INFORME EJECUTIVO

Lugar y fecha de emisión: Ciudad Autónoma de Buenos Aires, 8 de abril 2026.

Código de Proyecto: 10.25.02

Denominación del Proyecto: Sistemas Informáticos de Espacio Público e Higiene Urbana.

Tipo de Auditoría: Sistemas.

Dirección General: Dirección General Sistemas de Información.

Período bajo examen: 2024.

Objeto de la Auditoría: Sistemas Informáticos de Espacio Público e Higiene Urbana.

Objetivo de la Auditoría: Evaluar los sistemas informáticos y la infraestructura utilizada en el Ministerio de Espacio Público e Higiene Urbana.

Alcance: Verificar el desempeño de los sistemas y las tecnologías aplicadas a los procesos de gestión y control del espacio público.

Limitaciones al Alcance: Sin limitaciones.

Observaciones:

1) Se evidencia una limitación en la gobernanza de la información ya que no dispone del soporte documental que respalde la existencia de mecanismos implementados para medir el cumplimiento de las metas, objetivos y de satisfacción del usuario.
2) No adjunta documentación formal respaldatoria que incorpore la identificación de las áreas, roles y responsables a cargo de la definición de los objetivos estratégicos tecnológicos.
3) La Dirección no exhibe el Proceso de Evaluación y Clasificación de las Áreas Críticas ni la formalización de la delegación del proceso a la Agencia de Sistemas de Información.
4) La planificación aplicada al desarrollo de los sistemas carece de un desglose formal de las tareas a ejecutar, los requerimientos que las fundamentan y los responsables de las solicitudes.
5) Se constató la omisión de estudios de evaluación formal de los recursos tecnológicos y humanos a fin de asegurar el alineamiento de los sistemas con los objetivos estratégicos establecidos.
6) La evidencia analizada no incluye los Acuerdos de Nivel Operativo (OLA) formalizados con la Agencia de Sistemas de Información para los servicios tecnológicos provistos.

7) No se aporta evidencia documental formal que detalle los controles inherentes a los softwares utilizados para garantizar la integridad, trazabilidad y calidad de los datos procesados y emitidos.

   Falta de Políticas de Riesgos formalizadas orientadas a la protección de la información contenida en las bases de datos que eviten sustracciones o pérdidas.

8) Ausencia de un marco regulatorio formalizado que establezca los lineamientos para la seguridad física y lógica. La subsanación de este hallazgo incrementaría el control y la trazabilidad de los incidentes vinculados con los accesos.

   No se ha provisto soporte documental formal que certifique la existencia de un sistema de trazabilidad de accesos y transacciones, el tiempo de conservación de los registros y los controles de acceso aplicados. Indefinición en la corresponsabilidad de la gestión de los datos personales entre las áreas funcionales, la DGMYS y la Agencia de Sistemas de Información.

9) Se observa que el esquema de gobernanza de la información es conceptual. Carece de un mapeo formal entre los tipos de datos, roles y las responsabilidades asignadas.

   Ausencia de un marco metodológico para la normalización y consistencia de la información recibida, cuya implementación mejoraría el grado de precisión en el análisis y sus resultados. No exhibe una Política de Administración de Accesos a los Recursos de Infraestructura Tecnológica que formalice los criterios para la gestión de los privilegios en concordancia con las áreas funcionales.

10) La revisión identificó una insuficiencia de documentación sobre la infraestructura tecnológica, resaltando la inexistencia de registros de inventario que especifiquen y validen el equipamiento, junto con su ubicación.

    Asimismo, existe una limitación en la documentación de soporte que incluya el detalle técnico de la infraestructura de seguridad de red, el diagrama lógico de las interconexiones y el registro de los componentes de protección.

11) La documentación aportada no suministra el soporte formal suficiente para asegurar el cumplimiento tanto del Estándar desarrollo (ES 901) como del Proceso de Control de Cambios en Software de Aplicación provisto por Organismos (PC0901), ambos definidos por la Agencia para la gestión de los sistemas utilizados.

12) Carencia de procesos reglamentados de control de cambios y versionados de los desarrollos de software. El establecimiento de estas metodologías aseguraría la rastreabilidad de las modificaciones y optimizaría la restauración inmediata tras cualquier incidente. El análisis revela que la tecnología que suministra soporte operativo de los servicios de los sistemas se encuentra parcialmente basada en versiones ya no soportadas por el fabricante.

13) El organismo auditado no exhibió la totalidad de los manuales de usuario y la documentación técnica de las plataformas tecnológicas utilizadas.

14) Omisión en el soporte formal que certifique la existencia de un Registro de Componentes de la Configuración (CMDB) que favorezca la verificación y trazabilidad de las versiones de los activos y la gestión de los incidentes en los softwares utilizados.

15) Ausencia de soporte fehaciente que asegure la existencia de notificaciones y alertas preventivas automáticas en los sistemas que adviertan sobre la inminencia de eventos que deterioren la calidad del servicio.

16) La Dirección General Monitoreo y Sistemas no cuenta con un Plan de Contingencia de los sistemas formalmente establecido y validado, cuya activación optimizaría la continuidad operativa y la restauración de los servicios. Se verifica que el Plan de Recuperación de Desastres está desactualizado y no consta respaldo oficial que establezca el Acuerdo de Nivel Operativo que asegure la activación de un protocolo de respuesta eficiente ante una disrupción operativa.

17) Se determinó la insuficiencia de información formalizada que especifique los procesos, servicios y tecnologías aplicados a los inicios de sesión, procesos de autenticación y la gestión de los accesos a cada uno de los sistemas. De existir, incrementaría los controles destinados a la seguridad. El análisis concluye la carencia de una Política de Prevención de Software Malicioso formalmente definida, cuyo establecimiento, de materializarse, optimizaría los procesos de respuesta a incidentes.

18) La administración de incidentes carece de trazabilidad hacia la mejora continua. Se evidencia una debilidad en el control interno debido a la omisión de documentación que respalde la evaluación de los casos recibidos por la Mesa de Ayuda y las adecuaciones efectuadas en consecuencia para la optimización de la eficiencia operativa.

19) No se presentan los resultados de la evaluación formal de la adecuación al “Marco Normativo de Tecnología de Información” establecido por la Agencia de Sistemas de Información.

Conclusión/Dictamen:

La Dirección General de Monitoreo y Sistemas (DGMYS), dependiente del Ministerio de Espacio Público e Higiene Urbana (MEPHU), tiene a su cargo la implementación y administración de la tecnología que utiliza el Ministerio. Asimismo, coordina los sistemas informáticos que permiten gestionar los datos y realizar el seguimiento de los principales indicadores de gestión, favoreciendo el control de las actividades, la detección de desvíos y la toma de decisiones con información actualizada.
A través de estos sistemas, la Dirección administra y organiza la información vinculada con la recolección de residuos, la planificación de inspecciones y el registro digital de infracciones. En consecuencia, estos sistemas constituyen herramientas estratégicas para la gestión.
No obstante, el análisis realizado evidencia que, si bien la infraestructura tecnológica se mantiene operativa y se atienden los requerimientos funcionales, persisten debilidades relevantes en la organización y en el respaldo formal de la gestión. En particular, no se encuentran claramente definidas las áreas críticas, los objetivos de gestión ni las responsabilidades de los actores intervinientes, lo que limita la capacidad de control y coordinación.

En este contexto, la ausencia de una matriz formal de roles y responsabilidades, así como de acuerdos de trabajo debidamente establecidos con las áreas internas y con la Agencia de Sistemas de Información (Acuerdos de Nivel Operativo), genera indefiniciones en la asignación de tareas, superposición de funciones y falta de claridad en los niveles de servicio. En consecuencia, la Dirección debe avanzar en la formalización de estos instrumentos, a fin de ordenar la gestión, fortalecer el control interno y mejorar la calidad de los servicios prestados.

Asimismo, se verifican debilidades en aspectos centrales de la gestión tecnológica. En particular, los mecanismos actuales vinculados a la seguridad de la información, el control de accesos y la confiabilidad de los datos resultan insuficientes. Del mismo modo, la documentación técnica de la infraestructura y el seguimiento de los cambios en los sistemas presentan falencias que dificultan la trazabilidad y el control.

Adicionalmente, la gestión de incidentes no se encuentra suficientemente estructurada y no se dispone de un plan de contingencia adecuadamente formalizado que permita asegurar la continuidad operativa ante eventuales interrupciones del servicio. Tampoco se observan mecanismos formales de monitoreo que permitan evaluar de manera sistemática el cumplimiento de metas y el nivel de satisfacción de las áreas usuarias.

En función de lo expuesto, la Dirección debe corregir estas deficiencias mediante el fortalecimiento integral de sus procesos, incorporando estándares formales de seguridad, control, documentación, gestión de incidentes y monitoreo. La implementación de estas mejoras resulta necesaria para reducir riesgos, asegurar la continuidad de los servicios y garantizar una gestión de la información confiable y eficiente.

Finalmente, se observa que la integración de los sistemas de la Dirección con los sistemas de movilidad urbana del Gobierno de la Ciudad es aún limitada. En este sentido, la Dirección debe avanzar en dicha integración e incorporar herramientas de inteligencia artificial que permitan anticipar situaciones de congestión e incidentes, optimizando la planificación de las tareas de higiene urbana y reduciendo su impacto sobre la circulación vehicular.

Las tareas de auditoría finalizaron en noviembre de 2025.

Palabras Claves: Higiene, sistemas, espacio público, gestión de la información, control, gobierno tecnológico.

- **Se encuentra embebido el Informe Final -**

Auditoría de la Ciudad de Buenos Aires

-

Hoja Adicional de Firmas
Informe Gráfico

Número: IF-2026-00008155-AGCBA-DTACO

Buenos Aires,
Lunes 13 de Abril de 2026

Referencia: IF 10.25.02 "Sistemas Informáticos de Espacio Público e Higiene Urbana"

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by sade.agcba.gob.ar
Date: 2026.04.13 12:56:33 -03:00

Actuaciones Colegiadas
Departamento Actuaciones Colegiadas
Dto. Actuaciones Colegiadas
Auditoría General de la Ciudad de Buenos Aires

Digitally signed by sade.agcba.gob.ar
Date: 2026.04.13 12:56:34 -03:00