



AUDITORIA GENERAL
DE LA CIUDAD DE BUENOS AIRES

"2022- Año del 40° Aniversario de la Guerra de Malvinas. En homenaje a los veteranos
y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

Auditoría de la Ciudad de Buenos Aires

Informe Firma Conjunta

Número:

Buenos Aires,

Lugar y fecha de emisión	Ciudad Autónoma de Buenos Aires, Mayo 2022
Código de Proyecto	10.21.03
Denominación del Proyecto	Agencia de Sistemas de Información.
Tipo de Auditoría	Sistemas.
Dirección General	

	Dirección General Sistemas de Información.
Período bajo examen	2020
Objeto de la Auditoría	Agencia de Sistemas de Información.
Objetivo de la Auditoría	Evaluar la eficacia de la gestión de las comunicaciones y operaciones.
Alcance	Analizar el cumplimiento de la gestión de las comunicaciones y operaciones establecidas en el Marco Normativo Tecnológico vigente en el GCABA.
Limitaciones al Alcance	Sin limitaciones.
Observaciones Relevantes	1. Alinear, Planificar y Organizar - APO01 • Gestionar el marco de gestión de I&T • Dependencia jerárquica de la Dirección General Seguridad Informática respecto de la Dirección Ejecutiva de la Agencia de Sistemas de Información. La configuración funcional y jerárquica actual de la estructura organizativa no favorece el control interno de los sistemas de comunicaciones y operaciones. 2. Alinear, Planificar y Organizar - APO07 • Gestionar los recursos humanos • Falta de actualización en el dictado de cursos de concientización a usuarios para la Prevención de Software Malicioso, uso de Correo Electrónico y uso responsable de Internet. La carencia del dictado de cursos de actualización limita los conocimientos

específicos, habilidades y competencias del recurso humano.

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

3. Alinear, Planificar y Organizar - APO12

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

4. Construir, adquirir e implementar - BAI03

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

5. Construir, adquirir e implementar - BAI06

- Gestionar los cambios de TI
- **No expone documentos que definan un modelo de control de cambios en los sistemas que gestionan las comunicaciones y operaciones. Falta de metodología, solicitud, evaluación, priorización, procesos de control, aceptación y versionados de los cambios. Es necesario mitigar el riesgo de los cambios a**

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

	9. Entregar, dar servicio y soporte - DSS02 • Gestionar las peticiones y los incidentes de servicio • No consta la definición e implementación de un proceso de administración de peticiones e incidentes por fallos en los sistemas ligados con las comunicaciones y operaciones. Debe establecerse un esquema de clasificación y petición que incluya el registro, priorización, aprobación, resolución, seguimiento e informe de incidentes. La falta del proceso atenta contra la productividad, no minimiza los incidentes y favorece las interrupciones en los servicios asociados. 10. Entregar, dar servicio y soporte - DSS05 • Gestionar los servicios de seguridad • No se detallan procesos de gestión de seguridad en los sistemas para proteger la conectividad, red, dispositivos de punto final, vulnerabilidades y los ataques por parte de software malicioso. Es indispensable controlar los sistemas asociados a las comunicaciones y operaciones y evaluar el impacto ocasionado en la seguridad de la información para garantizar la continuidad y disponibilidad del servicio. 11. Entregar, dar servicio y soporte - DSS06 • Gestionar los controles de procesos de negocio • No se expone un proceso de gestión de roles, responsabilidades, privilegios para el acceso y niveles de autoridad en los sistemas de comunicaciones y operaciones. El incumplimiento en la utilización del mencionado proceso no garantiza que la información administrada sea íntegra, completa, válida, precisa, segura y oportuna. 12. Monitorizar, evaluar y valorar - MEA01 • Gestionar la supervisión del rendimiento y la conformidad
--	--

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

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

SE EMBEBE AL PRESENTE INFORME FINAL

