son los procesos requeridos que aseguran que el proyecto incluye sólo el total del proyecto requerido.
- Gestión del Cronograma del Proyecto: gestión de los tiempos para finalizar las tareas en el tiempo predefinido.
- Gestión de los Costos del Proyecto: son los procesos necesarios para estimar, presupuestar y financiar los costos para completar el proyecto.
- Gestión de la Calidad del Proyecto: incluye los procesos necesarios para planificar, gestionar y controlar la política de calidad.
- Gestión de los Recursos del Proyecto: procesos requeridos para administrar y adquirir los recursos necesarios para concluir el proyecto.
- Gestión de las Comunicaciones del Proyecto: procesos requeridos para asegurar la planificación, gestión y disposición final de la información del proyecto.
- Gestión de los Riesgos del Proyecto: procesos necesarios para planificar, gestionar y monitorear los riesgos del proyecto.
- Gestión de las Adquisiciones del Proyecto: procesos precisos para la adquisición de productos o servicios externos del equipo del proyecto.
- Gestión de los Interesados del Proyecto: procesos requeridos para identificar las expectativas de las personas u organizaciones afectadas al proyecto.

Las Áreas de Conocimiento están asociadas a los Grupos de Procesos de la Dirección de Proyectos. Están definidos como un agrupamiento lógico de procesos de la dirección de proyectos para el cumplimiento de los objetivos del proyecto (Inicio, Planificación, Ejecución, Monitoreo y Control, y Cierre). En la Parte 2 de la Guía PMBOK se desarrollan los cinco Grupos de Procesos de la Dirección de Proyectos. En la aplicación de cada uno de ellos, se observa un formato reiterado para facilitar la aplicación. En cada Grupo de Proceso de la Dirección de Proyectos se detalla el Grupo

de Proceso de Inicio, Grupo de Proceso de Ejecución, Grupo de Proceso de Monitoreo y Control y el Grupo de Proceso de Cierre.

Para cada Grupo de Proceso mencionado se detallan los Componentes del Plan para la Dirección del Proyecto (son los elementos o factores asociados para cumplimentar el plan), Ejemplos de Documentos del Proyecto (son los documentos que pueden ser considerados como entradas para el proceso en cuestión) y las Actualizaciones a los Documentos del Proyecto (son los documentos del proyecto que pueden actualizarse para llevar a cabo el proceso en cuestión).

PMBOK - Ventajas y Desventajas

- Ventajas: maximiza la eficiencia por proyecto, estandarización de las prácticas en las diversas áreas, aplica para cualquier tipo de industria y para la estandarización del sistema industrial y organizacional. Además, reduce los recursos utilizados a proyectos sin valor agregado, la autoridad y responsabilidad total sobre el proyecto es de su director y minimiza las líneas de comunicación.
- Desventajas: es necesario mayor productividad y un alto compromiso por parte de la Alta Dirección, mantiene los procesos de desarrollo de corta duración y es complejo para pequeños proyectos. Asimismo, compromete a toda la organización en la ejecución del programa y destina muchos recursos de la organización para varios proyectos.

ITIL v3

ITIL (Information Technology Infrastructure Library) surgió en el año 1980. Durante el año 2007 se lanzó la versión 3 de ITIL, mediante un enfoque de ciclo de vida para la gestión de servicios, con un mayor énfasis en la integración de negocios de TI. Es un marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI con un enfoque de administración de procesos. La versión 3 de ITIL define:

- Servicio: es un medio para entregar valor a los clientes sin que ellos estén obligados a asumir los costos y riesgos asociados. El objetivo de un servicio

es satisfacer una necesidad sin asumir las capacidades y recursos directamente.

- Gestión de Servicios: es un conjunto de capacidades especializadas necesarias para proveer valor a los clientes en forma de servicios.

- Valor del Servicio: valor percibido por parte del usuario por el servicio.

- Garantía del Servicio: es el cumplimiento de la disponibilidad, capacidad, continuidad y seguridad que se le brinda al cliente por el servicio.

El Ciclo de Deming constituye la estructura de todos los procesos de mejora continua, PHVA, sus iniciales indican: Planificar (Plan, definir los objetivos y medios para llegar a ellos), Hacer (Do, implementar la visión definida), Verificar (Check, logro de los objetivos con los recursos asignados) y Actuar (Act, corregir las desviaciones y proponer mejoras). El Ciclo de Vida del Servicio está compuesto por cinco fases:

1. Estrategia del Servicio: esta fase incluye la Gestión de estrategia para servicios de TI, Gestión del portafolio de servicios, Gestión financiera para servicios de TI, la Gestión de la demanda y la Gestión de las relaciones del negocio.

2. Diseño del Servicio: analiza nuevos servicios y los existentes, gestiona los proveedores y la seguridad tecnológica, asegura que cumpla los requisitos de los clientes y se adecuen a los objetivos estratégicos. Los procesos de esta fase son la Coordinación del diseño, Gestión del catálogo de servicios, Gestión de niveles de servicio, Gestión de la capacidad, Gestión de la disponibilidad, Gestión de la continuidad del servicio de TI, Gestión de seguridad de la información y la Gestión de proveedores.

3. Transición del Servicio: asegura que los cambios a los servicios y sus procesos se han llevado adelante de manera coordinada. Los procesos de esta fase son la Gestión de cambios, Evaluación de cambios, Planificación y soporte de la transición, Gestión de entregas y despliegues, Validaciones y pruebas de servicio, Gestión de la Configuración y Activos del Servicio y la Gestión del conocimiento.

4. Operación del Servicio: incluye la gestión del día a día en la operación del servicio, peticiones, eventos, accesos, operaciones, soporte técnico y aplicaciones. Los

procesos de esta fase son la Gestión de eventos, Gestión de incidencias, Solicitud de cumplimiento, Gestión de accesos, Gestión de problemas y Gestión de operaciones.

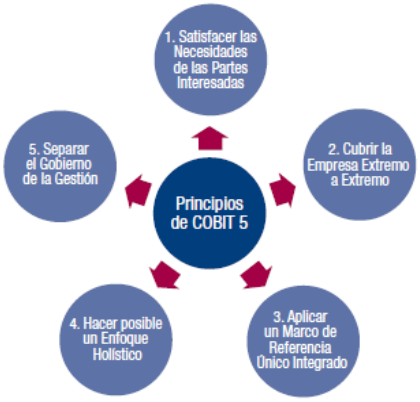
5. Mejora Continua del Servicio: define protocolos para generar informes sobre el rendimiento, resultados y calidad de los servicios. Es una guía para crear y mantener el servicio mediante el diseño, transición y operación. Los procesos que integran esta fase son el Reporte de servicio y la Revisión de los siete pasos del proceso de mejora.

Ventajas y Desventajas de ITIL con COBIT/ISO

- Ventajas: es sencillo y flexible, permite conectar el negocio con la tecnología y la entrega de servicios, incrementa la productividad, la eficiencia de la empresa y maximiza la comunicación.
- Desventajas: genera poca transparencia en los indicadores de resultados y desempeño, falta de fortalezas en la seguridad y exige mucho compromiso de los empleados en todos sus niveles.

COBIT 5

En el año 1996 ISACA (Information Systems Audit and Control Association)[45] publica la primera edición de COBIT, la cual fue actualizando. COBIT 5 provee un marco de trabajo integral para gobernar y gestionar la tecnología. La *figura 3, Principios de COBIT,* expresa los cinco principios claves:

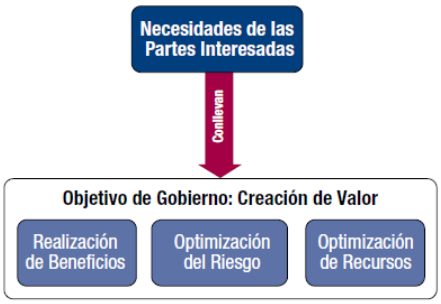


Fuente: ISACA[46]

[45] ISACA. Obtenido el año 2012 en la Word Wide Web: https://n9.cl/4xcr [Accedido el 27/6/19]

[46] ISACA. Obtenido el año 2011 en la Word Wide Web: https://n9.cl/eqcg [Accedido el 27/7/19]

- Principio 1: Satisfacer las Necesidades de las Partes Interesadas. COBIT 5 provee los procesos necesarios y los catalizadores para que la tecnología genere valor al negocio. Los catalizadores son los factores que influyen en el gobierno y la gestión de la organización de TI. Crear valor significa obtener beneficios, optimizando los riesgos a costos adecuados. En la próxima *figura 4*, se muestran las *Necesidades de las partes interesadas.*



Fuente: ISACA[46]

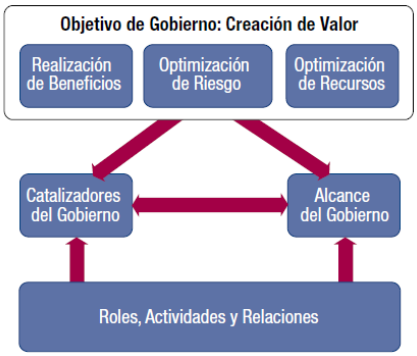
La cascada de metas de COBIT 5 es el mecanismo para transformar las necesidades de las partes interesadas del organismo en metas corporativas, luego en metas relacionadas con las TI y finalmente en metas catalizadoras. Se expresa en la *figura 5, Cascada de metas de COBIT 5.*

Fuente: ISACA[46]

La cascada de metas está impactada por diferentes conceptos y consta del Paso 1 (los motivos de las partes interesadas influyen en la estrategia y las tecnologías), Paso 2

(las necesidades de las partes interesadas desencadenan metas empresariales asociadas con los objetivos organizacionales), Paso 3 (cascada de metas del organismo apoyada por metas de TI) y Paso 4 (cascada de metas de TI hacia las metas catalizadoras).

- Principio 2: Cubrir la Empresa de Extremo a Extremo. COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo cubriendo todas las funciones y procesos de la organización. Considera al gobierno, la gestión de la información, la tecnología asociada de extremo a extremo, la integración del gobierno de la organización de TI en el gobierno corporativo y todos los procesos necesarios. Los mismos se exponen en la siguiente *figura 6, Enfoque de Gobierno de COBIT 5.*



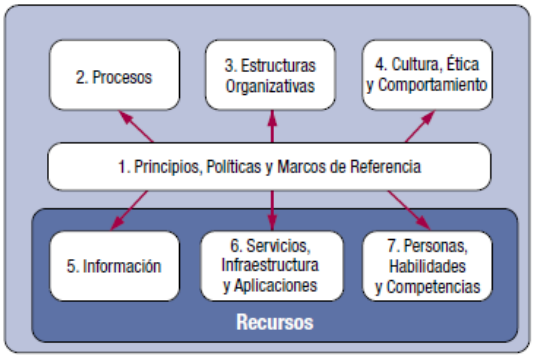
Fuente: ISACA[46]

Los catalizadores de gobierno son los recursos del gobierno para alcanzar los objetivos planteados. El alcance de gobierno es aplicado a diferentes áreas de la organización. Los roles, actividades y relaciones definen quienes, cómo se involucran, cómo interactúan y su alcance. Diferencia entre los dominios de gobierno y la gestión.

- Principio 3: Aplicar un marco de referencia único integrado. COBIT 5 se establece como un marco de trabajo principal, se nutre de otros estándares internacionales para cubrir todas las actividades de TI. Es un marco de referencia de gestión y gobierno, único e integrado.

- Principio 4: Hacer Posible un Enfoque Holístico. COBIT 5 establece un conjunto de catalizadores que permiten implementar un sistema de gobierno y gestión global para las TI de la organización. El marco de trabajo establece siete categorías de catalizadores: Principios, políticas y marcos de referencia (instrumento que permite implementar la gestión diaria), Procesos (conjunto de actividades para alcanzar ciertos objetivos y soportar las metas generales de TI), Estructuras organizativas

(son las entidades de la organización de tomas de decisión). También la Cultura, ética y comportamiento (actividades para el logro del éxito entre el gobierno y la gestión), Información (recurso para evaluar el estado actual de la organización y planificar a futuro). Asimismo los Servicios, infraestructuras y aplicaciones (proporcionan servicios y tecnologías de procesamiento de la información) y Personas, habilidades y competencias (el personal debe tener las habilidades y competencias necesarias). La próxima *figura 7 son los Catalizadores corporativos de COBIT 5.*



Fuente: ISACA[46]

- Principio 5: Separar el Gobierno de la Gestión. COBIT 5 destaca una clara diferencia entre gobierno y gestión. Para ello se necesita una estructura organizativa distinta. El Gobierno garantiza la evaluación de las necesidades, opciones y condiciones de las partes interesadas para establecer el alcance de las metas de la organización. Define la dirección, prioriza, mide el rendimiento y cumplimiento. La Gestión establece un plan, la construcción y ejecución. Controla si las actividades desarrolladas persiguen la dirección definida por el gobierno para el cumplimiento de las metas organizacionales.

<u>Interacción entre Gobierno y Gestión</u>

Gobierno y gestión están desarrollados por diferentes tipos de actividades y responsabilidades. No obstante, entre gobierno y gestión existen actividades de interacción. El gobierno ejecuta acciones conocidas por sus iniciales en inglés (EDM) Evaluar, Orientar y Supervisar. La gestión ejecuta acciones como (PBRM) Alinear, Planificar y Organizar. (BAI) Construir, Adquirir e Implementar. (DSS) Entregar, dar Servicio y Soporte. (MEA) Supervisar, Evaluar y Valorar. Cada dominio posee cierta cantidad de procesos, el número total de procesos de gobierno y de gestión de COBIT 5

es de treinta y siete. El Ciclo de Vida es una herramienta que permite implementar COBIT en las organizaciones, es un proceso iterativo para la construcción de un modelo de gobierno y gestión de TI. COBIT 5 contiene un modelo de capacidad de procesos. El nivel 0 es un proceso incompleto (no está implementado o no alcanza su propósito), el nivel 1 es un proceso que cumple su propósito. El nivel 2 es un proceso implementado y gestionado. El nivel 3 es un proceso gestionado que alcanza los resultados. El nivel 4 es un proceso predecible dentro de los límites definidos. El nivel 5 es un proceso optimizado y mejorado de forma continua.

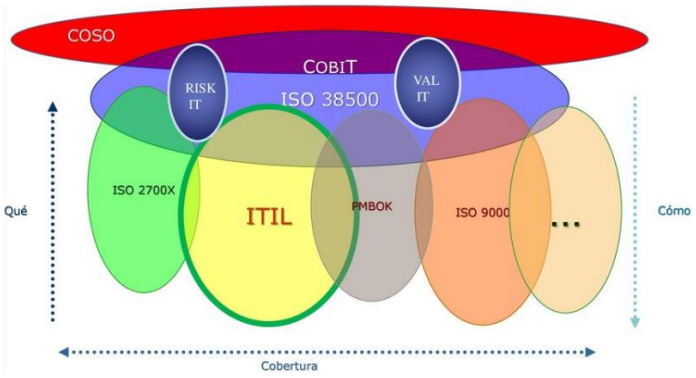
Ventajas y Desventajas de COBIT con ITIL/ISO

- Ventajas: es apto para cualquier empresa, mejora los criterios para la toma de decisiones, define planes estratégicos y favorece las auditorías.

- Desventajas: reduce la interacción entre gestión, seguridad, calidad y desarrollo y requiere un tiempo de implementación.

Coberturas de los marcos de trabajo

La *figura 8* refleja las *Coberturas de los Marcos de Trabajo,* la armonización de los marcos, alcance del ámbito de cobertura, que y como lo realiza cada estándar internacional.

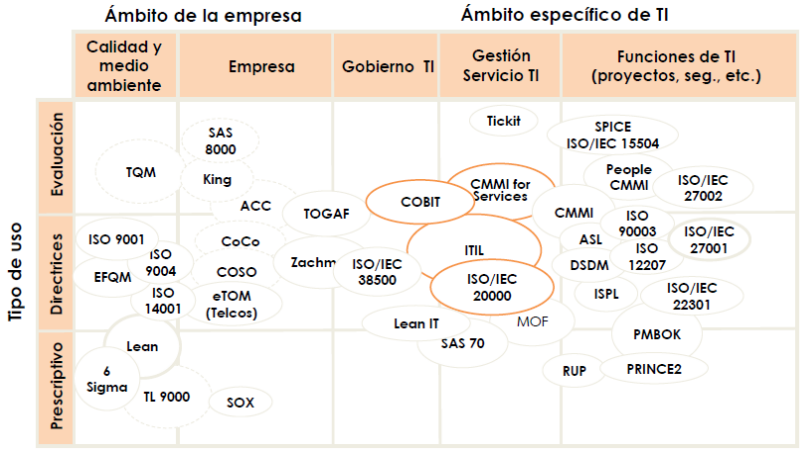


Fuente: Nuevo Marco de Control de las TI [47]

[47] Nuevo Marco de Control de las TI. Seminario Latinoamericanos de Contadores y Auditores. Lucio A. Molina Focazzio. Punta Cana. Obtenido el 5 de Agosto de 2011 en la Word Wide Web: https://n9.cl/mze3u [Accedido el 29/7/19]

Normas y marcos de referencia relacionados con las TI

Ante la diversidad de normas y marcos de referencia relacionados con la tecnología, es necesario destacar que cada cual tiene un enfoque determinado, dentro del Ámbito Específico de TI o el Ámbito de la Empresa. La siguiente *figura 9* muestra el *Mapa de normas y marcos de referencia relacionados con las TI*.



Fuente: Gartner e.p [48]

Conclusiones respecto de los marcos de trabajo

Cuando se desarrolló el antecedente del marco se destacó la importancia que el Nuevo Marco Tecnológico de la Ciudad Autónoma de Buenos Aires se desarrolle, en primer lugar, a través del gobierno de TI y luego profundizarlo mediante su gestión. Habiendo investigado los diversos estándares internacionales, las experiencias obtenidas, ámbitos de cobertura, orientación, principales fortalezas, sus ventajas y desventajas, se opta por implementarlo con COBIT 5. El marco provee la separación de funciones de gobierno y gestión tecnológica, establece un plan de capacitación que les permite a los organismos definir los requerimientos de TI necesarios para completar el Formulario único de requerimientos. Además, formaliza y fortalece el canal de comunicación entre ASInf y los organismos del GCABA el cual permite profundizar las necesidades tecnológicas. Dicha implementación será complementada con ITIL v3 que asegura la adecuada administración de las actividades de gestión dando solución al problema definido en el comienzo de este trabajo.

[48] SG Campus. Obtenido el 22 de Agosto de 2013 en la Word Wide Web: https://n9.cl/tn9o [Accedido el 2/8/19]

Capítulo 3 - Nuevo marco de tecnología de la Agencia de Sistemas de Información

Al evaluar la estructura organizativa vigente de ASInf, sus funciones y responsabilidades, se detecta que con dicha conformación no se encuentran mitigados ciertos riesgos existentes. En primer lugar, no están bien diferenciados los roles, responsabilidades y acciones asignadas al gobierno y a la gestión. Asimismo, la cantidad de controles ejercidos son insuficientes o realizados por el mismo personal que desarrolla las actividades.

Por otro lado, es necesario crear diversos comités con personal capacitado técnicamente en diversas disciplinas según los controles a ejecutar. En la estructura organizativa vigente de ASInf, la Dirección General de Seguridad Informática está ubicada en el mismo nivel de jerarquía que otras direcciones generales. La mencionada dirección no está sujeta al control de un comité y su unidad de mando superior es la Dirección Ejecutiva de la Agencia de Sistemas de Información.

Por tal motivo, para mitigar los riesgos de fraude y garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, es conveniente que la Dirección General de Seguridad Informática reporte al Consejo de Administración.

Por lo antes mencionado, se procede a diseñar un Nuevo Marco Tecnológico para la Agencia de Sistemas de Información basado en COBIT 5. No sólo se aplica a los objetivos estratégicos de ASInf, sino a toda la organización. Se define la misión, visión, valores, metas organizacionales, roles y responsabilidades. Conociendo la estructura del organismo que se encuentra en funciones, el propósito es aplicar COBIT 5 para reorganizar y reutilizar desde el gobierno hacia la gestión, los recursos existentes para evitar costos necesarios.

Misión

Implementar programas tecnológicos en políticas públicas que promuevan la inclusión digital y faciliten la conectividad a través de la innovación. Ofrecer a los ciudadanos servicios tecnológicos seguros mediante una gestión transparente y eficiente de los recursos estatales. Ser el órgano rector en materia de tecnologías de la

información que asegure la confidencialidad, integridad, disponibilidad y privacidad de los servicios electrónicos del Gobierno de la Ciudad Autónoma de Buenos Aires.

Visión

Ser una organización pública innovadora que impulse el bienestar y la inclusión social de los ciudadanos a través del uso masivo de la tecnología de la información.

Objetivos estratégicos

La Agencia de Sistemas de Información tiene como objetivo diseñar, implementar, operar, actualizar, innovar y controlar los servicios tecnológicos del Gobierno de la Ciudad Autónoma de Buenos Aires a través de una gestión eficiente y transparente que genere agilidad e inclusión digital para los ciudadanos garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información.

Valores

Responsabilidad, Integridad, Constancia, Eficiencia, Transparencia, Aprendizaje, Adaptabilidad, Espíritu de Equipo, Respeto Mutuo, Superación Continua y Vocación de Servicio.

Descripción de los roles

Se definen y describen los nuevos roles de ASInf basados en COBIT 5.

- Consejo de Administración: formado por un equipo de funcionarios a cargo de la gobernanza de ASInf que no forman parte de las direcciones, gerencias ni subgerencias. Reportan a la Jefatura de Gabinete de Ministros y establecen los lineamientos estratégicos del gobierno del organismo.

- Auditoría: desarrolladas por el auditor como máximo responsable a cargo. Interactúa y emite informes al Consejo de Administración.

- Comité Ejecutivo Estratégico de TI: está constituido por un equipo de funcionarios nombrados por el Consejo de Administración exceptuando al CIO. Responsables de la gestión de las inversiones facilitadas por la tecnología.

- Comité Estratégico (Desarrollo/Proyectos): está compuesto por un equipo de expertos responsables de la dirección de los proyectos. Incluye la gestión de los riesgos relacionados con los proyectos, planes, recursos y entrega de valor.

- Consejo de Arquitectura: está integrado por un equipo de expertos a cargo de los estándares y las políticas de la organización.

- Comité de Riesgo Corporativo: conformado por un equipo de funcionarios a cargo de las decisiones de la gestión de riesgos del organismo según los lineamientos de gobierno establecidos por el Consejo de Administración.

- Consejo de Riesgos de Tecnología: constituido por un equipo de expertos para evaluar en detalle los riesgos de la tecnología y asesorar al Comité de Riesgo Corporativo respecto del posible impacto en ASInf por las decisiones tecnológicas.

- Dirección General Ejecutiva (CEO): a cargo de un funcionario elegido por la Jefatura de Gabinete de Ministros, llamado CEO por sus siglas en inglés, responsable de la gerencia general de ASInf.

- Dirección General Financiera (CFO): a cargo de un funcionario llamado CFO por sus siglas en inglés, responsable en la gestión y el riesgo financiero.

- Dirección de Operaciones (COO): un funcionario llamado COO por sus siglas en inglés, responsable de los aspectos relacionados con la operación.

- Dirección General de Riesgos (CRO): tarea desarrollada por el responsable de la gestión de riesgos, llamado CRO por sus siglas en inglés.

- Dirección de Informática: llamado CIO, responsable de alinear la tecnología con las estrategias del organismo, reporta al Consejo de Administración.

- Dirección de Seguridad de la Información (CISO): responsable de comprender todo respecto de la seguridad de la información.

- Dirección de Privacidad de la Información: responsable de supervisar los riesgos e impactos generados por las leyes de privacidad en el organismo.

- Dirección de Recursos Humanos: es la responsable de las políticas y la planificación de los recursos humanos de la organización.

- Gerencia de Riesgos de Tecnología: responsable de la gestión de los riesgos de la tecnología que impacten con los riesgos de la organización.

- Gerencia de Arquitectura: a cargo del proceso de arquitectura de la organización, relacionada con la información, servicios, infraestructura y aplicaciones, es la responsable del rendimiento de un proceso.

- Gerencia de Desarrollo: encargada del desarrollo de soluciones asociadas con la tecnología. Propone al CIO la innovación tecnológica.

- Gerencia de Operaciones de TI: responsable de la infraestructura y los entornos para las operaciones tecnológicas. Define los acuerdos de servicio.

- Gerencia de Administración de TI: registra y soporta los procesos administrativos de la tecnología. Colabora con el sistema de gestión de la calidad.

- Gerencia de Gestión de Proyectos (PMO): cumple funciones en la planificación, evaluación y control de cambios relacionados a los proyectos.

- Gerencia de Gestión de Valor (VMO): encargado del apoyo de las inversiones, gestiona los servicios, evalúa y asesora las oportunidades de inversión.

- Gerencia de Seguridad de la Información: asesora a la Dirección de Seguridad de la Información respecto de la gestión de la seguridad.

- Gerencia de Infraestructura: asesora a la Dirección de Operaciones (COO) en la gestión de los recursos relacionados con la infraestructura tecnológica.

- Gerencia de Redes y Telefonía: orienta a la Dirección de Operaciones en la gestión de los recursos y garantiza la continuidad del servicio de redes y telefonía.

- Gerencia de Soporte a Usuarios: asiste a la Dirección de Operaciones en la gestión, registración, acceso autorizado y optimización de incidentes.

- Gerencia de Legales: responsable en asistir sobre aspectos administrativos y cumplimiento de los requerimientos regulatorios y legales.

- Gerencia de Compras y Patrimonio: brinda apoyo a la Dirección de Recursos Humanos, registra bienes patrimoniales y supervisa adquisiciones.

- Gerencia de Gestión de requerimientos: responsable de recibir el formulario de requerimientos. Evalúa, define y dimensiona el requerimiento. Prioriza las solicitudes del área, coordina los plazos, requisitos funcionales y técnicos de cada requerimiento con el responsable. Genera reuniones con los responsables de cada área para acordar soluciones de corto plazo y derivaciones a Gestión de Proyectos.

- Subgerencia de Continuidad de Negocio: colabora con la Gerencia de Seguridad de la Información, gestiona y asegura la continuidad de los servicios.

- Subgerencia de Servicios: asiste a la Gerencia de Seguridad de la Información, propone mejoras en servicios vigentes y nuevos servicios.

- Subgerencia Ejecutiva de Negocio: a cargo de la gestión de los recursos, rendimiento y cumplimiento de los objetivos de una unidad de negocio específico.

Metas relacionadas con las TI de ASInf

Se definen las metas relacionadas con las TI de ASInf y se mapean con los procesos de COBIT 5 permitiendo el desarrollo de las metas de los catalizadores de ASInf. Se establecen las siguientes metas:

✓ Garantizar el 80% de satisfacción de los ciudadanos respecto de las aplicaciones y sistemas provistos por ASInf.

✓ Lograr que el total de las metas y requerimientos estratégicos de ASInf sean soportados por las metas estratégicas de TI.

✓ Asegurar que el 100% de los roles de la gestión ejecutiva se encuentren cubiertos en las decisiones de TI.

✓ Ejecutar las acciones necesarias para no superar las 3 (tres) interrupciones mensuales calendario en los servicios de TI.

✓ Asegurar que el 60% de las inversiones de TI sean monitoreadas a través del ciclo de vida económico completo.

✓ Asegurar que el 80% de los servicios de TI provea los beneficios esperados.

✓ Obtener el 80% de la satisfacción de los ciudadanos por la calidad de los servicios de TI entregados y por la transparencia, comprensión y precisión de la información financiera de TI.

✓ Generar concientización de los agentes con nivel ejecutivo respecto de las oportunidades de innovación de TI en ASInf.

✓ Identificar el 100% de los procesos y servicios críticos de TI brindados por ASInf y que la frecuencia de actualización del perfil de riesgo sea semestral. También en los casos que se producen modificaciones importantes en los procesos.

✓ Asegurar que el tiempo para otorgar, modificar y eliminar los privilegios de acceso a la red sea menor a un día laboral desde la realización del pedido, identificando los perfiles críticos para generar un orden de prioridades.

✓ Lograr que no existan incidentes relacionados con el incumplimiento de las políticas internas.

✓ Obtener el alineamiento total entre el riesgo de TI y el riesgo de ASInf.

✓ Considerar el riesgo de TI en la totalidad de los proyectos de ASInf.

✓ Garantizar que sólo el 10% de los riesgos de TI excedan el riesgo de ASInf.

✓ Lograr el 80% de satisfacción del Consejo de Administración respecto de la capacidad de respuesta de TI a los nuevos requerimientos y los costos asociados.

✓ Obtener el 90% de satisfacción del personal con funciones en TI.

✓ Elaborar informes periódicos confeccionados por Auditoría Interna en base a los riesgos detectados.

✓ Lograr que el número de problemas de no conformidad con respecto a acuerdos contractuales con proveedores de servicios de TI no sea a mayor a 5 (cinco) por año calendario.

✓ Lograr que el 100% de las iniciativas estratégicas sean asignadas a un responsable.

✓ Diseñar e integrar una interfaz única de ingreso para el ciudadano que interactúe con todos los sistemas y aplicaciones ofrecidos por el GCABA.

✓ Obtener el 80% de satisfacción de los propietarios de los procesos de los servicios de TI.

✓ Lograr que el 80% de los proyectos desarrollados al año formen parte de la planificación anual.

✓ Implementar las mejoras definidas para los servicios vigentes en 1 (un) año y en 3 (tres) años para la puesta en marcha de nuevas tecnologías como internet de las cosas, sistemas predictivos, sistemas de detección temprana, sistemas de visión artificial, sistema de reconocimiento facial e inteligencia artificial aplicados a chatbot.

✓ La cantidad recomendada de horas anuales en capacitación de cada agente se estima en 20.

✓ Obtener el 80% de la satisfacción de los ciudadanos por la disponibilidad de la información en los servicios de TI.

✓ Lograr que el 100% de los nuevos proyectos cumplan con las metas de calidad.

✓ Se planifica para fines del año 2023 el comienzo de las pruebas de desarrollo de internet de las cosas para ser aplicado en las calles de la ciudad y en prevención médica. También para el sistema predictivo de mantenimiento del alumbrado público, los sistemas de detección temprana de humos en centros de cómputos con sistema de supresión, de visión artificial para control de semáforos, reconocimiento facial para trámites e inteligencia artificial aplicado a chatbot para la atención de consultas.

Nuevos servicios provistos por ASInf

Se planifica el desarrollo de nuevas tecnologías y se establece:

- ✓ Desarrollo y mantenimiento de sistemas y aplicaciones.
- ✓ Desarrollo de bases de datos.
- ✓ Administración, mantenimiento y actualización de bases de datos.
- ✓ Provisión, mantenimiento y actualización de internet.
- ✓ Mantenimiento y actualización del correo de organismos del GCABA.
- ✓ Generación de copias de respaldo de las bases de datos.
- ✓ Instalación y actualización de herramientas informáticas, hardware y software, servicio de videoconferencia y software antivirus.
- ✓ Gestión remota y presencial de hardware, software, internet e impresión.
- ✓ Creación de puntos de red.
- ✓ Administración y resguardo de la información en soportes magnéticos, custodia, traslado ante un incidente y recuperación.
- ✓ Gestión de la infraestructura, hardware y software de los centros de cómputos asegurando el funcionamiento 7 días por 24 horas.
- ✓ Contingencia por cortes de suministro de energía o catástrofe.
- ✓ Operación 7 días por 24 horas, acciones preventivas y correctivas de la red inalámbrica y fibra óptica del GCABA.
- ✓ Gestión de red de información, comunicaciones y telefonía del GCABA.
- ✓ Gestión y mantenimiento de Wifi público y privado del GCABA.
- ✓ Conexión a proveedores en frontera y redes de terceros, gestión de la plataforma y enlaces de internet del GCABA.

- ✓ Provisión de puntos de presencia de Wifi en eventos GCABA.
- ✓ Gestión de la infraestructura para la implementación de firma digital.
- ✓ Administración de los servidores.
- ✓ Almacenamiento de datos centralizados y descentralizados del GCABA.
- ✓ Gestión y mantenimiento de la red LAN y MAN del GCABA.
- ✓ Registración de incidentes y provisión de soporte.

Los servicios de TI recién mencionados para el Nuevo Marco Tecnológico de la Agencia de Sistemas de Información forman parte de los objetivos estratégicos de ASInf. La carencia o el funcionamiento degradado de alguno de ellos podría impactar de distinta manera en los entes del GCABA, por tal motivo se consideran servicios críticos.

Innovaciones Tecnológicas

Apoyando el desarrollo tecnológico, se reconoce la necesidad de implementar en ASInf innovaciones tecnológicas, no sólo para mejorar los servicios brindados actualmente sino también para generar valor. Por ello se planifica la investigación y el desarrollo de Sistemas de visión artificial, Internet de las cosas, Sistemas de reconocimiento facial, Sistemas de detección temprana de humos con sistema de supresión, Sistemas de inteligencia artificial y de Sistemas predictivos. Se proyecta el desarrollo de internet de las cosas para ser aplicado en las calles de la Ciudad Autónoma de Buenos Aires con la finalidad de predecir accidentes de tránsito y delitos. La misma tecnología se aplicará a la salud, en prevención médica a pacientes de riesgo mediante la colocación de marcapasos o biochips. Se planifica el desarrollo de sistemas predictivos implementados al mantenimiento del alumbrado público con el propósito de minimizar sus costos y agilizar las intervenciones ante incidentes.

Con la intención de proteger los activos informáticos y mitigar los riesgos por incendios, se diseña la implementación de sistemas de detección temprana de humos en centros de cómputos con sistema de supresión de fuegos. Se considera llevar a la práctica los sistemas de visión artificial implementados al tránsito vehicular y al control

de semáforos en la Ciudad Autónoma de Buenos Aires para evitar accidentes y agilizar la circulación. Asimismo se contempla el desarrollo y provisión de sistemas de reconocimiento facial para identificar y agilizar los trámites que realizan los ciudadanos en el Gobierno de la Ciudad Autónoma de Buenos Aires. Siguiendo la misma línea, a través de los sistemas de inteligencia artificial, desarrollar aplicaciones mediante chatbot para mejorar la atención de las consultas sobre el uso de TI por parte de los entes del GCABA y de los ciudadanos.

Nuevo Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires

Se implementa COBIT 5 para las áreas de gobierno y gestión de ASInf. Para cada proceso se definen las prácticas de gobierno y gestión asociadas. *Las palabras que poseen hipervínculo permiten acceder al detalle de implementación de la actividad señalada*. Las actividades EDM corresponden al dominio Evaluar, Orientar y Supervisar. **EDM01** se encarga de asegurar el establecimiento y mantenimiento del marco de referencia de gobierno. Analiza e implementa los requisitos para el gobierno de TI, estructuras, procesos y prácticas para alcanzar la misión, las metas y objetivos de ASInf. El nivel de capacidad observado del proceso no alcanza su propósito. EDM01.01. Establece un Comité Ejecutivo Estratégico de TI que considera la normativa vigente de control interno para ASInf, la ley 2095[49] de Compras y contrataciones, ley 4895 de Ética pública[50], Resolución Nº 596-MHGC/11 de Compras electrónicas de bienes y servicios[51] y ley 3304 del Sistema de administración de documentos electrónicos (SADE)[3]. También la Disposición Nº 36-DGCG/15[52] del Sistema integrado de gestión y administración financiera (SIGAF). Se define el proceso de adquisición o desarrollo de software. El impacto de TI en ASInf es significativo.

[49] Ley 2095. Ley de Compras y Contrataciones de la Ciudad. Obtenido el 2 de Noviembre de 2006 en la Word Wide Web: https://n9.cl/mxr6 [Accedido el 4/5/19]

[50] Ley 4895. Ley de Ética en el Ejercicio de la Función Pública. Obtenido el 15 de Enero de 2014 en la Word Wide Web: https://n9.cl/ozx6 [Accedido el 15/6/19]

[51] Resolución Nº 596-MHGC/11. Políticas, Términos y Condiciones de Uso del Sistema Electrónico de Adquisiciones y Contrataciones. Obtenido el 29 de Abril de 2011 en la Word Wide Web: https://n9.cl/1tlv [Accedido el 15/5/19]

[52] Disposición Nº 36-DGCG/15. Sistema integrado de gestión y administración financiera (SIGAF). Obtenido el 11 de Febrero de 2015 en la Word Wide Web: https://n9.cl/czn5d [Accedido el 8/12/19]

Respecto del contexto externo, se considera la ley 104/98 de Acceso a la Información, ley 1845/05 de Protección de Datos Personales de la Ciudad y la ley Nacional 25326/00 de Protección de Datos Personales[57]. La información personal y los datos sensibles sólo son usados con fines laborales, no pueden ser publicados ni comercializados. Se contempla la ley Nacional 11723/33 de Régimen Legal de la Propiedad Intelectual[58], ley 3784/11 de Uso Seguro de Internet[53], ley 5688 del Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires[54] y la Resolución Nº 398/MJYSGC/19. Los lineamientos del gobierno de TI son definidos por el Consejo de Administración y establecen que las metas estratégicas de ASInf sean soportadas por las metas estratégicas para TI. Se reconoce la situación actual a través de la medición de los servicios. Auditoría interna elabora y eleva un informe de control del Plan Estratégico del Área de TI.

EDM01.02. Se define un sistema de administración de comunicaciones y compromisos. La comunicación individual se realiza por correo electrónico o por el sistema SADE.[40] El Consejo de Administración de ASInf comunica masivamente, sólo hacia las direcciones o de forma individual. Se asignan roles, funciones y responsabilidades para apoyar la toma de decisión del gobierno de TI. Se establece un código de ética y conducta profesional para que el personal conozca las consecuencias que genera la realización de acciones prohibidas. Se desarrolla y comunica la cultura organizacional, con recompensas y beneficios y se establecen los aspectos culturales de ASInf para fomentar el aporte de ideas innovadoras que generen beneficios a ASnf en la cadena de valor mediante los servicios provistos. Se establece un sistema de encuestas y mediciones sobre la satisfacción de los ciudadanos y entes del GCABA respecto de la calidad de los servicios de TI.

EDM01.03. El Comité Ejecutivo Estratégico de TI mide el rendimiento de la organización jerárquica inferior en las tareas del gobierno de TI. Acuerda reuniones trimestrales con el Consejo de Administración y evalúa la efectividad de ASInf implementando acciones correctivas según la legislación vigente. Monitorea los eventos ocurridos en los servicios.

[53] Ley 3784/11. Semana del Uso Seguro de Internet. Obtenido el 12 de Mayo de 2011 en la Word Wide Web: https://n9.cl/i25x [Accedido el 15/6/19]

[54] Ley 5688. Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires. Obtenido el 17 de Noviembre de 2016 en la Word Wide Web: https://n9.cl/i38o [Accedido el 12/6/19]

EDM02 asegura la entrega de beneficios. Optimiza la contribución al valor de ASInf desde los procesos de negocio, servicios y activos de TI a costos aceptables. El nivel de capacidad del proceso es incompleto. EDM02.01 evalúa la optimización del valor, si la infraestructura, accesos a internet, sistemas y aplicaciones son seguros y a un costo adecuado. Asegura que las nuevas tecnologías generan beneficios en los servicios provistos. La Dirección General Financiera asegura que la gestión financiera genera valor para las inversiones y los servicios, que el beneficio y el riesgo financiero y no financiero se corresponde con la eficiencia y el costo. Se publica la información financiera de TI para que los ciudadanos comprendan las inversiones realizadas y mediante un sistema de encuestas expresen su nivel de satisfacción con la calidad de los servicios de TI entregados.

EDM02.02. El Consejo de Administración comunica al personal de ASInf las inversiones a realizar en infraestructura y sistemas. Establece los requerimientos, riesgo asociado, cronograma del proyecto, partida presupuestaria y asegura la entrega de los beneficios al ciudadano o entes del GCABA. El Comité Ejecutivo Estratégico de TI orienta al Consejo de Administración respecto de las oportunidades en innovaciones tecnológicas, mejoras en la confidencialidad, integridad, disponibilidad y privacidad de los servicios. Además, propone innovaciones potenciales en las bases de datos, seguridad lógica, física, aplicaciones y software. Recomienda nuevos desarrollos, para ser aplicados en el GCABA.

EDM02.03. El Comité Ejecutivo Estratégico de TI evalúa el acatamiento por parte de ASInf y de los entes del GCABA a la normativa regulatoria de TI. Se establecen metas para evaluar los niveles de servicios y se recopilan los datos pertinentes. Auditoría interna genera informes con los datos e información que son analizados por el Consejo de Administración. Revisa los informes de auditoría de capacidades y recursos.

EDM03 asegura que el apetito y la tolerancia al riesgo son entendidos y comunicados y el riesgo de ASInf en relación con la TI es el establecido. El nivel de capacidad observado del proceso no alcanza su propósito. EDM03.01. El Consejo de Riesgos de Tecnología y el Comité de Riesgo Corporativo asesoran al Consejo de Administración para definir el apetito de riesgo de TI tolerado, el grado de alineación de

la estrategia de riesgos y si la innovación proyectada genera consecuencias por encima del nivel de riesgos aceptados. El Consejo de Administración evalúa si los riesgos de TI y su gestión cubren las capacidades de ASInf y sus recursos.

EDM03.02. ASInf capacita y concientiza a su estructura organizativa y al personal de los entes del GCABA sobre los riesgos de TI y sus recursos. Impulsa los riesgos de TI mediante la política de riesgos y lo comunica a todo el personal de ASInf y entes del GCABA. Brinda capacitación respecto de los riesgos en los proyectos desarrollados por ASInf.

EDM03.03. El Director General Ejecutivo (CEO) junto con la Subgerencia Ejecutiva de Negocio supervisan el perfil de riesgo según los umbrales definidos por el Consejo de Administración de ASInf e implementa acciones correctivas ante desvíos. Promueve los informes de nivel de servicio, evalúa el progreso de los servicios e informa al Consejo de Administración ante la detección de desvíos. Capacita en el proceso para otorgar, modificar y eliminar los privilegios de acceso a la red y en la política interna vigente.

EDM04 garantiza que los recursos de TI, personas, procesos y tecnologías, soportan los objetivos de ASInf a un costo razonable. El nivel de capacidad actual observado del proceso es incompleto. EDM04.01. Examina la estrategia actual de ASInf como órgano de control y proveedor de servicios de TI. Considera la clasificación de la información, la generación de valor en los sistemas, aplicaciones y desarrollos innovadores. El Consejo de Administración revisa y aprueba el plan de recursos y las estrategias de desarrollo de la infraestructura física para generar beneficios a los ciudadanos y mitigar los riesgos con los recursos asignados. Alinea la gestión de los recursos humanos y las competencias con la planificación de ASInf según el presupuesto.

EDM04.02. Comunica formalmente las estrategias y el plan de gestión de los recursos al personal de ASInf y a los entes del GCABA por correo, noticias masivas internas o el sistema SADE.[40] El Consejo de Administración define las metas para la gestión y el seguimiento de la infraestructura tecnológica, sistemas y recursos humanos.

EDM04.03. Supervisa la asignación y optimización del acceso, almacenamiento, infraestructura y el incremento en el número de las estaciones de trabajo según la jerarquía y urgencia de los servicios definidos por ASInf. El aprovisionamiento de TI a los entes según la arquitectura de ASInf y las futuras necesidades tecnológicas.

EDM05 asegura la transparencia hacia las partes interesadas y garantiza la elaboración de los informes de desempeño y conformidad de TI de ASInf. El nivel de capacidad medido en ASInf no alcanza su propósito. EDM05.01. Los informes de Auditoría interna respetan la objetividad y legislación vigente, son elevados al Consejo de Administración. Se realizan periódicamente con un enfoque proactivo al desarrollo de innovaciones previniendo las amenazas a TI.

EDM05.02. Se publican los informes de Auditoría interna y externa en la web de ASInf para facilitar la consulta a los ciudadanos. Evita la exposición de datos sensibles que comprometan la seguridad. Garantiza que la información publicada cumpla con la normativa de control interno y externo de la ley 325[55] y ley 70[56] del GCABA. Define la aprobación formal de los informes, previo descargo del auditado y establece su escalado.

EDM05.03. Auditoría interna de ASInf planifica y presenta los informes al Consejo de Administración. Establece con las áreas el análisis de riesgos durante su ejercicio de 4 (cuatro) años. Los entes del GCABA son auditados por auditorías internas y externas.

[55] Ley 325/99. Obtenido el 28 de Diciembre de 1999 en la Word Wide Web: https://n9.cl/02ji [Accedido el 23/11/19]

[56] Ley 70. Sistemas de gestión, administración, financiera y control del sector público de la Ciudad. Obtenido el 27 de Agosto de 1998 en la Word Wide Web: https://n9.cl/fcwb [Accedido el 8/12/19]

También es necesaria la implementación en las áreas de gestión de ASInf del Nuevo Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires dentro del dominio alinear, planificar y organizar (APO). **APO01** gestiona el marco de TI, define la misión y visión. El nivel de capacidad del proceso actual observado cumple su propósito. APO01.01. La Dirección de Informática (CIO) define los roles de cada área. Con el presupuesto asignado por la Jefatura de Gabinete de Ministros, se establece la implementación del plan mediante la Dirección General Financiera (CFO). Se conforma el Comité Estratégico de TI que prioriza la inversión en tecnología. Se definen las metas para cada dirección, gerencia y subgerencia, los proyectos de TI, responsables y plazos. Se acuerdan reuniones semanales y la confección de actas firmadas por las partes intervinientes.

APO01.02. La Dirección de Informática (CIO) eleva a la Jefatura de Gabinete de Ministros los roles en ASInf que luego se comunicarán por medio del boletín oficial y publicación en la web. Se asignan las responsabilidades para garantizar la continuidad de los servicios y sistemas. Se analizan las habilidades requeridas por el personal y su capacitación técnica generando un documento por cada agente, el cual firme y acepte sus responsabilidades y adhesión a las políticas y al código ético profesional.

APO01.03. La Dirección General Ejecutiva concientiza sobre la visión de ASInf como una organización pública innovadora que impulse el bienestar y la inclusión social de los ciudadanos a través del uso masivo de la tecnología de la información. Define las políticas tecnológicas con los proveedores y entes del GCABA sobre el cumplimiento de las leyes que rigen el manejo de la información, ley 1845/05[33] y ley Nacional 25326/00 de Protección de Datos Personales[57], leyes Nacionales 11723[58] y 25036 de Propiedad Intelectual de software legal[59] y la Política de Privacidad de Datos,

[57] Ley 25326/00. Protección de Datos Personales. Obtenido el 2 de Noviembre de 2000 en la Word Wide Web: https://n9.cl/4wqp [Accedido el 27/7/19]

[58] Ley 11723/33 de Régimen Legal de la Propiedad Intelectual. Obtenido el año 2019 en la Word Wide Web: https://n9.cl/vk8or [Accedido el 27/7/19]

[59] Ley 25036/98. Propiedad Intelectual. Obtenido el año 1998 en la Word Wide Web: https://n9.cl/ml97 [Accedido el 27/7/19]

ley 104/98[32] de Acceso a la Información y ley 5688 del Sistema Integral de Seguridad Pública[54]. Establece un objetivo anual de no conformidad con los proveedores de servicios de TI no mayor a 5 (cinco).

APO01.04. La Dirección General Ejecutiva (CEO) provee los recursos necesarios para comunicar la misión, visión, los objetivos de servicio de TI, el código de ética, políticas, procedimientos y roles, los que son formalizadas y aceptados internamente por los responsables.

APO01.05. La Dirección General Ejecutiva (CEO) formaliza y garantiza la continuidad de los servicios de TI, su aprovisionamiento, almacenamiento y procesamiento. ASInf posee dos centros de datos, ubicados en Av. Independencia Nº 635 y Uspallata N° 3101, Caba. Utiliza los servicios de la nube, servicios públicos, privados, híbridos, comunitarios, con software, plataforma e infraestructura como servicio según el requerimiento.

APO01.06. La Subgerencia Ejecutiva de Negocio define las políticas del marco tecnológico de TI y asigna la propiedad de la información. La Gerencia de Arquitectura gestiona los centros de datos mediante un software de monitoreo. Establece y actualiza en un inventario de información que describe a los propietarios, custodios y clasificaciones, también incluye a los proveedores externos.

APO01.07. La Dirección de Operaciones (COO) identifica los procesos de los servicios de TI con impacto significativo como el acceso a internet y servidores, sistemas operativos, red de alimentación eléctrica, contingencias, recuperación y los servicios asociados a los sistemas de administración de la infraestructura de red y comunicaciones de TI en ASInf. La Dirección de Operaciones (COO) promueve la capacitación de los agentes, documentación y automatización de los servicios. Identifica la información obsoleta o el componente en desuso y activa su baja.

APO01.08. La Dirección General Ejecutiva (CEO) define el marco regulatorio, supervisa su cumplimiento y formaliza la comunicación al proveedor o al ente del GCABA. Ante la detección de un incumplimiento adopta acciones correctivas. Si

infringe la ley 4895 de Ética Pública[50] o las Normas éticas según la Resolución Nº 205/SGCBA/16[60], lo comunica a la Gerencia de Legales.

APO02 gestiona la estrategia, proporciona una visión holística de los servicios provistos por ASInf y su entorno de TI. El nivel de capacidad actual observado del proceso es incompleto. APO02.01. Si bien ASInf no tiene competencia externa que le quite porción de su mercado, sus costos y beneficios, son evaluados y podrían ser reemplazados por proveedores externos por una relación costo/beneficio más equilibrada. ASInf acuerda un SLA por cada provisión, define las prioridades y el desarrollo tecnológico en la nube. La nueva arquitectura desarrollada para ASInf cubre todos los procesos necesarios apoyados por aspectos del diseño de servicios.

APO02.02. La Dirección de Informática (CIO) proyecta el crecimiento de sus servicios, recursos, capacidades, inversiones en infraestructura, sistemas y recursos humanos. Establece el plazo de caducidad de la infraestructura, los potenciales riesgos de ataque y el impacto en los servicios suministrados. Identifica los problemas, fortalezas, oportunidades y amenazas en el entorno tecnológico actual y evalúa el incremento del uso de la nube.

APO02.03. ASInf implementa un proyecto bidireccional con los entes del GCABA que permite agilizar la comunicación de los requerimientos y las necesidades de TI. Evalúa, ante un pedido de proyecto de un ente del GCABA, si está desarrollado o existe la posibilidad de reutilización y personalización de uno existente. ASInf genera puntos de acceso a wifi para el ciudadano e incrementa el número de tótems de autogestión en lugares públicos.

APO02.04. Define los factores críticos de éxito y asigna agentes de cada área para investigar las nuevas tecnologías.

APO02.05. El Consejo de Administración establece el plan estratégico, asigna los responsables, recursos para su implementación, beneficios, riesgos e impactos. Define la conveniencia de la provisión y centralización para todos los servicios provistos por el GCABA y sólo el apoyo de los proveedores externos. Analiza los

[60] Resolución Nº 205/SGCABA/16. Normas Éticas. Boletín oficial de la Ciudad Autónoma de Buenos Aires, N° 5.037, página Nº 305 en la Word Wide Web: https://n9.cl/m7nk [Accedido el 15/8/19]

requerimientos para migrar el entorno tecnológico actual al deseado. Identifica el incremento en la dotación de personal.

APO02.06. Mantiene reuniones informativas con los entes del GCABA para comunicar el rumbo. Comunica la estrategia de TI internamente en forma mensual y ante cambios urgentes, diariamente. Informa las acciones para concientizar al agente responsable de ASInf el cumplimiento del proyecto en tiempo y forma.

APO03 gestiona la arquitectura empresarial y establece una arquitectura común integrada por las aplicaciones, la información y los datos. El nivel de capacidad observado del proceso no alcanza su propósito. APO03. El Consejo de Administración promueve una interfaz única de ingreso para que el ciudadano interactúe con todos los sistemas y aplicaciones ofrecidos por el GCABA. La Gerencia de Arquitectura define la arquitectura con componentes reutilizables que permitan la integridad y uniformidad de la plataforma de ASInf.

APO03.02. La Gerencia de Arquitectura de ASInf homologa los procesos, estandariza las herramientas y métodos de forma interna, con los proveedores y entes a los que suministra los servicios del GCABA. Realiza reuniones formales para definir los requerimientos de los proyectos y sus responsables, crea un documento de aceptación entre ASInf y el ente solicitante gestionado a través del sistema SADE.

APO03.03. La Dirección General Ejecutiva define la cultura de ASInf, el impacto de la arquitectura y los servicios brindados. La Subgerencia Ejecutiva de Negocio evalúa la migración a la nueva tecnología y su posible configuración.

APO03.04. La Dirección General Ejecutiva detalla el programa, presupuesto asignado, recursos y el plan de proyectos que ASInf ha definido y priorizado con los entes del GCABA. Establece las fases, progresos de la arquitectura, transición y su aceptación.

APO03.05. La Dirección de Operaciones y el Comité Ejecutivo Estratégico de TI establecen el alcance y las prioridades de la cartera de servicios, el que definen por ser el órgano rector del GCABA y acuerdan con los entes. Acepta los cambios que satisfagan los requerimientos.

APO04 gestiona la innovación y conoce la tecnología de la información y las tendencias asociadas al servicio. El nivel de capacidad actual del proceso cumple su propósito. APO04.01. La Dirección General Ejecutiva define el apetito por el riesgo, con un presupuesto total estimado para innovación en ASInf no menor al 10% del presupuesto total asignado. Promueve acuerdos de colaboración para complementar los conocimientos, ya sean nacionales o provinciales, como el Instituto Nacional de Tecnología Industrial (INTI).[61]

APO04.02. La Dirección de Operaciones genera reuniones mensuales con los entes del GCABA para conocer los requerimientos de TI, ya sea a través de innovaciones como de adecuaciones de los servicios vigentes.

APO04.03. La Dirección de Informática investiga nuevas tecnologías y recopila información, se asesora con proveedores expertos en TI, con entes nacionales y organismos con los que firmó acuerdos de cooperación. Consulta respecto de las migraciones, sus plazos estimados, impactos, incidentes, obstáculos y barreras tecnológicas que hayan tenido que superar.

APO04.04. La Dirección de Informática de ASInf acuerda con la Dirección General de Tránsito y Transporte de Caba sobre el valor que puede generar al tránsito el desarrollo de internet de las cosas y los sistemas de visión artificial para el procesamiento, captura de imágenes digitales y sensores electrónicos para ser aplicados en las calles de la ciudad para predecir accidentes de tráfico. Con el Ministerio de Salud de Caba respecto del valor que pueda aportar internet de las cosas en prevención médica a pacientes de riesgo mediante la implantación de microchip y marcapasos. Propone a Atención Ciudadana de Caba la posibilidad de desarrollar sistemas de reconocimiento facial de los ciudadanos para acceder de manera segura a los sistemas y aplicaciones de GCABA. Concientiza a los entes del GCABA que posean centros de operaciones de TI respecto de la implementación de sistemas de detección temprana de humos con sistema de supresión. Fomenta a la Dirección General de Atención y Cercanía Ciudadana el uso de sistemas de inteligencia artificial aplicados mediante chatbot para atender las consultas sobre el uso de TI por parte de los entes del GCABA y de los ciudadanos.

[61] Instituto Nacional de Tecnología Industrial. Obtenido en la Word Wide Web: https://www.inti.gob.ar/ [Accedido el 26/9/19]

También consulta a la Dirección General de Alumbrado Público de Caba, sobre la posibilidad de la implementación del sistema predictivo de mantenimiento del alumbrado público.

APO04.05. La Subgerencia Ejecutiva de Negocio y la Gerencia de Arquitectura ejecutan y documentan los resultados, a pequeña escala, del plan de desarrollo de ideas innovadoras. Evalúan, miden y comunican si las innovaciones encontraron obstáculos difíciles de superar.

APO04.06. El Comité Ejecutivo Estratégico de TI evalúa el ciclo de vida económico y el valor generado para los ciudadanos. ASInf incrementa y mejora los servicios ofrecidos y mide si las inversiones realizadas en los proyectos mantienen un equilibrio razonable entre costos y beneficios y si los ciudadanos perciben las mejoras y justifican la inversión.

APO05 gestiona el portafolio, prioriza los servicios, gestiona la demanda y apoya con recursos según los objetivos estratégicos, su valor y riesgo. El nivel de capacidad observado del proceso cumple su propósito. APO05.01. El Consejo de Administración define la mejor combinación de la cartera de inversión, costos, riesgos, valor, servicio ofrecido y percibido por el ciudadano durante todo el ciclo de vida económico de los proyectos. Establece plazos a 1 (un) año para la mejora en disponibilidad, seguridad y velocidad de los servicios vigentes de conexión a internet y un plazo de 3 (tres) años para la implementación de nuevas tecnologías.

APO05.02. La Dirección General Financiera analiza si los presupuestos establecidos en la planificación anual realizada por el Consejo de Administración son acordes a los asignados en la partida, caso contrario lo comunica a la Dirección General Ejecutiva (CEO). En el caso que el presupuesto sea inferior al necesitado, el Consejo de Administración adecuará la planificación o solicitará los recursos necesarios a la Jefatura de Gabinete de Ministros.

APO05.03. La Dirección General Ejecutiva clasifica las categorías del portafolio de inversiones en TI, vigente y de innovación. Evalúa si persigue las metas de ASInf y si el riesgo es menor que el apetito establecido. Determina si los proyectos rechazados deberían ser conservados para ser considerados en el futuro o dar la baja definitiva.

APO05.04. La Gerencia de Gestión de Valor revisa los proyectos para reconocer sinergias, eliminar duplicaciones e identificar y mitigar riesgos. En caso de nuevas priorizaciones, altas o bajas de proyectos, prioriza sus costos, riesgos, sinergias, metas y presupuestos.

APO05.05. El Comité Ejecutivo Estratégico de TI mantiene activos los proyectos y servicios de TI, interactúa con los responsables de la entrega del servicio, internos y proveedores externos. Comunica cuando los proyectos hayan alcanzado los beneficios esperados.

APO05.06. La Subgerencia Ejecutiva de Negocio da seguimiento a los proyectos, beneficios obtenidos, su evolución y entrega. Comunica los resultados al Comité Ejecutivo Estratégico de TI y en caso de desvíos, implementa acciones.

APO06 gestiona el presupuesto, los costos y administra las actividades financieras de los servicios de TI. El nivel de capacidad actual del proceso cumple su propósito. APO06.01. La Dirección General Financiera (CFO) define las responsabilidades y procesos para el manejo del presupuesto y la contabilización de los costos. La Dirección General Financiera define la asignación presupuestaria para nuevos proyectos, el proceso de gestión de beneficios y la optimización de los gastos recurrentes.

APO06.02. La Dirección de Informática (CIO) prioriza los recursos de TI y define la necesidad o no de proveedores de servicios externos dentro de la asignación presupuestarias para los proyectos aprobados. Considera si los servicios externos de desarrollo de aplicaciones y sistemas pueden implementarse internamente y mantenerse con recursos humanos propios de ASInf.

APO06.03. La Dirección General Financiera implementa un presupuesto formal de TI incluyendo los costos de desarrollo de los nuevos servicios. Si fuese necesario eleva el presupuesto y analiza fuentes de financiación externas con la autorización formal correspondiente. Registra, mantiene y comunica el presupuesto actual de TI, realiza su seguimiento y ante desvíos implementa acciones correctivas.

APO06.04. La Dirección de Informática calcula los costos para que los propietarios de los procesos verifiquen su cumplimiento y posibles mejoras. Define y

formaliza los SLA´s (Acuerdos de Nivel de Servicio) con los proveedores externos y OLA´s (Acuerdos de Nivel Operativo) con los entes del GCABA. Establece la forma de pago del desarrollo de proyectos de sistemas y aplicaciones según los requerimientos detallados.

APO06.05. La Dirección de Informática de ASInf establece la medición, gestión de los costos, contabilidad y recopila datos relevantes para identificar desviaciones entre lo presupuestado y lo consumido en los proyectos internos o servicios.

APO07 gestiona los recursos humanos y proporciona un enfoque que asegure las capacidades de decisión, las habilidades de los recursos humanos, la comunicación de las funciones y sus responsabilidades. El nivel de capacidad actual del proceso cumple su propósito. APO07.01. La Dirección de Informática planifica capacitaciones técnicas anuales específicas de los recursos humanos internos para soportar los servicios vigentes y los nuevos proyectos. Genera el apoyo de conocimientos por parte de los proveedores. Forma equipos específicos y los capacita para investigar nuevas tecnologías. Para los planes de capacitación, la cantidad recomendada de horas anuales para cada agente se estima en 20. Al finalizar la capacitación, cada agente evalúa el contenido suministrado en el curso y a sus capacitadores. Se implementa una metodología de consulta a los agentes de ASInf que permite recopilar las capacitaciones solicitadas por cada agente y que el nivel jerárquico evalúe la conveniencia del dictado de ese contenido. Se establecen mecanismos de búsquedas de personal técnico específico que genere una dotación de recursos humanos posibles a incorporar al plantel de ASInf.

APO07.02. La Dirección de Informática capacita a más de un agente para la realización de una función crítica de trabajo. En caso de desafectación del agente, existe otro que conoce y cubre su tarea. Cada rol tiene un responsable principal y otro agente que asume la misma responsabilidad en caso de ausencia del titular. Para cada proyecto se define un sponsor, líder, usuario referente, director y un coordinador.

APO07.03. La Dirección de Informática define las habilidades y competencias necesarias para los agentes según los servicios actuales y los proyectos de innovación. La dirección formaliza una carrera laboral y el desarrollo de competencias acordes a las funciones. Genera intenciones de ingresar, permanecer y profesionalizarse.

APO07.04. Se evalúa semestralmente el desempeño de los agentes. Las metas de desarrollo profesional y laboral de cada agente están alineadas con las metas de ASInf. La Dirección de Recursos Humanos implementa y comunica el proceso disciplinario y el programa de beneficios. Cada agente conoce los resultados de su desempeño y las acciones a desarrollar para generar mejoras.

APO07.05. El Comité Ejecutivo Estratégico de TI registra los recursos humanos de ASInf afectados a TI, especifica sus capacidades técnicas, roles actuales y los planificados para el futuro. Se identifican las carencias de conocimientos y se evalúa una capacitación acorde. En caso de requerir servicios externos, se analiza si un proveedor actual puede brindar el servicio o es necesario recurrir a uno nuevo.

APO07.06. Se promueve un vínculo laboral de los agentes con ASInf de largo plazo. Se recomienda formalizar a los agentes mediante una relación laboral en planta permanente. Se firman SLA con los proveedores respetando las leyes vigentes, nivel de servicios, plazos estipulados, medición del desempeño, frecuencia, y penalidades ante incumplimientos.

APO08 gestiona las relaciones con los entes del GCABA a través de la mejora de los servicios de TI de modo formal. El nivel de capacidad observado del proceso es ejecutado. APO08.01. ASInf, para los casos de apoyo en los servicios suministrados por proveedores externos, realiza mediciones y las contrasta contra los SLA firmados. La Dirección de Informática asegura la provisión de los servicios de TI y el flujo de los procesos asociados para la expansión de las nuevas tecnologías.

APO08.02. La Dirección de Informática comunica a los agentes de ASInf y a los entes del GCABA, las oportunidades, riesgos y limitaciones de la implementación de la innovación tecnológica.

APO08.03. La Dirección de Informática establece la tolerancia al riesgo, su impacto y el escalado de los incidentes para su solución. Coordina la periodicidad de las reuniones de revisión del servicio, medición del rendimiento, desempeño de los recursos humanos y las actividades de innovación tecnológica.

APO08.04. La Dirección de Informática comunica y acuerda con proveedores externos y entes de GCABA, el desarrollo de los proyectos, plazos, pruebas, riesgos, soporte, cambios, concientización del impacto y la capacitación.

APO08.05. La Dirección de Informática genera un sistema de medición de satisfacción con los servicios de TI de los ciudadanos, proveedores y los agentes de los entes del GCABA. Implementa mejoras en la conexión wifi en plazas y lugares públicos y la infraestructura de TI que recibe los servicios de los proveedores.

APO09 administra los acuerdos de servicio y alinea sus niveles con los requisitos y expectativas de ASInf. El nivel de capacidad del proceso cumple su propósito. APO09.01. La Subgerencia de Servicios define e integra la existencia de los servicios vigentes y los servicios requeridos para el futuro. Instrumenta mejoras en la velocidad, disponibilidad y seguridad en las conexiones por wifi. Evalúa y prioriza el catálogo de servicios, los plazos de obsolescencia de la infraestructura vigente y la migración de la información hacia las nuevas tecnologías.

APO09.02. La Subgerencia de Servicios comunica el paquete de servicios del catálogo vigente y garantiza la continuidad de los componentes afectados al servicio.

APO09.03. La Subgerencia de Servicios define los lineamientos para los acuerdos de servicio, sus parámetros como la capacidad, seguridad, continuidad, tiempos del servicio, disponibilidad, rendimiento y cumplimiento normativo. La Dirección de Privacidad de la Información de ASInf define los borradores de los acuerdos de nivel de servicio y operativos, SLA y OLA, con los entes del GCABA y con los proveedores externos.

APO09.04. La Subgerencia de Servicios mide y verifica el cumplimiento de los requerimientos acordados y la Gerencia de Arquitectura obtiene los datos, genera informes y las acciones correctivas en caso de detectar desvíos.

APO09.05. La Subgerencia Ejecutiva de Negocio revisa los términos de los acuerdos de servicio, ya sean OLA o SLA. Asegura que el nivel de servicio suministrado es el acordado.

APO10 gestiona y administra los servicios de TI prestados por los proveedores, gestiona las relaciones, contratos y el cumplimiento de lo pactado. El nivel de capacidad del proceso actual en ASInf es implementado y gestionado. APO10.01. La Dirección de Informática registra y categoriza a los proveedores externos y sus contratos. Evalúa la urgencia ante un requerimiento para elevar el nivel del servicio.

APO10.02. La Dirección de Informática define los requisitos técnicos según las peticiones recibidas. Para el caso de adquisición de software, se consideran los derechos y obligaciones de licenciamiento de la propiedad intelectual, mantenimiento, garantías, entrega del código fuente, actualización, depósito de garantía y derechos de acceso. Para la adquisición de desarrollos de nuevas tecnologías, se incluyen las pruebas, gestión de la calidad, rendimiento y garantías.

APO10.03. La Dirección de Informática define el contrato, la calidad del servicio, el cumplimiento de la ley 2095/06[49] y ley 70/98[56] y los conflictos con terceras partes. Si varios proveedores se unen para proveer un servicio, se asigna un rol de proveedor líder a uno de ellos como responsable global del contrato.

APO10.04. La Dirección de Informática gestiona los riesgos relacionados con la capacidad del proveedor por el suministro de internet, servicios para la infraestructura de TI, acceso a servidores, almacenamiento, servicio alternativo de procesamiento, contingencias y recupero. El contrato contempla los riesgos potenciales de interrupción del servicio, garantía, proveedores alternativos y la mitigación del riesgo.

APO10.05. La Dirección de Informática define formalmente y documenta los criterios del rendimiento y costos de los servicios de los proveedores. Las Gerencias de Desarrollo y de Operaciones de TI consideran nuevos requerimientos o mejoras en los servicios.

APO11 gestiona la calidad y comunica los requisitos en todos los procesos, controles y estándares de mejora continua. El nivel de capacidad observado del proceso es ejecutado. APO11.01. La Dirección de Operaciones de ASInf implementa un sistema de gestión de calidad medida en los procesos, proyectos y los objetivos estratégicos. Registra los datos de calidad en un proceso estandarizado, continuo, revisado y comunicado.

APO11.02. La Dirección de Informática (CIO) define la mejora continua y adaptación de los procesos de gestión de la calidad de ASInf. Considera la factibilidad de obtener una certificación internacional de calidad evaluando sus costos y sus beneficios.

APO11.03. La Subgerencia Ejecutiva de Negocio prioriza y alinea cada servicio de TI y la aceptación de su calidad. Comunica a toda la organización de ASInf los requisitos y expectativas de cada servicio.

APO11.04. La Dirección de Informática establece los lineamientos para que los propietarios de los procesos revisen el rendimiento.

APO11.05. La Dirección de Informática de ASInf define los niveles de servicio e integra la gestión de la calidad en los sistemas predictivos, de detección temprana, visión artificial e inteligencia artificial y reconocimiento facial. La Gerencia de Desarrollo documenta las no conformidades y comunica los resultados para que se adopten medidas correctivas.

APO11.06. La Dirección de Informática comunica los resultados y errores a ser corregidos. La Gerencia de Arquitectura identifica los errores recurrentes conocidos mediante un análisis comparativo de calidad con datos históricos.

APO12 administra y reduce el riesgo de TI según la tolerancia de ASInf. El nivel de capacidad observado del proceso cumple su propósito. APO12.01. La Dirección de Informática define el mecanismo para recopilar datos, clasificar, analizar y gestionar el riesgo. Mide y registra el contexto interno de ASInf y el externo, entes del GCABA y proveedores que pudieran elevar el nivel de riesgo. Releva los datos históricos respecto de los incidentes intencionales o no por el acceso a servidores, suministro eléctrico o ataques a la seguridad lógica y física causados en la infraestructura de TI.

APO12.02. La Dirección de Informática mitiga los riesgos en la infraestructura de TI, acceso a servidores, red eléctrica y ataques a la seguridad. Estima la frecuencia y magnitud de pérdidas por posibles escenarios de riesgo de TI según la tolerancia aceptada.

APO12.03. La Dirección General de Riesgos realiza un inventario de los procesos, recursos humanos, soporte, sistemas e infraestructura de proveedores y entes del GCABA. Determina eslabones débiles en los servicios según el perfil de riesgo de TI de ASInf y analiza los datos recopilados según los eventos registrados.

APO12.04. La Dirección de Informática comunica los resultados del análisis de riesgos a los comités, consejos de ASInf y entes del GCABA. Comunica el peor escenario, el más probable y la afectación a los servicios de TI. Informa las inconsistencias y posibles soluciones.

APO12.05. La Dirección General de Riesgos gestiona el apetito con la tolerancia al riesgo de TI, analiza las propuestas para reducir el riesgo en los servicios de TI evaluando sus costos y beneficios.

APO12.06. La Dirección de Informática establece acciones correctivas ante incidentes significativos. Categoriza los incidentes y comunica los impactos en los servicios de TI para actualizar el perfil de riesgo.

APO13 gestiona la seguridad de la información. El nivel de capacidad del proceso cumple su propósito. APO13.01. La Dirección de Seguridad de la Información define un sistema de seguridad de la información alineado con los objetivos de ASInf, ISO 27001 e ISO 17799.

APO13.02. La Dirección de Seguridad de la Información define un plan de riesgos de seguridad de la información según los objetivos, arquitectura y recursos de ASInf.

APO13.03. Las gerencias y subgerencias recopilan datos para el SGSI y generan informes de auditoría interna que permitan su evaluación.

Asimismo, en la gestión, se plantean las actividades dentro del dominio construir, adquirir e implementar (BAI01). **BAI01** gestiona los programas y proyectos en línea con la estrategia de ASInf. El nivel de capacidad actual del proceso en ASInf es gestionado. BAI01.01. La Dirección General Ejecutiva alinea el gobierno y la gestión de los proyectos de los servicios de TI cubriendo todo el ciclo de vida. Define alcance, recursos, riesgos y costos esperados de los sistemas predictivos, de detección temprana, visión e inteligencia artificial y reconocimiento facial aplicados a chatbot.

BAI01.02. La Subgerencia Ejecutiva de Negocio consulta a la Dirección General Financiera respecto del presupuesto e inversiones necesarias para los proyectos a desarrollar y asigna un responsable con las competencias y habilidades adecuadas.

BAIO01.03. La Dirección General Ejecutiva coordina y vincula la gestión interna en ASInf o con los responsables de cada ente del GCABA a lo largo de todo el ciclo de vida de cada proyecto. Recopila los requisitos internos de ASInf o de los entes afectados del GCABA.

BAI01.04. La Subgerencia Ejecutiva de Negocio planifica el proyecto, recursos técnicos y humanos con sus habilidades y competencias técnicas. El Comité Estratégico (Desarrollo/Proyectos) especifica el costo, financiación, cronograma, responsables, y si hubiere, proveedores externos. Genera informes de avance en todos los proyectos de los servicios de TI.

BAI01.05. La Subgerencia Ejecutiva de Negocio verifica la financiación y aprobación de cada etapa del proyecto. La Gerencia de Gestión de Proyectos (PMO) genera un formulario en el cual las partes aceptan la funcionalidad, rendimiento y calidad establecida.

BAI01.06. La Subgerencia Ejecutiva de Negocio supervisa cada proyecto. Auditoría interna emite informes respecto del cumplimiento de los cronogramas, financiación, funcionalidad y satisfacción de los usuarios internos o externos por el uso de internet, correo, sistemas, aplicaciones y accesos a servidores.

BAI01.07. Los proyectos de TI solicitados por los entes del GCABA se gestionan a través del sistema SADE con el formulario de requerimientos. Cada proyecto debe tener uno o más patrocinadores, incluyendo los factores críticos de éxito del proyecto y los indicadores críticos de rendimiento. Para los sistemas predictivos y de detección temprana se establece si existen cambios en la plataforma tecnológica. En los sistemas de visión artificial se evalúa si la infraestructura actual es obsoleta. Para la implementación del sistema de reconocimiento facial, se identifica si la tecnología que posee cada ciudadano es útil para la innovación.

BAI01.08. El Comité Estratégico (Desarrollo/Proyectos) establece para fines del año 2023 las pruebas de nuevas tecnologías. Se acuerda con cada ministerio el mencionado año como plazo para la implementación de los servicios provistos con innovación tecnológica.

BAI01.09. El Comité Estratégico (Desarrollo/Proyectos) identifica a los propietarios, responsables, criterios de éxito y las métricas de desempeño de cada uno de los proyectos de TI. Evalúa la velocidad y disponibilidad de conexión a internet, capacidad del almacenamiento, disponibilidad de los sistemas y aplicaciones. El Comité Estratégico (Desarrollo/Proyectos) valida y verifica la calidad de los entregables con cada ministerio.

BAI01.10. El Comité Estratégico (Desarrollo/Proyectos) asigna a los responsables de cada proceso y gestiona los riesgos de cada proyecto con los entes del GCABA.

BAI01.11. Los criterios de cada proyecto de TI son supervisados por el Comité Estratégico (Desarrollo/Proyectos). Define el alcance, el incentivo a mejorar la calidad de vida de los ciudadanos y como agilizar los servicios de TI del GCABA.

BAI01.12. La Gerencia de Desarrollo asigna el desarrollo del proyecto de internet de las cosas y los sistemas de visión artificial a un equipo con habilidades y conocimientos en el procesamiento y captura de imágenes digitales y sensores electrónicos. El proyecto de internet de las cosas para ser aplicado en prevención médica se asigna a un equipo de ASInf con conocimientos en medicina, sensores corporales y microchips. El proyecto del sistema de reconocimiento facial está afectado

a un equipo con habilidades en base de datos, algoritmos informáticos y procesamiento de imágenes en 3D. El proyecto del sistema de detección temprana de humos con sistema de supresión se asigna a un equipo que gestione sistemas, sensores, detectores de humos, de calor y detectores por muestreo de aire. En tanto que el desarrollo de los sistemas de inteligencia artificial aplicados a chatbot se asigna a un equipo con estudios en sistemas de aprendizaje automáticos y algoritmos informáticos. El proyecto del sistema predictivo de mantenimiento del alumbrado público afecta a un equipo de ASInf o a un proveedor externo compartido con habilidades y conocimientos en sistemas controladores de segmento de luminarias y diseño de subredes con módulos controladores.

BAI01.13. El Comité Estratégico (Desarrollo/Proyectos) evalúa la cadena de valor de los proyectos y gestiona con cada ministerio la obtención de los beneficios esperados. En caso de detectar actividades incompletas, se implementan acciones para solucionar los desvíos.

BAI01.14. Una vez verificados los proyectos que no ofrecieron los beneficios esperados, deben ser eliminados. La Subgerencia Ejecutiva de Negocio acuerda con el sponsor del proyecto la baja del mismo, informa y documenta el fundamento de la baja y la desafectación de los recursos asignados al proyecto.

BAI02 administra la definición de requisitos y asegura que estén en línea con los requerimientos estratégicos de ASInf. El proceso es ejecutado. BAI02.01. La Gerencia de Gestión de Proyectos (PMO) y la Gerencia de Arquitectura, gestionan al personal para la implementación técnica, procesos, automatización, cumplimiento de las leyes vigentes y los contratos con los proveedores externos de servicios de TI.

BAI02.02. El Comité Estratégico (Desarrollo/Proyectos) estudia la viabilidad y la obtención de los beneficios esperados para la aplicación de la innovación tecnológica a nuevos servicios. Propone alternativas que cumplan o mejoren la obtención de los resultados esperados.

BAI02.03. El Comité Estratégico (Desarrollo/Proyectos) acuerda los requisitos con los entes del GCABA que solicitan servicios de TI a través del sistema SADE. Evalúa impactos en costos y tiempos.

BAI02.04. El Comité Estratégico (Desarrollo/Proyectos) coordina la aprobación del proyecto con el sponsor. Para la solución de los aspectos técnicos son consultadas la Dirección de Informática (CIO) y las Gerencias de Arquitectura y Desarrollo.

BAI03 gestiona la identificación y construcción de soluciones según los requisitos. El nivel de capacidad del proceso actual en ASInf cumple su propósito. BAI03.01. La Gerencia de Desarrollo establece la factibilidad del rediseño en plataformas con tecnología innovadora para las aplicaciones, el procesamiento, administración del correo, acceso de equipos móviles y la seguridad lógica.

BAI03.02. La Gerencia de Desarrollo identifica las entradas y salidas de datos para sistemas predictivos, detección temprana, visión e inteligencia artificial y reconocimiento facial. Los desarrollos permiten auditar e identificar la trazabilidad de las transacciones. Los diseños realizados por ASInf poseen OLA y aquellos desarrollados por proveedores externos, sus respectivos SLA.

BAI03.03. La Gerencia de Desarrollo de ASInf elabora los procesos que aseguran a los entes del GCABA y a cada ciudadano, el acceso a internet, al correo, sistemas, aplicaciones y servidores. También desarrolla componentes que facilitan los nuevos servicios de TI. Para el caso de los servicios suministrados por proveedores externos, se garantiza el mantenimiento y las licencias de uso.

BAI03.04. El plan de adquisiciones de los componentes cubre el incremento futuro de capacidad de los servicios de TI considerando riesgos, costos, beneficios y conformidad técnica con los estándares de arquitectura de ASInf.

BAI03.05. La Gerencia de Desarrollo elabora los manuales de operación, de procesamiento y control. Implementa pistas de auditoría en la configuración e integración con la infraestructura del hardware y software que garantiza la disponibilidad e integridad. La Gerencia de Gestión de Proyectos (PMO) identifica y revalida los sistemas predictivos, de detección temprana, visión e inteligencia artificial y reconocimiento facial.

BAI03.06. La Gerencia de Desarrollo registra todas las versiones, resultados, pruebas automatizadas, integración de excepciones y correcciones del desarrollo e implementación de los servicios.

BAI03.07. Para el desarrollo de cada proyecto se elabora un plan de pruebas integradas y simulaciones que recrea el entorno real de ASInf, de los entes del GCABA y su interacción con los ciudadanos. La Dirección de Privacidad de la Información gestiona que las pruebas no afecten ni expongan la información sensible de las bases de datos.

BAI03.08. La Gerencia de Desarrollo prueba sistemas, bases de datos y asegura que la información es confidencial, íntegra, disponible y previene ataques de virus maliciosos. En los sistemas se definen los administradores, perfiles y atributos, claves de acceso, cuentas de usuarios de emergencia, los ambientes de desarrollo, calidad, homologación y producción, pruebas de ataques y penetración de la aplicación. Los microchip, sensores y cámaras para el reconocimiento facial son soportados por la infraestructura actual. La Gerencia de Operaciones de TI registra los fallos durante las pruebas.

BAI03.09. El Comité Estratégico (Desarrollo/Proyectos) prioriza la petición de cambio en cada proyecto, el impacto en el servicio de TI y en el presupuesto. La Gerencia de Gestión de Proyectos (PMO) acuerda con el sponsor del proyecto la aprobación de los cambios y la Gerencia de Desarrollo supervisa la integración y configuración de los componentes que conforman cada proyecto.

BAI03.10. Se implementa un plan de mantenimiento de nuevos servicios que gestionan las bases de datos, algoritmos informáticos, procesamiento de imágenes en 3D, sensores corporales, microchips y la infraestructura que procesa imágenes, capturas de imágenes digitales y sensores electrónicos. La Gerencia de Desarrollo analiza los riesgos, vulnerabilidades, requisitos de seguridad y la implementación de parches.

BAI03.11. La Subgerencia de Servicios establece una disponibilidad de 24 horas los 365 días para el acceso a internet, uso de correo, sistemas, aplicaciones, y en ciertos casos para el servicio alternativo de procesamiento, logística ante incidentes, contingencias y el plan de recupero. También para mantenimiento de nuevos servicios.

BAI04 administra la disponibilidad y capacidad actual y futura, rendimiento y costos. El nivel de capacidad observado del proceso no alcanza su propósito. BAI04.01. La Gerencia de Operaciones de TI evalúa la capacidad y disponibilidad actual y prevista

para el acceso a internet durante las horas comprometidas, las horas fuera de línea, velocidades de subida y bajada de archivos. La disponibilidad de 24 horas para sistemas y aplicaciones, interrupciones por mantenimiento de software y hardware, la infraestructura para las bases de datos y los terabytes de almacenamiento. Los tiempos máximos de interrupción de los procesos. La capacidad de procesamiento de las imágenes en 3D, sensores corporales, microchips, capturas de imágenes digitales, el acceso a los sensores electrónicos y la sensibilidad de los dispositivos para los sistemas de reconocimiento facial.

BAI04.02. La Gerencia de Arquitectura establece que los servicios de TI de alto impacto están compuestos por el acceso a internet, a servidores, base de datos, alimentación eléctrica de la red y grupos electrógenos, los sistemas de acceso al control y monitoreo de la infraestructura y la conexión punto a punto por fibra óptica con los entes del GCABA. Se mantienen actualizados los softwares y sus versiones, mediante los cuales se maximiza la predicción de incidentes y mitigación de riesgos asociados a la asignación de recursos tecnológicos.

BAI04.03. La Gerencia de Administración de TI establece que los servicios de correos, aplicaciones, sistemas para consultas, turnos y solicitudes para los ciudadanos generan un impacto no tan significativo. Si se verifica la falta de capacidad o disponibilidad del servicio de tecnología, se evalúa si es por incumplimiento y se realiza el reclamo correspondiente al proveedor interno o externo.

BAI04.04. La Gerencia de Operaciones de TI de ASInf confecciona informes con la recopilación de los datos respecto de los servicios de tecnología. El gobierno de TI evalúa dichos informes para ajustar el presupuesto a los nuevos requisitos solicitados mediante el sistema SADE.

BAI04.05. La Gerencia de Operaciones de TI elabora los manuales técnicos de los sensores corporales, microchips, dispositivos de captura de imágenes digitales, sensores electrónicos y los dispositivos con sistemas de reconocimiento facial. La finalidad es conocer el acceso, usabilidad y la capacidad de los dispositivos para obtener su máximo rendimiento e integración con las plataformas vigentes en ASInf.

BAI05 facilita el cambio organizativo y maximiza la probabilidad de implementación exitosa del cambio en ASInf con riesgo reducido durante el ciclo de vida completo. El nivel de capacidad del proceso no alcanza su propósito. BAI05.01. La Dirección General Ejecutiva (CEO) evalúa el informe sobre los cambios emitidos por Auditoría interna identificando si existe aceptación para el cambio, los riesgos e insatisfacciones.

BAI05.02. La Dirección de Informática (CIO) y la Gerencia de Desarrollo gestionan los cambios asociados a la tecnología, comunican e implementan junto con los proveedores externos de servicios de TI para que los cambios sean exitosos.

BAI05.03. La Dirección General Ejecutiva (CEO) informa a los entes del GCABA y a su estructura interna que ASInf desea ser una organización pública innovadora que impulsa el bienestar y la inclusión social de los ciudadanos a través de TI.

BAI05.04. La Dirección de Recursos Humanos concientiza a los recursos humanos para desarrollar la visión, compensación, ascensos de los agentes, reclutamiento y contratación para cubrir los puestos vacantes. Fomenta la obtención de los beneficios asociados con la visión e incentiva a los líderes de cada dirección para la obtención de los objetivos.

BAI05.05. La Subgerencia Ejecutiva de Negocio fomenta los cursos de formación y la transferencia del conocimiento. Establece métricas para medir el éxito en la implementación. Capacita a los responsables para permitir cubrir los cambios culturales y las tendencias de innovación en las soluciones digitales.

BAI05.06. La Subgerencia Ejecutiva de Negocio fomenta el cambio cultural de la innovación tecnológica para la inclusión social de los ciudadanos a través del uso masivo de la tecnología.

BAI05.07. La Subgerencia Ejecutiva de Negocio proporciona capacitación para obtener los beneficios deseados en los sistemas de visión e inteligencia artificial, procesamiento de imágenes en 3D, capturas de imágenes digitales, internet de las cosas, sistemas de reconocimiento facial y de detección temprana de humos con supresión.

BAI06 gestiona los cambios en los procesos de negocio, aplicaciones e infraestructura de forma controlada. El nivel de capacidad del proceso cumple su propósito. BAI06.01. La Subgerencia de Servicios, los entes del GCABA y las direcciones de ASInf que suministran servicios de TI evalúan el impacto negativo que generaría un incidente en la infraestructura de TI, el suministro eléctrico alternativo, almacenamiento, procesamiento, contingencias o recupero. El impacto significativo que pudiera generar en la iluminación ante la aparición de un incidente en los sistemas predictivos de mantenimiento del alumbrado público. La consecuencia poco significativa ante una falla en el sistema de inteligencia artificial aplicado a chatbot en la atención de consultas. El impacto significativo a los entes del GCABA que posean centros de operaciones de TI ante episodios imprevistos en los sistemas de detección temprana de humos. La consecuencia no tan significativa ante un evento inesperado en el reconocimiento facial de los ciudadanos para acceder a los sistemas y aplicaciones. Un impacto de riesgo ante la falla en los sistemas que gestionan la información que envían los microchip y marcapasos implantados en pacientes de riesgo.

BAI06.02. Los cambios de emergencia se evalúan y aprueban de forma preliminar, realizados una vez autorizados y registrados como cambio de emergencia. La solicitud, aprobación y ejecución son formales, mediante el sistema SADE y serán revocados una vez que se haya aplicado el cambio.

BAI06.03. La Dirección de Informática (CIO) categoriza las peticiones de cambio en cada proceso y realiza su seguimiento, si fue rechazado, aprobado sin iniciar, iniciado, en proceso o cerrado. Genera informes de los cambios de estado y métricas de rendimiento que faciliten la revisión. Elabora un historial de avances y antigüedad de las peticiones de cambio, el cierre, plazos y la prioridad prevista.

BAI06.04. Se documentan los cambios en TI respecto de la continuidad de los servicios, almacenamiento, servicio alternativo de procesamiento, logística, contingencias y recupero.

BAI07 administra la aceptación del cambio, la transición y comunica formalmente las nuevas soluciones. El nivel de capacidad observado del proceso es incompleto. BAI07.01. El Comité Estratégico (Desarrollo/Proyectos) de ASInf crea un plan con los recursos necesarios, el soporte en producción y la actualización para

implementar internet de las cosas, sistemas predictivos, detección temprana, visión e inteligencia artificial y reconocimiento facial. Cada sponsor aprueba y acuerda sus proyectos. En cada SLA firmado con los proveedores externos existe el compromiso de participar en la implementación de cada proyecto.

BAI07.02. Se define un plan de migración de los procesos, datos, servicios e infraestructura de TI. Evalúa si la infraestructura actual es óptima para obtener los máximos beneficios en la conexión a internet, infraestructura, sistemas y servidores.

BAI07.03. La Subgerencia Ejecutiva de Negocio documenta cada fase del plan de pruebas de cada proyecto y garantiza los recursos necesarios para probar la infraestructura de TI, sistemas, aplicaciones, acceso a servidores y bases de datos.

BAI07.04. El entorno de pruebas representa la realidad para las cámaras, sensores, incluidos los sistemas de visión artificial, internet de las cosas para prevención médica, sistemas de reconocimiento facial para acceso a los sistemas y aplicaciones del GCABA. Se protege el acceso, conservación y destrucción de los datos sensibles.

BAI07.05. La Gerencia de Desarrollo clasifica los errores ocurridos en las pruebas, corrige y los acepta formalmente. La Subgerencia Ejecutiva de Negocio acuerda con los propietarios de los procesos de negocio, sponsor y terceras partes, la aprobación y documentación formal. La Gerencia de Seguridad de la Información mide las debilidades y efectos de incidentes de seguridad en el plan de pruebas.

BAI07.06. Se ejecuta en paralelo, durante 15 (quince) días, una prueba piloto de los sistemas operativos, aplicaciones, sistemas de gestión de bases de datos, redes e infraestructura vigente en el GCABA, verificando si los resultados obtenidos son los esperados. Asegura que todas las bibliotecas de medios están actualizadas con la versión transferida al entorno de producción, archivando la versión existente y su documentación.

BAI07.07. Los recursos, capacitación y manuales de TI vigentes y de nuevos servicios son brindados por el Comité Estratégico (Desarrollo/Proyectos).

BAI07.08. El Comité Estratégico (Desarrollo/Proyectos) analiza la post-implantación, evalúa los beneficios obtenidos y la satisfacción de los usuarios.

BAI08 gestiona el conocimiento relevante para soportar todas las actividades y servicios de TI en ASInf. El nivel de capacidad observado del proceso es ejecutado. BAI08.01. La Subgerencia Ejecutiva de Negocio de ASInf fomenta la comunicación, compartición y transferencia del conocimiento de nuevas tecnologías como el procesamiento y captura de imágenes digitales, sensores electrónicos, sensores corporales y microchips entre otros.

BAI08.02. La Gerencia de Arquitectura clasifica el formato y categoriza la forma de comunicación de las fuentes de información.

BAI08.03. Se comparten los conocimientos usados para desarrollar los sistemas de reconocimiento facial, procesamiento y captura de imágenes digitales en 3D, sistemas de aprendizaje automático y de algoritmos informáticos para generar sinergia del conocimiento. Se diseña un sistema de gestión de la información del conocimiento (SKMS) basado en los roles y mecanismos de acceso utilizados en ASInf.

BAI08.04. La Gerencia de Arquitectura clasifica la información e identifica a los usuarios potenciales del conocimiento.

BAI08.05. Las direcciones, gerencias y subgerencias comunican a la Gerencia de Arquitectura cual es la información no relevante para considerarla como obsoleta y desafectarla del conocimiento a transferir en ASInf.

BAI09 gestiona los activos durante todo el ciclo de vida para garantizar su aporte a un valor óptimo. El nivel de capacidad del proceso es ejecutado. BAI09.01. La Gerencia de Operaciones de TI registra todos los activos en el sistema SIGAF[52] alineado con los procesos de gestión de cambios y configuración.

BAI09.02. La Gerencia de Operaciones de TI garantiza la existencia de un SLA con los proveedores para los activos que impactan significativamente en los servicios de acceso a internet, servidores, contingencias e infraestructura de TI.

BAI09.03. Se adquieren los activos contemplando la ley 2095/06[49] y ley 70/98[56]. Se identifica su origen, prueba, registro y etiquetado físico. Si el activo es propiedad de un ente del GCABA, se asigna y documenta a través del sistema SADE[40], con aceptación, firma y su registro mediante el SIGAF[52].

BAI09.04. La Dirección de Informática (CIO) determina la razonabilidad de los costos de mantenimiento y opciones más económicas. Se examina si la infraestructura y nuevas tecnologías están vigentes en el mercado o deben ser reemplazadas.

BAI09.05. La Dirección de Informática (CIO) registra las licencias de software adquiridas a terceras partes y sus acuerdos. Compara el número de copias instalado con el número de licencias en propiedad, en caso de ser inferiores, se evalúa su cancelación.

BAI10 gestiona la configuración y define la relación entre recursos y capacidades de TI. El nivel de capacidad observado del proceso es incompleto. BAI10.01. La Gerencia de Operaciones establece el alcance, la gestión de la configuración y sus atributos, tipos de relaciones y códigos de estado.

BAI10.02. La Gerencia de Operaciones de TI identifica, clasifica y registra todos los elementos que constituyen la configuración de los servicios de TI.

BAI10.03. La Dirección de Informática (CIO) identifica todos los cambios en los elementos de configuración y revisa si los cambios propuestos a los elementos de configuración de TI no alteran su integridad y la precisión.

BAI10.04. La Gerencia de Operaciones de TI identifica los cambios de estado de la configuración y lo contrasta con el registro. Recopila los requisitos de información de las direcciones y gerencias y produce informes con los requisitos identificados.

BAI10.05. Los desvíos detectados en las configuraciones físicas y lógicas se comunican a la Gerencia de Arquitectura para accionar correctivamente y revisar la completitud de los datos del registro.

Continuando con las áreas de gestión de ASInf, ahora dentro del dominio entregar, servicio y soporte (DSS), se define **DSS01**, el cual gestiona las operaciones y coordina los procedimientos operativos requeridos para entregar servicios de TI según los estándares planificados. El nivel de capacidad actual de ASInf observado del proceso es ejecutado. DSS01.01. La Gerencia de Operaciones de TI gestiona las velocidades de subida y bajada de archivos, disponibilidad de los sistemas y aplicaciones e interrupciones en la infraestructura de las bases de datos. También para las capturas y el procesamiento de imágenes 3D, velocidades de respuesta y conectividad de los sensores, microchips y marcapasos, sensibilidad, seguridad y confiabilidad de los dispositivos con reconocimiento facial.

DSS01.02. La Gerencia de Operaciones de TI integra los servicios de tecnología, su capacidad, gestión del cambio, configuración, incidentes, problemas, peticiones de servicio, seguridad, continuidad y el rendimiento.

DSS01.03. La Gerencia de Operaciones de TI establece criterios y umbrales de trabajo y clasifica si el evento ocurrido es menor o significativo. Define el filtrado, tratamiento del evento, clasificación, detección y escalado, disparador, alternativas de respuesta y la implementación de las acciones correctivas.

DSS01.04. Un alto porcentaje del equipamiento de los entes que posee el GCABA y centros de procesamiento están protegidos por limitadores de tensión en la red eléctrica, UPS (alimentación ininterrumpida) y grupos electrógenos. El centro de datos de Uspallata N° 3101 no ha podido homologar el estándar internacional TIER 3 por tener alimentación eléctrica de red de un solo proveedor. La norma TIER 3 exige la provisión del suministro eléctrico de 2 (dos) proveedores. El centro de datos recibe alimentación eléctrica por parte de Edesur SA (Empresa Distribuidora de Energía Sur Sociedad Anónima), no siendo posible recibir el suministro de Edenor SA (Empresa Distribuidora Norte Sociedad Anónima) ya que pertenece a otra zona geográfica. Por la ley 14772[62] vigente en el territorio argentino, no es posible obtener el suministro de dos

[62] Ley 14772/58. Energías y Combustibles. Obtenido el año 2019 en la Word Wide Web: https://n9.cl/0b9m2 [Accedido el 27/7/19]

distribuidoras eléctricas ya que el territorio de suministro está geográficamente limitado y no hay superposición en el servicio. El centro de datos ubicado en Av. Independencia N° 635 replica, casi en su totalidad, el almacenamiento de la información del centro ubicado en Uspallata N° 3101, Caba. En ambos existe la política de seguridad física para prevenir, limitar, controlar y resguardar los activos ubicados en las instalaciones. La Dirección de Seguridad de la Información (CISO) documenta y prueba los planes de evacuación, incidentes y alarmas contra fuego, humo y notificaciones.

DSS01.05. La Dirección de Seguridad de la Información (CISO) examina y diagnostica los requisitos de alimentación eléctrica, red, UPS y grupos electrógenos. Prueba periódicamente los mecanismos del sistema de alimentación en días y horarios de mínimo o nulo uso de los servicios, previa comunicación a los afectados. Se registran los días, horarios, responsables y resultados obtenidos en las pruebas.

DSS02 gestiona las peticiones e incidentes de servicio y suministra una respuesta efectiva a las peticiones de los usuarios y la resolución de todo tipo de incidentes. El nivel de capacidad del proceso cumple su propósito. DSS02.01. La Dirección de Informática (CIO) prioriza y clasifica los incidentes y errores conocidos en los sistemas, infraestructura, bases de datos y nuevos servicios. El inicio de contacto es la mesa de ayuda perteneciente a la Gerencia de Soporte a Usuarios.

DSS02.02. La Gerencia de Operaciones de TI genera un registro histórico con los incidentes y peticiones de servicio, según el tipo y categoría.

DSS02.03. Las solicitudes de petición de servicio se realizan mediante el sistema SADE[40] y se verifica si el solicitante posee los derechos necesarios autorizados.

DSS02.04. La Subgerencia de Servicios identifica las probables causas que generen los incidentes y establece la relación con la infraestructura, fallas o configuraciones. Evalúa y registra el evento, verifica si existe relación con incidentes conocidos registrados en la base de datos (KEDB).

DSS02.05. La Subgerencia de Servicios soluciona el incidente, ya sea permanente o temporal, en el último caso, registra y documenta la acción.

DSS02.06. La Gerencia de Operaciones de TI cierra la petición del incidente y obtiene el conforme por parte del solicitante.

DSS02.07. La Gerencia de Operaciones de TI verifica si el estado del incidente fue cumplimentado, escalado o solucionado. Analiza si posee tendencias definidas, patrones recurrentes o infracciones del proveedor en el Acuerdo de Nivel de Servicio.

DSS03 gestiona los problemas e identifica sus causas para brindar soluciones. El nivel de capacidad del proceso cumple su propósito. DSS03.01. La Subgerencia de Servicios supervisa todos los problemas y el acceso a los datos relevantes, sistema de gestión de cambios y los detalles de incidentes sobre la configuración y activos de TI. Define los equipos de soporte según el problema, su categorización y la solución. Si el incidente es generado por el incumplimiento de un SLA de un proveedor, lo registra en el catálogo de gestión de problemas.

DSS03.02. Se verifica si el incidente recibido existe en la base de datos y compara los datos del incidente con la base de datos de errores conocidos y lo categoriza. Genera informes, comunica el progreso de la resolución del problema y monitorea el impacto.

DSS03.03. La Gerencia de Operaciones de TI identifica el problema que genera el incidente, evalúa y procesa la gestión de cambios, el impacto en los servicios de TI y su solución. Los servicios críticos son priorizados y el costo-beneficio evaluado.

DSS03.04. El registro de cada problema es cerrado al obtener la solución definitiva o porque se gestiona una solución alternativa. La Subgerencia de Servicios actualiza el proceso de resolución a través de informes periódicos de gestión, impacto de los incidentes y confirmación de la resolución satisfactoria.

DSS03.05. La Subgerencia de Servicios recopila información de los incidentes de tecnología de innovación y profundiza el conocimiento específico con proveedores externos expertos. Optimiza el uso de los recursos y reduce las soluciones temporales.

DSS04 gestiona la continuidad y establece un plan para responder a incidentes en servicios. El nivel de capacidad del proceso es ejecutado. DSS04.01. La Dirección de Operaciones (COO) identifica si la interrupción en la continuidad es generada por

proveedores externos. Para ello verifica si se cumplen las metas y el alcance mínimo acordado en la política de continuidad del negocio.

DSS04.02. La Dirección de Operaciones (COO) mitiga el riesgo mediante una infraestructura con suficiente resiliencia en los centros de datos. Para el caso que uno de los dos centros de datos sea afectado en la totalidad, los servicios se suministran desde el otro centro. El tiempo de recuperación de los servicios no excedería el 10% como máximo de lo planificado. Los proveedores externos brindarían soporte para el acceso a internet, servidores, contingencias, recuperación y los servicios asociados a los sistemas de administración y comunicación de la infraestructura de TI en ASInf. El centro de datos de la calle Uspallata N° 3101 goza de una disponibilidad del 99,98 % para el suministro de sus servicios de TI. En Av. Independencia 635 debe actualizarse la infraestructura de telecomunicaciones, el cableado horizontal, armarios y asegurar la totalidad de los accesos redundantes.

DSS04.03. La Subgerencia de Continuidad de Negocio establece y documenta a los proveedores externos, las acciones de contingencia, logística, recupero, responsables y plazos máximos de reanudación. Documenta la información para asegurar el acceso al back up en disco duro, acceso a software y sistemas para procesar.

DSS04.04. La Subgerencia de Continuidad de Negocio acuerda y comunica los días, horarios y plazos de pruebas que generen una mínima disrupción en los servicios provistos. Al finalizar las pruebas, evalúa los logros y acciones correctivas necesarias.

DSS04.05. La Dirección de Operaciones (COO) revisa cada 6 (seis) meses el plan de continuidad y capacidad. Evalúa si es necesario recomendar cambios en las políticas, procesos, infraestructura, roles, y acuerdos con proveedores externos.

DSS04.06. La Subgerencia de Continuidad de Negocio promueve los cursos de formación para agentes de ASInf, de los entes del GCABA y proveedores externos según su rol y responsabilidad en TI.

DSS04.07. La Gerencia de Operaciones de TI define que las políticas de las copias de seguridad son automatizadas en línea con la localización física y lógica de las fuentes de los datos, crea registros, derechos de acceso y cifrado. Para los datos de los sistemas a conservar por larga duración, el servicio se acuerda con los entes del

GCABA, se establecen copias de seguridad diaria o semanal, incremental y en DVD-ROM con localización física. Las actividades se desarrollan en el centro de datos de Av. Independencia Nº 635 y su almacenamiento en discos en espejo en tiempo real en el centro de datos de la calle Uspallata Nº 3101, Caba. Los sistemas, aplicaciones, datos y documentación almacenados o procesados por proveedores serán respaldados con una copia semanal e incremental en el centro de datos de la calle Uspallata Nº 3101, Caba. Se prueban y documentan semestralmente las copias de seguridad archivadas.

DSS04.08. La Subgerencia de Continuidad de Negocio analiza si el acceso a la localización física y servidores, logística, traslados y equipos, están acordes a lo planificado. Evalúa debilidades u omisiones en el plan y acciona correctivamente.

DSS05 gestiona los servicios de seguridad, protege la información de ASInf y mantiene un nivel de riesgo de seguridad de la información. El nivel de capacidad del proceso cumple su propósito. DSS05.01. La Dirección de Seguridad de la Información (CISO) concientiza sobre los riesgos e impactos del software malicioso. La Gerencia de Operaciones de TI activa AVG Antivirus para la protección contra el software malicioso en las estaciones de trabajo, servidores, dispositivos móviles y sistemas con bases de datos. La actualización se realiza automáticamente. La Gerencia de Seguridad de la Información asesora sobre amenazas por virus, gusanos, troyanos y espías. Los agentes de ASInf y entes del GCABA con cuentas de correo y acceso a internet firman el acuerdo de política de uso de correo y de internet.

DSS05.02. La Dirección de Seguridad de la Información (CISO) crea y otorga los perfiles de usuario solicitados por los directores autorizados, con sus contraseñas con un mínimo de 8 (ocho) caracteres, que no contengan datos asociados al usuario, compuesto por letras mayúsculas, minúsculas, números y caracteres especiales. En el caso de no utilizar el perfil durante 60 días, es bloqueado y debe solicitarse formalmente el blanqueo de la clave. La transmisión y recepción de la información se realiza en forma cifrada para asegurar los datos.

DSS05.03. La Dirección de Seguridad de la Información (CISO) gestiona la configuración de los sistemas operativos deshabilitando las carpetas compartidas no utilizadas, asegurando la creación de perfiles de usuario con privilegios restringidos y no habilitando la ejecución automática de los dispositivos de almacenamiento

extraíbles. Garantiza la instalación de las últimas versiones en los sistemas operativos, configura el sistema para que se permitan ver los archivos ocultos, evita la instalación de archivos maliciosos ocultos y configura la visualización de las extensiones de archivos evitando ser víctima de técnicas como la doble extensión. El acceso físico a los centros de datos es custodiado por recursos humanos capacitados y provistos por registros de personal con autorización de ingreso. Además, existe el control digital y biométrico en cada acceso, autorizando sólo al personal de operaciones a los sectores de almacenamiento. Los entes del GCABA y proveedores externos que gestionan información del GCABA están obligados a implementar las políticas de seguridad física. La política de acceso remoto mediante dispositivos externos debe estar justificada y autorizada formalmente por el director a cargo del área en la que desarrolla las tareas el agente solicitante. El horario de acceso, fuera del horario normal laboral y su ubicación física, deben estar justificados con las tareas propias de sus funciones. La baja de un dispositivo obsoleto genera la destrucción de su información.

DSS05.04. Los entes del GCABA solicitan la creación del perfil de usuario y nivel de acceso por solicitud formal del director a cargo del área a la Dirección de Seguridad de la Información (CISO) que gestiona los cambios de derechos de acceso, modificación o eliminación a través de solicitudes aprobadas y documentadas. Asimismo, revisa las cuentas y sus privilegios dejando una pista de auditoría de los accesos a la información según la ley 104/98[32] y 1845/05[33].

DSS05.05. Todos los ingresos a los edificios, centros de datos y operaciones de ASInf, entes del GCABA y proveedores externos con información del GCABA respetan la política de seguridad física. Las peticiones de acceso a las instalaciones de procesamiento son formales, solicitadas por directores autorizados del área y registradas por sistema. La Dirección de Seguridad de la Información (CISO) elabora formularios de ingreso que identifiquen al individuo y su acceso autorizado a una zona definida, incluso para terceros por tareas eventuales. No existen autorizaciones a las áreas donde no se desempeñen funciones afectadas a su rol. El recurso humano ingresa mediante tarjeta o placa. Los dispositivos que registren el acceso, ante un intento de acceso no autorizado disparan una alama. Las placas, tarjetas llaves o escáneres biométricos, se conectan y configuran a la base de datos de registros de ingresos autorizados, la cual está formalizada y en línea.

DSS05.06. La Dirección de Informática (CIO) asigna el acceso a documentos sensibles y dispositivos de salida. La Gerencia de Operaciones de TI gestiona un inventario de dispositivos de salida, documentos sensibles y define los espacios según la política de seguridad física de ASInf. Los puertos de salida de las estaciones de trabajo y dispositivos móviles con acceso a la información crítica o sensible se configuran de forma tal que la extracción de datos sea bloqueada. Se crea y comunica un procedimiento para destruir por obsolescencia o falta de funcionamiento, los dispositivos de almacenamiento de datos, CD y memorias.

DSS05.07. La Dirección de Seguridad de la Información (CISO) registra los eventos de TI mediante tickets, en forma cronológica, identificado por usuario y recurso usado. Los usuarios no poseen permiso de modificación de los archivos de configuración ni el acceso a las funcionalidades para deshabilitar la grabación de los registros de los eventos. El resguardo de registro de los eventos es independiente de la información de producción. El propietario de la información puede acceder sólo con permiso de lectura al archivo de resguardo del registro del evento. Auditoría Interna de ASInf puede acceder a los registros de resguardo de eventos y el registro de todo tipo de evento de TI se resguarda como mínimo por 5 (cinco) años.

DSS06 gestiona los controles de proceso de negocio garantizando los servicios de TI de ASInf que satisfagan los requisitos relevantes para el control de la información. El nivel de capacidad del proceso cumple su propósito. DSS06.01. La Subgerencia Ejecutiva de Negocio coordina las interrupciones por mantenimiento de la infraestructura. Evalúa el cumplimiento del requerimiento solicitado para el procesamiento de las imágenes, sensores corporales y microchips para los sistemas de prevención médica en pacientes de riesgo.

DSS06.02 La Subgerencia Ejecutiva de Negocio integra los datos mediante el procesamiento analítico en línea, monitorea los centros de datos, aumenta el número de conexiones del servidor y del cliente y administra la disponibilidad y el rendimiento de los servicios.

DSS06.03. Para gestionar los usuarios existe un solo administrador y otro agente autorizado con capacidad de cubrir su rol ante urgencias. Para el desarrollo de sistemas, sólo el director de la Gerencia de Desarrollo tiene la autorización para habilitar al

sistema para el paso de ambientes. La puesta en producción es autorizada por la Dirección de Informática (CIO). La asignación de los atributos o la creación de nuevos perfiles son definidas por el director del área solicitante por pedido formal mediante SADE[40]. Para la asignación de los atributos de los perfiles existentes, el director menciona en su pedido el puesto a ocupar, de manera que el administrador pueda crear el perfil con los atributos ya definidos. Para el caso de la creación de un nuevo perfil, el director del área define junto con el administrador, los derechos de acceso, niveles, recursos tecnológicos a los que podrá acceder y los atributos con sus plazos de vigencia sin superponer las funciones.

DSS06.04. La Gerencia de Arquitectura revisa los errores, excepciones y desviaciones detectadas en la definición del perfil de usuario. Evalúa los derechos de acceso a sistemas, recursos y sus niveles. Define si posee acceso a los sistemas de reconocimiento facial con permisos de reconfiguración, capturas de imágenes digitales y al procesamiento de imágenes en 3D con modificación y borrado.

DSS06.05. La información de las bases de datos y transacciones bancarias se almacena como mínimo por 10 (diez) años. El tiempo de almacenamiento de los eventos de TI posee un mínimo de 5 (cinco) años. La Gerencia de Arquitectura captura la fuente de información, evidencia y registro. Se establece la conservación de la fuente de información en un plazo mínimo de 5 (cinco) años.

DSS06.06. La Gerencia de Arquitectura de ASInf sólo permite la consulta de información sensible a los agentes de los equipos asignados. La modificación o eliminación de datos sensibles sólo está autorizada a los jefes de equipos y directores. Para los agentes del equipo está permitida sólo la consulta de información por pantalla, estando prohibida la consulta con acceso remoto. No está autorizada la impresión ni extracción a través de los dispositivos de almacenamiento.

Continuando con la gestión de tecnología, se desarrolla el dominio Supervisar, Evaluar y Valorar, **MEA01**, el cual supervisa, evalúa el rendimiento y la conformidad de las métricas y objetivos de TI en ASInf. El nivel de capacidad del proceso actual en ASInf es incompleto. MEA01.01. La Dirección General Ejecutiva (CEO) identifica a los sponsors de los proyectos. Se establecen plazos trimestrales para los cambios que demanden desarrollos de servicios de TI con baja demanda y plazos semestrales para los

cambios con alto requerimiento del recurso humano en innovación tecnológica. Para los servicios de TI vigentes, lanzados en el último año, las reuniones serán semestrales y anuales para aquellos con más de un año de operación.

MEA01.02. La Subgerencia Ejecutiva de Negocio evalúa el cumplimiento de la disponibilidad de internet, horas fuera de línea y las velocidades de subida y bajada de archivos. Analiza, si con los recursos propios pueden estar disponibles los sistemas y aplicaciones las 24 horas. Si la capacidad de almacenamiento cubre los requisitos solicitados y satisface las contingencias y recuperación según lo planificado.

MEA01.03. La Dirección de Informática (CIO) revisa si las respuestas alternativas en los servicios de TI generaron las ventajas deseadas. Evalúa si las propuestas de adquisición de software y hardware generaron las mejoras previstas.

MEA02 supervisa, evalúa y valora el sistema de control interno. Monitorea el entorno de control identificando deficiencias. El nivel de capacidad del proceso actual no alcanza su propósito. MEA02.01. Auditoría interna y los órganos de control externo emiten informes con observaciones y recomendaciones que deben ser tenidos en cuenta. Se establece un plan de acción de 4 (cuatro) años, auditando una vez por año los procesos clasificados como de muy alto riesgo y como mínimo una vez a lo largo del plan a los procesos de muy bajo riesgo. En caso de desviaciones se aplican acciones correctivas.

MEA02.02. La Subgerencia Ejecutiva de Negocio identifica los controles clave a través de diversos softwares, monitoreando la infraestructura de los centros de datos, gestionando las bases de datos, administrando la infraestructura y el almacenamiento. Administrando el respaldo, recuperación, configuración y la administración de las computadoras en forma automatizada.

MEA02.03. La Dirección de Informática (CIO) promueve la realización de autoevaluaciones de control en forma semestral y las compara con las metas de ASInf. Se confrontan los resultados de los informes elaborados por Auditoría interna de ASInf y los órganos de control externo.

MEA02.04. La Dirección de Informática (CIO) comunica las deficiencias o excepciones, tales como exceder el plazo de 3 (tres) años para la puesta en marcha de

nuevas tecnologías. También, la continuidad de la vigencia de una cuenta de usuario sin uso por más de 60 días, o que el plazo entre reuniones de supervisión con los sponsors para proyectos en desarrollo sea mayor a 3 (tres) meses. Las excepciones requieren justificación y comunicación a la Dirección General Ejecutiva (CEO).

MEA02.05. La Dirección de Privacidad de la Información garantiza que los proveedores externos cumplan con las Normas éticas según la Resolución Nº 205/SGCABA/16[60] y la conveniencia de tener certificados en estándares internacionales de tecnología.

MEA02.06. La Dirección General Ejecutiva (CEO) prioriza los procesos con clasificación de nivel de muy alto riesgo y su relación con los servicios de TI. Valora la capacidad de aseguramiento del proveedor y estima el impacto del proceso con el servicio, su criticidad y la relación con los objetivos.

MEA02.07. Auditoría interna gestiona el aseguramiento de TI con las direcciones, gerencias y subgerencias, proveedores externos y entes. Los datos se recopilan en forma automatizada mediante software de monitoreo del servicio. Si existe la posibilidad de obtener los datos de cumplimiento o rendimiento con recursos humanos o software complementario aprobado formalmente, se utiliza.

MEA02.08. Auditoría interna aplica los controles aprobados para validar, contrastar los hallazgos y su eficiencia. Para el caso en el que los controles no suministren los resultados satisfactorios, define acciones para identificar el riesgo residual y comunicarlo. Examina y documenta si los controles claves para las tecnologías innovadoras permiten acceder, detectar y controlar las falencias.

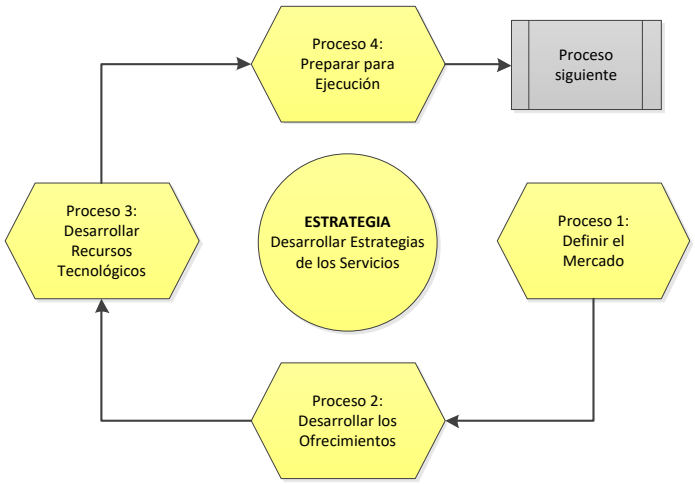
MEA03 supervisa, evalúa y valora la conformidad con los requisitos externos y analiza el cumplimiento de las normas regulatorias. El nivel de capacidad actual del proceso en ASInf cumple su propósito. MEA03.01. La Subgerencia Ejecutiva de Negocio garantiza el cumplimiento de las leyes aplicables a ASInf y a los entes del GCABA. Valora su cumplimiento, impacto sobre TI y datos de los entes del GCABA.

MEA03.02. Ante la detección de incumplimientos, la Subgerencia Ejecutiva de Negocio coordina acciones correctivas con las direcciones, gerencias y subgerencias de ASInf, proveedores externos y entes del GCABA.

MEA03.03. La Dirección de Privacidad de la Información gestiona el cumplimiento de la normativa vigente por parte de ASInf, evalúa periódicamente los procesos de TI y ante la detección de desvíos, establece acciones correctivas y plazos para su resolución.

MEA03.04. Auditoría interna de ASInf supervisa el cumplimiento de la normativa vigente y confecciona informes con los incidentes de incumplimiento, investiga las causas e informa a los comités para la implementación de acciones correctivas. En el caso de incumplimiento reiterado, aplica infracciones.

Es importante destacar que el enfoque que brinda ITIL no está orientado a la administración de los proyectos, crear productos ni servicios, sino que es un conjunto de mejores prácticas que se enfoca en la entrega de los servicios habilitados por las TI. En este capítulo se desarrollan los primeros once procesos de ITIL v3, definidos como etapa 1. Por ello, en este trabajo se busca complementar a COBIT 5 con ITIL v3. Este último posee cinco fases del ciclo de vida del servicio: estrategia, diseño, transición, operación y mejora continua, desarrolladas en 46 (cuarenta y seis) procesos. La siguiente *figura 10* detalla la *Fase 1, estrategia de servicios*.



Fuente: Diseño propio [63]

En el **proceso 1, definir el mercado,** se establecen los nuevos servicios provistos por ASInf, detallados anteriormente. El mercado está comprendido por toda aquella persona que utilice cualquier servicio de los mencionados, ofrecido al usuario final o a través de un ente dependiente del GCABA. ASInf provee valor en sus servicios incrementando la inclusión digital y facilitando la conectividad para el uso masivo de la tecnología de la información. Los potenciales usuarios de ASInf son aquellos que utilicen sus servicios, no importando su lugar de residencia. Los servicios provistos no exigen la diferenciación de la competencia para incrementar la participación en el mercado o mantener la existencia a largo plazo, aunque se brindan con eficiencia ya que son generados a través de recursos estatales. Los servicios suministrados por ASInf no tienen competencia en el mercado a excepción del servicio de internet en lugares

[63] Contenido extraído de ITIL v3. Obtenido en Diciembre de 2010 en la Word Wide Web: https://n9.cl/pkz6 [Accedido el 20/9/19]

públicos, también brindado por empresas privadas. La siguiente *matriz 1*, *FODA* permite obtener un diagnóstico y tomar las decisiones estratégicas oportunas que produzcan una mejora futura.

Análisis Interno	
Fortalezas	**Debilidades**
➢ Dependencia directa del usuario en algunos sistemas y aplicaciones. ➢ Estructura organizacional que permite la planificación del desarrollo de los servicios a escala minimizando sus costos. ➢ Presupuesto asignado elevado. ➢ Centro de datos ubicado en la calle Uspallata con alta capacidad y moderna estructura tecnológica. ➢ Personal técnico capacitado y equipos asignados a diversas ramas tecnológicas.	➢ Algunos agentes técnicos no poseen estabilidad en su relación laboral. ➢ Algunos agentes pueden estar desmotivados para realizar sus tareas. ➢ Lentitud en la capacitación de los sistemas y aplicaciones específicas del organismo para los agentes ingresantes. ➢ El formulario de requerimientos de servicios o proyectos es incompleto. ➢ Algunos procesos no se encuentran apegados a los estándares internacionales vigentes. ➢ El gobierno y la gestión del organismo tienen superposición funcional en la actual estructura organizativa.

Análisis Externo	
Oportunidades	**Amenazas**
➢ Nichos de mercados de nuevas tecnologías inexplorados. ➢ Mejorar el bienestar y aumentar la inclusión social de los ciudadanos a través del uso masivo de la tecnología. ➢ Expandir geográficamente los diversos puntos de conectividad a internet. ➢ Existe una gran cantidad de organismos, universidades y empresas privadas interesadas en participar y apoyar el desarrollo de TI con el GCABA.	➢ Cambios tecnológicos bruscos a nivel mundial. ➢ En ciertos lugares la infraestructura de la red eléctrica es obsoleta y puede impactar en los servicios de TI. ➢ Legislación vigente que no permite el suministro eléctrico simultáneo opcional con dos proveedores. ➢ Obsolescencia rápida de los recursos tecnológicos adquiridos.

Fuente: Elaboración propia

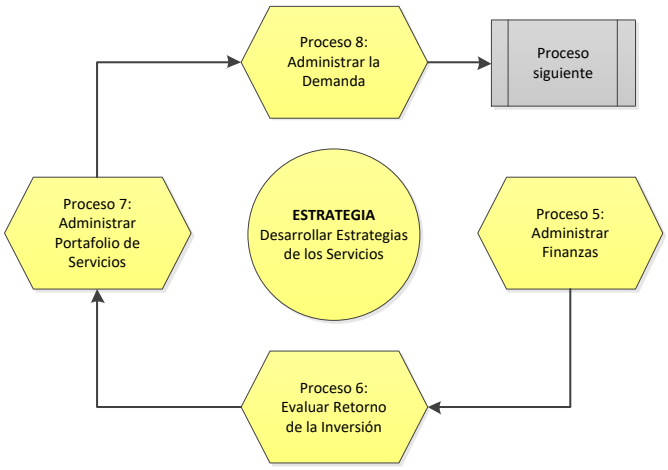
En el **proceso 2, desarrollar los ofrecimientos**, se define que todos los servicios del GCABA serán brindados en forma íntegra y centralizada a través de ASInf y los proveedores externos actuarán solamente como soporte. Se proyecta evaluar nuevas tecnologías con cada ministerio y su aporte de valor. Con el Ministerio de Salud de Caba con internet de las cosas para ser aplicado en prevención médica a pacientes de

riesgo mediante la implantación de microchips y marcapasos. ASInf junto con la Dirección General de Tránsito y Transporte de Caba, analizan el desarrollo de sistemas de visión artificial para ser aplicado en las calles de la ciudad para predecir accidentes de tráfico. La Dirección de Informática de ASInf propone a la Dirección de Atención Ciudadana de Caba la posibilidad de implementar sistemas de reconocimiento facial de los ciudadanos para acceder de manera segura a los sistemas y aplicaciones de GCABA. ASInf ofrece a los entes del GCABA que posean centros de operaciones de TI, la implementación de sistemas de detección temprana de humos con sistema de supresión. La implementación para la Dirección General de Atención y Cercanía Ciudadana de los sistemas de inteligencia artificial aplicados a chatbot para atender las consultas sobre el uso de TI por parte de los entes del GCABA y de los ciudadanos. También consulta a la Dirección General de Alumbrado Público de Caba sobre la posibilidad de implementar sistemas predictivos de mantenimiento del alumbrado público. El **proceso 3**, utilizado para **desarrollar los recursos tecnológicos**, crea una tabla de correlación de los servicios y recursos de TI y establece los recursos necesarios para desarrollar adecuadamente cada servicio. Teniendo en cuenta que ASInf actualmente provee servicios a través de recursos propios apoyados por terceros, se confecciona una tabla con los parámetros para establecer la necesidad o no de adquisición o renovación de los recursos afectados para brindar los nuevos servicios de TI. Se considera que el presupuesto total estimado para el desarrollo de servicios innovadores en ASInf no debe ser menor al 10% del presupuesto total asignado al organismo. La siguiente *tabla 2* representa los *Parámetros de correlación de servicios y recursos de TI*.

	Adquirir conocimientos en nuevas tecnologías	Nuevos proveedores externos	Adquirir nuevos dispositivos	Modernizar la infraestructura de comunicaciones	Expandir la infraestructura informática	Actualizar las redes telefónicas	Computación en nube	Recursos Humanos técnicos	Servicio de videoconferencia	Sistema de gestión de contenido (web, portal soporte)	Sistema de gestión de relaciones con los usuarios
Servicios provistos por ASInf.											

Fuente: Elaboración Propia

El **proceso 4**, denominado **preparar para la ejecución**, es el modelo de estrategia de servicios que considera la misión y visión para apoyar los objetivos estratégicos de ASInf, se define la estrategia de los servicios de TI mediante la aplicación del Modelo de las 4 Ps de Mintzberg. La *Perspectiva* establece las ya mencionadas metas de TI. La *Posición* de ASInf con los servicios provistos en el mercado es dominante. Sólo el servicio de provisión de internet en lugares públicos también es brindado sin costo por algunas empresas privadas. La *Planificación* de ASInf viene definida desde la Jefatura de Gabinete de Ministros. Se planifica la proyección de la innovación tecnológica, el incremento de los puntos de acceso a internet y la expansión geográfica de los servicios para la inclusión de nuevos usuarios. El *Patrón* de contacto formal de ASInf, es a través de sus responsables, con los proveedores y los entes del GCABA. Genera reuniones, requerimientos y solicitudes digitales por sistemas formales como SADE[40]. El Plan Estratégico de ASInf impulsa la implementación de programas tecnológicos a través de políticas que promueven la inclusión digital y facilitan la conectividad a través de la innovación. La *cadena de valor* está compuesta por las actividades principales y los vínculos que relacionan los eslabones para la prestación de los servicios de TI tales como: adquisición de hardware (computadoras, dispositivos de almacenamiento, servidores, dispositivos de control y acceso), adquisición de infraestructura (módems, switches y routers para redes), adquisición de instalaciones y servicios públicos (oficinas, centros de datos, y servicios públicos) y adquisición de software (enlatado o personalizado). También mediante el desarrollo de sistemas, aplicaciones y servicios (prueba, implementación, distribución, soporte y actualización) y usuarios (entes o finales). La política de gestión de riesgos tecnológicos de ASInf está compuesta por la estructura de la tecnología de la información (áreas, funciones y recursos), planificación de TI (planes, adquisición, presupuestos, inversiones y cultura organizacional de seguridad), operación de TI (gestión física, lógica, licencias, accesos, comunicaciones y usos) y servicios prestados por proveedores externos (SLA). También están incluidos el riesgo (identificación, medición, monitoreo y divulgación), planes de contingencia, procesos para recuperación de desastres, continuidad de las operaciones, seguridad de la información y soporte de operaciones. A continuación, la *figura 11* expresa la *Fase 2, estrategia de servicios.*



Fuente: Diseño propio [63]

El **proceso 5**, llamado **administrar las finanzas**, describe el manual de políticas de costos asociados a cada servicio, está compuesto por el recurso humano (personal ejecutivo, técnico y administrativo), hardware (computadoras, dispositivos de almacenamiento, servidores, impresoras, dispositivos de control y acceso), software (programas, licencias, sistemas operativos y aplicaciones), infraestructura (redes, módems, switches y routers), instalaciones (oficinas, centros de datos y servicios públicos), servicios externos (servicios de seguridad para el acceso físico a las instalaciones, servicios de recuperación de desastres y servicios de logística para el traslado durante los incidentes técnicos) y transferencias (costos internos asociados a otros centros de costos que son distribuidos dentro de ASInf). Habiendo definido que todos los servicios son centralizados y provistos por la agencia, es necesario conocer cuál sería el costo si fuese suministrado por un proveedor externo, solamente como modelo de comparación. La clasificación de los elementos que componen los costos son: costos fijos (no varían por un factor determinado, no asociados a su forma o tiempo de uso), costos variables (varían según un factor, asociado a su forma o tiempo de uso), costos operativos (asociados a la ejecución diaria de los servicios de TI), costos directos (pueden ser atribuidos directamente a un servicio suministrado a un ente del GCABA). También están los costos indirectos (incurridos por brindar un servicio a través del cual no se puede individualizar su costo) y costos de capital (provienen de la amortización del material inmovilizado o inversiones a largo plazo).

ASInf provee sus servicios en forma gratuita, sólo se calculan los costos para estimar si el presupuesto los cubre adecuadamente. El contenido y las etapas del presupuesto de ASInf son la programación (planeamiento y asignación de los diferentes

pliegos presupuestarios según la estructuración de su gasto), formulación (después de estimar los gastos y contrastarlos con los recursos disponibles, se estructura el presupuesto con los montos a gastar según los objetivos y metas). Luego, la aprobación (se remite al Poder Ejecutivo para su aprobación), ejecución (etapa en la que se realizan los gastos según la programación realizada) y evaluación (se analizan los resultados de la gestión y monitorea la existencia de desvíos). Ante una reformulación de partida presupuestaria, el Comité Ejecutivo Estratégico de TI aprueba los cambios generales en el presupuesto de TI. Las variables a considerar para el análisis de los costos por servicio son usuario (número, tipo, licencias en uso y servicios utilizados), licencia (número, tipo, proveedor del servicio y cantidad de usuarios), costos de mantenimiento del centro de datos (recurso humano, software, hardware, licencias, infraestructura, cantidad de usuarios, cantidad de servicios, servicios públicos, seguridad para el acceso y pólizas de seguro). También existen los mecanismos de distribución (recurso humano, logística e infraestructura tecnológica) y procesamiento y almacenamiento (servicios públicos, seguridad para el acceso, software, hardware, licencias, infraestructura, tipo de servicio, cantidad de usuarios, cantidad de servicios, cantidad de dispositivos, tipos de contingencias, mantenimiento edilicio y pólizas de seguro). Es importante analizar los componentes del impacto por el uso de la tecnología en los servicios de ASInf para evaluar su aceptación o rechazo, tales como la exclusión social por falta de acceso a la tecnología, exposición de la privacidad, carencia de protección de la propiedad intelectual, falta de control de confidencialidad y anonimato.

La Subgerencia de Servicios es la responsable de la confección de los contratos con los proveedores, SLA (Acuerdo de Nivel de Servicio) siendo asesorada técnicamente por la Dirección de Informática (CIO). El documento contiene la definición del servicio, objetivos, propuestas, fecha de comienzo, partes del acuerdo, duración, exclusiones, ámbito de trabajo, plazo de cobertura, mantenimiento, revisiones y validaciones de los servicios. También la definición, la gestión y escalabilidad de los problemas, gestión financiera, gestión de cambios del servicio, desarrollo, indicadores y monitorización. Incluye los umbrales mínimos y máximos de tolerancia del servicio y su disponibilidad, términos para el pago, intereses y multas por pago atrasado y rescisiones por incumplimiento. La capacitación de usuarios, acuerdos e información, normativa legal y derechos de la propiedad intelectual deben estar presentes. Comprende la formalización de la inscripción de la base de datos con información

sensible, derechos de confidencialidad, acuerdo de conformidad legal, procesos de resolución de conflictos, finalización, entrega y conformidad. El inventario de existencias de hardware se clasifica por su dirección IP asociada, nombre del usuario, marca, modelo, tipo, espacio total en disco, espacio disponible en disco, ubicación física, fecha de instalación y número de serie. Se elabora un inventario de existencias de software que se clasifica por nombre, fecha de instalación, versión, desarrollador, tipo de procesamiento, ubicación física, lenguaje, número de usuarios, fecha de instalación, número de licencias y descripción.

El **proceso 6**, responsable de **evaluar el retorno de la inversión**, establece el desarrollo de nuevos servicios mediante innovaciones en TI planteadas anteriormente, las que van en línea con los objetivos estratégicos de ASInf. Sin dudas, el organismo no persigue el objetivo de maximizar el retorno de la inversión, ya que fue creado persiguiendo otras metas, pero es importante que el Comité Estratégico (Desarrollo/Proyectos) sea el responsable de evaluar los nuevos servicios y sus beneficios, riesgos, costos e impacto financiero. ASInf adquiere hardware, software, cámaras, sensores, marcapasos y microchips. Para analizar su rendimiento, durante todo su ciclo de vida, es esencial registrar su fecha y costo de adquisición, costo de operación y actualización, mantenimiento, fecha de baja, servicio afectado, % de afectación al servicio y los beneficios obtenidos.

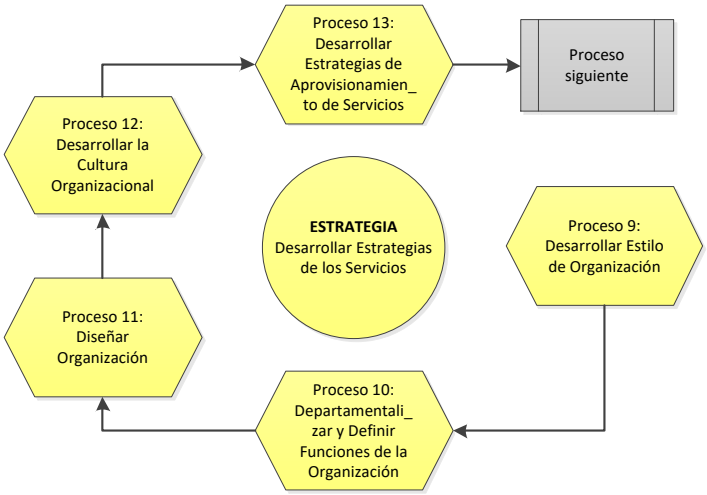
El **proceso 7**, a cargo de **administrar el portafolio de servicios**, gestiona el portafolio eficientemente, ya que es importante evaluar la demanda futura para proyectar las inversiones necesarias. Según el presupuesto asignado, se realizan inversiones para Mantener el Servicio (RTB) en aquellos en los que a corto y mediano plazo no se detecta un alto incremento de la demanda, tales como el mantenimiento y actualización del correo de los organismos del GCABA, provisión de puntos de presencia de wifi en eventos GCABA o la registración de incidentes y provisión de soporte. Para servicios en los que se detecta un incremento en la demanda se realizan inversiones para hacer Crecer el Servicio (GTB), como desarrollos de sistemas y aplicaciones, base de datos o la gestión de la infraestructura, hardware y software de los centros de cómputos. Para los que se pretende Transformar el Servicio (TTB) o desarrollar nuevas TI, se asignan las mayores inversiones, tales como sistemas predictivos, inteligencia y visión artificial, reconocimiento facial e internet de las cosas.

Administrar la Demanda es el objetivo del **proceso 8**, a través del Comité Ejecutivo Estratégico de TI, responsable de gestionar la demanda de los servicios. Para administrar la demanda se analiza la infraestructura de TI que apoya el suministro de los servicios y realiza un mantenimiento sin intervención de sus componentes. La infraestructura que soporta el desarrollo de los sistemas predictivos, inteligencia y visión artificial, reconocimiento facial o internet de las cosas, se proyecta a largo plazo, definido a tres años. Se plantea una tecnología para la infraestructura a mediano plazo para la creación de puntos de red, contingencia por cortes de suministro de energía o catástrofe y administración de los servidores, entre otros. La infraestructura a corto plazo soporta servicios de TI tales como el servicio de videoconferencia, registración de incidentes, provisión de soporte y los servicios de telefonía del GCABA. En cada servicio de TI ofrecido se detalla, para cada agente, un perfil de usuario por servicio. Cada usuario, en cada servicio cuenta con diversos privilegios y roles: usuario local, usuario móvil o usuario temporal, con capacidades para leer, leer y escribir, modificar o ser administrador. Asimismo puede tener acceso a la red, a los recursos, ser administrador, importador o exportador de la base de datos. Los servicios están cubiertos por paquetes (Pack) que definen su disponibilidad, capacidad, continuidad y seguridad. La diversidad y el nivel de cobertura de los servicios de TI que cada ente necesita son muy variados. Si bien ASInf no percibe ingresos por sus servicios, cada ente debe solicitar el nivel de servicio mínimo y necesario para desarrollar sus actividades con eficiencia, definiendo uno de los tres niveles posibles en la siguiente *tabla 3, Garantía del servicio*.

Garantía del Servicio	Pack 1	Pack 2	Pack 3
Disponibilidad	24 horas x 365 días	24 horas de lun a sáb	24 horas de lun a vie
Capacidad	Capacidad de almacenamiento alta Banda ancha prioritaria	Capacidad de almacenamiento media Banda ancha prioritaria	Capacidad de almacenamiento básica Banda ancha básica
Continuidad	Copia de seguridad y restauración - Soporte in situ y remoto	Copia de seguridad y restauración - Soporte in situ y remoto	Copia de seguridad y restauración - Soporte in situ
Seguridad	Factor de autenticación múltiple Red privada virtual y Token	Factor de autenticación múltiple Red privada virtual y Token	Factor de autenticación múltiple Red privada virtual

Fuente: Elaboración propia

La siguiente *figura 12* muestra la *Fase 3, estrategia de servicios*.



Fuente: Diseño propio [63]

El **proceso 9**, cuya finalidad es **desarrollar el estilo de la organización**, proyecta a ASInf como una organización pública innovadora en tecnologías que promueva la inclusión digital y facilite la conectividad a los ciudadanos. Actúa como órgano rector en materia de tecnologías de la información asegurando la confidencialidad, integridad, disponibilidad y privacidad de los servicios electrónicos del GCABA. El **proceso 10**, **departamentalizar y definir las funciones de la organización**, analiza los servicios brindados por ASInf. Tomando como referencia el estándar COBIT 5, se han desarrollado los nuevos roles de ASInf detallados a niveles de comités, direcciones, gerencias y subgerencias, la descripción de sus roles, la misión, visión y valores. Para **diseñar la organización** existe el **proceso 11**. En el mismo se evalúa el crecimiento del sector de TI en ASInf, condicionado a contar con recursos humanos calificados. La competencia entre las empresas del mercado interno y externo por sumar a su plantilla a profesionales capacitados es feroz. Por tal motivo, es necesario generar un esquema de compensación para el personal del área de TI que asegure que el agente desarrollará su carrera profesional en ASInf y no será tentado de abandonarla ante el ofrecimiento de un paquete de compensación superador. La Dirección de Recursos Humanos de ASInf establece un esquema de compensación para los agentes del área de TI.

Los elementos que componen la compensación son: sueldo, incentivos, prestaciones, equidad interna y competitividad externa. ASInf establece una política salarial dinámica que considera el pago fijo, pago variable y un perfil deseado de competencias para puestos jerárquicos y del personal del área de TI. Los agentes que conforman los equipos de ASInf, según el rol a desempeñar, es conveniente que cuenten con el título habilitante requerido y sean capacitados periódicamente en la función a desarrollar. La próxima *tabla 4* describe el perfil deseado con las *Competencias del personal*.

Rol / Función	Profesional (P) Terciario (T) Secundario (S)	Título en TI (T) Legales (L) Economía (E) Otros (O)	Posgrado	Maestría	Experiencia laboral mínima (años)	Antigüedad mínima de título (años)
Consejo de Administración	P			M	20	15
Auditoría	P	L	P		20	15
Comité Ejecutivo Estratégico de TI	P	T		M	20	15
Comité Estratégico (Desarrollo/Proyectos)	P	T		M	20	15
Consejo de Arquitectura	P	T		M	20	15
Comité de Riesgo Corporativo	P	T		M	20	15
Consejo de Riesgos de Tecnología	P	T		M	20	15
Dirección General Ejecutiva (CEO)	P	T		M	20	15
Dirección General Financiera (CFO)	P	E		M	15	10
Dirección de Operaciones (COO)	P	T		M	15	10
Dirección General de Riesgos (CRO)	P	T		M	15	10
Dirección de Informática (CIO)	P	T	P		15	10
Dirección de Seguridad de la Información (CISO)	P	T	P		15	10
Dirección de Privacidad de la Información	P	T	P		15	10
Dirección de Recursos Humanos	P	O	P		15	10
Gerencia de Riesgos de Tecnología	P	T	P		10	5
Gerencia de Arquitectura	P	T	P		10	5
Gerencia de Desarrollo	P	T	P		10	5

Rol / Función	Profesional (P) Terciario (T) Secundario (S)	Título en TI (T) Legales (L) Economía (E) Otros (O)	Posgrado	Maestría	Experiencia laboral mínima (años)	Antigüedad mínima de título (años)
Gerencia de Operaciones de TI	P	T	P		10	5
Gerencia de Administración de TI	P	T	P		10	5
Gerencia de Gestión de Proyectos (PMO)	P	T	P		10	5
Gerencia de Gestión de Valor (VMO)	P	T	P		10	5
Gerencia de Seguridad de la Información	P	T	P		10	5
Gerencia de Infraestructura	P	T	P		10	5
Gerencia de Redes y Telefonía	P	T	P		10	5
Gerencia de Soporte a Usuarios	P	T	P		10	5
Gerencia de Legales	P	L	P		10	5
Gerencia de Compras y Patrimonio	P	O	P		10	5
Subgerencia de Continuidad de Negocio	P	T	P		10	5
Subgerencia de Servicios	P	T	P		15	10
Subgerencia Ejecutiva de Negocio	P	T	P		15	10

Fuente: Elaboración propia

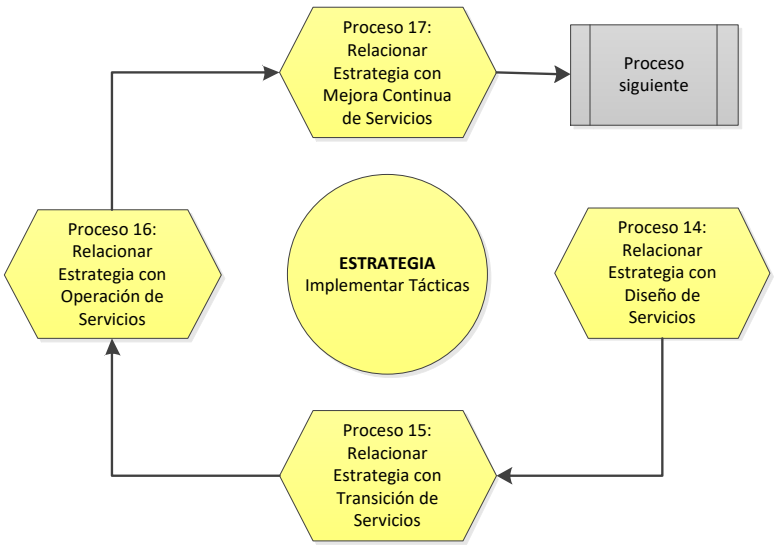
El personal ingresante al organismo es sometido a un período de prueba de tres meses. Luego de finalizado será evaluado por su jefe directo, el que podrá recomendar o no su contratación definitiva y deberá cumplir las cláusulas del contrato, leyes laborales, reglamentos que regulan a ASInf y guardar discreción con la información confidencial. La capacitación del personal del área de TI es esencial para el desarrollo del recurso humano que genera la mejora continua en la calidad de los servicios provistos. Su alcance es para todos los agentes de ASInf, usuarios de entes del GCABA y proveedores. La metodología es mediante el dictado de contenido teórico por demanda de los agentes o definido por ASInf, casos de negocio, talleres prácticos o exposiciones. El nivel de capacitación podrá, según necesidad, ser básico, medio o avanzado. El tipo de capacitación podrá ser inductiva (dictada a ingresantes), preventiva, correctiva o para desarrollo. La capacitación podrá ser de formación, actualización, especialización o perfeccionamiento. La evaluación de la capacitación, una vez finalizado el curso, será

realizada por el docente mediante una planilla con preguntas a responder por el agente, para desarrollar o mediante la elección de una respuesta correcta entre varias opciones. El nivel de respuestas correctas será como mínimo del 70%, caso contrario, el agente cursará nuevamente la capacitación. La capacitación específica se realizará por demanda o por necesidad de ASInf. El plan de carrera laboral es el recurso que permite al personal conocer cuál será su recorrido de crecimiento profesional en ASInf, por ello se establecen premios e incentivos.

ASInf comunica la estrategia, misión, visión, valores, objetivos estratégicos, roles, funciones, normas y políticas. También las inversiones, riesgos, apetito al riesgo, capacitación, contratación del personal, compensación y perfil de competencias por puesto. El mismo incluye las habilidades, capacidades, fortalezas para potenciar y debilidades para reforzar, competencias requeridas y capacitaciones necesarias. La Dirección de Recursos Humanos gestiona el talento evaluando el conocimiento y experiencia de los agentes y su potencial. La gestión de los factores de desempeño se desarrolla con el apoyo del superior jerárquico inmediato, la comunicación de las oportunidades generadas, la igualdad de oportunidades para los agentes, el interés del agente y la satisfacción personal. La dirección también comunica las vacantes producidas mediante una publicación, comunicación del rol a cubrir, competencias, experiencia, mecanismo de postulación, plazo y evaluación. En la gestión de las habilidades de los recursos humanos se consideran la información, comunicación, colaboración, convivencia con el ambiente digital y la tecnología. Se evalúa al personal contratado y agentes en planta permanente mediante indicadores de competencias, conocimientos, tareas, interacción con su jefe, usuarios e integrantes de su equipo, actitud y cumplimiento de objetivos laborales y aporte al organismo.

Capítulo 8 - ITIL v3, etapa 2 del nuevo marco tecnológico para el GCABA

La etapa 2 de la implementación de ITIL v3 abarca los procesos 12 al 22. El **proceso 12**, **desarrollar la cultura organizacional** con el respeto por las normas, proyecta a ASInf con una cultura colaborativa (fomenta la visión compartida) y el clima organizacional (promueve la interconsulta). Fomenta el clima laboral (favorece la interacción) y la cultura participativa (apoya la participación). Impulsa la comunicación, formación de equipos interdisciplinarios y la seguridad del entorno físico. El código de ética y conducta es de cumplimiento obligatorio para todos los agentes del organismo y quienes interactúan con él. Por tal motivo ASInf adhiere a las Normas Éticas dictadas por la Sindicatura General de la Ciudad Autónoma de Buenos Aires en la Resolución Nº 205/SGCBA/16[60]. La estrategia de provisión de servicios tiene relación directa con la estrategia de diseño de los servicios, por ello se evalúan los recursos tecnológicos y humanos con los que cuenta ASInf. El **proceso 13**, **desarrollar estrategias de aprovisionamiento de servicios**, direcciona el tipo de provisión de servicios, interna y soportada a través de proveedores. El tipo y criticidad del servicio a suministrar, costos, capacidad técnica, humana y demanda son algunos de los componentes evaluados para definir la provisión del servicio. A continuación, en la *figura 13* se detalla la *Fase 4, estrategia de servicios*.



Fuente: Diseño propio[63]

La estrategia de los servicios depende de las capacidades dinámicas propias de ASInf y de los proveedores externos que permiten dar respuestas efectivas. El **proceso 14**, creado para **relacionar la estrategia con el diseño de los servicios**, está a cargo de

la Subgerencia Ejecutiva de Negocio. Los proveedores suministran actualizaciones, mantenimientos, desarrollos o soporte. De esta manera la gestión y el control son ejercidos por ASInf el cual permite la creación rápida de los prototipos y el mayor control de las políticas y procesos internos. La desventaja existe en las limitaciones de la gestión del costo por escala, el incremento del costo y el tiempo en la gestión de los servicios. Puede utilizarse la configuración de servicio compartido, ya sea mediante una asociación externa de proveedores o a través de un proveedor externo de conocimiento. Para casos tales como la actualización y mantenimiento de sistemas y aplicaciones, administración, mantenimiento y actualización de bases de datos, mantenimiento y actualización del correo de los organismos del GCABA o gestión remota y presencial de hardware, software, internet e impresión, entre otros. El diseño del servicio está compuesto por procesos, para los cuales existen responsables de llevarlo adelante. El máximo responsable para la Gestión del catálogo de servicios es la Gerencia de Gestión de Valor (VMO), para la Gestión de la capacidad es el Comité Ejecutivo Estratégico de TI, en tanto que para la Gestión de Proveedores y la Gestión de seguridad de la información es la Dirección de Informática (CIO). La Gestión de niveles de servicio es llevada a cabo por el Comité Estratégico (Desarrollo/Proyectos). Por último, la responsabilidad de la Gestión de la continuidad del servicio de TI es de la Dirección de Operaciones (COO).

La solicitud de un servicio o proyecto se inicia mediante la elaboración del Nuevo formulario de requerimientos de servicios con formato digital mediante el sistema SADE[40], confirmando que está alineado con la planificación estratégica de ASInf. El requerimiento es formal y contiene parámetros tales como el nombre del proyecto, propósito, justificación, objetivos, fecha de comienzo, límites, supuestos, restricciones, alcance, autorización, responsable y recursos. También debe especificarse si se realizó un análisis de viabilidad, si el proyecto es nuevo, desarrollo de un sistema, servicio o aplicación, su funcionalidad y justificación. Asimismo, los beneficios para el GCABA y el solicitante, posibles usuarios, análisis de riesgos, impacto, presupuesto, monto asignado, ejecución anual o plurianual, entre otros. Es indispensable evaluar la cadena de valor de cada proyecto, formada por los recursos de ASInf utilizados o adquiridos para la generación del servicio. Para el caso que un proyecto no cumpla con los beneficios esperados, se acuerda con el sponsor las acciones correctivas para lograr lo planificado o la baja del mismo detallando los motivos. En ITIL se destacan cinco

aspectos individuales del diseño del servicio tales como servicios nuevos o modificados, sistemas y herramientas de gestión de los servicios y la cartera de servicios que incluye el catálogo de servicios, arquitectura tecnológica y sistemas de gestión, procesos requeridos y métodos de medición y métricas. La arquitectura del centro de datos de ASInf se define en el "Estándar de Arquitectura para los Sistemas de Información e Infraestructura del Centro de Datos ES0101[6], siendo sus componentes la arquitectura de sistemas, arquitectura física, red local, entornos (desarrollo, prueba, homologación y producción). También lo componen la arquitectura lógica, los servicios (motor de bases de datos, sistemas operativos, gestión documental, correo electrónico, protocolo de sincronización de relojes, documentos en formato portable y firma digital), mensajería instantánea y servidores de dominio por entorno. Contiene los logs, componentes de aplicaciones y servidores, actualizaciones de aplicaciones, solicitud de servicios, backups/almacenamiento, interfaces con el usuario y configuraciones estándar.

El plan de administración del tiempo del proyecto define y secuencia las actividades, estima los recursos, desarrolla y controla el cronograma. Se elabora un informe con el estado de avance del proyecto expresando el alcance, la calidad, planificación, los resultados, si los beneficios obtenidos están en línea con los planificados, los costos y riesgos. El plan de comunicación transmite la estrategia, diseño, transición, operación, la mejora continua, el rendimiento, los cambios del proyecto, capacitación en procesos y en servicios nuevos o personalizados. La administración de las adquisiciones del proyecto incluye la planificación, compra, administración y cierre. El informe de ejecución y control de administración del proyecto evalúa el cumplimiento de los objetivos, metas, fases, tareas, presupuesto, recursos y la programación cronológica. Existen seis tipos de riesgos presentes en diferentes procesos, áreas o recursos tales como gerenciales y de negocio (alineación estratégica, composición del Comité de Dirección, comunicación, sponsor y compromiso), administración y control (planeación, metodología, proyectos, gestión de conflictos, gestión de riesgos y monitoreo del progreso).

Además existen riesgos en los procesos y funciones (definición, requisitos del negocio, controles de aplicación, personalización, interfaces y localización), (recursos, presupuestos, dotación personal, competencias del equipo), organización (entrenamiento, gestión del cambio, comunicación, alineamiento organizacional y

continuidad del negocio). Por último, los riesgos técnicos (conversión de datos, arquitectura del sistema, creación de redes, rendimiento, seguridad, disponibilidad y recuperación de desastres). El apetito al riesgo es el nivel de exposición establecido a los impactos adversos potenciales que ASInf está dispuesta a aceptar para alcanzar sus objetivos estratégicos. La tolerancia al riesgo es el umbral de alerta que ASInf utiliza para evitar que sus objetivos estratégicos sean impactados significativamente y afecten los requisitos, la continuidad o disponibilidad del nivel de los servicios de TI. Las funciones críticas en los servicios están cubiertas por más de un agente, los cuales deben estar capacitados técnicamente para afrontar la responsabilidad asignada.

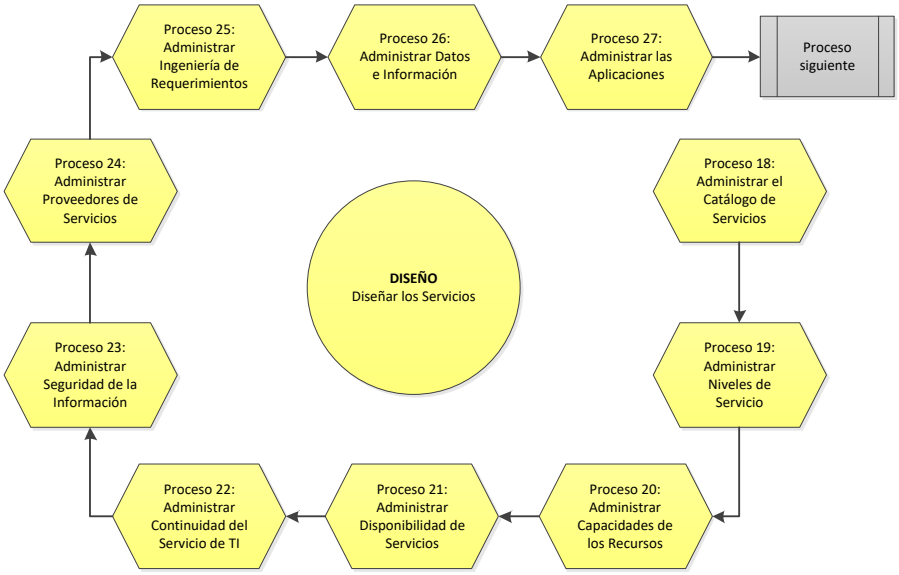
El **proceso 15**, es concebido para **relacionar la estrategia con la transición de los servicios**. Los sistemas y procesos de transición de los servicios brindan la visión necesaria para evaluar y aprobar las iniciativas estratégicas planteadas por ASInf. Evalúa los costos, riesgos, activos del servicio y configuraciones. También los posibles escenarios, asignación actual de los recursos y los planes de contingencia para contener los cambios de impacto. La transición del servicio está compuesta por procesos, para los cuales existen responsables de llevarlos a cabo. La máxima responsabilidad para la Gestión de entrega y despliegue y para la Planificación y soporte de la transición recae en el Comité Estratégico (Desarrollo/Proyectos), para la Validación y pruebas del servicio, el responsable es la Subgerencia Ejecutiva de Negocio, en tanto que para la Evaluación de cambios es el Comité Estratégico (Desarrollo/Proyectos). Asimismo, el responsable máximo en la Gestión de configuración y activos del servicio es la Gerencia de Operaciones de TI y para la Gestión del conocimiento es la Subgerencia Ejecutiva de Negocio. La fase de operación de los servicios es la más crítica, ya que los agentes de los entes del GCABA perciben la calidad de los servicios prestados por ASInf. El responsable de **relacionar la estrategia con la operación de los servicios** es el **proceso 16**. La operación del servicio está compuesta por procesos, para los cuales existen responsables de desarrollarlos.

El máximo responsable de la Gestión de eventos es la Gerencia de Operaciones de TI. De la Gestión de incidencias y Gestión de problemas es la Subgerencia de Servicios y de la Gestión de accesos es la Subgerencia Ejecutiva de Negocio. Los procesos involucrados en la operación del servicio son la Gestión de eventos (monitorea los eventos en la infraestructura de TI), Gestión de incidencias (registra las incidencias en el servicio) y la Petición de servicios de TI (gestiona las peticiones de los usuarios).

La Gestión de problemas (propone soluciones a los incidentes) y la Gestión de acceso (asegura el acceso a los recursos autorizados).

El **proceso 17** acciona para **relacionar la estrategia con la mejora continua de servicios**. La mejora del servicio ofrece información para la fase de estrategia respecto de la calidad, optimización y rendimiento. La mejora continua enriquece atributos como la calidad, conformidad, rendimiento y valor en los servicios provistos por ASInf.

La mejora continua del servicio incluye varios procesos, para los cuales existen responsables de llevarlos a cabo. El máximo responsable de la revisión de los siete pasos del proceso de mejora y de los Informes de servicios es la Dirección de Operaciones (COO). La próxima *figura 14* especifica el *Diseño de servicios*.



Fuente: Diseño propio [63]

La Gerencia de Gestión de Valor (VMO) es responsable del **proceso 18**, **administrar el catálogo de servicios**, compuesto por los servicios vigentes provistos por ASInf.

El flujo de creación incluye los servicios en desarrollo como sistemas predictivos, internet de las cosas, reconocimiento facial, detección temprana de humos, inteligencia y visión artificial.

La siguiente *matriz 2* identifica el *Catálogo de servicios* y la celda coloreada muestra un vínculo entre el registro y el componente de la columna.

Catálogo de servicios															
Servicios	Demanda			Proveedor			Nivel de Servicios						Acuerdo y Soporte			
	Ente del GCABA	Usuario final	Proveedor externo	Soporte al servicio	Compartido con ASInf	Servicio externo	Número máximo de interrupciones mensuales	Tiempo máximo interrupción mensual (horas)	Tiempo de respuesta (horas)	Disponibilidad (%)	Continuidad < a (horas)	Horarios de contacto (horas)	Contrato de Soporte	Acuerdos de Niveles de Servicio	Acuerdos de Niveles Operacionales	En desarrollo
Servicios provistos por ASInf.							3	5	2	99	5	24				
Desarrollo de nuevas tecnologías.																

Fuente: Elaboración propia

El Comité Estratégico (Desarrollo/Proyectos) de ASInf es el responsable del **proceso 19**, **administrar los niveles de servicios**. Se mide el rendimiento de los servicios de TI ofrecidos por ASInf en el lapso del mes calendario. El *Plan de Calidad del Servicio (SQP)* provisto por ASInf se define en la próxima *tabla 5*.

Plan de Calidad del Servicio (SQP)														
	Usuarios activos	Flujo de usuarios	Velocidad de navegación	Correos enviados	Correos rebotados	Versión de software	Infraestructura obsoleta	Hardware obsoleto	Número de interrupciones mensuales < a	Tiempo de respuesta < a (horas)	Disponibilidad > a (%)	Continuidad < a (horas)	Horarios de contacto (horas)	Costos totales
Servicios provistos por ASInf														

Fuente: Elaboración propia

Los Acuerdos de Niveles de Servicio (SLA) son acuerdo firmados entre ASInf (pudiendo representar a un ente del GCABA) con un proveedor externo. Garantizan los niveles de calidad de los servicios de TI prestados por ASInf. Los Requerimientos de los Niveles de Servicio (SLR) recolectan la información detallada respecto de las

necesidades del usuario, rendimiento y el nivel de servicios. El SLR es confeccionado para cada servicio de TI y contiene como mínimo parámetros del servicio como la continuidad, disponibilidad, funcionalidad, características y nivel de calidad. Además de integración e interacción con la infraestructura de TI, integración con otros servicios de TI, plazo de implementación, tiempos de respuesta ante incidentes y escalabilidad. Los Acuerdos de Niveles Operacionales (OLA) contienen la descripción y especificación del servicio, descripción de la demarcación de un servicio, duración del contrato y las condiciones para su extensión, descripción de los procedimientos para la seguridad de los datos, establecimiento de la tarifa, términos y formas de pagos. También la frecuencia de los informes, establecimiento de las responsabilidades entre ambos, descripción de las condiciones de cambios ocasionales, detalle de las condiciones de una posible suspensión del acuerdo y las sanciones por el incumplimiento. La siguiente *matriz 3* expresa los *Acuerdos de niveles operacionales (OLA) para aplicaciones.*[64]

Acuerdos de niveles operacionales (OLA) para aplicaciones												
Servicios	Número máximo de usuarios activos	Cantidad máxima de conexiones simultáneas	Velocidad básica de navegación (Mbps)	Hardware base	Software base	Infraestructura básica	Número máximo de interrupciones mensuales	Tiempo máximo por interrupción < a (horas)	Tiempo de respuesta < a (horas)	Disponibilidad > a (%)	Continuidad < a (horas)	Horarios de contacto
Aplicaciones provistas por ASInf	S	S	20	D	D	D	3	5	2	98	5	24

Fuente: Elaboración propia

Los sistemas que gestionan urgencias, como SIGEHOS (Sistema de Gestión Hospitalaria), cuentan con Acuerdos de Niveles Operacionales (OLA) de mayor nivel que el resto de los sistemas. La siguiente *matriz 4* expresa los *Acuerdos de niveles operacionales (OLA) para sistemas*[64].

[64] D: son los parámetros a definir en los Acuerdos de niveles operacionales
S: sin límites

Acuerdos de niveles operacionales (OLA) para sistemas													
Descripción	Número máximo de usuarios activos	Carga mínima de usuarios a la vez	Cantidad máxima de conexiones simultáneas	Velocidad básica de navegación (Mbps)	Hardware base	Software base	Infraestructura básica	Número máximo de interrupciones mensuales	Tiempo máximo de interrupción mensual (horas)	Tiempo de respuesta < a (horas)	Disponibilidad > a (%)	Continuidad (horas) < a	Horarios de contacto
Sistema con niveles OLA´s elevados	S	S	S	100	D	D	D	2	2	1	99	3	24
Sistema con niveles OLA´s estándares	S	100	S	20	D	D	D	3	5	2	98	5	24

Fuente: Elaboración propia

El informe de nivel de servicios, elaborado por Auditoría interna de ASInf, opina respecto del estado de las solicitudes de mejoras para los servicios, si las peticiones se realizaron por canales formales, si contenían los plazos de ejecución, su aceptación o rechazo y si fue concluida. El Comité Ejecutivo Estratégico de TI de ASInf es el responsable de **administrar las capacidades de los recursos, proceso 20**, incluye el conocimiento (que posee el recurso humano), procesos (definidos mediante los estándares internacionales) y la gestión (estandarización de los procesos).

Los activos del servicio son los recursos y las capacidades que posee ASInf, que a través de su personal brindan servicios de TI aportando valor a los entes del GCABA. Los recursos de ASInf están definidos por la infraestructura (centros de datos y procesamiento, redes MAN y LAN, hardware y software), la información (bases de datos), aplicaciones (desarrollos propios o tercerizados) y financieros (presupuesto y financiación externa). La próxima *matriz 5* detalla las *Capacidades de recursos*. La intersección de la celda coloreada con la letra “P” establece una dependencia primaria de la capacidad del recurso asociado al servicio y con la letra “S” una dependencia secundaria.

Servicios	Capacidades de recursos							
	Organización	Conocimiento	Proceso	Gestión	Infraestructura	Información	Aplicaciones	Financieros
Desarrollo de sistemas y aplicaciones.	P	P	P	P	P	S	P	P
Actualización y mantenimiento de sistemas y aplicaciones.	P	P	P	P	P	S	P	S
Desarrollo de bases de datos.	P	P	P	P	P	S	P	P
Administración, mantenimiento y actualización de bases de datos.	P	P	P	P	P	S	P	S
Provisión, mantenimiento y actualización de internet.	P	P	P	P	P	S	S	P
Mantenimiento y actualización del correo de los organismos del GCABA.	P	P	P	P	P	S		S
Generación de copias de respaldo de las bases de datos.	P	P	P	P	P	S	S	S
Instalación y actualización de herramientas informáticas, hardware y software, servicio de videoconferencia y software antivirus.	P	P	P	P	P	S		S
Gestión remota y presencial de hardware, software, internet e impresión.	P	P	P	P	P	S		S
Creación de puntos de red.	P	P	P	P	P	S		P
Administración y resguardo de la información en soportes magnéticos, custodia, traslado ante un incidente y recuperación.	P	P	P	P	P	S	S	S
Gestión de la infraestructura, hardware y software de los Centros de Cómputos asegurando el funcionamiento 7 días por 24 horas.	P	P	P	P	P	S	S	S
Contingencia por cortes de suministro de energía o catástrofe.	P	P	P	P	P	S	S	P
Operación 7 días por 24 horas, acciones preventivas y correctivas de la red inalámbrica y fibra óptica del GCABA.	P	P	P	P	P	S	S	S
Administración de la red de información, comunicaciones y telefonía del GCABA.	P	P	P	P	P	S	S	S
Administración y mantenimiento de la arquitectura de wifi público y privado del GCABA.	P	P	P	P	P	S	S	S
Conexión a proveedores en frontera y redes de terceros, gestión de la plataforma y enlaces de internet del GCABA.	P	P	P	P	P	S	S	P
Provisión de puntos de presencia de wifi en eventos GCABA.	P	P	P	P	P	S	S	P
Gestión de la infraestructura necesaria para la implementación de firma digital.	P	P	P	P	P	S		S
Administración de los servidores.	P	P	P	P	P	S	S	S
Gestión del almacenamiento de datos centralizados y descentralizados del GCABA.	P	P	P	P	P	S	S	S
Gestión y mantenimiento de los servicios de red LAN y MAN del GCABA.	P	P	P	P	P	S	S	S
Registración de incidentes y provisión de soporte.	P	P	P	P	P	S	S	S
Desarrollo de sistemas de visión artificial.	P	P	P	P	P	S		P
Desarrollo de internet de las cosas.	P	P	P	P	P	S		P
Desarrollo de sistemas de reconocimiento facial.	P	P	P	P	P	S		P
Desarrollo de sistemas de detección temprana de humos con sistema de supresión.	P	P	P	P	P	S		P
Desarrollo de sistemas de inteligencia artificial.	P	P	P	P	P	S		P
Desarrollo de sistemas predictivos.	P	P	P	P	P	S		P

Fuente: Elaboración propia

El informe de capacidades de recursos y rendimientos para servicios de TI revela la suficiencia o no de los recursos para proveer el servicio requerido, si no es el deseado, se identifica el recurso afectado. La gestión de la disponibilidad por servicio y recurso asegura su disponibilidad según los OLA acordados. El responsable del **proceso 21**,

administrar la disponibilidad de los servicios, es la Dirección de Seguridad de la Información (CISO). La disponibilidad de los servicios es la capacidad de suministrar el servicio correctamente según lo acordado. La confiabilidad es la medida del tiempo durante la cual los servicios son suministrados de forma ininterrumpida. La capacidad de mantenimiento es la capacidad de recuperar el servicio en caso de interrupción. En la siguiente *tabla 6* se detallan los parámetros para la *Administración de la disponibilidad*.

Administración de la disponibilidad						
Servicio	Disponibilidad > a (%)	Confiabilidad > a (%)	Capacidad de mantenimiento < a (horas)	Capacidad de servicio > a (%)	Interrupción mensual por mantenimiento < a (horas)	Tiempo de detección < a (horas)
Servicios provistos por ASInf.	99	99	5	99	2	1

Fuente: Elaboración propia

La coordinación de Parada de Servicio Prevista (PSO) es un proceso acordado entre ASInf y el ente del GCABA (usuario) para la actualización del servicio. Auditoría elabora el informe de Administración de Disponibilidad de Servicios que detalla la disponibilidad, confiabilidad y capacidad de mantenimiento. La Dirección de Operaciones (COO) es la responsable del **proceso 22**, **administrar la continuidad del servicio de TI** que impide una interrupción imprevista en los servicios y su falta de continuidad. Los servicios se diseñan con recuperación, Cold standby (recuperación luego de los 4 días), Warm standby (recuperación entre 24 y 72 horas) y Hot standby (replicación continua). La *Administración de la continuidad* se muestra en la *tabla 7*.

Administración de la continuidad															
	Impacto por interrupción del servicio			Incremento significativo de costos			Pérdida de participación en sociedad			Pérdida de imagen pública			Recuperación (standby)		
Servicio / Nivel	Alto	Medio	Bajo	Alto	Medio	Bajo	Alta	Media	Baja	Alta	Media	Baja	Hot	Warm	Cold
Servicios provistos por ASInf															

Fuente: Elaboración propia

Capítulo 9 - ITIL v3, etapa 3 del nuevo marco tecnológico para el GCABA

La etapa 3 de la implementación de ITIL v3 abarca los procesos 23 al 40. El objetivo del **proceso 23** es **administrar la seguridad de la información**, cuyo responsable es la Dirección de Informática (CIO). Las políticas fueron descriptas anteriormente. El informe de gestión de la seguridad de la información es confeccionado por Auditoría interna de ASInf, expone la gestión de la seguridad de la información evaluando el cumplimiento de las políticas de seguridad por parte de ASInf, los entes del GCABA y los proveedores externos. **Administrar los proveedores de servicios** forma parte del **proceso 24**, siendo responsable la Dirección de Informática (CIO) mediante la gestión de los proveedores, comunicación y administración de la relación con los suministradores externos. La tercerización con un proveedor externo está amparada por los acuerdos de confidencialidad estipulados por ASInf. El Jefe de Gobierno de la Ciudad Autónoma de Buenos Aires mediante el Decreto Nº 116/2014, creó la "Plataforma de Gestión Electrónica de Proveedores -GEP- como medio de procesamiento de información, documentación y antecedentes para los procesos de contrataciones de bienes, servicios y obras públicas, que efectúen los distintos Organismos del Gobierno de la Ciudad Autónoma de Buenos Aires".[65] La plataforma se integra como módulo al SADE[40]. Para ser proveedor del sector público de la Ciudad Autónoma de Buenos Aires es necesario que el interesado complete y adjunte la documentación y el formulario de pre-inscripción.[66] Una vez aprobado el trámite el postulante podrá ser proveedor de bienes y servicios según la normativa vigente. Para la contratación de servicios de transmisión de datos, adquisición de bienes y servicios informáticos que superen los montos definidos en el Decreto Nº 1036/GCBA/08[67], en la Resolución 44/ASInf/08[68] y sus modificatorias, deben ser autorizadas por ASInf. Los organismos del GCABA podrán contratar los servicios con los proveedores

[65] Decreto Nº 116/2014. Obtenido el 1 de Abril de 2014 en la Word Wide Web: https://n9.cl/azui [Accedido el 22/5/19]

[66] Formulario de pre-inscripción. Obtenido en la Word Wide Web: www.buenosairescompras.gov.ar [Accedido el 22/5/19]

[67] Decreto N° 1036/GCABA/08. Obtenido el 27 de Agosto de 2008 en la Word Wide Web: https://n9.cl/h8z6 [Accedido el 22/5/19]

[68] Resolución Nº 44/ASInf/08. Obtenido el 15 de Setiembre de 2008 en la Word Wide Web: https://n9.cl/tax92 [Accedido el 22/5/19]

directamente o mediante ASInf. Tanto ASInf como los entes del GCABA, en sus distintas formas de contratación, valoran si el servicio puede desarrollarse internamente. Es necesario establecer y gestionar los riesgos con los proveedores, los cuales permiten alcanzar mejores condiciones de entrega en los servicios. El Consejo de Arquitectura de ASInf es responsable de evaluar los requisitos solicitados, analizar los recursos y proponer una solución integral de los servicios, actividad establecida en el **proceso 25**, **administrar la ingeniería de los requerimientos**. Coordina los servicios según los requisitos del sponsor, desarrolla el proyecto, verifica que los SLAs, OLAs y UCs sean acordes a las necesidades de los entes del GCABA y los proveedores externos. Además, asegura los requisitos de los sponsor, los niveles operativos y técnicos de TI y prioriza la asignación de los recursos existentes en ASInf.

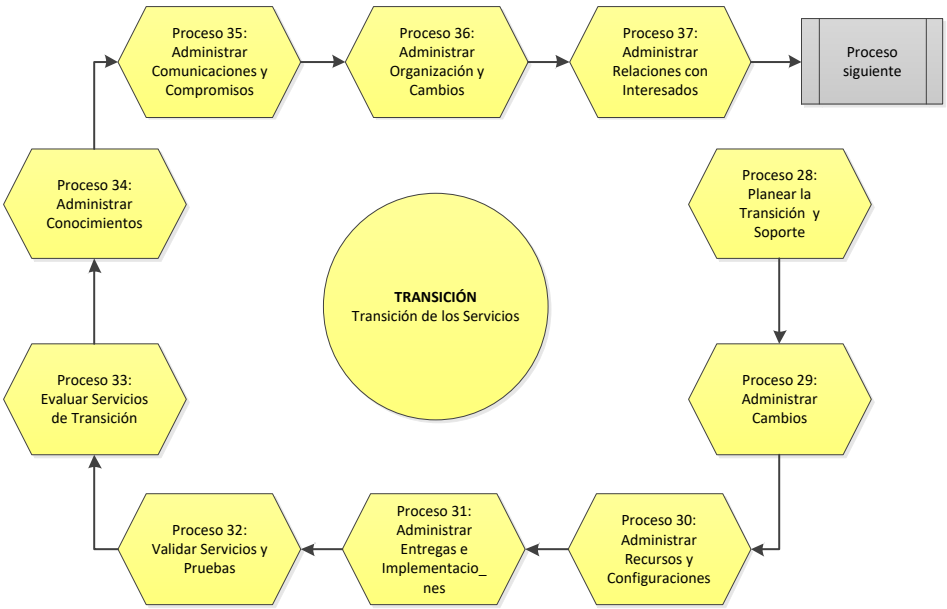
La Subgerencia Ejecutiva de Negocio de ASInf es responsable del **proceso 26**, **administrar los datos e información** del organismo, al igual que los utilizados por los entes del GCABA y proveedores externos. Por esta razón en el marco tecnológico del GCABA se han definido dos políticas asociadas a la gestión de la información con la PO0401[5] (Política de Responsabilidades sobre la Información) y la PO0402[5] (Política de Clasificación de la Información). En la primera se definen a los propietarios, custodios, usuarios, control interno y agentes responsables de la información. En la segunda, Política de Clasificación de la Información, se establecen los criterios a considerar para clasificar la información del GCABA y su nivel de criticidad. El informe de administración de datos e información es elaborado por Auditoría interna, opina respecto del propietario de la información, asignación, requisitos de acceso y clasificación de la criticidad.

La Subgerencia Ejecutiva de Negocio de ASInf es responsable de **administrar las aplicaciones**, su soporte y mantenimiento, **proceso 27**. Ante la necesidad de desarrollar una aplicación, sea solicitada por un ente o definida por estrategia de ASInf, se evalúa la reutilización y personalización de una aplicación existente. Con desarrollo interno o externo, se respeta e implementa la política de separación de ambientes para segregar funciones y limitar el acceso. En la siguiente *matriz 6* se detallan los componentes a considerar para la *Administración de aplicaciones*.

Administración de aplicaciones															
Descripción	Tipo						Atributos				Nuevas Aplicaciones				
	Laboral	Tránsito y transporte	Conectividad	Trámites	Medios	Comunidad y eventos	Ciclo de vida mínimo (años)	Transacciones	App Store	Google Play	Reutilizable	Costo de desarrollo	Plazo de desarrollo (meses)	Ciclo de vida mínimo (años)	Costo de soporte y actualización
Aplicaciones provistas por ASInf															
Nuevas aplicaciones															

Fuente: Elaboración propia

La siguiente *figura 15* especifica la *Transición de los servicios*.



Fuente: Diseño propio[63]

Planear la transición y el soporte forma parte del **proceso 28** y está a cargo del Comité Estratégico (Desarrollo/Proyectos) de ASInf. La Gestión de cambios aprueba la modificación de los servicios. La Gestión de la configuración y los activos del servicio registran los elementos de la configuración (CIs) del servicio. La Gestión de entregas y despliegues implementa las nuevas versiones de los servicios. La Validación y pruebas aseguran el cumplimiento de los requisitos planteados por los entes del GCABA. La Subgerencia Ejecutiva de Negocio es responsable de **administrar los cambios** a través

del **proceso 29**, también de garantizar la calidad y continuidad del servicio de TI. Los cambios se registran para solucionar un problema previo y evalúa la pertinencia del proceso. La Subgerencia Ejecutiva de Negocio soluciona la Petición de Cambio (RFC) solicitada.

La prioridad en los cambios puede ser Baja (junto con otros servicios), Normal (si no entorpece otro cambio con mayor prioridad), Alta (a ejecutar porque genera errores en el servicio) o Urgente (con prisa porque genera interrupción). Los cambios realizados por emergencia son el resultado de una planificación poco eficiente. ASInf posee en vigencia el Proceso de Control de Cambios en Software de aplicación provisto por organismos (PC0901). En la siguiente *tabla 8* se detalla la *Administración de cambios*.

Administración de cambios																													
	RFC registrada									RFC en proceso																			
	Fecha de recepción	Número de RFC	Error asociado	Detalle del cambio propuesto	Motivo	Propósito	Elementos de configuración (CI)	Recursos estimados	Tiempo estimado	Estado Registrado	Estado Aceptado	Estado Rechazado	Estado Implementado	Motivo del Rechazo	Fecha de aceptación/negación	Evaluación preliminar	Prioridad baja	Prioridad normal	Prioridad alta	Prioridad urgente	Categoría	Acciones de retroceso	Recursos asignados	Fecha de implementación	Plan de implementación	Cronograma	Revisión post-implementación	Evaluación final	Fecha de cierre
Servicios provistos por ASInf.																													

Fuente: Elaboración propia

El Comité Estratégico (Desarrollo/Proyectos) está a cargo de **administrar los recursos y configuraciones**, detallados en el **proceso 30**. Gestiona los recursos y las configuraciones de los activos de tecnología mediante la creación de la Base de Datos de la Configuración (CMDB) integrando los componentes del servicio.

Actualiza la CMDB con incidencias, problemas, cambios y entregas y despliegues. La siguiente *tabla 9* muestra la *Administración de recursos y configuraciones*.

Administración de recursos y configuraciones																																
		Software o sistema																														
	Infraestructura	Virtualización de centro de datos	Administración de servidores	Automatización	Gestión y copias de máquinas virtuales	Optimización de recursos	Continuidad en aplicaciones	Operativo para aplicaciones	Gestión de base de datos	Gestión de base de datos relacionales	Gestión de base de datos multilenguaje	Operativo para red, servidores e impresión	Automatización para aplicaciones	Gestión para recursos en la nube	Gestión y configuración	Gestión para recursos basado en web	Visualización en tiempo real	Almacenamiento en la nube	Gestión para el entorno de TI	Almacenamiento físico y virtual	Gestión de subsistemas de almacenamiento	Gestión de almacenamiento individual	Gestión de infraestructura	Gestión de bases de datos multiformato	Gestión de bases de datos local y en la nube	Servidores web para aplicaciones	Servidores web multiplataforma	Multiconexión servidor-cliente	Infraestructura en centros de datos	Integración de datos	Supervisión de eventos
Servicios provistos por ASInf																																

Fuente: Elaboración propia

Administrar entregas e implementaciones es parte del **proceso 31**, el cual controla la calidad del hardware y software instalado en producción, asiste a la administración de cambios y a la administración de recursos y configuraciones.

Se elabora en ASInf una Biblioteca de Medios Definitivos (DML) a través de la cual se almacenan las copias históricas de las versiones de sistemas operativos, aplicaciones y controladores de dispositivos. Se registra un almacén de Recambios Definitivos (DS) con repuestos y su documentación para una rápida solución en el entorno de producción.

El desarrollo de software es interno o provisto por proveedores externos. En este último caso el Comité Estratégico (Desarrollo/Proyectos) asegura que el paquete de software o hardware cumpla las especificaciones de la RFC.

La próxima *tabla 10* describe la *Administración de entregas e implementaciones* para cada servicio de TI de ASInf.

Administración de entregas e implementaciones																														
	Software usado	Versión	Software legal	En desarrollo	En prueba	En producción	Archivado	Fecha de adquisición	Fecha de Implementación	Cantidad de hardware de repuesto	Actualizar documentación del hardware	Verificar no deterioro calidad de servicio	Copia código fuente	Copia código objeto (ejecutable)	Objetos reusables	Documentación software técnica	Documentación software usuario	Copia de software	Prevención de software malicioso	Actualizar RFC	Actualizar CMDB	Actualizar DML	Actualizar DS	Cantidad de hardware de repuesto	Actualizar documentación	Actualizar código fuente	Actualizar código objeto	Actualizar reusables	Nueva versión	Impacto nueva versión en calidad del servicio	Impacto nueva versión en otro servicio
Servicios provistos por ASInf																														

Fuente: Elaboración propia

La Subgerencia Ejecutiva de Negocio es la máxima responsable del **proceso 32**, diseñado para **validar servicios y pruebas** que aseguren la calidad de las nuevas versiones. Se define una prueba piloto durante 15 (quince) días en paralelo con el actual suministro, que incluye servicios e infraestructura y verifica los resultados. La siguiente *tabla 11* detalla la *Validación de servicios y pruebas*.

Validación de servicios y pruebas																														
	Calendario de pruebas de funcionalidades	Verificar existencia en catálogo de servicios	Activos involucrados	Soporte planificado	Recursos involucrados	Número de Petición de Cambio (RFC)	Riesgos estimados	Prueba de los requisitos de calidad	Prueba integral de funcionalidad	Prueba automática	Prueba manual	Incidentes por incompatibilidad	Error generado por el incidente	Error conocido	Descripción del incidente	Versión	Nivel de utilidad obtenido	Nivel de garantía obtenido	Nivel de servicio obtenido	Nivel de calidad obtenido	Verificar SLR requerido	Verificar SQP requerido	Verificar SLA requerido	Verificar UC requerido	Retroceso a la versión anterior	Razón del retroceso	Aceptación de la prueba	Generación de la documentación
Servicios provistos por ASInf.																														

Fuente: Elaboración propia

Evaluar los servicios de transición y valorar la puesta en marcha, están establecidos en el **proceso 33**, siendo responsabilidad de la Subgerencia Ejecutiva de Negocio de ASInf. Es un proceso iterativo encargado de recopilar y examinar la información obtenida del nuevo servicio a proveer o de los cambios en los servicios de TI vigentes. La evaluación proporciona información para diagnosticar si un componente mejora el servicio, incrementa la productividad y aporta valor para ASInf. Para ello se diseña la siguiente *tabla 12* de *Evaluación de los servicios de transición*.

Evaluación de los servicios de transición																							
	Rendimiento del componente del servicio	Cambio (RFC) aplicado a un componente del servicio	Rendimiento en otros servicios por cambio aplicado	Impacto en el servicio por el cambio aplicado	Impacto en ASInf por el cambio aplicado	Impacto en otros servicios por el cambio	Impacto en ASInf por el nuevo servicio	Impacto en otros servicios por nuevo servicio	Pruebas completas, precisas y oportunas	Tiempo de evaluación del cambio en el servicio	Tiempo de implementación del cambio	Capacidad de la provisión	Tolerancia del servicio	Modelo y métricas planificadas	Recursos tecnológicos y financieros	Recursos humanos asignados	Expectativas del servicio	Propósito de uso del servicio	Riesgos por incumplimiento del SLR requerido	Riesgos por incumplimiento del SQP requerido	Riesgos por incumplimiento del SLA requerido	Riesgos por incumplimiento del UC requerido	Opinión del usuario en ambiente de prueba	Satisfacción del usuario en ambiente de prueba
Servicios provistos por ASInf.																							

Fuente: Elaboración propia

El **proceso 34**, gestionado a través de la Subgerencia Ejecutiva de Negocio de ASInf fue definido para **administrar los conocimientos**. Establece los criterios para evaluar, clasificar, registrar, almacenar, actualizar y compartir periódicamente los datos disponibles. Se comparte la sabiduría y experiencia de cada integrante hacia toda ASInf. Apoyado en otras fases del ciclo de vida, desde la gestión de incidencias y errores, se actualiza la Base de Datos de Errores Conocidos (KEDB) para facilitar el registro de fallos sucedidos y minimizar el tiempo de catalogación y solución futuro. La administración de conocimientos centraliza toda la información en un repositorio común

llamado Sistema de Gestión del Conocimiento del Servicio (SKMS). Es una herramienta estructurada que proporciona la presentación, procesamiento, integración y fuente de datos de la información que facilita el uso para cualquier agente de TI de ASInf. Se identifican a los propietarios del conocimiento y sus potenciales usuarios, el tipo de información que puede serle útil y los destinatarios tales como entes del GCABA, proveedores o personal de soporte. En la próxima *tabla 13* se detallan los componentes para la *Administración de conocimientos*.

Administración de conocimientos																		
	Definir políticas del SKMS	Definir un modelo SKMS estructurado por capas	Establecer las áreas del modelo SKMS	Fijar los propietarios del conocimiento	Detectar necesidades SKMS	Creación de Base de Datos de Errores Conocidos (KEDB)	Coordinación de la transferencia de las áreas para la KEDB	Recopilación de datos para la KEDB	Clasificación de datos para la KEDB	Definir criterios para subsanar incoherencias en los datos	Evaluar la calidad de los datos	Evaluar la utilidad de los datos	Completitud, precisión y oportunidad de los datos	Actualización de Base de Datos de Errores Conocidos (KEDB)	Herramientas de acceso para el uso del SKMS	Capacitación a los recursos humanos del SKMS	Canales de comunicación para usuarios del SKMS	Documentación de los datos obtenidos para el SKMS
Servicios provistos por ASInf.																		

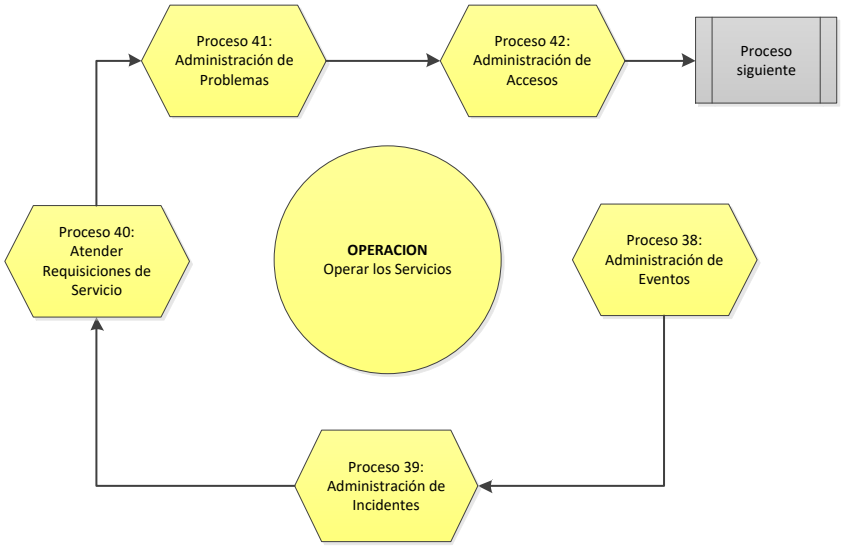
Fuente: Elaboración propia

La Dirección General Ejecutiva (CEO) está a cargo de **administrar las comunicaciones y compromisos** de ASInf, fijado en el **proceso 35**. Mediante encuestas realizadas a los entes del GCABA y a los proveedores, garantiza una comunicación efectiva. Las comunicaciones de ASInf a entes y proveedores se realizan a través de talleres, boletines informativos, capacitaciones grupales, individuales, reuniones de equipos y comunicaciones masivas. La Dirección General Ejecutiva (CEO) con el **proceso 36**, **administra la organización y los cambios**. Para lograr el cambio es esencial liderarlo a través de los aspectos culturales de ASInf, a través del lenguaje, la comunicación, conocimiento, liderazgo, premios y motivaciones. La siguiente *matriz 7* identifica las *Responsabilidades de cambios* asignadas en la estructura organizativa de ASInf, asignando A (Responsable de que se haga), R (Responsable de hacer), C (consultado) e I (informado).

Responsabilidades de cambios																	
Actividad	Consejo de Administración	Dirección General Ejecutiva (CEO)	Dirección General Financiera (CFO)	Dirección de Operaciones (COO)	Subgerencia Ejecutiva de Negocio	Comité Ejecutivo Estratégico de TI	Comité Estratégico (Desarrollo/Proyectos)	Gerencia de Gestión de Proyectos (PMO)	Dirección de Recursos Humanos	Dirección de Informática (CIO)	Gerencia de Arquitectura	Gerencia de Desarrollo	Gerencia de Operaciones de TI	Subgerencia de Servicios	Gerencia de Seguridad de la Información	Subgerencia de Continuidad de Negocio	Dirección de Privacidad de la Información
Establece los cambios	R	A	C	C	R	R	R		R	R	C	C	C	C	C		
Comunica los cambios		A	C	C	R	R	I	I	I	R	I	I	I	I	I	I	I
Facilita la implementación de los cambios				C	A			R		R	C	R	R	R	R	R	R
Mantiene los cambios	R	R	R	R	A			R		R	C	R	R	R	R	R	R

Fuente: Elaboración propia

El Consejo de Administración a través del **proceso 37**, **administra las relaciones con los interesados**, mantiene las relaciones con los entes del GCABA, sponsor, proveedores y usuarios finales. La Dirección de Informática genera un sistema de medición de satisfacción de los servicios de TI mediante un formulario, el que deben completar los agentes de los entes del GCABA, los ciudadanos y los proveedores. La información recopilada detalla el servicio utilizado, tipo de ingreso, dispositivo de conexión al servicio, nivel de satisfacción y posibilidad de recomendación de uso a un tercero. La siguiente *figura 16* especifica la *Operación de los servicios*.



Fuente: Diseño propio[63]

La Gerencia de Operaciones de TI **administra los eventos** y su clasificación en el **proceso 38** a través de la *tabla 14* con la *Administración de eventos en los servicios*.

Administración de eventos en los servicios																																
	Filtrado y tratamiento del evento										Clasificación del evento							Detección y escalado			Monitoreo		Disparador de respuesta					Opciones de respuesta					
	Aparición e Identificación	Notificación	Detección	Clasificación	Categoría	Prioridad	Importancia	Disparador	Opciones de respuesta	Verificación de acciones y cierre	Normal	Informativo	Excencional	Alerta	Operación inusual	Excención	Documentar el evento	Puntos de entrada al proceso	Rendimiento real vs SLA, OLA y UC	Acciones para mejora continua del servicio	Monitoreo activo	Monitoreo pasivo	Incidentes	Cambios	Procedentes de una RFC	Comando automatizado	Base de datos	Registro de eventos	Respuesta automática	Alerta y respuesta humana	Emisión de un RFC	Generación registro de incidencia	Generación de vínculo al registro
Servicio provisto por ASInf.																																

Fuente: Elaboración propia

El software o sistema se configura para filtrar, clasificar, categorizar, priorizar y proceder a dar una respuesta automática o de preferirlo, mediante un recurso humano. La siguiente *tabla 15* describe los atributos de *Administración de eventos en el software*.

Administración de eventos en el software																																
	Filtrado y tratamiento del evento										Clasificación del evento							Detección y escalado			Disparador de respuesta					Opciones de respuesta						
	Aparición	Notificación	Detección	Clasificación	Categoría	Prioridad	Importancia	Disparador	Opciones de respuesta	Verificación acciones y cierre	Normal	Informativo	Excencional	Alerta	Operación inusual	Excención	Documentar el evento	Puntos de entrada al proceso	Real vs SLA, OLA y UC	Acciones para mejora continua	Incidentes	Cambios	Procedentes de una RFC	Comando automatizado	Base de datos	Registro de eventos	Respuesta automática	Alerta y respuesta humana	Emisión de un RFC	Registro de incidencia	Vinculación al registro
Software o sistema usado por ASInf.																																

Fuente: Elaboración propia

El informe de administración de eventos los clasifica por tipo, categoría, prioridad e impacto. La **administración de incidentes**, **proceso 39**, soluciona la interrupción del servicio. La Subgerencia de Servicios soluciona el incidente o lo escala cuando no es resuelto. ASInf posee la Política de Respuesta ante Incidentes (PO1001). La próxima es la *tabla 16* que muestra la *Administración de incidentes*.

Administración de incidentes																												
	Proceso de registro						Estado					Proceso de clasificación									Escalado		Incidente solucionado					
	Admisión	Comprobación	Asignación	Registro	Información útil asociada	Notificar a usuarios impactados	Registrado	Activo	Suspendido	Resuelto	Cerrado	Categoría	Prioridad	Recursos necesarios	Impacto	Urgencia	Monitoreo del estado	Tiempo de respuesta estimado	Solución temporal	Solución definitiva	Verificación del SLA	Funcional	Jerárquico	Confirmar a usuarios	Actualizar SKMS	Reclasificación del incidente	Actualizar CMDB	Cerrar incidente
Servicios provistos por ASInf.																												

Fuente: Elaboración propia

La Gerencia de Operaciones de TI está a cargo de **atender las requisiciones de los servicios** en el **proceso 40** y dar cumplimiento a la solicitud, vinculación o escalado. Para éste último caso, la derivación puede dirigirse a la administración de incidentes (proceso 39), administración de accesos (proceso 42) o a desarrollar los ofrecimientos (proceso 2). La *tabla 17* muestra la *Atención de requisiciones de servicios*.

Atención de requisiciones de servicios															
	Solicitud					Escalado			Actualizar				Documentar	
Servicio	Recepción	Filtrado	Clasificación	Registro	Evaluación	Administración de incidentes (proceso 39)	Administración de accesos (proceso 42)	Desarrollar los ofrecimientos (proceso 2)	Base de datos de la configuración (CMDB)	Base de datos de los errores conocidos (KEDB)	Sistema de gestión del conocimiento del servicio (SKMS)	Base de datos de la configuración (CMDB)	Generación	Formalización
Servicios provistos por ASInf.														

Fuente: Elaboración propia

La etapa 4 de ITIL v3 incluye los procesos 41 al 46. La **administración de problemas**, comprendida en el **proceso 41**, restaura el servicio sin identificar las causas. La Subgerencia de Servicios de ASInf investiga las causas, recomienda soluciones, propone las peticiones de cambio y verifica las revisiones Post-Implementación (PIR) que garanticen las soluciones deseadas. ASInf implementa la próxima *tabla 18* de *Administración de problemas* para cada servicio, desde su identificación hasta la revisión post implementación y su cierre.

Administración de problemas																																		
	Identificación			Registración								Estado		Clasificación y asignación de recursos								Causa			Análisis y diagnóstico			Estimación y consecuencias				Revisión Post Implementación y cierre		
	Existencia en la base de datos	Verificar sistemas e infraestructura	Evaluar deterioro en servicios	Componentes implicados	Causas del problema	Síntomas provocados	Soluciones temporales	Servicios afectados	Prioridad	Urgencia	Impacto	Activo	Error conocido	Hardware	Software	Redes	Instalaciones	Recursos humanos	Recursos tecnológicos	Configuración de activos	Impacto en áreas funcionales	Falta de acuerdo entre áreas	Errores procedimentales	Documentación incorrecta	Definir causas del problema	Proponer soluciones temporales	Proponer soluciones definitivas	Estimar impacto en infraestructura	Costos asociados	Consecuencias en los SLAs	Evaluar RFC de emergencia	Verificar solución del problema	Actualizar base datos errores conocidos (KEDB)	Cambiar a estado cerrado
Servicios provistos por ASInf.																																		

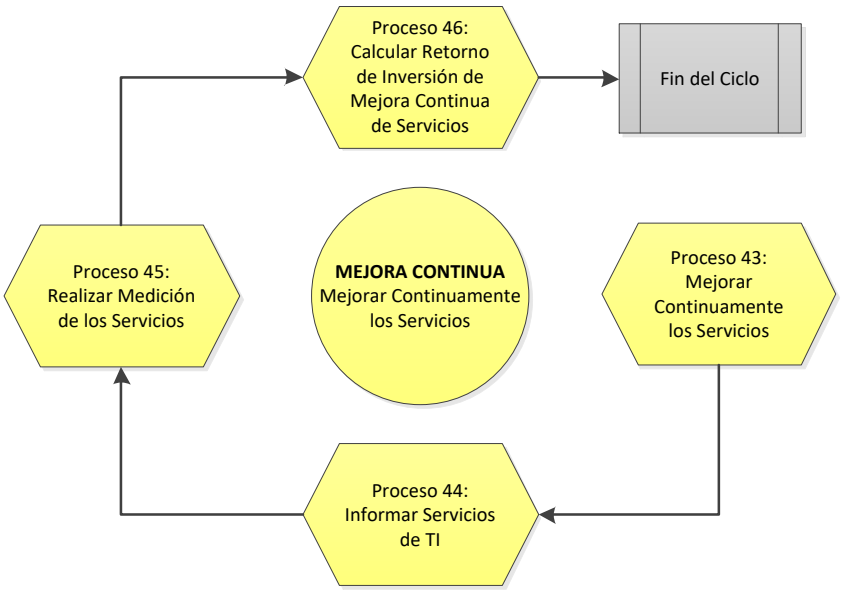
Fuente: Elaboración propia

Auditoría interna de ASInf prepara informes de administración de problemas que permiten el análisis de los aspectos claves relacionados con los problemas en los suministros de TI tales como el número total de problemas registrados, la cantidad de actualizaciones mensuales de la base de datos de errores conocidos (KEDB), etc. La Dirección de Seguridad de la Información (CISO) es la responsable de la **administración de los accesos** a usuarios autorizados de ASInf, entes del GCABA o proveedores externos que acceden a ciertos servicios de TI, comprendidos en el **proceso 42**. En la siguiente *tabla 19* se describen las etapas de *Administración de accesos*.

Administración de accesos																																
	Solicitado por				Petición de acceso		Verificación del solicitante						Supervisión de identidad y cambios				Monitoreo		Bajas y restricciones									Actualización			
	Recursos humanos	Petición de Cambio (RFC)	Actividad automática	Catálogo de servicios	Identificar al ente solicitante	Identificar agente responsable	Identidad del usuario	Responsabilidad	Verificar autorización	Identificar nivel de permiso	Motivos del acceso	Plazo para el acceso	Verificar identidad del usuario	Verificar nivel del autorizante	Reasignación de permisos	Gestionar cambios de acceso	Monitorear acceso	Monitorear el uso	Baja temporal de usuario	Restricción de permiso	Baja definitiva de usuario	Restricción definitiva de permiso	Motivo de la baja	Motivo de la restricción	Agente responsable solicitante	Organismo y cargo del solicitante	Administración de Aplicaciones	Datos de usuarios y derechos	Excepciones en incidencias	Administración de seguridad
Servicios provistos por ASInf.																																

Fuente: Elaboración propia

La siguiente *figura 17* especifica la *Mejora continua de los servicios*.



Fuente: Diseño propio[63]

Mejorar continuamente los servicios (MCS) es una actividad incluida en el **proceso 43**. La Dirección de Operaciones (COO) de ASInf es la responsable de gestionar la mejora continua. Genera un programa de premios a empleados que presenten ideas tecnológicas innovadoras. Define los Indicadores Críticos de Rendimiento (KPIs) tales como costos totales del presupuesto asignado, número de

servicios entregados o número total de incumplimientos. Para cumplir los objetivos, se definen los Factores Críticos de Éxito (CSF), tales como mejorar la planificación, incrementar los controles o minimizar la reasignación presupuestaria. La Dirección de Operaciones es la responsable del **proceso 44** establecido para **informar los servicios de TI**, generar los informes y exponer el estado de situación. La generación y el envío se realizan a través del sistema SADE, el cual permite el caratulado, vinculación, pases y consultas de los documentos. La siguiente *tabla 20* detalla los componentes contenidos en los *Informes de servicios de TI.*

Informes de servicios de TI																					
	Fuente		Destinatario			Frecuencia				Recopilación		Metodología				Respuesta			Propuesta de mejora			
	Recursos humanos	Recursos tecnológicos	Personal jerárquico	Personal técnico	Agente administrativo	Continuo	Diario	Semanal	Mensual	Manual	Automático	Observación	Entrevista	Encuesta	Reporte de sistemas	Personal jerárquico	Personal técnico	Agente administrativo	Servicios	Infraestructura	Organización	Procesos
Servicios provistos por ASInf.																						

Fuente: Elaboración propia

Para poder lograr las metas planificadas es necesario el **proceso 45**. El mismo **realiza la medición de los servicios de TI** en ASInf. Es esencial medir el desempeño actual y plantear los objetivos futuros. La siguiente *tabla 21* define las *Métricas para la administración de las finanzas de los servicios*. Si existe vinculación del KPI con el CSF se indica coloreando la celda, al igual que si expresa una medición directa.

Métricas para la administración de las finanzas de los servicios							
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la planificación financiera	Incrementar los controles financieros	Minimizar la reasignación presupuestaria		
CPA	Costos totales del presupuesto asignado					
CCP	Costos totales del presupuesto planificado					

Métricas para la administración de las finanzas de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la planificación financiera	Incrementar los controles financieros	Minimizar la reasignación presupuestaria		
CCA	Costos totales del presupuesto actual	■			■	
IFP	Número de informes financieros planificados		■		■	
IFF	Número de informes financieros planificados entregados en fecha		■		■	
IFT	Número de informes financieros planificados entregados fuera de fecha		■		■	
PAH	Presupuesto asignado a hardware	■		■	■	
PAS	Presupuesto asignado a software	■		■	■	
VAC	Variación de costos sin planificación	■		■		CCP-CCA
IPC	Índice de precisión de costos	■		■		CCP/CCA
IIF	Índice de informes financieros entregados con demora		■			IFT/IFP

Fuente: Elaboración propia

La posterior *tabla 22* exhibe las *Métricas para la administración de niveles de servicio.*

Métricas para la administración de niveles de servicio						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Gestionar calidad de servicios según requerimientos	Asegurar el nivel de SLR	Asegurar el soporte de los servicios		
SEG	Número de servicios entregados por ASInf al GCABA		■		■	
SAX	Número de servicios entregados por ASInf y por proveedores		■		■	
SSO	Número de servicios internos entregados sin OLA		■	■	■	
SSA	Número de servicios entregados sin SLA	■		■	■	
ILA	Número total de incumplimientos de SLA	■		■	■	
ALA	Número total de apercibimientos por incumplimiento de SLA	■		■	■	

Métricas para la administración de niveles de servicio						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Gestionar calidad de servicios según requerimientos	Asegurar el nivel de SLR	Asegurar el soporte de los servicios		
MIS	Número total de imposición de multas por incumplimiento de SLA	■		■	■	
MPS	Número total de multas pagadas por incumplimiento de SLA	■		■	■	
AES	Número total de agentes entrevistados por satisfacción en los servicios				■	
ASS	Número total de agentes satisfechos con los servicios	■	■	■	■	
AIS	Número total de agentes insatisfechos con los servicios	■	■	■	■	
IMP	Índice de multas pagadas por incumplimiento de SLA					MPS/MIS
IAS	Índice de agentes satisfechos con los servicios	■	■	■		ASS/AES

Fuente: Elaboración propia

La siguiente *tabla 23* define las *Métricas para la administración de las capacidades de los recursos*.

Métricas para la administración de las capacidades de los recursos						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la planificación de recursos de TI	Renovar los recursos de hardware	Renovar los recursos de software		
IFC	Número de incidentes provocados por falta de capacidad de hardware		■		■	
IFS	Número de incidentes de capacidad provocados por software inadecuado			■	■	
ICR	Número de incidentes provocados por falta de				■	
RRP	Número de recursos de TI planificados	■			■	

Métricas para la administración de las capacidades de los recursos						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la planificación de recursos de TI	Renovar los recursos de hardware	Renovar los recursos de software		
RPF	Número de recursos de TI planificados fallidos					
IPQ	Variación en la planificación de los recursos de TI					RRP- RPF

Fuente: Elaboración propia

La siguiente *tabla 24* define las *Métricas para la administración de la disponibilidad de los servicios*.

Métricas para la administración de la disponibilidad de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la disponibilidad de los servicios	Garantizar el cumplimiento del SLA	Asegurar el cumplimiento del OLA		
NTR	Número de incidentes registrados					
NII	Número de incidentes graves con impacto en la disponibilidad					
TDS	Tiempo total de disponibilidad del servicio					
TNS	Tiempo total de no disponibilidad del servicio					
IID	Número de incidentes de seguridad que impactan la disponibilidad					
CRS	Número de componentes de red, hardware y software					
CRA	Número de componentes de red, hardware y software soportados por ASInf					
CRP	Número de componentes de red, hardware y software soportados por proveedores externos					
PCC	Índice de tiempo promedio de confiabilidad					TNS/TDS

Métricas para la administración de la disponibilidad de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la disponibilidad de los servicios	Garantizar el cumplimiento del SLA	Asegurar el cumplimiento del OLA		
IRD	Índice de recuperación de la disponibilidad					NII/NTR

Fuente: Elaboración propia

La *tabla 25* muestra *Métricas para la administración de la continuidad de los servicios*.

Métricas para la administración de la continuidad de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la continuidad de los servicios	Asegurar el cumplimiento del SLA	Incrementar el control en la continuidad de los servicios		
NTR	Número de incidentes registrados					
IGC	Número de incidentes graves con impacto en la continuidad					
TCS	Tiempo total de continuidad del servicio					
TSS	Tiempo total sin continuidad en el servicio					
IIC	Número de incidentes de seguridad que impactan la					
SCS	Número de servicios en el catálogo de servicios					
SPC	Número de servicios cubiertos con un plan de continuidad					
SSC	Número de servicios sin cubrir con un plan de continuidad					
TTP	Tiempo transcurrido sin pruebas en el servicio					
SPF	Número de servicios con pruebas fallidas					
ISL	Número de incidentes de continuidad por					
ITC	Índice de tiempo de continuidad					TSS/TCS

Métricas para la administración de la continuidad de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar la continuidad de los servicios	Asegurar el cumplimiento del SLA	Incrementar el control en la continuidad de los servicios		
ICC	Índice de cobertura de continuidad					SPC/SCS

Fuente: Elaboración propia

La *tabla 26* define las *Métricas para la administración de cambios de los servicios*.

Métricas para la administración de cambios de los servicios						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mitigar los cambios no autorizados	Minimizar los cambios por emergencias	Agilizar los tiempos de los cambios autorizados		
NTC	Número total de cambios					
NCI	Número de cambios implementados autorizados					
NCS	Número de cambios implementados sin autorización					
NCP	Número de cambios pendientes					
TCI	Tiempo total de cambios implementados					
CPI	Número de cambios solicitados por incidentes					
CPE	Número de cambios por emergencia					
ICE	Índice de cambios por emergencia					CPE/NCI
TID	Tiempo promedio de implementación de cambios					TCI/NCI
IFX	Índice de cambios sin autorización					NCS/NCI

Fuente: Elaboración propia

La *tabla 27* son *Métricas para la administración de recursos y configuraciones*.

Métricas para la administración de recursos y configuraciones						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Minimizar fallos por actualización de la CMDB	Falta de registro de los RFC aprobados en la CMDB	Falta de existencia de componentes en la CMDB		
NCC	Número total de componentes en la CMDB					
NCE	Número total de componentes erróneos					
CSR	Número de componentes por cambios sin RFC					
SCS	Número de servicios en el catálogo de servicios					
SIX	Número de servicios vigentes inexistentes en el catálogo de servicios					
CDC	Número total de cambios de componentes					
CIE	Número de componentes con información errónea o					
IAQ	Índice de actualización de servicios					SIX/SCS
ICM	Índice de precisión de la CMDB					NCE/NCC

Fuente: Elaboración propia

La *tabla 28* son *Métricas para la administración de entregas e implementaciones*.

Métricas para la administración de entregas e implementaciones						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar servicios actualizando el histórico de versiones	Agilizar el tiempo de entregas e implementaciones	Minimizar la cantidad de entregas fallidas		
NTE	Número total de entregas					
NEI	Número de entregas implementadas					
TTE	Tiempo total de entregas implementadas					

Métricas para la administración de entregas e implementaciones						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Mejorar servicios actualizando el histórico de versiones	Agilizar el tiempo de entregas e implementaciones	Minimizar la cantidad de entregas fallidas		
EPI	Número de entregas que provocaron incidentes	■		■	■	
EER	Número de entregas con errores conocidos	■		■	■	
IEF	Índice de entregas fallidas	■		■		EPI/NEI
TIX	Tiempo promedio de entregas implementadas	■	■			TTE/NEI

Fuente: Elaboración propia

La siguiente *tabla 29* define las *Métricas para la administración de incidentes*.

Métricas para la administración de incidentes							
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)				Medición directa	Cálculo
		Incidentes resueltos	Mejorar calidad servicios de TI	Incrementar la productividad de ASInf	Incrementar la satisfacción de entes del GCABA		
NTR	Número de incidentes registrados	■	■	■	■	■	
NIL	Número de incidentes leves		■	■	■	■	
IGZ	Número de incidentes graves		■	■	■	■	
NIZ	Número de incidentes resueltos		■	■	■	■	
NXI	Número de incidentes pendientes		■	■	■	■	
NRI	Número de incidentes repetidos		■	■	■	■	
TTI	Tiempo total de solución de todos los incidentes	■	■	■	■	■	
TPS	Tiempo promedio de solución de incidentes	■	■	■	■		TTI/NTR
IIR	Índice de incidentes repetidos		■	■	■		NRI/NTR
IRI	Índice de resolución de incidentes		■	■	■		NIZ/NTR
IIS	Índice de incidentes con impacto significativo		■	■	■		IGZ/NTR

Fuente: Elaboración propia

La siguiente *tabla 30* define las *Métricas para la administración de problemas*.

Métricas para la administración de problemas						
Sigla	Indicador Crítico de Rendimiento (KPI)	Factor Crítico de Éxito (CSF)			Medición directa	Cálculo
		Minimizar la ocurrencia de problemas en servicios	Minimizar los errores de escalado	Minimizar problemas por falta de actualización de las bases de datos		
NIX	Número de incidentes derivados a problemas	■	■	■	■	
NTR	Número total de problemas registrados	■			■	
NUR	Número de problemas repetidos	■	■		■	
NPL	Número de problemas leves	■			■	
NIG	Número de problemas graves	■			■	
NIR	Número de problemas resueltos	■			■	
NIP	Número de problemas pendientes	■	■		■	
TTS	Tiempo total de solución de todos los problemas	■	■		■	
TPP	Tiempo promedio de solución de problemas	■	■			TTS/NTR
IPR	Índice de problemas repetidos	■	■			NUR/NTR
RII	Índice de resolución de problemas	■	■			NIR/NTR
IIP	Índice de incidentes repetidos derivados a problemas	■	■			NIX/NTR
ISI	Índice de problemas con impacto significativo	■				NIG/NTR

Fuente: Elaboración propia

La medición de los servicios de TI provistos por ASINF se puede realizar usando diversos recursos durante diferentes plazos. La medición planificada puede implementarse automáticamente o en forma manual con recursos humanos durante períodos establecidos, en ciertos horarios pico para medir la congestión o durante plazos para medir la disponibilidad o continuidad de un servicio. El **proceso 46** está establecido para **calcular el retorno de inversión de la mejora continua de los servicios**. Desde el punto de vista financiero, se entiende el retorno sobre la inversión

(ROI) como una razón financiera que compara el beneficio obtenido en relación con la inversión realizada. Como se aclaró anteriormente, ASInf como organismo estatal, desarrolla sus actividades procurando la eficiencia, ya que gestiona recursos públicos.

Nuevo formulario de requerimientos de servicios

Como se detalló anteriormente, el formulario único de requerimientos utilizado actualmente por ASInf carece del contenido necesario para comenzar con la modificación del servicio vigente de TI o de un nuevo servicio. Se confecciona el nuevo formulario digital de requerimientos de servicios gestionado a través del sistema SADE[40] y canalizado mediante la Gerencia de Gestión de requerimientos. La solicitud es enviada a ASInf a través del formulario con todos sus campos completos, no siendo requisito el detalle técnico, pero sí estableciendo la base de análisis que permita a los agentes de ASInf establecer el estado de la solicitud como rechazada, aceptada o en evaluación. Este procedimiento permite optimizar los recursos de la Agencia de Sistemas de Información y eficientizar las solicitudes de servicios. Mediante la próxima *tabla 31* se detalla el *Nuevo formulario de requerimientos de servicios*.

Nuevo formulario de requerimientos de servicios	
Fecha: / /	Hora: :
Horario de contacto:	
Repartición solicitante:	
Ministerio:	Organismo:
Agente solicitante:	Cargo:
Teléfono fijo:	Celular:
Correo institucional:	Dirección:
Autoriza:	Cargo:
Nombre del Proyecto/Sistema:	
Marque con una “X” lo que corresponda	
Proyecto nuevo:	Mejora/Funcionalidad:
Solicitud de servicio:	Solicitud de hardware/software:
Incidente de hardware:	Incidente de software:
Incidente de impresora/escáner:	Incidente de telefonía:
Mantenimiento de hardware:	Incidente de conectividad:
Solicitud de insumos de impresión:	Cambio de equipo:
Cambio de área:	Configuración de correo:

Nuevo formulario de requerimientos de servicios	
Solicitud de back up:	Solicitud de equipo:
Problemas con clave de usuario:	Compra de hardware/software:
Actualización de software:	Nueva conectividad:
Proyecto nuevo / Funcionalidad	
Propósito	**Descripción**
Proyecto nuevo	SI / NO
Desarrollo de software	SI / NO
Desarrollo de sistema	SI / NO
Desarrollo de aplicación	SI / NO
Funcionalidad	
Justificación	
Beneficios para el GCABA	
Beneficios para el organismo solicitante	
Fecha estimada de lanzamiento	
Alcance	
Límites	
Responsable del proyecto	
Objetivos medibles del proyecto	
Partes interesadas	
Posibles usuarios	
Análisis de viabilidad	SI / NO
Análisis de riesgos	SI / NO
Análisis de impacto del proyecto	SI / NO
Presupuesto para el proyecto	SI / NO
Monto asignado para el proyecto	
Ejecución del proyecto anual	SI / NO
Ejecución del proyecto plurianual	SI / NO
Recursos propios	SI / NO
Tiempo de funcionamiento del proyecto	
Demanda del proyecto	
Estimación del incremento de la demanda futura	
Necesidad de capacitación	SI / NO
Necesidad de recursos humanos para la operación	SI / NO
Velocidad de navegación	
Disponibilidad	
Continuidad	
Número máximo de interrupciones mensuales	
Tiempo máximo de interrupción mensual	
Tiempo de respuesta por incidente	
Nivel de impacto por la interrupción del servicio	
Nivel de recuperación	Cold / Warm / Hot
Nivel de criticidad de la información	
Gestiona transacciones	SI / NO

Fuente: Elaboración propia

Conclusiones

Hace ya varios años comenzaba el debate sobre cuál debía ser el papel del Estado frente a las nuevas tecnologías de la información y la comunicación (TIC). Algunos defensores de las tecnologías exponían como ventajas la maximización de la eficiencia en los procesos, los detractores decían que su implementación incrementaba los riesgos por la exposición de datos sensibles. El tiempo transcurría y la velocidad de la revolución tecnológica era mayor que la del debate.

La aceptación de la tecnología por parte de las empresas privadas y la visualización de sus ventajas fueron mucho más rápidas que el reconocimiento por parte del Estado. El rol del Estado fue cambiando, sus procesos lentos, formales y burocráticos, empujados por la tecnología, se fueron modernizando.

Aquellos dirigentes críticos de la implementación tecnológica visualizaron que también promovía la inclusión social, no sólo era una herramienta eficiente y productiva. Aún no me queda muy claro si el Estado evaluó y reconoció las ventajas de la tecnología o se vio forzado a comenzar a implementarlas porque la globalización marcó el único camino a recorrer. Sea cual fuere la respuesta, y no es objetivo de este trabajo, el desarrollo tecnológico en el Estado es bienvenido. Lo que no me genera dudas es que actualmente el Estado brega por estar a la vanguardia de la tecnología, investigando, invirtiendo y actualizando la infraestructura tecnológica. Quizás la asignación presupuestaria y el desarrollo tecnológico podrían ser mayores, pero en esa dirección vamos.

Nadie puede desconocer que la tecnología está en constante evolución, viaja a una velocidad difícil de medir, es prácticamente imposible alcanzarla, invertir y capacitar a los recursos humanos. Cuando pensamos que nada nuevo va a aparecer, la tecnología y la innovación nos vuelven a sorprender y la frase “todavía no está todo inventado” repetida hasta el cansancio, vuelve a ser usada. Robótica, Inteligencia Artificial, Biotecnología, Internet de las Cosas y un sinfín de innovaciones comienzan a aparecer.

Al describir los antecedentes del marco, quedaron expuestas algunas falencias y creencias. La necesidad de la tecnología es reconocida mundialmente, el uso tanto en el

sector público como privado es significativo. En algunos países desarrollados sólo está implementada la gestión de TI y no su gobierno y en ciertos casos se implementa el gobierno luego de la gestión de TI. Las investigaciones dejan dudas respecto de la relación directa entre el nivel de desarrollo del país y el patrón de madurez de la gobernanza de TI. Pero está probado que aunque la madurez en los procesos de TI sea relativamente baja, igualmente aporta ventajas para la toma de decisiones.

En estándares internacionales como ISO 27001, las investigaciones reflejaron que la capacitación y el nivel técnico del equipo a cargo de su implementación resultó ser un obstáculo significativo y que la falta de participación de la dirección fue un obstáculo secundario. En diversas organizaciones bancarias públicas y privadas de distintos países, los marcos de TI brindaron transparencia, permitieron cumplir las Normas de Basilea III y mejoraron la medición del nivel de logros de sus metas.

En la actualidad, el reconocimiento de TI llegó a las universidades internacionales. No es como años atrás, ya no son cursos complementarios sólo para profesionales de la carrera, sino que se promueven líneas de investigación estratégica de las TI, buenas prácticas de gobierno y transformación digital.

Cuando decidí desarrollar esta tesis no apuntaba a criticar la normativa ni los estándares internacionales vigentes en el marco tecnológico del Gobierno de la Ciudad Autónoma de Buenos Aires, por el contrario, apuntaba a sumar, fortalecer y aportar mi grano de arena a la estructura tecnológica vigente. Estoy totalmente convencido que no se debe caer en la crítica fácil de “lo anterior”, porque para poder avanzar, alguien tuvo que haber dado el paso inicial. Con la convicción de contribuir con los avances en la plataforma tecnológica en la Ciudad Autónoma de Buenos Aires, se plantean tres objetivos desarrollados en varios capítulos.

El primer objetivo específico que se plantea es “Analizar los instrumentos de evaluación y estandarización generados por el Gobierno de la Ciudad Autónoma de Buenos Aires”. Se expone la misión, visión, roles, responsabilidades y normativa. También los sistemas, aplicaciones vigentes, infraestructura, políticas tecnológicas y su impacto, el formulario único de requerimientos y los procesos llevados a cabo por cada área.

Lo expuesto anteriormente me permite concluir que el Gobierno de la Ciudad Autónoma de Buenos Aires a través de la Agencia de Sistemas de Información ha desarrollado e implementado la tecnología. Si bien se observan avances tecnológicos a través de un centro de datos de última generación y la actualización de la infraestructura vigente, la metodología de solicitud de servicios mediante un formulario único de requerimientos carece de detalles. La solicitud del requerimiento es básica y puede ser confeccionada, en ciertos casos, por personal sin conocimientos técnicos, resultando el suministro de un servicio que no es el necesitado.

Este proceso debe formalizarse y desarrollarse a través de un proyecto mediante la asignación de los responsables con conocimientos técnicos, relevamiento, análisis de servicios reutilizables, costos y evaluación respecto del lineamiento con los objetivos estratégicos de ASInf. En el nuevo marco tecnológico, para solicitar un nuevo servicio de TI o modificar uno existente, se debe completar el nuevo formulario digital de requerimientos de servicios, el cual cuenta con los parámetros establecidos en ITIL v3. Asimismo, como ya se precisó anteriormente, la solicitud debe gestionarse digitalmente mediante el sistema SADE. El canal de contacto, es a través de la Gerencia de Gestión de requerimientos de ASInf, mediante la cual se genera la interacción entre el organismo y el responsable de la solicitud. En el proceso se acuerdan plazos y se prioriza respecto de otros requerimientos. Se evalúa y dimensiona la conveniencia de derivarlo a la Gerencia de Gestión de Proyectos (PMO). El mecanismo fluido y bidireccional de la Gerencia de Gestión de requerimientos de ASInf con los entes, permite elaborar un ranking de requerimientos entre las áreas, asignar los recursos necesarios y acordar los plazos con los responsables de crear las solicitudes. A lo largo de este trabajo también se desarrolla el mecanismo de capacitación de los agentes de ASInf, entes del GCABA y proveedores, indispensable para facilitar la confección y precisión del formulario de requerimientos de servicios de TI.

La capacitación no es un tema menor, asociado a los agentes que brindan el servicio, entes usuarios del GCABA, usuarios finales y proveedores de ASInf. Si los agentes de TI que forman parte de ASInf no están capacitados en los servicios provistos, la implementación y actualización no logrará los objetivos planteados. Si los proveedores no cuentan con los conocimientos necesarios, sobretodo en los sistemas y aplicaciones específicas del GCABA, el soporte complementario planeado a los

servicios no será el suficiente. Para el caso que la carencia de capacitación impacte en los usuarios, no podrá explotarse al máximo el nivel de los servicios suministrados.

El Marco Normativo de Tecnología de Información vigente fue desarrollado partiendo de la base de dos estándares internacionales, ISO 27001 e ISO 17799, los que aseguran un sistema de gestión de seguridad de la información. A partir de estos se desarrolló la estructura de ASInf, que desde su creación ha sufrido modificaciones y reasignación de responsabilidades.

La carencia actual más visible en la estructura organizativa es la falta de separación entre el gobierno de las tecnologías de la información y su gestión, lo que puede provocar un solapamiento y una confusa identificación de las responsabilidades primarias de cada dirección, gerencia o subgerencia. Se observa la falta de niveles superiores en su organigrama, los que impedirían la evaluación específica en algunos temas como el riesgo corporativo, desarrollo de proyectos y financiero.

El segundo objetivo que se proyecta en este trabajo, “Determinar las normas técnicas a utilizar por los organismos de la Ciudad Autónoma de Buenos Aires” se desarrolla mediante la recopilación y el análisis de los estándares tecnológicos internacionales vigentes. Se evalúan los principios, componentes, modelos, alcances, limitaciones, procesos, niveles de cobertura y versiones. Se plantean sus ventajas, desventajas, estructuras, tipos de uso y comparaciones.

Habiendo comparado y destacado las ventajas y desventajas de los diversos estándares internacionales, es importante remarcar una diferencia clave por la cual se optó por COBIT 5 para desarrollar el nuevo marco tecnológico en reemplazo del anterior basado en las normas ISO 17799 e ISO 27001.

ISO 27001 actúa como un marco para la gestión estandarizada de la seguridad de la información y se centra estrictamente en las mejores prácticas orientadas a la seguridad. COBIT 5 tiene un alcance más amplio, es orientado a la tecnología, abarca la organización de extremo a extremo, separa y administra el gobierno y la gestión de los procesos de negocios de tecnología de la información, dentro de los cuales la seguridad de la información también forma parte del marco.

El enfoque de COBIT 5 es más global, apunta a cerrar la brecha entre los objetivos comerciales y los procesos de tecnología. Por ello se habla de la complementariedad entre los marcos ISO 17799, ISO 27001 y COBIT 5.

Luego de mucho investigar puedo concluir que ningún estándar internacional provee una cobertura total, cada uno abarca distintos ámbitos, tales como calidad, gobierno de TI, gestión de servicios de TI y sus funciones. Algunos como ISO 27001 e ISO 17799 se especializan en la seguridad de la tecnología. PMBOK se orienta más al desarrollo de los proyectos mediante sus diez áreas de conocimiento. La especificidad de algunos marcos genera ventajas en ciertos aspectos y limitaciones en otros tantos.

En cuanto a lo abordado con anterioridad y habiendo evaluado los diversos estándares tecnológicos, puedo concluir que la aplicación de dos estándares internacionales complementarios entre sí como lo son COBIT 5 e ITIL v3, proveen un modelo adecuado para implementar el Nuevo Marco Tecnológico para la Ciudad Autónoma de Buenos Aires.

Lo logro partiendo primero desde el estándar tecnológico COBIT 5, cuya decisión está respaldada y justificada en la clara separación entre el gobierno de TI y su gestión que permite cubrir la carencia observada en el inicio de este trabajo. Garantizo procesos esenciales, hasta hoy no cubiertos, como el aseguramiento del establecimiento y mantenimiento del marco de referencia de gobierno, la entrega de los beneficios, la optimización del riesgo y recursos y la transparencia hacia las partes interesadas.

Además, COBIT 5 provee satisfacción a las necesidades de las partes interesadas, cubre a ASInf de extremo a extremo, aplica un marco de referencia único integrado y hace posible un enfoque holístico. Por otro lado, ITIL v3 complementa y genera sinergia con COBIT 5, a través de mejores prácticas, incrementando la confiabilidad en la entrega de los servicios tecnológicos, beneficiando el proceso de mejora continua y la conexión de todo el organismo con la entrega de los servicios de TI.

Por último, en esta tesis, se plantea el tercer objetivo específico, a través del cual se proyecta “Desarrollar el Marco Tecnológico para el Gobierno de la Ciudad

Autónoma de Buenos Aires". Por ello avanzo en este sentido, para poder concluir y lograr el objetivo general planteado al inicio de este trabajo.

En el curso de mi investigación y habiendo definido a COBIT 5 complementado con ITIL v3 comienzo a desarrollar el nuevo Marco Tecnológico de la Agencia de Sistemas de Información. Para agilizar y facilitar la implementación de ambos estándares parto de la "reutilización" de los recursos tecnológicos existentes. No propongo la idea de "dar de baja y destruir" lo construido y vigente, sino de respetar el modelo COBIT 5 e ITIL v3 ordenando y modernizando la infraestructura tecnológica, capacitando y reasignando los recursos humanos.

Por lo antes dicho propongo la nueva misión, visión, valores y la descripción de los roles para la Agencia de Sistemas de Información. Basado en COBIT 5 defino los objetivos estratégicos de ASInf, su relación con las metas de TI y sus procesos catalizadores. Proyecto a la agencia como una organización pública innovadora que impulse el bienestar y esté orientada a la tecnología como un instrumento de desarrollo. Entiendo que el GCABA puede llegar con la tecnología a niveles sociales con carencias para brindarle acceso a material educativo que los ciudadanos no podrían adquirir. Informarlos respecto de las fechas de vacunación y controles médicos necesarios por edades y enfermedades existentes fomentando la previsión y protección sanitaria.

Destaco valores como la responsabilidad, transparencia y la vocación de servicio, indispensables para que cada empleado del GCABA cumpla con la tarea que le fue asignada. Planteo roles, hoy no existentes como el Consejo de Administración, Comité Ejecutivo Estratégico de TI, Consejo de Arquitectura o el Comité de Riesgo Corporativo, entre otros. Con ellos logro la especificidad y conocimientos en cada área para evaluar y colaborar en las decisiones del gobierno de TI.

Defino las metas relacionadas con las tecnologías de ASInf para lograr o mejorar los objetivos organizacionales planteados. Establezco servicios provistos por ASInf, a los actuales le agrego otros desarrollados mediante innovación tecnológica.

Proyecto el desarrollo de internet de las cosas para ser aplicado en las calles con el objetivo de predecir accidentes de tránsito y delitos. El mismo permite conectar el flujo de circulación de los vehículos con los sistemas de información con la finalidad de

ofrecer fluidez y asegurar el camino más ágil. Con ello se minimizan los riesgos de accidentes trazando la ruta con menor tránsito.

También, se utiliza para detectar actitudes sospechosas en áreas críticas que incrementen la atención del personal de vigilancia para predecir delitos callejeros, asignando con mayor agilidad al personal adecuado. La misma tecnología será aplicada a la salud, para la prevención médica en pacientes de riesgo mediante la colocación de marcapasos o biochips que emitan alertas y el paciente pueda recibir instrucciones de salud adecuadas ante una situación de emergencia hasta que sea asistido por personal médico.

Además, defino el desarrollo de sistemas predictivos para el mantenimiento del alumbrado público con el propósito de minimizar sus costos utilizándolo sólo ante la necesidad y agilizando las intervenciones ante incidentes. Sistemas que emitan alertas y asignen al personal técnico adecuado con mayor cercanía para solucionar el evento. Para proteger los activos informáticos y mitigar los riesgos por incendios, dispongo la implementación de sistemas de detección temprana de humos en los centros de cómputos con un sistema de supresión de fuegos, que generen alertas y actúen ante la detección de llamas o eventos que puedan producir un incendio.

También considero los sistemas de visión artificial para el tránsito vehicular y el control de semáforos en la Ciudad Autónoma de Buenos Aires para evitar los accidentes y agilizar la circulación. Estos sistemas apoyan la implementación de la inteligencia artificial aplicada al tránsito. Para identificar a un ciudadano que requiera hacer un trámite en el Gobierno de la Ciudad Autónoma de Buenos Aires contemplo el desarrollo y la provisión de sistemas de reconocimiento facial, evitando el ingreso manual de su usuario y clave. Persiguiendo la misma dirección, con sistemas de inteligencia artificial, brindar aplicaciones mediante chatbot, con agentes virtuales para mejorar la atención de las consultas sobre el uso de TI a los entes del GCABA y a los ciudadanos.

En consecuencia, puedo concluir que el objetivo general de esta tesis “Elaborar una propuesta de Marco Tecnológico para el Gobierno de la Ciudad Autónoma de Buenos Aires desarrollado a través de COBIT 5 (Control Objectives for Information and related Technology) y complementado mediante ITIL v3 (Information Technology

Infrastructure Library) fue logrado. La profundidad y el alcance de esta tesis estuvieron circunscriptos a la obtención de los datos provenientes desde ASInf.

Mediante ITIL v3 defino lineamientos generales para la gestión en ASInf, algunos de ellos existentes, pero sin la formalización correspondiente. Se definen sus fortalezas, debilidades, oportunidades y amenazas.

Determino nuevos servicios de TI y los procedimientos para evaluar los recursos necesarios, la gestión de las finanzas, la demanda y la proyección de las inversiones a mediano y largo plazo. También distingo el perfil de estilo de organización, funciones y direcciones que apoyen el cumplimiento de los objetivos planteados. La gestión de los recursos humanos, estudios, habilidades y capacidades para cubrir cada puesto. La imperiosa necesidad de capacitación, con una carga horaria recomendada en 20 horas anuales para cada agente, mediante cursos establecidos por solicitud del personal jerárquico y también por demanda de los agentes afectados.

Preciso planes de seguridad, calidad, continuidad y disponibilidad de los servicios, definiendo componentes para priorizar la asignación de los recursos. Especifico los componentes para la administración del cambio, entregas e implementaciones, validaciones de servicios y pruebas. El formato de las comunicaciones, digitales, masivas o individuales y la firma de los acuerdos de compromisos de conducta y ética por parte de los agentes de ASInf, hoy vigentes y formalizados, pero en ocasiones sin la documentación que acredite la aceptación de la normativa por parte del empleado.

También aclaro los parámetros para definir los Acuerdos de nivel operacional (OLA) con los entes del GCABA, en la actualidad utilizados en contadas ocasiones. Los Acuerdos de Niveles de Servicio (SLA), actualmente con mayor nivel de formalización, firmados con los proveedores externos.

Puntualizo la gestión de eventos, incidentes, problemas y el escalado al área responsable según el rol definido. El proceso de alta, baja, modificación, bloqueo, asignación del perfil de usuario y acceso a los recursos tecnológicos.

Es justo destacar que el marco obtenido tiene limitaciones temporales, no será de utilidad con el paso de los años si no es actualizado. Habiendo destacado que la

tecnología está en permanente evolución, el paso del tiempo y la constante innovación exige la actualización de la infraestructura, el incremento de los servicios y su integración, la capacitación de la dirección, los recursos humanos y usuarios.

Las entidades públicas cada día interactúan más con el sector privado, brindando y obteniendo información, motivo por el cual, la desactualización y el uso de tecnología obsoleta, no sólo deja a ASInf y a los entes del GCABA con servicios de TI con poca utilidad, sino también los aísla y minimiza la relación con el sector privado y público establecidos a la vanguardia tecnológica.

Procesos como la mejora continua de los servicios son inevitables para progresar y renovar los servicios de TI ofrecidos. Para establecer una mejora es imprescindible conocer la situación actual con los parámetros de los servicios y su medición correspondiente. Así se puede proyectar a futuro una mejora desde el estado real del servicio. Para ello defino los indicadores críticos de rendimiento y los factores críticos de éxito, para lograr una adecuada gestión y obtención de las metas definidas.

Por todos estos motivos, creo conveniente implementar el nuevo marco tecnológico en la Ciudad Autónoma de Buenos Aires y actualizarlo temporalmente según los nuevos servicios de TI ofrecidos y los avances tecnológicos.

Bibliografía

Normas Técnicas

GTI4U. Obtenido el año 2019 en la Word Wide Web: http://www.gti4u.es/ [Accedido el 13/8/20]

Estándar de Desarrollo (año 2019). Obtenido el 1 de Abril de 2019 en la Word Wide Web: https://n9.cl/2ywv6 [Accedido el 16/5/19]

Evaluation of Patient Information System in Public Health Service Using the COBIT 5 Framework. Trianto. Obtenido el año 2018 en World Wide Web: https://n9.cl/cgmax [Accedido el 13/8/20]

Infraestructura de centro de datos. TIER 3. Obtenido en el año 2017 en la Word Wide Web: https://n9.cl/2ezxw [Accedido el 27/6/19]

International Journal of Applied Engineering. Obtenido el año 2017 en World Wide Web: https://n9.cl/ungbv [Accedido el 13/8/20]

Information Technology Governance challenges facing the public sector in South Africa. Wits Business School. Obtenido el año 2017 en la Word Wide Web: https://n9.cl/y2w8 [Accedido el 14/8/20]

PMBOK. Obtenido el 6 de Setiembre de 2017 en la Word Wide Web: www.pmi.org [Accedido el 27/7/19]

Journal of Information Systems Engineering and Business Intelligence. Obtenido en Octubre de 2016 en la Word Wide Web: https://n9.cl/du8t [Accedido el 13/8/20]

¿ITIL o COBIT? Javier Peris. Obtenido el 22 de Septiembre de 2015 en la Word Wide Web: https://n9.cl/171y [Accedido el 12/8/20]

Asociación Colombiana de Ingenieros de Sistemas. Obtenido el 14 de Septiembre de 2015 en la Word Wide Web: https://n9.cl/izjrb [Accedido el 2/9/20]

Benchmarking of COBIT 5 PAM Assessments Performed in Brazilian Public Sector Banking Organizations. Obtenido el 24 de Agosto de 2015 en World Wide Web: https://n9.cl/c3ts7 [Accedido el 13/8/20]

ES0101. Obtenido el 22 de Junio de 2015 en la Word Wide Web: https://n9.cl/5i05 [Accedido el 15/5/19]

Estándares ASI. Obtenido el Obtenido el 30 de Diciembre de 2014 en la Word Wide Web: https://n9.cl/crgm [Accedido el 15/5/19]

Estándar de Desarrollo (año 2014). Obtenido el 30 de Diciembre de 2014 en la Word Wide Web: https://n9.cl/9qh9 [Accedido el 15/5/19]

PC0901. Proceso de control de cambios en software de aplicación provisto por Organismos. Obtenido el año 2014 en la Word Wide Web: https://n9.cl/jlw3 [Accedido el 16/5/19]

ISO 27001. Obtenido el año 2013 en la Word Wide Web: https://n9.cl/tetg [Accedido el 26/6/19]

University of Southern Queensland. Implementation of IT Infrastructure Library (ITIL) in Australia. Obtenido el 2 de Julio de 2013 en la Word Wide Web: https://n9.cl/1qge [Accedido el 12/8/20]

Mapping of BASEL III and COBIT 5 framework in Banking Sector of India. Obtenido en Junio de 2013 en la Word Wide Web: https://n9.cl/qjpw [Accedido el 12/8/20]

ISACA. Obtenido el año 2012 en la Word Wide Web: https://n9.cl/4xcr [Accedido el 27/6/19]

ISACA. Obtenido el año 2011 en la Word Wide Web: https://n9.cl/eqcg [Accedido el 27/7/19]

Australian Information Security Management Conference. Obtenido el 1 de Enero de 2011 en la Word Wide Web: https://n9.cl/trovx [Accedido el 14/8/20]

ITIL v3. Obtenido en Diciembre de 2010 en la Word Wide Web: https://n9.cl/pkz6 [Accedido el 20/9/19]

IT Governance Maturity in the Public Sector Organizations in a Developing Country. Obtenido en Septiembre de 2010 en la Word Wide Web: https://n9.cl/uxxq [Accedido el 12/8/20]

COBIT 5. Obtenido el año 2009 en la Word Wide Web: https://n9.cl/4qy9 [Accedido el 15/5/19]

ITIL v3. Obtenido el año 2007 en la Word Wide Web: https://n9.cl/lgxs [Accedido el 15/5/19]

ISO 17799. Obtenido el año 2005 en la Word Wide Web: https://n9.cl/4gyw [Accedido el 26/6/19]

ISO/IEC 27001. Obtenido el año 2005 en la Word Wide Web: https://n9.cl/tetg [Accedido el 27/7/19]

International Organization for Standardization. Obtenido en el año 2005 en la Word Wide Web: https://n9.cl/ydcgc [Accedido el 27/7/19]

Instituto Nacional de Tecnología Industrial. Obtenido en la Word Wide Web: https://www.inti.gob.ar/ [Accedido el 26/9/19]

Norma IRAM. Obtenido el 28 de junio del año 2002 en la Word Wide Web https://n9.cl/awhv [Accedido el 27/6/19]

Estándares de aseguramiento y auditoría de TI de ISACA. Obtenido en la Word Wide Web: https://n9.cl/bu26 [Accedido el 27/6/19]

Normas Jurídicas

Gobierno Nacional

Ley 25326/00. Protección de Datos Personales. Obtenido el 2 de Noviembre de 2000 en la Word Wide Web: https://n9.cl/4wqp [Accedido el 27/7/19]

Ley 25036/98. Propiedad Intelectual. Obtenido el año 1998 en la Word Wide Web https://n9.cl/ml97 [Accedido el 27/7/19]

Ley 14772/58. Energías y Combustibles. Obtenido el año 2019 en la Word Wide Web: https://n9.cl/0b9m2 [Accedido el 27/7/19]

Ley 11723/33 de Régimen Legal de la Propiedad Intelectual. Obtenido el año 2019 en la Word Wide Web: https://n9.cl/vk8or [Accedido el 27/7/19]

Gobierno de la Ciudad Autónoma de Buenos Aires

Ley 5688. Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires. Obtenido el 17 de Noviembre de 2016 en la Word Wide Web: https://n9.cl/i38o [Accedido el 12/6/19]

Ley 4895. Ley de Ética en el Ejercicio de la Función Pública. Obtenido el 15 de Enero de 2014 en la Word Wide Web: https://n9.cl/ozx6 [Accedido el 15/6/19]

Ley 3784/11. Semana del Uso Seguro de Internet. Obtenido el 12 de Mayo de 2011 en la Word Wide Web: https://n9.cl/i25x [Accedido el 15/6/19]

Ley 3304. Obtenido el 7 de Enero de 2010 en la Word Wide Web: https://n9.cl/zy8e [Accedido el 27/7/19]

Ley 2689. Obtenido el 17 de Abril de 2008 en la Word Wide Web: https://n9.cl/5b2c7 [Accedido el 22/5/20]

Ley 1845/05. Obtenido el 17 de Agosto de 2007 en la Word Wide Web: https://n9.cl/hs9r [Accedido el 25/5/19]

Ley 2095. Ley de Compras y Contrataciones de la Ciudad. Obtenido el 2 de Noviembre de 2006 en la Word Wide Web: https://n9.cl/mxr6 [Accedido el 4/5/19]

Ley 325/99. Obtenido el 28 de Diciembre de 1999 en la Word Wide Web: https://n9.cl/02ji [Accedido el 23/11/19]

Ley 104/98. Obtenido el 19 de Noviembre de 1998 en la Word Wide Web: https://n9.cl/mz7yd [Accedido el 25/5/19]

Ley 70. Sistemas de gestión, administración, financiera y control del sector público de la Ciudad. Obtenido el 27 de Agosto de 1998 en la Word Wide Web: https://n9.cl/fcwb [Accedido el 8/12/19]

Decreto Nº 116/2014. Obtenido el 1 de Abril de 2014 en la Word Wide Web: https://n9.cl/azui [Accedido el 22/5/19]

Decreto Nº 196/11. Expediente electrónico. SADE. Obtenido el 28 de Marzo de 2011 en la Word Wide Web: https://n9.cl/r51f [Accedido el 7/3/19]

Decreto N° 1036/GCABA/08. Obtenido el 27 de Agosto de 2008 en la Word Wide Web: https://n9.cl/h8z6 [Accedido el 22/5/19]

Decreto Nº CABA Nº 139/96. Sistema de Control Interno. Obtenido el 11 de Setiembre de 1996 en la Word Wide Web: https://n9.cl/5tf1 [Accedido el 7/9/19]

Resolución Nº 398/MJYSGC/19. Sistema de Reconocimiento Facial de Prófugos. Obtenido el 24 de Abril de 2019 en la Word Wide Web: https://n9.cl/bh10 [Accedido el 15/9/19]

Resolución Nº 224/ASINF/2018. Obtenido el 18 de Diciembre de 2018 en la Word Wide Web: https://n9.cl/760m [Accedido el 16/5/19]

Resolución N° 12/ASInf/17. Marco Normativo Cloud Computing. Obtenido el 1 de Febrero de 2017 en la Word Wide Web: https://n9.cl/p2wx [Accedido el 15/5/19]

Resolución N° 134/ASInf/16. Obtenido el 29 de Agosto 2016 en la Word Wide Web: https://n9.cl/xwhg [Accedido el 16/5/19]

Resolución Nº 205/SGCABA/16. Normas Éticas - Boletín oficial de la Ciudad Autónoma de Buenos Aires, N° 5.037, página Nº 305 en la Word Wide Web: https://n9.cl/m7nk [Accedido el 15/8/19]

Resolución N° 239/ASInf/15. Marco Normativo de IT. Obtenido el 12 de Enero de 2015 en la Word Wide Web: https://n9.cl/ivc1 [Accedido el 15/8/19]

Resolución N°177/ASInf/13. Obtenido el 6 de Noviembre de 2013 en la Word Wide Web: https://n9.cl/12dwx [Accedido el 15/5/19]

Resolución N° 190/MMGC/12. Obtenido el 11 de Mayo de 2012 en la Word Wide Web: https://n9.cl/5jua [Accedido el 15/5/19]

Resolución Nº 596-MHGC/11. Políticas, Términos y Condiciones de Uso del Sistema Electrónico de Adquisiciones y Contrataciones. Obtenido el 29 de Abril de 2011 en la Word Wide Web: https://n9.cl/1tlv [Accedido el 15/5/19]

Resolución N° 97/ASINF/10. Obtenido el 4 de Junio de 2010 en la Word Wide Web: https://n9.cl/bhnax [Accedido el 15/5/19]

Resolución N° 44/ASInf/08. Obtenido el 15 de Setiembre de 2008 en la Word Wide Web: https://n9.cl/tax92 [Accedido el 22/5/19]

Disposición N° 36-DGCG/15. Sistema integrado de gestión y administración financiera (SIGAF). Obtenido el 11 de Febrero de 2015 en la Word Wide Web: https://n9.cl/czn5d [Accedido el 8/12/19]

Disposición N° 143/08. Inscripción de bases de datos del centro de protección de datos personales. Obtenido el 15 de Julio de 2008 en la Word Wide Web: https://n9.cl/tgke [Accedido el 8/12/19]

Disposición N° 89/08. Obtenido el 23 de Junio de 2008 en la Word Wide Web: https://n9.cl/zs8e [Accedido el 22/5/19]

Formulario de pre-inscripción. Obtenido en la Word Wide Web: www.buenosairescompras.gov.ar [Accedido el 22/5/19]

Informe AGCBA. Proyecto 10.18.03. Obtenido el 3 de Agosto de 2017 en la Word Wide Web: https://n9.cl/akxb [Accedido el 20/5/19]

Informe AGCBA. Proyecto 10.10.1. Obtenido el 2 de Mayo de 2011 en la Word Wide Web: https://n9.cl/akxb [Accedido el 20/5/19]

Glosario, siglas y acrónimos

AES - Número total de agentes entrevistados para la satisfacción en los servicios, es la cantidad de agentes del GCABA que expresan su nivel de satisfacción respecto de los servicios de TI brindados por ASInf.

AGC - Agencia Gubernamental de Control de la Ciudad de Buenos Aires.

AGCBA - Auditoría General de la Ciudad de Buenos Aires, es un organismo creado por la Constitución de la Ciudad Autónoma con el objetivo de ejercer el control externo del sector público, centralizado y descentralizado de la Ciudad y de las empresas, sociedades o entes en los que tenga participación la Ciudad en sus aspectos económicos, financieros, patrimoniales y de gestión de legalidad.

AIS - Número total de agentes insatisfechos con los servicios, es la cantidad de agentes del GCABA que expresan su insatisfacción respecto de los servicios de TI brindados por ASInf.

ALA - Número total de apercibimientos por incumplimiento de los acuerdos de nivel de servicio, son las notificaciones formales que reclaman al proveedor el cumplimiento de los objetivos establecidos en los acuerdos.

Alineamiento - es el estado en el cual los elementos facilitadores del gobierno y de la gestión de tecnología de la información colaboran con las metas y las estrategias de la organización.

Ansible Orchestration - es una plataforma de software libre de configuración y administración automatizada de computadoras que evita las tareas repetitivas. Automatiza gran número de módulos utilizando un lenguaje común para todos los entornos y procesos de TI.

Antispyware - es un tipo de software diseñado para detectar y eliminar programas maliciosos que captan y envían información personal de un individuo sin su consentimiento.

Apache Tomcat Java Platform - es un servidor web para aplicaciones, desarrollado por Java, con código abierto que permite funcionar en cualquier sistema operativo con su máquina virtual java correspondiente.

Apache WebServer - es un servidor web multiplataforma de código abierto que almacena, procesa y entrega las páginas web a los usuarios.

ASInf - es la Agencia de Sistemas de Información de la Ciudad Autónoma de Buenos Aires.

ASS - número total de agentes satisfechos con los servicios, es la cantidad de agentes del GCABA que expresan su satisfacción respecto de los servicios de TI brindados por ASInf o por proveedores externos.

Atributo de capacidad de un proceso - es la característica que permite medir la capacidad de un proceso aplicable en la norma ISO/IEC 15504.

Autenticación - es la acción de verificar la identidad de un usuario y sus derechos de acceso a cierta información utilizada por los sistemas.

AVG - es un software antivirus desarrollado por la empresa AVG Technologies. Está disponible para sistemas operativos Windows, Android, iOS, Linux y Windows Phone, entre otros.

Back Up - en informática, es un respaldo, una copia de seguridad o de reserva para preservar los datos originales, con la finalidad de disponer de un medio para recuperarlos en caso de su pérdida.

Catalizador - es un proceso mediante el cual se busca causar, provocar, acelerar o disminuir una reacción determinada.

CCA - costos totales del presupuesto actual, representan los egresos o gastos necesarios en los que incurrirá un organismo en el desarrollo normal de sus operaciones.

CCP - costos totales del presupuesto planificado, representan los egresos o gastos planificados para ASInf para el desarrollo normal de sus operaciones.

CDC - número total de cambios de componentes, es la cantidad total de modificaciones realizadas en los componentes de los servicios de TI.

CEO - Chief Executive Officer, (en español Director Ejecutivo), es el máximo responsable de la gestión y dirección administrativa de una empresa.

CFO - Chief Financial Officer, (en español Director Financiero), es quien decide la inversión, financiación y el riesgo con el objetivo de conseguir el incremento del valor de la empresa para sus propietarios, sean accionistas o socios.

Chatbot - también llamado bot de charla o bot para una conversación, es un programa que simula mantener una conversación con una persona al proveer respuestas automáticas a las entradas configuradas por el usuario. Generalmente, la conversación es establecida a través de texto, siendo posible mediante una interfaz de usuario multimedia.

CI - en el estándar ITIL, son los elementos involucrados en la configuración.

CIE - número de componentes con información errónea o desactualizada, es la cantidad total de componentes con información inconsistente de los servicios de TI que constan en la base de datos de la configuración.

Cifrar - es un procedimiento a través del cual se usa un algoritmo con una clave para transformar un mensaje, no posee significado lógico ni comprensible. Es necesario la clave secreta de descifrado del algoritmo para obtener los datos originales.

CIO - Chief Information Officer, (en español Director de Sistemas de Información), es el máximo responsable a cargo de los sistemas de información de la empresa.

CISO - Chief Information Security Officer, (en español Director de Seguridad de la Información), es el máximo responsable de alinear las iniciativas de seguridad con los programas de la organización y los objetivos de negocio.

Cloud Computing - es un modelo tecnológico mediante el cual se prestan servicios de almacenamiento, acceso y uso de recursos informáticos a través de internet, tales como la utilización de software, el almacenamiento y sincronización de archivos, bases de datos, correo electrónico y la gestión remota de la información.

Cloudform Cloud Orchestration - es un servicio que permite crear, actualizar y administrar los recursos de la nube y sus componentes de software como una sola unidad y luego implementarlos de forma automatizada y repetible a través de una plantilla.

CMDB - en el estándar ITIL, es la Base de Datos de la Configuración de todos los componentes involucrados en la prestación de todos los servicios con el objetivo de facilitar la detección del componente que afecta al servicio.

COBIT - Control Objectives for Information and related Technology, (en español Objetivos de Control para Tecnologías de la Información), es un marco de trabajo que ayuda a comprender el gobierno y la gestión de las tecnologías de la información y evalúa el estado en el que se encuentran actualmente.

Código abierto - es el término mediante el cual se conoce al software distribuido y desarrollado libremente, puede ser usado y modificado por los usuarios sin ninguna restricción.

Código fuente - es un conjunto de líneas de texto que expresan, en un determinado lenguaje de programación, los pasos a seguir por la computadora para la correcta ejecución de un programa.

Código objeto - se llama código objeto al código obtenido de la compilación del código fuente.

Competencia - es la habilidad de realizar determinada acción o función de manera exitosa.

Continuidad de negocio - es la acción de evitar, mitigar y recuperarse de una interrupción.

COO - Chief Operating Officer, (en español Director de Operaciones), es el máximo responsable de la gestión del ámbito estratégico, táctico y operativo dentro de una organización.

CPA - costos totales del presupuesto asignado, representan los egresos o gastos asignados a ASInf para el desarrollo normal de sus operaciones.

CPE - número de cambios por emergencia, es la cantidad de alteraciones solicitadas en los componentes de los servicios para modificar su uso o propósito que deben llevarse a cabo con urgencia para lograr el retorno de la funcionalidad del servicio de TI.

CPI - número de cambios solicitados por incidentes, es la cantidad de modificaciones solicitadas en los componentes de los servicios de TI para dar solución a la interrupción generada por eventos imprevistos.

CRA - número de componentes de red, hardware y software soportados por ASInf, es la cantidad de recursos tecnológicos soportados técnicamente por ASInf para suministrar la disponibilidad acordada en el servicio de TI.

Creación de valor - es el objetivo principal del gobierno de una organización, obtenido mediante el cumplimiento, en equilibrio, de los 3 (tres) objetivos subyacentes como la consecución de los beneficios, optimización de riesgo y optimización de recursos.

CRO - Chief Risk Officer, (en español Director de Riesgos), es el máximo responsable de coordinar los procesos de gestión y control del riesgo.

CRP - número de componentes de red, hardware y software soportados por proveedores externos, es la cantidad de recursos tecnológicos soportados técnicamente por los proveedores externos correspondientes para suministrar la disponibilidad acordada en el servicio de TI.

CRS - número de componentes de red, hardware y software, es la cantidad de recursos tecnológicos asociados para suministrar el servicio de TI adecuadamente.

CSF - factor crítico de éxito, es un punto clave que si es correctamente ejecutado garantiza la obtención de los objetivos propuestos.

CSI - Continual Service Improvement, (en español Servicio de Mejora Continua), tiene como finalidad mejorar los procesos asociados al suministro del servicio para incrementar el rendimiento y la calidad de los servicios de TI.

CSR - número de componentes por cambios sin petición de cambio RFC, es la cantidad de componentes de un servicio de TI modificados sin la petición de cambio correspondiente.

Debilidad Tecnológica - es la falta de recursos tecnológicos implementados para poder repeler una acción que dejan a la organización altamente susceptible a que ocurra una amenaza.

DML - Definitive Media Library, (en español Biblioteca de Medios Definitivo), permite el almacenamiento de las copias del histórico completo de todas las versiones de los sistemas operativos, aplicaciones, controladores de dispositivos y su documentación asociada.

DS - en el estándar ITIL, es el almacén de Recambios Definitivos donde se almacenan las piezas de repuesto y su documentación para el entorno de producción que permite la rápida reparación a los problemas de hardware.

DVD-ROM - (en español disco versátil digital de memoria de solo lectura), pertenece al tipo de soportes para grabar por única vez y puede ser leído o reproducido muchas veces.

EER - número de entregas con errores conocidos, es la cantidad de versiones de software, nuevas o actualizaciones de los servicios de TI vigentes que provocaron eventos y constan en la base de datos de errores conocidos (KEDB) del servicio correspondiente.

ELK ElasticSearch Kibana - es un conjunto de herramientas de código abierto para recolectar, cargar, buscar y visualizar información en tiempo real en cualquier formato. Permite el monitoreo, consolidación y análisis de los registros históricos generados en múltiples servidores. Permite conocer la disponibilidad y métricas de desempeño de los servidores o recolectar métricas de servicios.

EPI - número de entregas que provocaron incidentes, es la cantidad de versiones de software correspondientes a nuevos servicios de TI o actualizaciones de servicios vigentes que provocaron eventos no deseados sobre el servicio correspondiente.

Espía Informático - es un programa no deseado que recopila información de un dispositivo informático que luego transmite esa información a una entidad externa sin el consentimiento del propietario de la computadora.

ESXI - forma parte de la plataforma VMware vSphere, es una plataforma que permite aplicar técnicas de control de virtualización para utilizar en una misma computadora diferentes sistemas operativos al mismo tiempo. Es un sistema operativo con un hipervisor integrado.

ETSI - European Telecommunications Standards Institute (en español Instituto Europeo de Normas de Telecomunicaciones), es una organización de estandarización independiente, sin fines de lucro, perteneciente a la industria de las telecomunicaciones, fabricantes de equipos y operadores de redes en Europa.

F5 LTM Load Balancer - es un módulo que permite aumentar las conexiones del lado del servidor y del usuario. Toma decisiones sobre el equilibrio de la carga en cuanto a la disponibilidad, rendimiento y persistencia.

Funciones de la Tecnologías - es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar, crear bienes y servicios que facilitan la adaptación al medio ambiente y la satisfacción tanto de las necesidades esenciales como de los deseos de las personas.

Gestión de Servicios de TI - es un conjunto de capacidades o habilidades organizativas específicas para proporcionar valor a los usuarios en forma de servicios. Es la alineación sistemática a la planificación, desarrollo, entrega, y soporte de los servicios TI para la organización.

Gestor del Servicio - en el estándar ITIL, es el responsable de la gestión de un servicio durante todo su ciclo de vida: desarrollo, implementación, mantenimiento, monitoreo y evaluación.

Gobierno de TI - es el alineamiento de las tecnologías de la información y la comunicación con la estrategia del negocio. Hereda las metas y la estrategia a todos los departamentos de la empresa, proporciona el mejor uso de la tecnología y de sus estructuras organizativas para alcanzarlas.

Grafana Monitoring - es un software de código abierto que permite la visualización, monitoreo y análisis de datos. Permite monitorear el estado técnico de los sistemas de software creando cuadros de mando y gráficos a partir de múltiples fuentes, incluidas las bases de datos de series de tiempo.

GTB - Grow the Business, (en español Inversiones para hacer Crecer el Negocio), son aquellas inversiones diseñadas para ayudar a hacer crecer el negocio actual.

Gusano Informático - es un programa que genera copias de sí mismos almacenándolas en diferentes ubicaciones de la computadora. La finalidad de este programa es colapsar el equipo y las redes informáticas, impidiendo trabajar a los usuarios.

HDS Device Manage Management - es un software utilizado para unificar, simplificar y monitorear los subsistemas de almacenamiento conectados a los servidores.

HDS Storage Advisor Management - es una solución de administración de infraestructura que unifica las soluciones de almacenamiento y la protección de datos. Simplifica la administración de los centros de datos a gran escala al proporcionar un servicio de software inteligente y extensible.

HDS Storage Navigator Management - es un software que permite gestionar, habilitar y optimizar los sistemas de almacenamiento individuales. Permite establecer distintos niveles de configuración, definir rutas entre sistemas, configurar y administrar la replicación.

Hipervisor - también llamado monitor de máquina virtual, es una plataforma que permite aplicar técnicas de control de virtualización para utilizar en una misma computadora diferentes sistemas operativos al mismo tiempo.

IAQ - índice de actualización de servicios, es el índice expresado a través del cociente entre el número de servicios vigentes inexistentes en el catálogo de servicios y el número vigente de servicios detallado en el catálogo.

IAS - índice de agentes satisfechos con los servicios, es el cociente entre el número total de agentes satisfechos con los servicios y el número total de agentes entrevistados por la satisfacción en los servicios. Provee una estimación del nivel de satisfacción en los servicios de los agentes respecto del total.

IBM Spectrum Management - es un producto de respaldo y recuperación, que se puede utilizar con almacenamiento físico o virtual. Proporciona replicación de sitios múltiples y gestión de recuperación ante desastres.

ICC - índice de cobertura de continuidad, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de servicios cubiertos con un plan de continuidad y el número de servicios total en el catálogo de servicios de TI.

ICE - índice de cambios por emergencia, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de cambios por emergencia y número de cambios autorizados implementados.

ICM - índice de precisión de la CMDB, es el índice que se expresa como el cociente entre el número total de componentes erróneos respecto del número total de componentes existentes en la CMDB.

ICR - número de incidentes provocados por falta de capacidad de la red, es cualquier evento excluido del desarrollo habitual del servicio que provoca o puede provocar una interrupción o una reducción de la calidad del servicio por carecer de la capacidad necesaria en la red para desarrollar normalmente el servicio.

IEC - International Electrotechnical Commission, (en español Comisión Electrotécnica Internacional), es una organización de normalización en los campos eléctricos, electrónicos y las tecnologías relacionadas.

IEF - índice de entregas fallidas, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de entregas que provocaron incidentes y el número de entregas implementadas.

IFC - número de incidentes provocados por falta de capacidad de hardware, es cualquier evento excluido del desarrollo habitual del servicio que provoca o puede provocar una interrupción o una reducción en la calidad del servicio por falta de capacidad del hardware instalado.

IFF - número de informes financieros planificados entregados en fecha, son aquellos informes financieros entregados en la fecha planificada.

IFP - número de informes financieros planificados, es la cantidad estipulada de informes financieros que deben ser entregados con su detalle y fecha planificada.

IFS - número de incidentes de capacidad provocados por software inadecuado, es cualquier evento excluido del desarrollo habitual del servicio que provoca o puede provocar una interrupción o una reducción de la calidad del servicio por poseer software inadecuado.

IFT - número de informes financieros planificados entregados fuera de fecha, son aquellos informes financieros entregados luego de la fecha planificada.

IFX - índice de formalidad de cambios, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de cambios implementados sin autorización y el número de cambios implementados autorizados.

IGC - número de incidentes graves con impacto en la continuidad, es la cantidad de eventos que provocan una interrupción imprevista y genera consecuencias significativas en la continuidad del servicio de TI.

IGZ - número de incidentes graves, es la cantidad de eventos que provocan una interrupción imprevista y genera consecuencias significativas en el servicio de TI.

IIC - número de incidentes de seguridad que impactan la continuidad, es la cantidad de eventos de seguridad que provoca una interrupción imprevista en el servicio de TI por falta de continuidad.

IID - número de incidentes de seguridad que impactan la disponibilidad, es la cantidad de eventos asociados con la seguridad que provoca la interrupción del servicio por falta de disponibilidad.

IIF- índice de informes financieros entregados con demora, es el resultado del cociente entre la cantidad de informes financieros planificados entregados fuera de fecha y la cantidad de informes financieros planificados. Brinda idea sobre el cumplimiento de la entrega de informes respecto de la fecha planificada.

IIP - índice de incidentes repetidos derivados a problemas, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de incidentes derivados a problemas y el número total de problemas registrados.

IIR - índice de incidentes repetidos, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de incidentes repetidos y el número de incidentes registrados.

IIS - índice de incidentes con impacto significativo, es la medida estadística que recoge la evolución relativa en un período determinado definido por la relación entre el número de incidentes graves y el número de incidentes registrados.

ILA - número total de incumplimientos de SLA, es la cantidad de incumplimientos de los objetivos establecidos por el servicio de TI en el Acuerdo de Nivel de Servicio por parte del proveedor.

IMP- índice de multas pagadas por incumplimiento de SLA, es el cociente entre el número total de multas pagadas por incumplimiento de SLA y el número total de imposición de multas por incumplimiento de SLA. Brinda idea del cumplimiento de pago.

Inteligencia artificial - es el campo científico de la informática cuyo objetivo es la creación de programas y mecanismos que puedan mostrar comportamientos considerados inteligentes. Se define como el concepto a través del cual se busca que las máquinas piensen como seres humanos.

Internet de las cosas - es la interconexión a través de internet de objetos físicos o virtuales, sensores, personas, servicios o plataformas con la capacidad de transferir los datos de forma independiente.

INTI - Instituto Nacional de Tecnología Industrial, ente autárquico dependiente del Ministerio de Producción y Trabajo cuyo objetivo es promover e impulsar el crecimiento de las pymes argentinas mediante el desarrollo industrial federal, la innovación y la transferencia de tecnología.

IP - la dirección IP es un conjunto de números que identifica de manera lógica y jerárquica, a una interfaz en la red de un dispositivo conectado que corresponde al nivel de red del modelo TCP/IP.

IPC - índice de precisión de costos, es el resultado del cociente de los costos totales del presupuesto planificado y los costos totales del presupuesto actual.

IPQ - variación en la planificación de los recursos de TI, es la variación entre el nivel de planificación de los recursos de TI asignados y los fallidos.

IPR - índice de problemas repetidos, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de problemas repetidos y el número total de problemas registrados.

IRD - índice de recuperación de la disponibilidad, es el cociente entre el número de incidentes graves con impacto en la disponibilidad y el número de incidentes registrados. Permite estimar la relación y el grado de impacto en los servicios de ASINF.

IRI - índice de resolución de incidentes, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el número de incidentes resueltos y el número de incidentes registrados.

ISACA - Information Systems Audit and Control Association (en español, Asociación de Auditoría y Control de Sistemas de Información), es una asociación internacional que ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución, ofreciendo conocimientos, estándares, relaciones, acreditación y desarrollo de una carrera innovadora.

ISI - índice de problemas con impacto significativo, es la medida estadística que recoge la evolución relativa en un período determinado, es la relación entre el número de problemas graves y el número total de problemas registrados.

ISL - número de incidentes de continuidad por incumplimiento de SLA, es la cantidad de eventos que provocan una interrupción imprevista en el servicio de TI por falta de cumplimiento en los Acuerdos de Niveles de Servicio.

ISO/IEC 17799 - estándar de seguridad publicado por la Organización Internacional para la Estandarización (ISO).

ISO/IEC 20000 - estándar de calidad publicado por la Organización Internacional para la Estandarización (ISO).

ISO/IEC 27000 - estándar de seguridad publicado por la Organización Internacional para la Estandarización (ISO).

ISO/IEC 27001 - es un estándar para la seguridad de la información, define los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

ITC - índice de tiempo de continuidad, es la medida estadística que recoge la evolución relativa en un período determinado de la relación entre el tiempo total sin continuidad y el tiempo total con continuidad en el servicio de TI.

ITGI - IT Governance Institute, (en español Instituto de Gobierno de TI), fue fundado en 1998 por ISACA, asociación sin fines de lucro, para ayudar a ejecutivos y profesionales de tecnología, para garantizar que las tecnologías entreguen valor y mitiguen sus riesgos a través del alineamiento con los objetivos del negocio.

ITIL - Librería de Infraestructura de TI de la Oficina Gubernamental del Reino Unido. Es un conjunto de buenas prácticas utilizadas para la gestión, el desarrollo y las operaciones de los servicios de tecnologías de la información.

KEDB - en el estándar ITIL, es la Base de Datos de Errores Conocidos que contiene un registro de los fallos sucedidos anteriormente que facilita y minimiza el tiempo de catalogación y solución de los mismos para el futuro.

KPI - Key Performance Indicator (en español Indicador Clave de Rendimiento) es un indicador que mide el desempeño o rendimiento. Es un nivel para la medición del rendimiento de un proceso.

LAN - Local Area Network (en español Red de Área Local), es una red que interconecta una o más computadoras dentro de un área geográfica limitada.

Logs - es el historial de registros, la grabación secuencial en una base de datos de todos los eventos o acciones ocurridas que afectan a un proceso determinado, ya sea una actividad en una red informática, una aplicación, etc.

MAN - Metropolitan Area Network (en español Red de Área Metropolitana), es una red de alta velocidad que cubre un área geográfica extensa. Posee la capacidad de integrar múltiples servicios mediante la transmisión de datos, voz y vídeo.

Marco de gobierno - es la estructura conceptual básica utilizada para entender, afrontar, resolver y responder a temas complejos relacionados con las entidades involucradas.

Marco tecnológico - es un conjunto estandarizado de conceptos, prácticas y criterios relacionados con la tecnología, para orientar un problema determinado, el cual sirve como referencia para enfrentar otros problemas de índole similar.

Mariadb Database - es un derivado del sistema de gestión de bases de datos relacionales MySQL, compatible con gran cantidad de lenguajes. Es un software libre de código abierto.

MIS - número total de imposición de multas por incumplimiento de SLA, son las notificaciones formales al proveedor por el incumplimiento de los objetivos establecidos por el servicio de TI en el Acuerdo de Nivel de Servicio.

MOF - Microsoft Operations Framework (en español Marco de Operaciones de Microsoft), es una guía para las organizaciones de tecnología que ayuda a crear, operar y dar soporte a los servicios de tecnología, asegura que las inversiones en tecnología entreguen el valor esperado al negocio con un nivel de riesgo aceptable.

MongoDB Database - es un sistema de gestión de bases de datos de código abierto que utiliza un modelo orientado a documentos el cual admite datos en distintos formatos. En lugar de usar tablas y filas como en las bases de datos relacionales, la arquitectura está formada por colecciones y documentos.

MPS - número total de multas pagadas por incumplimiento de SLA, son las multas efectivamente pagadas por el proveedor por el incumplimiento de los objetivos establecidos por el servicio de TI en el Acuerdo de Nivel de Servicio.

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.

NCC - número total de componentes en la CMDB, es el número de componentes registrado en la base de datos de la configuración que facilita la administración de incidencias, problemas, cambios, entregas y despliegues.

NCE - número total de componentes erróneos, es el número total de componentes erróneos encontrados en la Base de Datos de la Configuración (CMDB).

NCI - número de cambios implementados autorizados, es la cantidad de alteraciones autorizadas e implementadas en los componentes de los servicios de TI para modificar su uso o propósito.

NCP - número de cambios pendientes, es la cantidad de alteraciones pendientes de realizar en los componentes de los servicios de TI para modificar su uso o propósito.

NCS - número de cambios implementados sin autorización, es la cantidad de alteraciones implementadas no autorizadas en los componentes de los servicios de TI para modificar su uso o propósito.

NEI - número de entregas implementadas, es la cantidad total de versiones de software correspondientes a nuevos servicios de TI o actualizaciones de servicios vigentes que ya fueron implementadas.

NIG - número de problemas graves, es la cantidad de inconvenientes generados en los servicios de TI por no acceder a las causas subyacentes, las que generan inconvenientes significativos en el suministro del servicio.

NII - número de incidentes graves con impacto en la disponibilidad, es cualquier evento excluido del desarrollo habitual del servicio que provoca la interrupción del servicio por falta de disponibilidad.

NIL - número de incidentes leves, es la cantidad de eventos que provocan una interrupción imprevista generando consecuencias leves en el servicio de TI.

NIP - número de problemas pendientes, es la cantidad de inconvenientes generados en los servicios de TI, aún sin acceso a la solución para la normalización del suministro del servicio.

NIR - número de problemas resueltos, es la cantidad de inconvenientes generados en los servicios de TI solucionados al identificar las causas subyacentes, proveer su solución y normalizar el suministro del servicio.

NIX - número de incidentes derivados a problemas, es la cantidad de eventos ocurridos que provocaron una interrupción imprevista generando consecuencias en el servicio de TI. Por su repetición o por carecer de solución fue derivado al proceso de administración de problemas.

NIZ - número de incidentes resueltos, es la cantidad de eventos que provocaron una interrupción imprevista del servicio de TI, las causas raíz fueron identificadas e implementada su solución logrando la normalización del servicio.

Norma internacional - también llamado estándar internacional, es el proceso de elaborar, aplicar y mejorar las normas empleadas en diversas actividades, industriales o económicas, con el objetivo de ordenarlas y mejorarlas.

NPL - número de problemas leves, es la cantidad de inconvenientes generados en los servicios de TI que por no acceder a las causas subyacentes, generan inconvenientes leves en el suministro del servicio.

NRI - número de incidentes repetidos, es la cantidad de eventos frecuentes que provocan una interrupción imprevista en el servicio de TI.

NTC - número total de cambios pedidos, es la cantidad de alteraciones solicitadas en los componentes de los servicios de TI para modificar su uso o propósito.

NTE - número total de entregas, es la cantidad total de versiones de software correspondientes a nuevos servicios de TI o actualizaciones de servicios vigentes que aún no fueron implementadas.

NTR - número de incidentes registrados, es la inscripción de cualquier evento excluido del desarrollo habitual del servicio que provoca o puede provocar una interrupción o una reducción de la calidad del servicio.

NUR - número de problemas repetidos, es la cantidad de inconvenientes generados en los servicios de TI, los cuales generan impedimentos para encontrar y analizar las causas subyacentes para su solución.

NXI - número de incidentes pendientes, es la cantidad de eventos que provocan una interrupción imprevista en el servicio de TI y aún no pudieron ser resueltos.

OLA - Operational Level Agreement, (en español Acuerdo de Nivel Operativo), es un contrato que describe el nivel de operación que los grupos de tecnología de información funcionales se prometen entre sí.

Openshift Platform Private Container Cloud Platform - es una plataforma empresarial de aplicaciones con operaciones automatizadas integrales, de código abierto y multifacética, para gestionar los servicios múltiples en la nube.

Oracle Enterprise Database - es un sistema de gestión de base de datos que permite ser usado en cualquier plataforma, almacenar y recuperar datos de forma rápida, segura y puede ser implementado en las instalaciones o en la nube.

Oracle Enterprise Manager Management - es un conjunto de herramientas basadas en la web para administrar software y hardware. Brinda una solución integrada para implementar, operar, monitorear, diagnosticar y resolver problemas en los entornos de TI. Proporciona una plataforma de administración de sistemas integrada y completa para administrar los productos de Oracle.

Ovitrampas - son trampas sencillas utilizadas estadísticamente como muestreo de la mosquita Aedes en áreas urbanas.

PAH - presupuesto asignado a hardware, es el plan financiero para estimar los gastos asignados a hardware en un período específico de tiempo.

PAS - presupuesto asignado a software, es el plan financiero para estimar los gastos asignados a software en un período específico de tiempo.

PCC – índice de tiempo promedio de confiabilidad, es el índice definido entre el tiempo del servicio de TI en el que puede cumplir la función acordada cuando le es requerida sin interrupción respecto del tiempo en el que no puede dar cumplimiento.

Pentaho Ops BI - es un software de inteligencia empresarial que proporciona integración de los datos. Ofrece servicios de procesamiento analítico en línea, informes, paneles de información, extracción de datos y capacidades de extracción.

PIR - en el estándar ITIL, es la revisión post-Implantación desarrollada en una fase de soporte posterior a la implementación de los cambios que asesora a todas las partes involucradas.

PMBOK - Project Management Body of Knowledge (en español Guía de los Fundamentos para la Dirección de Proyectos) es un instrumento desarrollado por el Project Management Institute (PMI), que establece un criterio de buenas prácticas relacionadas con la gestión, administración y dirección de proyectos.

PMI - Project Management Institute (en español Instituto de Dirección de Proyecto), es una organización estadounidense sin fines de lucro que asocia a profesionales relacionados con la Gestión de Proyectos.

PMO - Project Management Office (en español Oficina de Gestión de Proyectos) es un departamento que define y mantiene estándares de procesos relacionados a la gestión de proyectos dentro de una organización.

Proceso - es un conjunto de actividades interrelacionadas orientadas a cumplir un objetivo específico, definidas por las políticas y procedimientos de la organización. Toma entradas de una serie de fuentes, las manipula y genera salidas.

Prometheus Monitoring - es una aplicación de software utilizada para la supervisión y los alertas de eventos en los servicios. Permite configurar y registrar métricas en tiempo real en una base de datos.

Propietario de la Información - es la persona responsable de la integridad, confidencialidad, disponibilidad y privacidad de cierta información. Es el responsable de clasificar la información mediante el proceso de evaluación del riesgo.

Propietario del Proceso - es el último responsable frente a la organización de TI del cumplimiento de los objetivos del proceso, del diseño exitoso, desarrollo, ejecución y el desempeño de un proceso completo del negocio de extremo a extremo. Incluye el patrocinio, gestión de cambios, mejora continua del proceso y sus métricas.

Propietario del Servicio - en el estándar ITIL, es el último responsable de la organización de TI frente al cliente que presta el servicio específico. A cargo de la gestión de uno o más servicios a través del ciclo de vida completo. Son esenciales para el desarrollo de la estrategia de servicio y responsables del portafolio de servicios.

PSO - en el estándar ITIL, Parada de Servicio Prevista, es un procedimiento para el mantenimiento y la actualización del servicio coordinado entre el proveedor y el usuario.

RACI - por sus iniciales Responsible, Accountable, Consulted, Informed, (en español Responsable, Ejecutor, Consultado, Informado), es la matriz de asignación de responsabilidades, utilizada para relacionar las actividades con los recursos en la gestión de proyectos.

Recurso - es todo activo que posee una organización a través del cual puede conseguir sus objetivos.

Redhat Linux OS - es un sistema operativo abierto que sirve de base a las aplicaciones actuales, se puede implementar en equipos sin sistema operativo, en entornos virtuales, en contenedores y en entornos de la nube.

RFC - Request for Change, (en español, Petición de Cambio), es la solicitud formal para efectuar cambios en los servicios de tecnología.

Riesgo - es la combinación de la probabilidad de un evento y sus consecuencias asociadas.

RII - índice de resolución de problemas, es la medida estadística que recoge la evolución relativa en un período determinado, es la relación entre el número de problemas resueltos y el número total de problemas registrados.

ROI - por sus iniciales Return On Investment, (en español retorno sobre la inversión) es una razón financiera que compara el beneficio obtenido en relación a la inversión realizada.

Router - es un dispositivo que permite interconectar computadoras que funcionan conectadas a través de una red. Su función es definir la ruta por medio de la cual destinará cada paquete de datos dentro de una red informática.

RPF - número de recursos de TI planificados fallidos, es la planificación errónea respecto de los activos necesarios de ASInf que no permite la entrega adecuada del servicio.

RRP - número de recursos de TI planificados, son los activos necesarios planificados de ASInf para la prestación del servicio.

RTB - Run the Business, (en español Inversiones para Administrar el Negocio), son aquellas inversiones para mantener operativos los servicios actuales.

SAC - en el estándar ITIL, es el criterio de aceptación del servicio.

SADE - Sistema de Administración de Documentos Electrónicos, engloba todo el universo de aplicativos que administran los documentos digitalizados del Gobierno de la Ciudad Autónoma de Buenos Aires. Incluye los actos administrativos, expedientes, legajos del personal, registro civil, gestor único de proveedores y el sistema integrado de archivo entre otros.

SAX - número de servicios entregados por ASInf y por proveedores, es un medio a través del cual ASInf y proveedores externos, conjuntamente, entregan valor a los entes del GCABA cubriendo sus necesidades sin que éstos asuman los costos y riesgos asociados a la consecución de dichos resultados.

Schneider DCIM Datacenter Infraestructure Manager - es un software que brinda a los operadores de los centros de datos la capacidad de ejecutar operaciones eficientes y mejorar la planificación y el diseño de su infraestructura.

SCS - número de servicios en el catálogo de servicios, es la base de datos que contiene la información detallada respecto de todos los servicios vigentes de TI.

SEG - número de servicios entregados por ASInf al GCABA, es un medio a través del cual ASInf entrega valor a los entes del GCABA cubriendo sus necesidades sin que éstos asuman los costos y riesgos asociados a la consecución de dichos resultados.

SEI - Software Engineering Institute, (en español Instituto de Ingeniería de Software), es un centro de investigación y desarrollo estadounidense. Sus actividades abarcan seguridad cibernética, garantía de software, ingeniería, adquisición de software y capacidades de componentes críticas para el Departamento de Defensa.

Servicio de Tecnología de la Información - es un conjunto de recursos que son provistos a los clientes para soportarlos en la operación de una o más áreas del negocio.

SGC - un sistema de gestión de la calidad, es la gestión de los servicios ofrecidos que incluye la planificación, control y mejora de los elementos de una organización que afectan la satisfacción del cliente y el logro de los resultados deseados por la organización.

SGSI - un sistema de gestión de seguridad de la información, es un conjunto de políticas de administración de la información. Es un término usado por la norma internacional ISO/IEC 27000, aunque no es la única que lo utiliza.

Sistema de Reconocimiento Facial - es un software automatizado de identificación biométrica que permite identificar a una persona mediante el análisis y la comparación de modelos basados en sus rasgos y contornos faciales.

Sistema predictivo - es aquel que agrupa una diversidad de técnica estadística de modelización, aprendizaje automático y análisis de un grupo de datos reales actuales e históricos, que permite predecir un aspecto del futuro. Genera optimización de costos y recursos humanos.

Sistema SAP - es una plataforma abierta y flexible para el ingreso, organización y análisis de datos, la cual permite tomar decisiones basadas en la información actualizada y confiable del GCABA.

Sistemas de detección temprana de humo - permite actuar de manera proactiva a una eventual situación de incendio, mediante la detección de humo por aspiración, garantizando la continuidad del negocio de una empresa previniendo falsas alarmas. Descubre el fuego en su etapa más temprana, alerta ante concentraciones de humo y acciona su sistema de supresión.

SIX - número de servicios vigentes inexistentes en el catálogo de servicios, es el número de servicios provistos que no constan en el catálogo de servicios.

SKMS - Service Knowledge Management System, (en español Sistema de Gestión del Conocimiento del Servicio), es una herramienta de presentación, procesamiento y gestión, estructurada de forma estratificada que almacena información según su clasificación.

SLA - Service Level Agreement, (en español Acuerdo de Nivel de Servicios), es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

SLR - Requisitos de Nivel de Servicio, es el conjunto de parámetros necesarios definidos por el usuario respecto del rendimiento y nivel de servicio requerido.

SOA - Service Oriented Architecture, (en español Arquitectura Orientada a Servicios), es un marco de trabajo conceptual cuya arquitectura orientada a servicios permite a las organizaciones unir los objetivos de negocio con la infraestructura de TI integrando los datos y la lógica de negocio de sus sistemas separados.

Software de aplicación - es un tipo de software de computadora diseñado para realizar un grupo de funciones, tareas o actividades coordinadas para el beneficio del usuario.

Software de base - es el conjunto de instrucciones que permite el manejo de la computadora. Consiste en un software que sirve de base para interactuar con el hardware y otros programas.

Software Malicioso - término que engloba a todo tipo de programa o código informático malicioso cuyo objetivo es dañar un sistema o causar un mal funcionamiento.

SPC - número de servicios cubiertos con un plan de continuidad, es la cantidad de servicios de TI cubiertos por ASInf que mediante un plan podrá recuperar o continuar la operación cuando ocurra un evento imprevisto.

SPF - número de servicios con pruebas fallidas, es la cantidad de servicios de TI sometidos a pruebas respecto de su uso, propósito, adecuación y cuyo resultado no fue el esperado.

Sponsor - es un patrocinador, un ente, organismo o una persona que apoya o financia una actividad o un proyecto. Participa en la obtención de los recursos para su ejecución, autoriza el presupuesto para el desarrollo del proyecto. Defiende y apoya el proyecto, sus metas y objetivos, es el máximo responsable en la toma de decisiones.

Spyware - es un programa espía que recopila y transmite información de una computadora a una entidad externa sin el conocimiento del propietario.

SQL Server Database - es un sistema de gestión de bases de datos relacionales de Microsoft que permite programar en entornos híbridos ya sea de forma local o en la nube de Microsoft.

SQP - Service Quality Program, (en español Plan de Calidad del Servicio), asegura los niveles de servicio de TI y provee la información necesaria para medir su rendimiento.

SSA - número de servicios entregados sin SLA, son los servicios de TI provistos por un proveedor externo a ASInf o a los entes del GCABA, directa o indirectamente, sin la existencia formal de un Acuerdo de Nivel de Servicios.

SSC - número de servicios sin cubrir con un plan de continuidad, es la cantidad de servicios de TI no cubiertos por ASInf con un plan de continuidad que le asegure la recuperación de la operación cuando ocurra un evento imprevisto.

SSO - número de servicios internos entregados sin OLA, son los servicios de TI provistos por ASInf a los entes del GCABA sin la existencia formal de un Acuerdo de Nivel Operativo.

Stage-Gate - es una metodología, una lógica de gestión de innovación con el objetivo de coordinar un proceso creativo multifuncional, a través de la cual integra una estructura de toma de decisiones de inversión basadas en diversas opciones. La finalidad es acelerar el tiempo de comercialización, elevar la rentabilidad y minimizar el riesgo.

SUACI - Sistema Único de Atención al Ciudadana, es el sistema mediante el cual los ciudadanos pueden realizar solicitudes, denuncias, quejas, sugerencias, consultas o pedir turnos respecto al espacio público, seguridad, arbolado, espacios verdes y calles entre otros.

Switch - es un dispositivo digital lógico de interconexión de equipos en una red. Es un conmutador que se utiliza cuando se desean conectar múltiples tramos de una red.

TCI - tiempo total de cambios implementados, es el tiempo que demandó el cambio en los componentes de los servicios de TI para modificar su uso o propósito.

TCS - tiempo total de continuidad del servicio, es el tiempo durante el cual el servicio de TI tiene la capacidad de cumplir sus funciones sin interrupciones de forma adecuada.

TDS - tiempo total de disponibilidad del servicio, es el tiempo durante el cual el servicio de TI tiene la capacidad de cumplir sus funciones de forma adecuada cuando le son requeridas.

Tecnología - es la ciencia aplicada a la resolución de problemas concretos. Constituye un conjunto de conocimientos científicamente ordenados, que permiten diseñar y crear bienes o servicios que facilitan la adaptación al medio ambiente y la satisfacción de las necesidades esenciales y los deseos de la humanidad.

Template - es una herramienta utilizada para separar el diseño web de la programación de las funcionalidades de una página web.

TI - tecnología de la información (TI, más conocida como IT por su significado en inglés, Information Technology) es la aplicación de computadoras y equipos de comunicaciones para almacenar, recuperar, transmitir y manipular datos para utilizarlos el contexto de los negocios u otras empresas.

TIC - son las iniciales de tecnologías de la información y la comunicación, aquellas tecnologías que agrupan los elementos y las técnicas utilizadas en el tratamiento de la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

TID - tiempo promedio de implementación de cambios, es el cociente entre el tiempo total de cambios implementados y el número de cambios autorizados implementados.

Tiempos de respuesta - es el tiempo que transcurre entre el momento en que se crea una solicitud de soporte y el primer contacto, remoto o presencial para dar solución al pedido.

TIER - es una norma que detalla los criterios para diferenciar sus cuatro clasificaciones de topología de infraestructura del sitio, basada en los crecientes niveles de los componentes de capacidad redundantes y sus vías de distribución.

TIER 3 - es un método para evaluación y certificación de la seguridad física y la disponibilidad de los centros de datos. El nivel 3 clasifica la calidad de los sistemas de suministro de servicios públicos y otros componentes que determinan la inexistencia de punto único de falla en los sistemas de suministro, mayor resistencia al robo, protección de tuberías de suministro, contención de incendios y monitoreo de estado.

TIX - tiempo promedio de entregas implementadas, es el cociente entre el tiempo total de entregas implementadas y el número de entregas implementadas.

TNS - tiempo total de no disponibilidad del servicio, es el tiempo durante el cual el servicio de TI no tiene la capacidad de cumplir sus funciones de forma adecuada cuando le son requeridas.

Token - es un dispositivo físico de seguridad utilizado para acceder a un recurso restringido electrónicamente. Es como una llave electrónica que se usa para complementar o reemplazar una contraseña.

TPP - tiempo promedio de solución de problemas, es el cociente entre el tiempo total de solución de todos los problemas y el número total de problemas registrados.

TPS - tiempo promedio de solución de incidentes, es el cociente entre el tiempo total de solución de todos los incidentes y el número de incidentes registrados.

Troyano Informático - es un programa aparentemente inofensivo y legítimo, pero que al ser ejecutado, le provee al atacante un acceso remoto del equipo infectado.

TSS - tiempo total sin continuidad en el servicio, es el tiempo durante el cual el servicio de TI se encuentra interrumpido sin capacidad de cumplir las funciones establecidas.

TTB - Transform the Business, (en español Inversiones para Transformar el Negocio), son aquellas inversiones que desarrollan capacidades para nuevos mercados.

TTE - tiempo total de entregas implementadas, es el tiempo demandado para la implementación de versiones de software correspondientes a nuevos servicios de TI o actualizaciones de servicios vigentes.

TTI - tiempo total de solución de todos los incidentes, es el tiempo total requerido para resolver los eventos ocurridos y normalizar el suministro del servicio de TI.

TTP - tiempo transcurrido sin pruebas en el servicio, es el tiempo durante el cual no se realizan pruebas al servicio de TI que aseguren que el servicio cumple con su propósito, funcionalidad, usabilidad y accesibilidad.

TTS - tiempo total de solución de todos los problemas, es el tiempo requerido para implementar la solución a los problemas y gestionar la normalización del suministro del servicio.

Turbonomic Management - es un software que garantiza automáticamente el rendimiento de las aplicaciones para que funcionen de forma ininterrumpida.

UC - en el estándar ITIL es un Contrato de Provisión de Soporte acordado con un proveedor externo para la prestación de servicios no suministrados por la propia organización.

UPS - Uninterruptible Power Supply, (en español Sistemas de alimentación ininterrumpida), es un dispositivo que mediante sus baterías u otros elementos almacenadores de energía, en los casos de interrupción de suministro eléctrico, proporciona energía por un tiempo limitado a todos los dispositivos que tenga conectados.

VAC - variación de costos sin planificación, es la diferencia entre los costos totales del presupuesto planificado y los costos totales del presupuesto actual.

Veeam Availability Suite Backup - es un producto que gestiona de forma intuitiva el almacenamiento físico o en la nube y brinda disponibilidad a los servicios. Permite la recuperación de los servicios de TI, aplicaciones y datos basados en la nube desde una consola de administración individual. Automatiza los procesos asociados a la protección de los datos, recuperación y monitoreo, también brinda protección contra el secuestro de información.

Veeam One Management - es un software para visibilizar y administrar el entorno de TI. Permite que las operaciones de TI comuniquen información a los responsables de TI para la toma de decisiones. Monitorea e informa sobre la infraestructura, diagnostica y resuelve de forma automatizada.

Virtualizar - es la emulación de un recurso tecnológico a través de un software como puede ser un sistema operativo, una plataforma de hardware o cualquier otro recurso de red.

Virus informático - es un software que tiene por finalidad alterar el normal funcionamiento de un dispositivo informático. Dicha acción se realiza sobre el dispositivo con fines maliciosos y sin el permiso del usuario.

Visión artificial - es una disciplina científica formada por métodos para adquirir, procesar y analizar imágenes del mundo real con la finalidad de generar información que permita ser procesada por una máquina.

VMO - Value Management Office (en español Oficina de Gestión de Valor), responsable de asesorar en inversiones y oportunidades de inversión.

VMware Esxi - es el sistema operativo que permite correr otros sistemas operativos dentro de él, se instala fácilmente en el servidor y crea particiones en múltiples máquinas virtuales.

VMware Site Recovery Manager Orchestration - es un software de automatización integrado para proporcionar administración basada en políticas de planes de recuperación. Permite a los usuarios probar y automatizar las aplicaciones entre distintos sitios con un tiempo de inactividad mínimo, mantiene la disponibilidad y la movilidad dentro de los sitios en la nube privada.

Vmware vCenter Management - es una herramienta de sistemas que permite manejar una plataforma aplicando técnicas de control de virtualización para utilizar en una misma computadora diferentes sistemas operativos al mismo tiempo y gestionar varias máquinas virtuales de la manera más eficiente.

VMware vRealize Operation Management - es un sistema que ofrece optimización continua de los recursos de TI y gestiona el rendimiento basado en el propósito, la

eficiencia, la capacidad y la planificación. Optimiza, planifica y escala las implementaciones de la nube y del centro de datos.

Vmware vSphere esxi Hypervisor - es una plataforma de virtualización a nivel de centro de datos. Está compuesta por un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software. Los servicios y los servidores permiten la interacción con el software de gestión, la administración y las máquinas virtuales.

VMware vSphere Replication - es una extensión de la herramienta para el sistema VMware vCenter Server que proporciona replicación y recuperación de máquinas virtuales. Permite la elección de las máquinas virtuales y crea una copia de la máquina virtual conectada al disco replicado.

Vulnerabilidad Tecnológica - es una debilidad presente en un sistema operativo, software o sistema que le permite a un atacante violar la confidencialidad, integridad, disponibilidad, privacidad, control de acceso, consistencia del sistema, de sus datos o aplicaciones.

WAN - Wide Area Network (en español Red de Área Amplia), es una red de computadoras que se extiende en un territorio, ya sea en una ciudad, país o a nivel mundial.

Windows Server OS - es el sistema operativo diseñado para servidores de la compañía Microsoft, permite a un equipo manejar funciones de red como servidor de impresión, controlador de dominio, servidor web y servidor de archivos.

Guía de Tablas

Guía de Matrices

Guía de Figuras