AUDITORÍA GENERAL
DE LA CIUDAD DE BUENOS AIRES

Informe Final de Auditoría
Con Informe Ejecutivo

Proyecto N° 10.25.07

Login miBA

Auditoría de Sistemas

Período 2024

BUENOS AIRES - DICIEMBRE 2025

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

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

JEAN JAURES 220 - CIUDAD DE BUENOS AIRES

Presidente

Dra. Mariana Inés GAGLIARDI

Auditores Generales

Dr. Juan José CALANDRI

Dra. Jorgelina Marisa CARNEVALE

Lic. Patricia Alejandra CASERES

Dr. Pablo CLUSELLAS

Lic. José Luis GIUSTI

Dr. Lisandro Mariano TESZKIEWICZ

Código de Proyecto: 10.25.07

Nombre del Proyecto Auditoría: Login miBA.

Tipo de auditoría: Sistemas.

Organismo auditado: Dirección General de Ciudadanía Digital (DGCIUD).

Objeto: Login miBA.

Objetivo: Evaluar la seguridad de acceso (usuarios, contraseñas, sesiones), complementación de procesos productivos e integración con otros sistemas, satisfacción del usuario y cumplimiento de metas y objetivos, indicación de desempeño, soporte técnico, protección de datos personales y los mecanismos de control interno del sistema Login miBA.

Alcance: Verificar el entorno y los procesos utilizados para el gobierno, la gestión de la tecnología y la información.

Jurisdicción / Unidad Ejecutora: Jurisdicción 21 Jefatura de Gabinete de Ministros (MJGGC) – Unidad Ejecutora 7313 Subsecretaría de Ciudad Inteligente (SSCIUI).

Presupuesto: – Programa 107 “Ciudad Inteligente” y Programa 111 “Gobierno e identidad Digital.

Período a Auditar: 2024

Director de Proyecto: N/A

Supervisor: Abg. Mariano Monzón Font

Las tareas de auditoría comenzaron en febrero de 2025.

FECHA DE APROBACIÓN DEL INFORME: 17 DE DICIEMBRE DE 2025
APROBADO POR: UNANIMIDAD

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

INFORME EJECUTIVO

Lugar y fecha de emisión: Buenos Aires, 17 de diciembre de 2025
Código de Proyecto: *10.25.07*
Denominación del Proyecto: Login miBA
Tipo de Auditoría: Auditoría de Sistemas.
Dirección General: DG de Sistemas de Información.
Período bajo examen: *2024*
Objeto de la Auditoría: Login miBA.
Objetivo de la Auditoría: Evaluar la seguridad de acceso (usuarios, contraseñas, sesiones), complementación de procesos productivos e integración con otros sistemas, satisfacción del usuario y cumplimiento de metas y objetivos, indicación de desempeño, soporte técnico, protección de datos personales y los mecanismos de control interno del sistema Login miBA.
Alcance: Verificar el entorno y los procesos utilizados para el gobierno, la gestión de la tecnología y la información.
Limitaciones al Alcance: No existieron limitaciones al alcance.
Principales Observaciones:

Observación N° 1:

Se advierte que la política de contraseñas implementada en Login miBA no cumple con algunos de los requerimientos establecidos por los estándares internacionales actuales, como el NIST SP800-63B. En particular, no se impide el uso de identificadores del usuario como contraseña, no se conserva un historial que evite la reutilización, ni se realiza validación contra contraseñas comunes o previamente comprometidas, y el sistema no permite la autenticación con doble factor ni cuenta con dicha funcionalidad prevista.

Además, durante las pruebas realizadas se comprobó que el sistema acepta contraseñas débiles o comprometidas y presenta mensajes de error genéricos que dificultan la comprensión del motivo de rechazo. Asimismo, no envió correos electrónicos al usuario informando sobre la modificación de la contraseña.

En consecuencia, el esquema actual de contraseñas resulta parcialmente alineado con las buenas prácticas internacionales, pero requiere una revisión técnica integral que garantice niveles adecuados de seguridad y usabilidad.

Observación N° 2:

Se observó que no se encuentran documentadas ni implementadas de manera formal diversas prácticas de seguridad vinculadas a la autenticación y gestión de sesiones. En particular, no se evidencian evaluaciones de seguridad basadas en el estándar OWASP Top 10, escaneos automatizados de vulnerabilidades ni ejercicios orientados a la detección proactiva de fallas.

Asimismo, se detecta la ausencia de documentación técnica sobre configuraciones críticas del sistema de identidad Keycloak. Esta falta de evidencia limita la trazabilidad y dificulta la verificación de la robustez de los controles de seguridad implementados.

Observación N° 3:

Se observó que la versión de Java utilizada se encuentra discontinuada, sin actualizaciones de seguridad públicas y con vulnerabilidades (CVE) conocidas, mientras que la versión de Keycloak implementada es antigua, carece de soporte activo de la comunidad y presenta riesgos similares. Esta situación expone al sistema

a posibles fallas de seguridad no corregidas y limita la capacidad de aplicar actualizaciones o parches críticos para mantener la integridad y protección del entorno de autenticación.

Observación N° 4:

Se constató la inexistencia de un marco formal de gobernanza de integraciones que establezca políticas, roles, métricas y responsabilidades para la administración y control de las conexiones activas entre sistemas. Asimismo, no se hallaron acuerdos de nivel de servicio (SLA) con los organismos externos involucrados —en particular con el RENAPER— ni con reparticiones del GCABA, especialmente la Agencia Gubernamental de Ingresos Públicos (AGIP). Tampoco se hallaron acuerdos operativos internos (OLA) entre las áreas internas responsables del mantenimiento y soporte de dichas integraciones. En consecuencia, no existen compromisos documentados sobre tiempos de respuesta, niveles de disponibilidad, protocolos de escalamiento ni procedimientos de gestión ante incidentes.

Observación N° 5:

Se identifica que, si bien los sistemas miBA y Login miBA cuentan con algunos mecanismos potenciales para relevar la satisfacción del usuario —como las calificaciones en tiendas de aplicaciones, los canales de soporte y las opciones internas de retroalimentación—, no existe un plan estratégico integral ni un sistema formalmente implementado para medir de manera sistemática el cumplimiento de metas, objetivos y el nivel de satisfacción de los usuarios.

Asimismo, no se aplican métricas estandarizadas de satisfacción como NPS (Net Promoter Score), CSAT (Customer Satisfaction Score) post-interacción, CES (Customer Effort Score), ni se realizan encuestas periódicas o análisis de comportamiento de los usuarios que permitan obtener información representativa y comparable a lo largo del tiempo. Esta situación limita la capacidad de la organización para evaluar objetivamente la experiencia de los usuarios, identificar áreas de mejora y verificar el cumplimiento de sus objetivos de servicio y calidad.

Observación N° 6:

El sistema cuenta con mecanismos de registro y análisis de casos a través del software Plataforma de Análisis de Datos (PAD), que permiten monitorear volúmenes, tiempos de resolución y principales incidencias. Sin embargo, no se relevan métricas de satisfacción del usuario ni procedimientos sistemáticos para incorporar el feedback ciudadano en la mejora continua del servicio, lo que limita la evaluación integral de la calidad del soporte técnico.

Observación N° 7:

Si bien la plataforma Login miBA cuenta con normativa, políticas, un Acuerdo de Procesamiento de Datos (DPA) con su proveedor e implementa medidas técnicas de seguridad como cifrado de datos, autenticación segura y control de accesos; no se evidencian medidas o prácticas activas de protección de datos personales, no se constató la existencia de una Evaluación de Impacto en la Protección de Datos (DPIA), especialmente relevante por el uso de datos biométricos, ni se evidencian evaluaciones de riesgo de privacidad ni medidas de mitigación formalmente aprobadas.

Asimismo, se observa que la “Política de Privacidad” del, al tratar sobre almacenamiento, contempla la posibilidad de que los datos sean alojados “pudiendo

o no encontrarse dentro de las regiones adecuadas" para el caso de transferencia internacional de datos. Ello sin perjuicio de que en la actualidad la totalidad de los datos personales se encuentran alojados en los data centers de la ASINF.

Por último, la Base de Datos se encuentra inscripta en el centro de Protección de Datos Personales (CPDP) de la Defensoría del Pueblo de la CABA conforme a Ley CABA N° 1.845 de Protección de Datos Personales, pero no se encuentra registrada ante la Agencia de Acceso a la Información Pública (AAIP), autoridad de aplicación nacional de la Ley N° 25.326 de Protección de Datos Personales.

Observación N° 8:

La DG de Ciudadanía Digital (DGCIUD) no cuenta con procedimientos de control interno formalizados ni con mecanismos sistemáticos de monitoreo y revisión periódica aplicables al sistema Login miBA. No se identifican políticas, metodologías ni marcos de referencia (como COSO o COBIT) que estructuren los controles internos, ni se evidenció la realización de pruebas de penetración documentadas o auditorías de seguridad externas. Asimismo, se evidenció la inexistencia de auditorías internas o externas previas, técnicas o de gestión.

Aunque el sistema dispone de herramientas técnicas de control y monitoreo, estas prácticas operan de manera aislada y sin un marco formal de control. La ausencia de una estructura documentada de gestión de riesgos, matriz de controles clave y procesos de autoevaluación limita la capacidad institucional de asegurar la eficacia y trazabilidad de los controles implementados

Conclusión/Dictamen:

El sistema Login miBA constituye la plataforma central de autenticación e identidad digital del Gobierno de la Ciudad de Buenos Aires, permitiendo a la ciudadanía acceder de manera unificada y segura a múltiples servicios digitales. Su implementación representa un componente estratégico dentro del modelo de gobierno digital, al facilitar la trazabilidad de usuarios, la simplificación de trámites y la interoperabilidad entre organismos.

Durante la auditoría se identificaron fortalezas relevantes, entre ellas la existencia de mecanismos técnicos de seguridad como el uso de cifrado robusto, la autenticación segura y la integración con proveedores especializados para la verificación biométrica. Asimismo, se relevó la presencia de herramientas operativas de soporte, monitoreo y análisis que contribuyen al funcionamiento cotidiano del sistema.

No obstante, se advirtieron oportunidades de mejora significativas. En primer lugar, la política de contraseñas presenta debilidades en relación con estándares internacionales como NIST SP 800-63B, permitiendo contraseñas débiles o previamente comprometidas y careciendo de mecanismos como historial, validación de listas prohibidas y autenticación multifactor.

En segundo término, se constató la ausencia de prácticas formalizadas de seguridad para la autenticación y gestión de sesiones, incluyendo la falta de evaluaciones basadas en OWASP Top 10, escaneos automatizados de vulnerabilidades y documentación técnica del sistema de identidad.

Finalmente, se verificó la inexistencia de un marco de gobernanza para las integraciones del sistema, con ausencia de políticas, roles, métricas, acuerdos de nivel de servicio (SLA) y acuerdos operativos internos (OLA), lo que limita la capacidad de asegurar la continuidad operativa y el funcionamiento coordinado con organismos internos y externos.

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

En síntesis, Login miBA constituye un sistema sólido desde el punto de vista operativo y con medidas técnicas adecuadas, pero requiere atender a las observaciones halladas en este informe.

Palabras Claves: miBA, Login, identidad digital, ciudadanía digital, DGCIUD, contraseña.

ÍNDICE

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

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

INFORME FINAL DE AUDITORÍA
"LOGIN miBA"
PROYECTO N° 10.25.07

DESTINATARIO

Señora
Presidenta
Legislatura Ciudad Autónoma de Buenos Aires
Dra. Clara Muzzio
S / D

En uso de las facultades conferidas por los artículos 131, 132 y 136 de la Ley 70 de la Ciudad Autónoma de Buenos Aires, y conforme a lo dispuesto en el artículo 135 de la Constitución de la Ciudad, la Auditoría General de la Ciudad de Buenos Aires ha procedido a efectuar una Auditoría de Sistemas en el ámbito de la repartición Dirección General de Ciudadanía Digital (DGCIUD) con el objeto detallado en el apartado siguiente.

I. OBJETO DE AUDITORIA.

Sistema Login miBA.

II. OBJETIVO DE LA AUDITORIA.

Evaluar la seguridad de acceso (usuarios, contraseñas, sesiones), complementación de procesos productivos e integración con otros sistemas, satisfacción del usuario y cumplimiento de metas y objetivos, indicación de desempeño, soporte técnico, protección de datos personales y los mecanismos de control interno del sistema Login miBA.

Asimismo, se plantearon los siguientes Objetivos Específicos:

- **OE1: Seguridad de acceso: usuarios, contraseñas, sesiones.**

  Evaluar las políticas de creación de usuarios, asignación y resguardo de contraseñas, administración de roles y permisos, y los procedimientos para altas, bajas y modificaciones. Se analizará también la gestión de sesiones, mecanismos de seguridad aplicados, y el uso de técnicas de cifrado.

- **OE2: Complementación de Procesos productivos e Integración con otros sistemas.**

  Se analizará el grado de integración y articulación del sistema con los procesos de otras reparticiones del GCABA, en especial con los sistemas SADE, TAD, Registro Civil y Boti, así como con organismos nacionales como RENAPER,

ARCA (ex AFIP), o ANSeS. Se evaluará el nivel de interoperabilidad, normalización de datos, y la eficiencia en el intercambio de información.

- **OE3: satisfacción del usuario y cumplimiento de metas y objetivos.**

  Relevar si existen mecanismos para medir la satisfacción del usuario, así como indicadores y funcionalidades orientadas al cumplimiento de metas y objetivos operativos. Se considerará si la plataforma emite informes o métricas periódicas que permitan su seguimiento.

- **OE4: Indicadores de desempeño.**

  Identificar y analizar los indicadores de desempeño implementados para evaluar la eficiencia, eficacia y calidad de las funcionalidades del sistema. Se considerará la existencia de reportes periódicos y mecanismos de mejora continua.

- **OE5: Soporte técnico.**

  Evaluar la existencia y funcionamiento de la mesa de ayuda interna y externa. Se analizará la cobertura del soporte técnico en primer y segundo nivel, la existencia de sistemas de registro y seguimiento de incidentes (tickets), y si se realizan análisis sobre los casos para derivar en mejoras o adecuaciones.

- **OE6: Protección de datos personales.**

  Existencia, incidencia y políticas y prácticas de protección de datos personales en la información procesada.

- **OE7: Auditorías y Control interno.**

  Verificar la existencia de auditorías previas, relevamientos o seguimientos efectuados por organismos de control, así como los cambios implementados en función de observaciones o recomendaciones. Se revisarán también los procedimientos de control interno y los mecanismos de monitoreo vigentes.

III. ALCANCE DEL EXAMEN.

Verificar los procesos y resultados de gestión y de la información del sistema de Login miBA.

III.1.- Marco Normativo de la Auditoría de Sistemas:

Se utilizó el siguiente marco normativo y de buenas prácticas internacionales:

Nuevas Normas Básicas de Auditoría Externa[1] de la AGCBA y las Normas Básicas de Auditoria de Sistemas[2] de la AGCBA, la Ley 70 CABA, Ley 325 CABA y complementarias.

Normas COBIT 2019[3] (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Association (ISACA). Capítulo Buenos Aires.

Las normas y recomendaciones de Tecnologías de la Información (TI) establecidas por la ASINF (Res 177/ASInf/13[4] y ampliaciones).

Estándar NIST SP 800-63 (Digital Identity Guidelines)[5] de la National Institute of Standards and Technology (NIST)[6] de los Estados Unidos.

La referencia de buenas prácticas reconocida internacionalmente OWASP Top 10[7] de la Open Web Application Security Project (OWASP)[8].

III.2.- Procedimientos realizados.

Se remitió una nota de Inicio de Auditoría al Director General de la Dirección General de Ciudadanía Digital (DGCIUD), se realizó una reunión con el Director General, se presentó al equipo de trabajo, se explicó el alcance del proyecto, se aclararon temas relacionados y se acordaron los pasos a seguir.

Se envió una nota de pedido de información al área auditada inquiriendo sobre su normativa, presupuesto, personal, funcionamiento, procesos, sistemas informáticos y tecnologías.

---

[1] https://www.agcba.gob.ar/docs/norm_2024-10-07_normas-basicas-de-auditoria-externa.pdf [Accedido el 13/10/2025]
[2] https://www.agcba.gov.ar/web/doc/ni-normas_basicas_de_auditoria_sistemas.pdf [Accedido el 13/10/2025]
[3] Normas COBIT 2019. https://www.isaca.org/resources/cobit [Accedido el 13/10/2025]
[4] https://boletinoficial.buenosaires.gob.ar/normativaba/norma/232269 y https://boletinoficialpdf.buenosaires.gob.ar/util/imagen.php?idn=232269&idf=1 [Accedidos el 13/10/2025]
[5] Es un estándar técnico publicado por el NIST cuyo objetivo es establecer lineamientos para la gestión de identidades digitales, autenticación y control de acceso en sistemas en línea. https://pages.nist.gov/800-63-3/ [Accedido el 14/10/2025].
[6] El NIST (National Institute of Standards and Technology) es el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, una agencia federal que forma parte del Departamento de Comercio de EE. UU. Su función principal es desarrollar estándares, guías técnicas y mediciones que garanticen la seguridad, interoperabilidad y calidad en sectores como la industria, la ciencia, la tecnología y —muy especialmente— la ciberseguridad. El NIST es especialmente reconocido por la serie de guías SP (Special Publicatios), la que en particular atañe a este punto es la NIST SP 800-63 (Digital Identity Guidelines). https://www.nist.gov/ [Accedido el 14/10/2025].
[7] El Top 10 de OWASP es un documento estándar de concientización para desarrolladores y seguridad de aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web. https://owasp.org/www-project-top-ten/ [Accedido el 14/10/2025].
[8] OWASP es una fundación sin fines de lucro dedicada a mejorar la seguridad del software y ofrece recursos abiertos y gratuitos como guías, estándares y herramientas de testeo. https://owasp.org/ [Accedido el 14/10/2025].

Se creó una carpeta compartida mediante la solución en la nube de Onedrive, otorgándose permisos de edición a los emails de los funcionarios y agentes del órgano dedicados a esta auditoría.

Se revisaron 2 Programas que afectan al ecosistema miBA: el Programa 107 “Ciudad Inteligente” y el Programa 111 “Gobierno e identidad Digital”. Jurisdicción 21 Jefatura de Gabinete de Ministros (MJGGC) - Unidad Ejecutora 7313 Subsecretaría de Ciudad Inteligente (SSCIUI).

Se evaluó la información recibida.

Se realizaron entrevistas con los responsables de las áreas operativas relacionadas con el objeto de esta auditoría.

Se solicitaron y revisaron los informes de auditoría previos tanto de la AGCBA como de la Sindicatura General de la Ciudad Autónoma de Buenos Aires (SGCBA) y Unidades de Auditoría Interna de ministerio o ente.

IV.- LIMITACIONES AL ALCANCE.

No existieron limitaciones al alcance.

V.- ACLARACIONES PREVIAS.

Sistema miBA. Dirección General de Ciudadanía Digital (DGCIUD):

1.0 - Sistema Login miBA. Introducción.

El sistema miBA fue establecido formalmente en el año 2021 mediante la Resolución Nº 536/MJGGC/21[9], que lo definió como la herramienta oficial y centralizada para la atención digital de la ciudadanía. Asimismo, se creó el Perfil Digital Ciudadano, un mecanismo para verificar de forma segura la identidad de las personas, garantizando el respeto por la privacidad y la protección de sus datos personales.

A partir de esa resolución fundacional, se dictaron otras normas que ampliaron el alcance y funcionalidades del sistema miBA, entre las que se puede nombrar a:

- La Resolución Nº 33/SSCIUI/21[10] aprobó el procedimiento para validar la identidad digital dentro de miBA, asegurando que el acceso a la plataforma sea confiable y seguro.
- La Resolución Nº 186/SECITD/24[11] dispuso que los documentos digitales generados por el Gobierno y almacenados en miBA —como credenciales, certificados o constancias— tienen la misma validez legal que sus versiones en papel.

[9] https://boletinoficial.buenosaires.gob.ar/normativaba/norma/567638
[10] https://boletinoficial.buenosaires.gob.ar/normativaba/norma/578914
[11] https://boletinoficial.buenosaires.gob.ar/normativaba/norma/758991

- Por último, la Resolución Nº 20/OGDAI/23[12] permitió que se puedan presentar reclamos o solicitudes de información pública a través de miBA, en el marco de la Ley Nº 104 de acceso a la información.

El ecosistema Login miBA – miBA está concebido para brindar a los ciudadanos una plataforma segura y eficiente de gestión de identidad digital y acceso unificado a los servicios digitales del Gobierno de la Ciudad de Buenos Aires (GCABA).

La presente auditoría se circunscribe al sistema Login miBA, quedando excluida la aplicación miBA.

Login miBA:

Login miBA actúa como el punto central de autenticación del ecosistema, verificando la identidad de los usuarios mediante distintos mecanismos (contraseñas, autenticación multifactor y credenciales verificables). Emplea estándares abiertos como OpenID Connect (OIDC)[13] y OAuth 2.0[14], que garantizan la interoperabilidad, la seguridad y el inicio de sesión único (SSO) [15] para acceder a múltiples servicios del GCABA.

El desarrollo y mantenimiento del ecosistema ha estado a cargo de diferentes proveedores tecnológicos contratados por la administración: El desarrollo y mantenimiento del ecosistema miBA es realizado por empresas proveedoras bajo contratación de licitaciones públicas y eventuales prórrogas:

- En 2021, Line64 S.R.L. asumió el mantenimiento inicial del sistema.
- En 2022, Epidata S.A. fue adjudicada para la continuidad de las tareas de mantenimiento y desarrollo, con sucesivas prórrogas y ampliaciones.
- Desde 2024, Werden IT S.A. es la empresa responsable del desarrollo y mantenimiento integral, en el marco de un contrato con vigencia de 12 meses.

La plataforma miBA se encuentra integrada con otros sistemas esenciales del Gobierno porteño, como por ejemplo TAD (Trámites a Distancia), que emplea las credenciales de Login miBA para autenticar a sus usuarios. También mantiene conexión con RENAPER, a través de un sistema interno de interoperabilidad denominado Enterprise Service Boost (ESB)[16], desarrollado por la Agencia de Sistemas de Información (ASINF).

En cuanto a su infraestructura, los sistemas utilizados por miBA están alojados en entornos gestionados por ASINF, utilizando tecnologías como OpenShift, máquinas virtuales (VMs) y bases de datos Exadata. ASINF también tiene a su cargo

[12] https://boletinoficial.buenosaires.gob.ar/normativaba/norma/649851
[13] Ver Objetivo Especifico 1.
[14] Ver Objetivo Especifico 1.
[15] El inicio de sesión único (*Single Sing On* SSO) es un proceso de autenticación que permite a un usuario acceder a múltiples aplicaciones con un único conjunto de credenciales de inicio de sesión. https://www.techopedia.com/definition/4106/single-sign-on-sso [Accedido el 24/05/2025]
[16] Es un desarrollo específico de la ASINF de un Enterprise Service Bus (ESB), es decir, un sistema de interoperabilidad / middleware que permite integrar y mediar el intercambio de información entre distintos sistemas (por ejemplo, entre Login miBA y RENAPER).

los servicios de conectividad local y troncal, mesa de ayuda, procesamiento, backups y recuperación ante desastres, así como la definición y gestión de los Acuerdos de Nivel de Servicio (SLA). El soporte técnico al equipamiento físico asociado al sistema es provisto directamente por la Subsecretaría de Ciudad Inteligente (SSCIUI).

En cuanto a la propiedad del código fuente, los derechos de propiedad intelectual y cualquier otro derecho sobre los trabajos realizados por proveedores, documentación, estudios, análisis y cualquier otro producto derivado del cumplimiento del contrato pertenecen exclusivamente al Gobierno de la Ciudad Autónoma de Buenos Aires (GCABA). Así como los datos y bases de datos generadas son propiedad exclusiva del GCABA y no podrán ser utilizados para fines distintos a los previstos en el contrato.

1.1 - Normativa - Estructura Orgánico-Funcional.

El sujeto de la presente auditoría es la Dirección General de Ciudadanía Digital (DGCIUD). Depende de la Subsecretaría de Ciudad Inteligente (SSCIUI). Esta, a su vez, forma parte de la Secretaría de Innovación y Transformación Digital (SECITD) bajo la órbita de la Jefatura de Gabinete de Ministros (MJGGC).

Es importante destacar que la Subsecretaría de Ciudad Inteligente (SSCIUI) tiene bajo su responsabilidad diversas Direcciones Generales cuyas funciones se articulan entre sí:

- DG Canales Digitales (DGCDI): responsable de los medios de contacto virtual con la ciudadanía.

- DG Sistema de Atención Ciudadana (DGSACIU): encargada de gestionar y optimizar los mecanismos de atención y respuesta al público.

- DG Ciudadanía Digital (DGCIUD): es el sujeto de la presente auditoría, cuya función principal es garantizar una identidad digital segura y facilitar el acceso eficiente a los servicios digitales.

En el ámbito interno de la Dirección General Ciudadanía Digital (DGCIUD), se identifican tres (3) **Gerencias Operativas:**

- **GO Tecnología**: brinda soporte técnico y desarrolla herramientas digitales.
- **GO Identidad Digital:** se enfoca en los procesos de validación y autenticación de personas en entornos digitales. De esta gerencia depende la Subgerencia Operativa de Resoluciones de Contingencias, que interviene en casos especiales relacionados con problemas en las identidades digitales.
- **Integraciones de Mesa de Ayuda:** se encarga de articular y dar soporte a los distintos canales de asistencia ciudadana.

1.2 - Organigrama.

En la siguiente imagen se puede ver la ubicación de la DG de Ciudadanía Digital (DGCIUD) dentro de organigrama de la Jefatura de Gabinete de Ministros (MJGGC).

1.3 - Competencia - Responsabilidades Primarias.

Las responsabilidades primarias de la DG Ciudadanía Digital (DGCIUD), fueron definidas por el Decreto GCABA 199/2024[17]. Entre las más relevantes con el objeto de esta auditoría podemos destacar:

- "Administrar el portal de acceso único del ciudadano a los aplicativos de los servicios del Gobierno de la Ciudad Autónoma de Buenos Aires, e implementar en las reparticiones el login/acceso del ciudadano a los productos digitales."

- "Generar el mecanismo para validar la identidad de los ciudadanos de forma remota."

1.4 - Presupuesto – Jurisdicción – Programa.

En la ley de presupuesto 2024[18], en la Jurisdicción 21 – Jefatura de Gabinete de Ministros, y la Unidad Ejecutora 7313 Subsecretaría de Ciudad Inteligente (SSCIUI), existen 2 Programas que afectan al sistema miBA: el Programa 107 "Ciudad Inteligente" y el Programa 111 "Gobierno e identidad Digital".

Programa: **107 Ciudad Inteligente**

Unidad Ejecutora: Subsecretaría de Ciudad Inteligente
Jurisdicción: 21.JEFATURA DE GABINETE DE MINISTROS
Finalidad: Administración Gubernamental
Función: Dirección ejecutiva

PRESUPUESTO FINANCIERO	
Inciso Principal	**IMPORTE**
Gastos en personal	**368.333.236**
Personal Permanente	216.831.756
Asistencia social al personal	5.150.372
Gabinete de autoridades superiores	146.351.108
Bienes de consumo	**3.407.266**
Productos alimenticios, agropecuarios y forestales	3.255.495
Otros bienes de consumo	151.771
Servicios no personales	**341.613.196**
Servicios profesionales, técnicos y operativos	299.375.218
Servicios Especializados, Comerciales y Financieros	37.942.848
Pasajes, viáticos y movilidad	728.502
Otros servicios	3.566.628
TOTAL	**713.353.698**

lustración 1 Fuente Presupuesto 2024

[17] https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-DEC-AJG-AJG-199-24-ANX-1.pdf Páginas 91 a 93 [Accedido el 26/07/2025].
[18] https://buenosaires.gob.ar/sites/default/files/2024-02/21-JefaturadeGabinete.pdf página 62 a 66.

Programa: **111 Gobierno e Identidad Digital**

Unidad Ejecutora: Subsecretaría de Ciudad Inteligente
Jurisdicción: 21.JEFATURA DE GABINETE DE MINISTROS
Finalidad: Administración Gubernamental
Función: Dirección ejecutiva

PRESUPUESTO FINANCIERO	
Inciso Principal	**IMPORTE**
Gastos en personal	**42.139.483**
Personal Permanente	41.536.582
Asistencia social al personal	602.901
Servicios no personales	**980.457.735**
Servicios Especializados, Comerciales y Financieros	980.457.735
TOTAL	**1.022.597.218**

PRESUPUESTO FÍSICO			
VARIABLE	**DENOMINACIÓN**	**U. MEDIDA**	**CANTIDAD**
META	CONVERSACIONES DIGITALES CON EL CIUDADANO	Conversación	30.000.000

Ilustración 2 Fuente Presupuesto 2024

En el Presupuesto 2024[19], correspondiente a la Jurisdicción 21 – Jefatura de Gabinete de Ministros, Unidad Ejecutora 7313, en el Programa 107, no se especifican metas cuantitativas que permitan una evaluación precisa de los objetivos o resultados esperados para dicha dependencia. Sí se especifican metas cuantitativas para el Programa 111, pero están referidas al chatbot Boti, y no se aplican a la presente auditoría.

En los objetivos previstos para el Programa 111 “Gobierno e Identidad Digital” mencionados en la Ley de Presupuesto 2024, cabe destacar:

- “En esta línea, se continúa con el proyecto "Login", instancia de autenticación para acceder de forma oficial a los portales web del GCABA o cualquier otro activo digital.”

1.5 - Procesos en el sistema:

Los procesos en el sistema versan sobre la creación, autenticación, inicio de sesión de usuarios, y acreditación y vinculación con otros sistemas y servicios.

1. Creación de Usuario en Login MiBA:

Cuando una persona accede por primera vez al sistema de Login miBA, debe crear un perfil en la plataforma de autenticación. Para ello, se le solicita la carga de

[19] https://buenosaires.gob.ar/sites/default/files/2024-02/21-JefaturadeGabinete.pdf página 62 a 66.

un conjunto mínimo de datos personales, que incluye: Nombre, Apellido, CUIT, Fecha de nacimiento, Género.

Con esta información, se genera un registro de usuario, el cual estará asociado a una credencial de acceso. Esta credencial puede ser la propia clave tributaria o una dirección de correo electrónico. En caso de optar por el uso de correo electrónico como credencial, se requiere una validación previa, mediante el envío de un enlace de confirmación al buzón proporcionado por la persona usuaria.

La plataforma de autenticación funciona como el sistema centralizado de gestión de identidad digital para la ciudadanía. Constituye un padrón único que unifica y administra la información personalizada de quienes interactúan digitalmente con el Gobierno. Cada usuario registrado queda identificado de forma unívoca mediante una clave interna BAID (Buenos Aires ID), que permite asegurar la trazabilidad de sus operaciones dentro de los sistemas integrados.

2. Servicios asociados a la autenticación e identificación

La plataforma ofrece un conjunto de servicios destinados a las distintas áreas del Gobierno de la Ciudad que operan con activos digitales. Estos servicios permiten:

- La posibilidad de integración con otros sistemas del GCABA.
- Consultar información en bases oficiales del Estado Nacional (como el Registro Nacional de las Personas) para verificar la identidad de los usuarios.
- Obtener los datos básicos de una persona registrada, a partir de su clave única interna.
- Realizar búsquedas de usuarios dentro del padrón unificado, utilizando sus datos personales.
- Permitir la creación asistida de perfiles de usuario, en aquellos casos en que organismos del Gobierno requieran registrar ciudadanos de forma delegada. En estos casos, la persona completará el proceso de activación a través de un correo electrónico.
- Verificar la identidad de manera presencial, otorgando un nivel superior de validación, utilizado principalmente para personal que trabaja en las comunas u otras dependencias del Gobierno.

OBJETIVO ESPECÍFICO 1. Seguridad de acceso: usuarios, contraseñas, sesiones.

OE1.1– Política de Administración de contraseñas.

El sistema Login miBA constituye la puerta de acceso única al ecosistema miBA, con la idea de permitir la autenticación unificada mediante usuario y contraseña o credenciales digitales verificables. Dicha autenticación se basa en los protocolos

OpenID Connect[20] y QuarkID[21], con el objetivo de garantizar interoperabilidad y trazabilidad.

Existen tres **métodos de autenticación** disponibles:

- **Usuario y Contraseña tradicional:** basado en protocolo OpenID Connect y las políticas de contraseña del BO, con almacenamiento cifrado mediante funciones de hash[22]. La cuenta puede ser creada en el portal Login miBA por el propio usuario o por un operador autorizado.
- **Credencial Ciudadana:** credenciales verificables basadas en protocolo QuarkID (tecnología blockchain[23]). Desde la app miBA, el usuario puede obtener su credencial ciudadana (nivel 3), utilizable para autenticarse.
- **Active Directory (para usuarios y administradores BackOffice):** con acceso mediante VPN y gestión centralizada por ASINF.

El **proceso de otorgamiento de claves para usuarios ciudadanos** incluye la validación de identidad (por DNI o CUIL contra RENAPER), la verificación del correo electrónico y la activación de la cuenta mediante un enlace seguro.

- **Registro web o app miBA:** el usuario ingresa su DNI y datos personales; luego recibe un enlace de verificación por correo, y al acceder a él la cuenta queda activada.
- **Registro por operador:** n sede comunal, un operador autorizado carga los datos del usuario (DNI y datos personales). En el primer ingreso, el usuario crea su contraseña, recibe el enlace de verificación y, al confirmarlo, activa su cuenta.

[20] OpenID Connect (OIDC) es un protocolo de autenticación construido sobre OAuth 2.0 que permite a aplicaciones (relying parties) verificar la identidad de un usuario mediante un ID Token (normalmente un JWT) emitido por un proveedor de identidad (Identity Provider), y obtener información básica del usuario a través del endpoint UserInfo; simplifica el inicio de sesión único (SSO), define flujos/alcances (authorization code, implicit, hybrid), y añade estándares para claims, verificación de firmas y gestión de sesiones, facilitando integraciones seguras y estandarizadas entre servicios web y proveedores de identidad.
En palabras sencillas se utiliza para que, en lugar de crear un usuario y contraseña nuevos cada vez, el sistema le pide permiso a un proveedor de identidad (como Google, miBA u otro) para confirmar quien es el usuario, y ese proveedor envía la información necesaria para autenticarlo. Así, el usuario puede acceder a distintos servicios sin repetir contraseñas y de manera más segura. https://auth0.com/docs/articles [Accedido 13/10/2025]

[21] QuarkID es un protocolo de identidad digital autosoberana (Self-Sovereign Identity, SSI) creado en Buenos Aires, que permite que las personas sean dueñas de sus datos personales, almacenándolos y compartiéndolos de forma segura a través de credenciales verificables, con respaldo de tecnología blockchain (zkSync Era) y criptografía moderna como pruebas de conocimiento cero (zero-knowledge proofs). https://quarkid.org/ [Accedido 13/10/2025]

[22] Un hash es una función criptográfica que convierte una entrada de datos en una cadena de longitud fija, única para cada contenido, y se utiliza comúnmente para verificar integridad o almacenar contraseñas de forma segura. https://www.pcmag.com/encyclopedia/term/hash [Accedido el 13/10/2025]

[23] Blockchain es una tecnología que permite registrar transacciones o datos en una base distribuida, inmutable y segura mediante criptografía y consenso entre múltiples nodos. Es la tecnología que sustenta bitcoin y las criptomonedas.
https://www.techopedia.com/definition/30246/blockchain [Accedido el 13/10/2025]

- **Para operadores y administradores de Back Office (BO):** el alta se gestiona mediante Active Directory (AD) [24] del GCABA provisto por la ASINF, con aprobación formal y control de acceso centralizado.

Características de la contraseña:

Login miBA implementa políticas específicas de contraseñas en su Backoffice (BO), utilizando funciones criptográficas de hash seguras bajo el algoritmo pbkdf2-sha256[25] con 30.000 iteraciones[26].

La longitud mínima exigida es de 8 caracteres, sin obligatoriedad de incluir diferentes tipos de caracteres (mayúsculas, minúsculas, números y símbolos), ni exigencia de cambio periódico.

Estas **características no cumplen con** lo establecido con lo establecido en **la "PO0807 - Política de Administración de Contraseñas"[27]** del Marco Normativo IT **de la ASINF** establecido por la Resolución N°177/ASInf/13 en su ANEXO I.

Durante la auditoría se realizaron pruebas simples en el formulario web de cambio de contraseña, observándose lo siguiente:

- El formulario indica erróneamente que la contraseña "debe tener 6 caracteres", aunque el sistema requiere al menos 8. Si se ingresa una contraseña más corta, no se muestra un mensaje específico, sino uno genérico ("Algo salió mal...") en una nueva pantalla y sugiere intentarlo con posterioridad o consultarlo con Boti, lo cual dificulta la comprensión del error.
- El formulario permite establecer contraseñas demasiado débiles, incluyendo claves comunes ("12345678", "Password1!"), direcciones de correo o CUIT del usuario (es decir el propio nombre de usuario), así como contraseñas reutilizadas.
- Se comprobó que el sistema Login miBA no permite y no tiene previsto la autenticación con doble factor.
- Durante los sucesivos cambios de contraseña realizados, se comprobó que el sistema no envía correos electrónicos notificando al usuario sobre la modificación de su contraseña.

[24] Active Directory es un servicio de directorio del sistema operativo Microsoft Windows que facilita trabajar con usuarios, grupos y recursos de red interconectados, complejos y diferentes de manera unificada. Está estructurado internamente con un marco jerárquico con forma de árbol. https://www.techopedia.com/definition/25/active-directory [Accedido el 01/02/2025]

[25] PBKDF2-SHA256 es un algoritmo de derivación de claves que aplica la función criptográfica SHA-256 de manera iterativa para generar claves seguras a partir de contraseñas. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf [Accedido el 13/10/2025]

[26] Las 30.000 iteraciones indican que el algoritmo aplica la función de hash SHA-256 treinta mil veces consecutivas sobre la contraseña, aumentando el tiempo y el esfuerzo necesarios para intentar descifrarla por fuerza bruta.

[27] https://boletinoficialpdf.buenosaires.gob.ar/util/imagen.php?idn=232269&idf=1 páginas 130 a 135 [Accedido el 13/10/2025]

En consecuencia, el sistema no cumple con las siguientes previsiones de la "PO0807 - Política de Administración de Contraseñas"[28] del Marco Normativo IT de la ASINF:

- No permitir identificadores de usuario (nombre, apellidos o ID).
- Obligar la combinación de caracteres especiales, números y letras mayúsculas y minúsculas.
- Solicitar el cambio obligatorio de la contraseña de forma periódica.
- Conservar un historial de contraseñas previas para evitar su reutilización.

No obstante, cabe destacar que algunas exigencias de la "PO0807 - Política de Administración de Contraseñas" se encuentran deprecadas (es decir, desaconsejadas o en desuso) según los estándares actuales de la industria[29]. El National Institute of Standards and Technology (NIST[30]) de los EEUU en su documento NIST SP800-63B[31] establece que:

- No es necesario exigir combinaciones específicas de caracteres.
- No es necesario forzar el cambio periódico de contraseñas.

Ello se debe a que dichas prácticas tienden a degradar la seguridad práctica, ya que los usuarios generan patrones predecibles (como sustituir letras por números o agregar un símbolo al final) o reutilizan variaciones mínimas de la misma clave. En su lugar, los estándares actuales recomiendan:

- **Validación contra diccionarios de contraseñas comunes**[32].
- **Verificar que no se encuentren comprometidas** (por ejemplo, mediante servicios como Have I Been Pwned[33]).

El sistema **Login miBA no implementa actualmente estas medidas.**

El siguiente cuadro resume las características del esquema de contraseñas de Login miBA frente a los requisitos de la política "PO0807 - Política de Administración de Contraseñas" de la ASINF y el estándar NIST SP800-63B:

---

[28] https://boletinoficialpdf.buenosaires.gob.ar/util/imagen.php?idn=232269&idf=1 páginas 130 a 135 [Accedido el 13/10/2025]

[29] Téngase en cuenta que la "PO0807 - Política de Administración de Contraseñas" de la ASINF fue establecida en el año 2013 -si bien modificada en años posteriores-, mientras que el estándar NIST SP800-63 es de este 2025.

[30] El NIST (*National Institute of Standards and Technology*) es el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, una agencia federal que forma parte del Departamento de Comercio de EE. UU. Su función principal es desarrollar estándares, guías técnicas y mediciones que garanticen la seguridad, interoperabilidad y calidad en sectores como la industria, la ciencia, la tecnología y —muy especialmente— la ciberseguridad. El NIST es especialmente reconocido por la serie de guías SP (Special Publicatios), la que en particular atañe a este punto es la NIST SP 800-63 (Digital Identity Guidelines).

[31] NIST SP800-63B Digital "Identity Guidelines" es el volumen específico de la SP 800-63 (Digital Identity Guidelines) donde, entre otras consideraciones técnicas, se establece cómo se deben crear, validar y manejar contraseñas.
https://pages.nist.gov/800-63-4/sp800-63b.html#passwordver [Accedido el 13/10/2025]

[32]

[33]

Característica Contraseña	Login miBA cumple	"PO0807 - Política de Administración de Contraseñas" Marco Normativo IT ASINF requiere	Estandar NIST SP800-63B requiere
Longitud mínima de ocho (8) caracteres			
No permitir identificadores de usuario (nombre, apellidos o ID).			
Obligar la combinación de caracteres especiales, números y letras mayúsculas y minúsculas.			
Bloquear el usuario frente a repetidos intentos de acceso.			
Obligar su cambio cuando el usuario ingrese por primera vez al sistema o servicio			
Solicitar el cambio obligatorio de la contraseña de forma periódica.			
Conservar un historial de contraseñas previas para evitar su reutilización.			
Validación contra diccionarios de contraseñas comunes			
Validación contra contraseñas previamente comprometidas (HaveIBeenPwned)			

Ilustración 3 Comparación de características de la contraseña de Login miBA y los requisitos según la PO0807 – "Política de Administración de Contraseñas" de la ASINF y según el estándar NIST SP800-63B.

De esta revisión se arriba a la Observación N° 1.

OE1.2- Usuarios, Roles y Permisos en los sistemas.

Los usuarios del ecosistema miBA se clasifican en tres categorías principales:

- **Usuarios Ciudadanos:**
  Acceden a: miBA a través de Login miBA.
  Métodos de Autenticación: Usuario/contraseña o credenciales verificables.
  Permisos:
  • Acceso a la aplicación miBA y sus documentos digitales.
  • Uso de credenciales verificables.
  • Verificar el estado de sus gestiones (tramites, solicitudes y turnos) de GCABA.
  Roles: Dependiendo de su nivel de seguridad:
  • Nivel 1: Validado con RENAPER y verificación de mail. Puede ver credenciales y documentos externos.
  • Nivel 3: Nivel 1 y Validación Biométrica o Presencial. Puede obtener todos los documentos de la ciudad asociados al usuario.

- **Operadores de BO:**
  Acceden a: Consolas de soporte de miBA y BackOffice.
  Métodos de Autenticación: Mediante Active Directory (AD) y permisos específicos según área de trabajo y rol asignado.
  Permisos:
  • Gestionar datos de los usuarios que solicitan soporte.
  • Monitorear comportamiento por medio de registro de actividad de los usuarios.
  • Gestionar credenciales y documentos de los usuarios que solicitan soporte.
  Roles: Dependiendo de sus tareas con respecto a soporte de usuarios:
  • Soporte Nivel 1: Puede ayudar a los usuarios gestionando sus datos y accesos.
  • Soporte Nivel 2: Puede ayudar a los usuarios gestionando sus datos y accesos e investigando su comportamiento por medio de registro de actividad.

- **Administradores de BO:**
  Acceden a: Consolas de administración de miBA y BackOffice. Configuración y monitoreo de los sistemas.
  Métodos de Autenticación: Mediante Active Directory y permisos específicos según área de trabajo y rol asignado.
  Permisos:
  • Gestionar las configuraciones avanzadas de flujos de miBA y Login miBA.
  • Auditar accesos y establecer parámetros de seguridad.
  • Gestionan la infraestructura, monitorean el funcionamiento y realizan ajustes técnicos.
  • Acceso controlado a entornos de desarrollo, prueba y producción.
  Roles: Dependiendo de sus tareas con respecto a administración del producto:
  • Administrador Nivel 1: Puede gestionar y monitorear operadores y sus accesos.

• Administrador Nivel 2: Pueden gestionar y monitorear operadores, administradores y configuraciones de la plataforma.

Procedimiento de Alta, Baja y Modificación de Usuarios.

- **Alta de Usuarios.**

Ciudadanos: Se registran a través de Login miBA o por medio de creación delegada por un Operador de BO. La cuenta se activa tras la validación por mail y configuración de autenticación.

Operadores y Administradores de BO: Se gestionan mediante Active Directory (AD), por solicitud al equipo de Seguridad Informática de la ASINF. La solicitud de alta es realizada por el área responsable y aprobada por la DG de Ciudadanía Digital (DGCIUD).

- **Baja de Usuarios.**

Ciudadanos: Pueden solicitar la baja de su cuenta a través de los canales oficiales de soporte. O pueden realizarlo desde su perfil de autogestión.

Operadores y Administradores de BO: La baja se solicita formalmente desde la DG de Ciudadanía Digital (DGCIUD) y es procesada por el equipo de seguridad informática de la ASINF.

- **Modificación de Permisos.**

Cualquier cambio en permisos requiere aprobación formal del área responsable de la plataforma. Todas las modificaciones quedan registradas en un sistema de auditoría para garantizar la trazabilidad.

- **Formalidad del Procedimiento.**

Todos los cambios y accesos son registrados y auditados regularmente. Este esquema permite garantizar la seguridad y trazabilidad de los accesos a miBA y Login miBA, asegurando que cada usuario acceda únicamente a la información que le corresponde.

Se relevó que el esquema de roles y permisos está adecuadamente definido y documentado, con control de acceso basado en roles (RBAC)[34] y niveles de privilegio bien diferenciados.

Asimismo, Login miBA tiene diferentes "realms"[35] (o Reinos), que permiten tener diferentes ámbitos de seguridad, y de esta manera tener diferentes permisos y

[34] El control de acceso basado en roles (RBAC, por sus siglas en inglés — Role-Based Access Control) es un modelo de seguridad que asigna los permisos a los usuarios según los roles que desempeñan dentro de una organización, en lugar de hacerlo directamente a cada individuo.
Cada rol agrupa un conjunto de permisos necesarios para cumplir ciertas funciones, y los usuarios heredan esos permisos al asumir dicho rol. NIST Special Publication 800-162.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf página 2 [Accedido el 13/10/205].

[35] Un Realm o Reino es una política de seguridad que refiere a entornos o dominios de autenticación independientes dentro del sistema, cada uno con su propio conjunto de usuarios, credenciales, permisos y configuraciones de seguridad.
https://docs.oracle.com/cd/E19798-01/821-1841/6nmq2cpjd/index.html Accedido el 13/10/205].

grupos de usuarios. La plataforma tiene un realm para usuarios y clientes WEB y otro para usuarios y clientes mobile.

No obstante, no se hallaron los procedimientos y prácticas de revisión periódica de usuarios activos y roles asignados a fin de garantizar la vigencia y pertinencia de los permisos otorgados.

OE1.3- Sesiones, autenticaciones y medios de acceso a los sistemas.

Login miBA está desarrollado sobre la plataforma Keycloak[36], herramienta de gestión de identidades (IAM)[37] que administra sesiones y autenticaciones mediante estándares OAuth 2.0, OpenID Connect (OIDC) y SAML 2.0[38].

El sistema genera tokens JWT[39] para controlar las sesiones y autorizar el acceso a los recursos protegidos.

En términos sencillos: Login miBA implementa mecanismos estandarizados de autenticación y gestión de sesiones que permiten identificar de manera segura a los usuarios y mantener activa su sesión durante el uso de los servicios. Para ello, el sistema emite credenciales digitales temporales denominadas tokens JWT (JSON Web Tokens), que contienen información codificada sobre la identidad del usuario y los permisos otorgados, y actúan como comprobantes de autenticación para acceder a los recursos protegidos sin requerir el reingreso constante de las credenciales. Estos procesos se apoyan en protocolos internacionales reconocidos (OAuth 2.0, OpenID Connect y SAML 2.0), que garantizan la interoperabilidad, la trazabilidad y la protección de la información intercambiada entre sistemas.

Asimismo, Login miBA implementa políticas para garantizar la seguridad de las sesiones:

Gestión de sesiones:

- Ciudadanos y operadores: sesiones que expiran automáticamente tras 15 minutos de inactividad.

[36] Keycloak es una plataforma de gestión de identidades y accesos (IAM) que permite autenticar usuarios, gestionar sus permisos y controlar sesiones de manera segura mediante estándares como OAuth 2.0, OpenID Connect y SAML 2.0. Es de código abierto, pero el soporte empresarial lo brinda Red Hat. https://www.keycloak.org/ [Accedido 13/10/2025]

[37] La gestión de identidades y accesos (IAM) es el proceso que se utiliza en empresas y organizaciones para otorgar o denegar a empleados y otras personas la autorización para proteger los sistemas. https://www.techopedia.com/definition/23922/identity-and-access-management-iam [Accedido 13/10/2025]

[38] SAML 2.0 (Security Assertion Markup Language) es un estándar abierto desarrollado y mantenido por OASIS (Organization for the Advancement of Structured Information Standards), creado para proporcionar el inicio de sesión único (SSO) entre dominios. En otras palabras, permite que un usuario se autentique en un sistema y acceda a otro proporcionando una prueba de su autenticación. https://auth0.com/es/intro-to-iam/what-is-saml y https://wiki.oasis-open.org/security/FrontPage [Accedido 13/10/2025]

[39] JSON Web Token (JWT) es un estándar abierto (RFC 7519) que define una forma compacta y autónoma de transmitir información de forma segura entre partes como un objeto JSON. Esta información se puede verificar y es confiable gracias a su firma digital. Los JWT se pueden firmar mediante un secreto (con el algoritmo HMAC) o un par de claves pública/privada mediante RSA o ECDSA. https://www.jwt.io/introduction#what-is-json-web-token [Accedido 13/10/2025]

- Áreas/Clientes integrados: sesiones que expiran automáticamente tras 1 minuto.
- Expiración automática y revocación inmediata ante detección de anomalías.

Seguridad complementaria:

- Autenticación multifactor (credencial verificable QuarkID).
- Protección frente a ataques de fuerza bruta[40].
- Cifrado de datos en tránsito y almacenamiento.
- Auditoría y registro de todas las actividades de autenticación.

La gestión de sesiones y autenticación cumple con estándares internacionales y mecanismos robustos de control. Se evidencia el uso de herramientas modernas de IAM, autenticación unificada y medidas de protección acordes a los requerimientos de seguridad del GCABA.

Sin embargo, se identifican las siguientes **evaluaciones de seguridad faltantes o no documentadas**:

- documentación de evaluaciones según **OWASP Top 10[41]**.
- ejecución de **vulnerability scanning automatizado[42]**.
- No se registran ejercicios de **Red Team / Blue Team**[43].
- la **estrategia de refresh tokens[44].**
- el **mecanismo de revocación de tokens[45]** en detalle.
- la validación de **audience** e **issuer[46]** en tokens.

[40] Un ataque de fuerza bruta es un método de ciberataque que consiste en probar sistemáticamente todas las combinaciones posibles de letras, números y símbolos para descifrar contraseñas, credenciales de inicio de sesión o claves de cifrado. Es una técnica de prueba y error que utiliza software automatizado para intentar obtener acceso no autorizado a una cuenta o sistema. https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack [Accedido el 14/10/2025].

[41] El Top 10 de OWASP es un documento estándar de concientización para desarrolladores y seguridad de aplicaciones web. Representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones web. https://owasp.org/www-project-top-ten/ [Accedido el 14/10/2025].

[42] El análisis de vulnerabilidades, también llamado "evaluación de vulnerabilidades", es el proceso de evaluar redes o activos de TI para detectar vulnerabilidades, fallos o debilidades de seguridad que actores de amenazas externos o internos puedan explotar. https://www.ibm.com/think/topics/vulnerability-scanning [Accedido el 14/10/2025].

[43] Un ejercicio de equipo rojo vs. equipo azul es una simulación de ciberseguridad donde un equipo rojo (atacantes) intenta penetrar las defensas de una organización, mientras que el equipo azul (defensores) trabaja para detectar y repeler el ataque. Este ejercicio ayuda a identificar https://csrc.nist.gov/glossary/term/red_team_blue_team_approach [Accedido el 14/10/2025].

[44] Una estrategia de token de actualización es un sistema para gestionar el acceso a largo plazo a las aplicaciones mediante un token de actualización de larga duración para obtener nuevos tokens de acceso de corta duración cuando el token de acceso original caduca. https://auth0.com/docs/secure/tokens/refresh-tokens/refresh-token-rotation [Accedido el 14/10/2025].

[45] Un mecanismo de revocación de tokens es un proceso de seguridad que invalida un token de autenticación o autorización, dejándolo inutilizable antes de su fecha de vencimiento natural. Esto se utiliza para revocar el acceso inmediatamente después de que un usuario cierre sesión, cambien sus credenciales o se vulnere un token. La revocación es crucial para la seguridad. https://datatracker.ietf.org/doc/html/rfc7009 [Accedido el 13/10/2025]

[46] La validación del emisor y la audiencia del token son comprobaciones de seguridad que realiza un servidor para garantizar que un token sea legítimo, provenga de la fuente correcta y esté destinado a su uso. La validación del emisor confirma que el token fue emitido por un proveedor de autenticación confiable, mientras que la validación de la audiencia verifica que el token estaba destinado a ese servidor o API específico.

- la política de **rotación de claves de cifrado**[47].
  De aquí surge la Observación N° 2.

Además, se relevó que la versión de Java utilizada se encuentra discontinuada; si bien cuenta con soporte extendido comercial por algunos años más, carece de actualizaciones de seguridad públicas gratuitas y presenta algunas vulnerabilidades y exposiciones conocidas (CVE)[48].

De manera similar, la versión Keycloak es bastante anterior, se encuentra sin soporte activo de la comunidad y presenta vulnerabilidades conocidas, lo que puede implicar riesgos adicionales para la seguridad del sistema.

Esto motiva la Observación N° 3.

OE1.4 - Medios de acceso al sistema.

Los **medios de acceso** se diferencian por tipo de usuario:

- **Ciudadanos**: Acceso web (https://buenosaires.gob.ar/miba) o app móvil (Android/iOS). Autenticación centralizada mediante Login miBA.

- **Operadores y Administradores de BO:** Acceso web mediante URL seguras al entorno de producción o ambientes bajos (https://login.buenosaires.gob.ar/auth/admin/…). Ingreso restringido a redes internas del GCABA (GCABA MAN[49]) o mediante VPN[50] provista por ASINF.
  En todos los casos se emplea cifrado SSL/TLS[51], monitoreo en tiempo real de accesos e intentos fallidos, y expiración automática de sesiones inactivas.

---

https://auth0.com/docs/secure/tokens/access-tokens/validate-access-tokens [Accedido el 14/10/2025].

[47] Una política de rotación de claves de cifrado es una práctica de seguridad que consiste en reemplazar periódicamente las claves criptográficas por otras nuevas para mejorar la seguridad y reducir el riesgo de vulneración de claves. Esto se realiza de forma automática según un calendario establecido o manualmente tras un evento específico, como un presunto incidente de seguridad. Una política robusta es fundamental para una estrategia de seguridad sólida. https://cloud.google.com/kms/docs/key-rotation?hl=es-419 [Accedido el 14/10/2025].

[48] Las CVE (Common Vulnerabilities and Exposures) son identificadores únicos asignados a vulnerabilidades de seguridad conocidas en software o hardware. Cada CVE corresponde a un fallo de seguridad documentado que permite a usuarios, administradores y herramientas de seguridad referirse de manera consistente a la misma vulnerabilidad. https://www.cve.org/ [Accedido el 13/10/2025]

[49] Una red MAN (Metropolitan Area Network) es una red de área metropolitana, similar a una red de área local (LAN), pero abarca toda una ciudad o campus, o algún otro territorio municipal u rganizativo. Las MAN se forman conectando varias LAN.
https://www.techopedia.com/definition/8238/metropolitan-area-network-man [Accedido el 03/02/2025]

[50] Una red privada virtual (VPN) es una conexión de red privada que se construye sobre una infraestructura de red pública como Internet, utilizando mecanismos de encriptación y autenticación. https://www.techopedia.com/definition/4806/virtual-private-network-vpn [accedido el 01/02/2025]

[51] Transport Layer Security (TLS) es un protocolo criptográfico que ayuda a proteger las comunicaciones a través de redes informáticas no protegidas, como Internet. https://www.ibm.com/think/topics/transport-layer-security [Accedido el 13/10/2025]

OBJETIVO ESPECÍFICO 2. Complementación de procesos productivos e Integración de los sistemas.

El sistema Login miBA presenta, por su naturaleza, un alto nivel de integración con distintas plataformas del Gobierno de la Ciudad de Buenos Aires (GCABA) y con organismos nacionales, con el propósito de centralizar, normalizar y asegurar el acceso a los servicios digitales ofrecidos al ciudadano.
Esta integración favorece la interoperabilidad entre los sistemas de gestión, autenticación, documentación y atención ciudadana, con el objetivo de lograr una experiencia de usuario unificada y una gestión más eficiente de la información pública.

Principales integraciones identificadas:

Sistema / Plataforma	Grado de Integración	Características Principales
AGIP (Agencia Gubernamental de Ingresos Públicos)	**Alta**	Integración de Login miBA como medio de identificación y acceso a los servicios de la AGIP.
RENAPER (Registro Nacional de las Personas)	**Alta**	Validación en línea de identidad y datos biométricos. Permite verificar la autenticidad del DNI y la identidad del usuario en tiempo real durante el registro o autenticación. Se encuentra integrado a nivel de servicios mediante el ESB (Enterprise Service Boost), desarrollado por la ASINF.
TAD (Trámites a Distancia)	**Alta**	Autenticación federada mediante Login miBA, lo que posibilita el acceso unificado con las mismas credenciales a los servicios de TAD.
X-BA (Plataforma de interoperabilidad del GCABA)	**Alta**	Utilizada para el intercambio seguro, confiable y auditado de datos. Implementa autenticación y autorización de sistemas, cifrado TLS, logs inmutables, no almacenamiento intermedio y firma digital de mensajes.

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

GCI miBA (Gestión Ciudadana Integral)	**Media**	Sincroniza y consulta información del perfil del ciudadano, permitiendo mantener actualizados los datos personales y servicios asociados dentro del ecosistema miBA.
SADE (Sistema de Administración de Documentos Electrónicos)	**Media**	Vincula la autenticación de miBA con la gestión de documentos y la firma digital, asegurando trazabilidad y validez documental dentro de los procesos administrativos.
BOTI (Asistente virtual del GCABA)	**Media**	Permite que los usuarios autenticados por miBA accedan a gestiones personalizadas y consultas seguras dentro del canal conversacional.

En términos técnicos, miBA y Login miBA operan sobre un ecosistema de APIs y webservices que permiten la interoperabilidad y el intercambio seguro de información entre múltiples sistemas.

La arquitectura técnica se encuentra alineada con los lineamientos de la Agencia de Sistemas de Información (ASINF), promoviendo la normalización, el cifrado de datos sensibles y la adopción de buenas prácticas en interoperabilidad.

Login miBA: API[52]s y Webservices[53] Provistos.

- **Consumo de APIs de Identidad Digital:** Consume servicios de Active Directory para la autenticación de usuarios administrativos en entornos internos del GCABA, permitiendo el acceso al backoffice de Login miBA.
- **Consumo de APIs de Guía e Información:** Integra APIs de BOTI (Chatbot del GCABA) para consultas automatizadas, orientación a ciudadanos y asistencia en flujos de soporte.
- **APIs de Autenticación y Autorización:** Implementa los protocolos OAuth 2.0 y OpenID Connect (OIDC), brindando APIs estandarizadas que permiten a otras aplicaciones del GCABA autenticar y autorizar usuarios de manera segura. Incluye servicios para la gestión de tokens de acceso (JWT), sesiones activas y permisos de usuario.

[52] Una interfaz de programación de aplicaciones (API) es un conjunto de protocolos, rutinas, funciones y/o comandos que los programadores utilizan para facilitar la interacción entre distintos servicios de software.
https://www.techopedia.com/definition/24407/application-programming-interface-api [Accedido el 13/10/2025]

[53] Un Web service (servicio web) es una aplicación de software con una forma estandarizada de proporcionar interoperabilidad entre aplicaciones dispares. Lo hace a través de HTTP utilizando tecnologías como XML, SOAP, WSDL y UDDI.
https://www.techopedia.com/definition/25301/web-service [Accedido el 13/10/2025]

- **APIs de Gestión de Usuarios:** Provee servicios para el registro y administración de usuarios (funcionalidad “Crear Cuenta” en el front). Ofrece APIs para la obtención y actualización de datos y la gestión de información de usuarios en el backoffice de Login miBA.
- **APIs de Validación de Identidad:** Integra servicios del RENAPER para la validación de identidad de ciudadanos argentinos, validaciones presenciales mediante el servicio onsite-BAID[54], validaciones de identidad digital autosoberana[55] con el protocolo QuarkID y validaciones biométricas.
- **APIs de Gestión de Identidad Descentralizada (Quark ID):** Permite la gestión de DID (Identificadores Descentralizados)[56] para identidad digital autosoberana, con integración a estándares internacionales como DIDComm[57] y W3C Verifiable Credentials[58].
- **APIs de Control de Acceso:** Integra Keycloak y Active Directory para la administración de roles, perfiles y permisos de acceso, bajo modelos RBAC (control basado en roles) y ABAC (control basado en atributos).

En cuanto a la Interoperabilidad y transmisión segura de información entre Login miBA y los sistemas integrados del GCABA se realiza mediante X-BA[59], la plataforma de interoperabilidad basada en X-Road[60], que garantiza un intercambio cifrado, autenticado y trazable.

---

[54] El servicio onsite-BAID se refiere a ls validación presencial, se utilizan lectores de DNI, cámaras o dispositivos biométricos conectados al sistema BAID (Buenos Aires ID) para verificar la identidad de la persona.

[55] La identidad digital autosoberana (Self-Sovereign Identity, SSI) es un modelo descentralizado de identidad digital donde el usuario es dueño y controlador de sus datos personales, sin depender totalmente de un proveedor central (como el Estado). En este caso, se menciona el protocolo QuarkID, que es una implementación concreta de SSI utilizada en Argentina. https://www.w3.org/TR/did-1.0/ [Accedido el 13/10/2025].

[56] Los Identificadores Descentralizados (DID) son identificadores únicos globales que el usuario controla, a diferencia de los tradicionales que dependen de una autoridad central como una empresa o gobierno. Permiten una identidad digital verificable y descentralizada, otorgando al usuario el control sobre su propia identidad sin necesidad del permiso de terceros. https://www.w3.org/TR/did-1.1/ y https://buenosaires.gob.ar/innovacionytransformaciondigital/protocolo-quarkid/documentacion/identificadores-descentralizados-dids [Accedidos el 13/10/2025]

[57] DIDComm es un protocolo de código abierto para la comunicación segura, directa y privada entre partes que utilizan identificadores descentralizados (DID). Permite interacciones confidenciales entre pares para diversos casos de uso, como el intercambio de credenciales verificables, el chat seguro y las transacciones en línea, sin depender de servidores centralizados. https://didcomm.org/ [Accedido el 13/10/2025]

[58] Las Credenciales Verificables del W3C son credenciales digitales, criptográficamente seguras, que permiten a un usuario (el "titular") demostrar sus propias afirmaciones a un tercero (el "verificador") de forma fiable. Están estandarizadas por el Consorcio World Wide Web (W3C). https://www.w3.org/TR/vc-overview/ [Accedido el 13/10/2025]

[59] X-BA es un sistema de interoperabilidad para el intercambio de información por parte de las diferentes reparticiones del GCABA. Es gestionado por la Secretaría de Innovación y Transformación Digital (SECITD). https://buenosaires.gob.ar/innovacionytransformaciondigital/sistema-de-interoperabilidad/x-ba [Accedido el 13/10/2025]

[60] X-Road es una solución de interoperabilidad de código abierto que permite el intercambio seguro de datos entre distintos sistemas de información, garantizando confidencialidad, integridad y trazabilidad. Fue desarrollado inicialmente en Estonia, y actualmente su núcleo es mantenido por el Nordic Institute for Interoperability Solutions (NIIS). https://x-road.global/ [Accedido el 13/10/2025]

Los mecanismos implementados incluyen:

- Autenticación y autorización de sistemas participantes.
- Cifrado extremo a extremo (TLS).
- Firma digital e integridad de mensajes.
- Registros inmutables de auditoría.
- No almacenamiento intermedio de datos.

El uso de X-BA asegura los niveles de seguridad en la transmisión y consumo de datos entre sistemas, con el objetivo de cumplir con los lineamientos de interoperabilidad definidos por ASINF

Como se ha visto, el sistema Login miBA mantiene múltiples integraciones activas tanto con sistemas internos del GCABA (como TAD, X-BA, SADE, GCI miBA y BOTI) como con organismos externos, en particular con RENAPER a través del servicio de validación de identidad. Estas integraciones facilitan la interoperabilidad funcional entre los distintos sistemas y permiten una autenticación unificada de los usuarios.

Sin embargo, se constató la ausencia de un marco formal de gobierno de integraciones que establezca políticas, roles y responsabilidades para la administración y control de las conexiones activas. Tampoco se identificaron procedimientos estandarizados de monitoreo, auditoría o registro centralizado de los consumos de API.

No se hallaron acuerdos de nivel de servicio (SLA)[61] formalizados con los organismos externos involucrados, en especial con RENAPER, o reparticiones del GCABA, así tampoco acuerdos operativos internos (OLA)[62] entre las áreas internas responsables del mantenimiento y soporte de las integraciones. Por lo tanto, no existen compromisos documentados respecto de tiempos de respuesta, disponibilidad mínima del servicio o protocolos de escalamiento en caso de fallas o caídas.

Lo expuesto justifica la Observación N° 4.

Integración con Agencia Gubernamental de Ingresos Públicos (AGIP):

Durante el transcurso de esta auditoría se dictó la Resolución 442/AGIP/25, publicada el 9 de octubre de 2025 que estableció que la Clave “miBA” Nivel 3 será de carácter obligatorio para la utilización de los servicios virtuales de AGIP.

[61] SLA (o Service Level Agreement) es un contrato o convenio entre un proveedor de servicios y un cliente que define el servicio que se prestará y el nivel de rendimiento esperado. Un ANS también describe cómo se medirá y aprobará el rendimiento, y qué sucede si no se cumplen los niveles de rendimiento.
https://www.ibm.com/think/topics/service-level-agreement [Accedido el 13/10/2025]

[62] OLA (u Operational Level Agreement) es a diferencia del SLA, un documento que define cómo los distintos grupos de TI de una organización planean prestar un servicio o un conjunto de servicios, las responsabilidades internas, tiempos de atención, flujos de soporte y protocolos de escalamiento. https://www.techtarget.com/whatis/definition/operational-level-agreement-OLA [Accedido el 13/10/2025]

La medida entró en vigencia el 27 de octubre de 2025[63], fecha en la que se concretó la integración de los servicios de identidad y autenticación con la AGIP. No obstante, tampoco se identificó un SLA con dicho organismo, situación que se adiciona a la Observación N° 4.

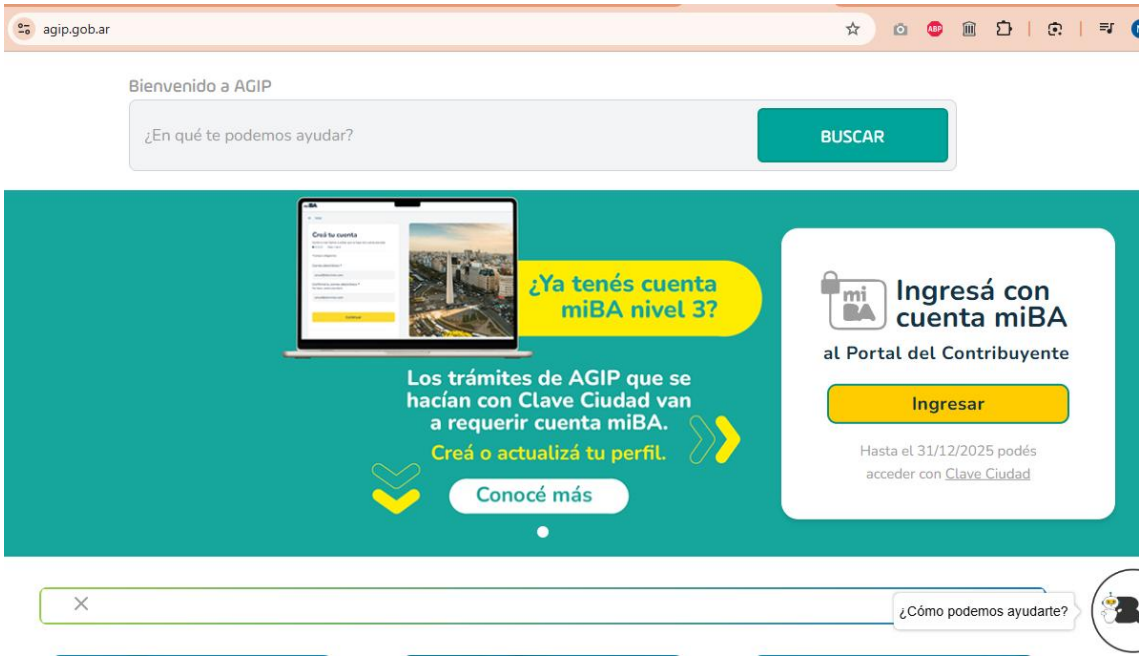


Ilustración 4 Ingreso a AGIP con cuanta miBA

OBJETIVO ESPECIFICO 3. Cumplimiento de metas y objetivos - Satisfacción del usuario.

Los sistemas miBA y Login miBA cuentan con diversas funcionalidades y mecanismos que podrían utlizarse para medir el cumplimiento de metas, objetivos y la satisfacción del usuario:

- **Calificaciones y Opiniones en Tiendas de Aplicaciones (Google Play y App Store):**
  Se encuentran vinculadas con la aplicación miBA. Se realiza una revisión trimestral de las calificaciones y opiniones dejadas por los usuarios en las tiendas de aplicaciones. Es trabajo del Equipo de Experiencia de la Dirección General el armado de reportes y el análisis de estas.
  Valores de Referencia y Resultados: Según la DGCIUD, los valores de referencia serían las calificaciones promedio históricas y la distribución de las opiniones (positivas, negativas, neutras).

[63] Hasta el 31 de diciembre de 2025 podrá usarse indistintamente la Clave Ciudad y la clave miBA, pero a partir del 1° de enero de 2026 será obligatorio Login miBA para AGIP.

- **Opciones "Ayudanos a Mejorar" y "Valora la app" dentro de la App miBA:**
  También vinculadas a miBA, los usuarios tienen a su disposición estas opciones en el menú de la aplicación para enviar mensajes y comentarios directamente al equipo de desarrollo, soporte y diseño.
  Valores de Referencia y Resultados: La DGCIUD sostiene que el volumen de mensajes recibidos, la categorización de los temas reportados y el análisis del sentimiento expresado en los mensajes podrían utilizarse como indicadores.

- **Métodos de Soporte y Ayuda a Usuarios:**
  Se ofrece soporte a través de múltiples canales:
  • Chat con BOTI: Proporciona respuestas automatizadas a preguntas frecuentes y asistencia inicial. También se brinda asistencia a partir de una cola de atención en tiempo real por medio del chatbot.
  • Tiquetera de mail: Permite a los usuarios reportar problemas y recibir asistencia por correo electrónico.
  • Tiquetera de BA Colaborativa: Sistema formal de gestión de incidencias y solicitudes de soporte. Se puede brindar asistencia por medio de chat con los usuarios.
  • Tiquetera de NOC: Recibe reportes de inconsistencias o errores provenientes de otras áreas del GCABA, y proporciona información sobre la estabilidad y el funcionamiento de las aplicaciones desde una perspectiva interna.
  Valores de Referencia y Resultados: De acuerdo con la DGCIUD, las métricas clave incluirían el volumen de tickets por canal, el tiempo de respuesta promedio, el tiempo de resolución promedio y la tasa de resolución en el primer contacto.
  No obstante, no se recolecta información sobre la satisfacción del usuario respecto del soporte recibido ni sobre la resolución efectiva de los casos, como se detallará en el OE5 - Soporte Técnico.

- **Métricas de Actividad y Comportamiento de las Comunas:**
  Se monitorea el comportamiento de los usuarios por medio del equipo de soporte de las comunas, que tienen acceso al back office de Login miBA, observando la cantidad de asistencias brindadas y las acciones realizadas (blanqueos, eliminaciones, resolución de inconsistencias).
  Valores de Referencia y Resultados: La DGCIUD sostiene que el volumen de asistencias y el tipo de acciones realizadas por comuna podrían compararse a lo largo del tiempo para identificar tendencias y áreas de mejora.

- **Asistencia del Equipo de Integraciones:**
  Se brinda asistencia directa a clientes (que pueden ser otras áreas del GCABA u organismos externos) y a áreas internas a través del contacto con el Equipo de Integraciones. Esta asistencia se enfoca en apoyar los procesos de integración con miBA y Login miBA, así como en identificar y mejorar aspectos específicos para satisfacer las necesidades particulares de estos clientes y áreas.
  Valores de Referencia y Resultados: Según el auditado, el número de contactos y casos gestionados por el Equipo de Integraciones, el tipo de

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

consultas o problemas resueltos y el feedback recibido de los clientes y áreas asistidas serían indicadores relevantes de la efectividad de este canal y del nivel de satisfacción de los integradores. El seguimiento de las mejoras implementadas a raíz de estas interacciones también sería importante.

Sin embargo, el auditado manifiesta que los valores de referencia y resultados mencionados constituyen propuestas y no métricas actualmente implementadas. Una salvedad debe hacerse para el caso de la valoración trimestral de la aplicación miBA en Google Play y App Store. Se constata que no existe un plan estratégico específico, integral y multiplataforma para medir de manera formal y continua el cumplimiento de metas, objetivos y la satisfacción del usuario.

Asimismo, se evidencia la ausencia de otras políticas y prácticas complementarias orientadas a este objetivo, tales como la aplicación de métricas estandarizadas como NPS (Net Promoter Score)[64], CSAT (Customer Satisfaction Score) post-interacción[65], CES (Customer Effort Score)[66], encuestas de satisfacción periódicas, análisis de abandono en flujos críticos (funnel analysis) o la recopilación estructurada de feedback cualitativo de los ciudadanos.

Por lo tanto, se formula la Observación N° 5.

OBJETIVO ESPECÍFICO 4. Indicadores clave de desempeño (KPI)[67].

Los sistemas Login miBA y miBA App cuentan con herramientas de monitoreo y visualización de datos que permiten analizar el comportamiento de los usuarios y el rendimiento de los servicios. Entre estas herramientas se incluyen dashboards interactivos en Power BI y Looker Studio, tableros de control de Login miBA y miBA App, sistemas de gestión de tickets como Redmine, y soluciones de monitorización técnica como Dynatrace, PRTG y Kibana.

Estas herramientas permiten visualizar en tiempo real o de forma periódica métricas de rendimiento, disponibilidad, uso de APIs, consumo de recursos, tasas de error, registros de acceso y comportamiento de usuarios, mediante gráficos, tablas y dashboards personalizables.

---

[64] NPS (Net Promoter Score) es una métrica de experiencia del cliente/usuario que mide la disposición de los usuarios a recomendar un producto o servicio. https://www.ibm.com/think/topics/net-promoter-score [Accedido el 13/10/2025]

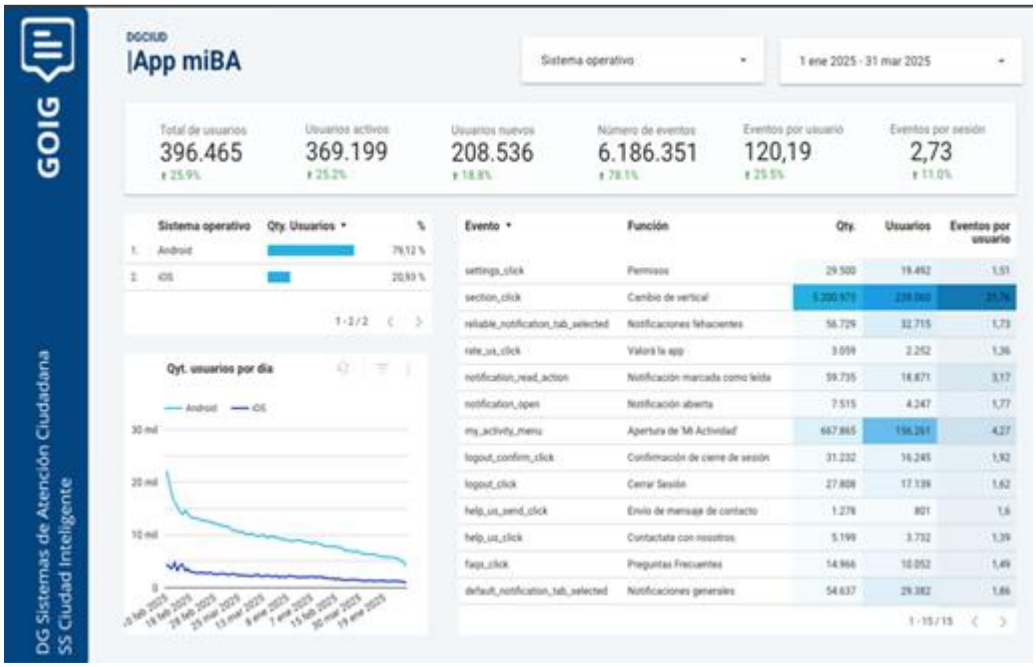
[65] CSAT (Customer Satisfaction Score) post-interacción es una métrica que evalúa la satisfacción del usuario inmediatamente después de una interacción específica. https://www.ibm.com/think/topics/csat-customer-satisfaction-score [Accedido el 13/10/2025]

[66] CES (Customer Effort Score) es una métrica que cuantifica el esfuerzo que percibe el usuario para interactuar con un sistema, una empresa o utilizar sus productos o servicios. https://www.ibm.com/think/topics/customer-effort-score [Accedido el 13/10/2025]

[67] Los indicadores clave de rendimiento (KPI) son medidas que se utilizan para identificar y cuantificar el rendimiento empresarial, de los sistemas y procesos, por miedo de objetivos claros mensurables, cuantitativa y cualitativamente. https://www.techopedia.com/definition/24759/key-performance-indicators-kpi [Accedido el 17/09/2025]

Tableros de control de Login miBA:

Tableros de control de miBA App:



Sí puede señalarse que sería conveniente agregar algunos indicadores adicionales (por ejemplo: MAU, DAU, tasa de adopción, tasa de conversión, retención de usuarios, abandono en flujos críticos y tiempo hasta la primera autenticación). Tampoco se cuenta con un Balanced Scorecard (BSC) ni con OKRs (Objectives and Key Results) que vinculen los KPIs técnicos con las metas de negocio.

OBJETIVO ESPECÍFICO 5. Soporte Técnico.

OE5.1- Soporte Técnico.

El sistema Login miBA ofrece soporte técnico a usuarios y clientes mediante una estructura de mesa de ayuda cuyos canales, niveles y áreas de soporte se comparten con la app miBA. Los mecanismos principales incluyen:

- **Tiquetera de NOC:** Otras áreas del GCABA pueden derivar consultas relacionadas con el funcionamiento de las aplicaciones miBA y Login miBA a través de la tiquetera gestionada por ASINF, denominada NOC. Este canal actúa como punto de contacto inicial, registrando las incidencias reportadas y derivándolas al equipo técnico responsable. La tiquetera permite realizar el seguimiento de cada caso desde su reporte hasta su resolución, asegurando trazabilidad y registro histórico de las incidencias.

- **Contacto con el Equipo de Integraciones:** Para requerimientos más especializados, el equipo de Integraciones brinda asistencia directa a clientes internos y externos, enfocándose en la resolución de problemas vinculados a la integración con otros sistemas, así como en la optimización de procesos. Los contactos y tareas se registran y gestionan mediante herramientas de gestión de proyectos (Redmine[68]) y registros internos, permitiendo seguimiento, control y mejora continua de las integraciones.

Niveles de soporte**:**

- **Primer Nivel:** Equipo de atención ciudadana o mesa de ayuda de la DGCIUD, encargado de la recepción, clasificación y resolución de consultas sencillas.
- **Segundo Nivel Especializado:** Equipo Técnico de miBA/Login miBA: responsable de problemas técnicos relacionados con la funcionalidad, seguridad o rendimiento de las aplicaciones y APIs.
- **Equipo de Integraciones:** Encargado de incidencias relacionadas con integraciones y conectividad con otros sistemas; formalmente depende de la Gerencia Operativa de Integraciones.

[68] Redmine es una herramienta para la gestión de proyectos, que con sus diversas funcionalidades permite a los usuarios de diferentes proyectos realizar el seguimiento y organización de los mismos. Además es posible optimizar su funcionamiento agregando funcionalidades. Incluye un sistema de seguimiento de incidentes con seguimiento de errores. https://www.redmine.org/ [Accedido el 14/10/2025].

OE5.2- Soporte técnico a los usuarios externos (ciudadanos).

Se realiza soporte a los usuarios externos (ciudadanos) de los sistemas miBA y Login miBA a través de distintas mesas de ayuda con múltiples canales de contacto y sistemas de tickets para la registración y seguimiento de los casos:

- **Chat con BOTI (Chatbot del GCABA):** BOTI actúa como primer nivel de atención, con capacidad de escalar a un segundo nivel en tiempo real. Los usuarios pueden interactuar con BOTI desde la aplicación miBA, otros puntos de acceso del GCABA o mediante WhatsApp al número 11-5050-0147 escribiendo “miBA”. Las interacciones iniciales son registradas en el sistema de BOTI para seguimiento y análisis, y pueden derivarse a una cola de atención en tiempo real donde un agente humano atiende las consultas más complejas. Si el caso requiere seguimiento adicional o resolución más especializada, se genera un ticket formal en la plataforma BA Colaborativa.

- **Tiquetera de BA Colaborativa[69]:** BA Colaborativa funciona como plataforma formal de mesa de ayuda, permitiendo a los ciudadanos reportar problemas o solicitar asistencia a través de la app o la web oficial: BA Colaborativa. El sistema de tickets de BA Colaborativa permite registrar, categorizar, asignar, realizar seguimiento y resolver los casos reportados, asegurando trazabilidad y control sobre el ciclo completo de atención al usuario.

OE5.3 –Seguimiento, análisis y mejora de casos de soporte.

Todos los casos que ingresan a las mesas de ayuda vinculadas a los sistemas miBA y Login miBA son registrados y gestionados a través de los tableros de control de gestión denominados PAD (Plataforma de Análisis de Datos), desarrollados por la Dirección General de Sistemas de Atención Ciudadana. Estos tableros permiten visualizar indicadores de desempeño, trazabilidad de casos y evolución temporal de los incidentes reportados.

Las consultas se agrupan en dos grandes categorías:

- **Prestación privada (interna):** comprende los casos levantados por operadores de sedes comunales y por equipos como la Gerencia Operativa de Plataformas de Atención (GOPA). Los tipos de casos más frecuentes incluyen:

  - Consultas e inconvenientes con el registro de miBA.
  - Consultas e inconvenientes con el registro de miBA – relevados en sede.
  - Consultas sobre datos miBA.

[69] https://bacolaborativa.buenosaires.gob.ar/ [Accedido el 9/10/2025]

Durante el año 2024 se registraron 2.438 solicitudes provenientes de la prestación privada, de las cuales 2.437 fueron resueltas y 1 permanecía en proceso al momento del relevamiento.

- Prestación pública: incluye reclamos ingresados directamente por los vecinos. En 2024 se contabilizaron 17.622 solicitudes, todas con resolución registrada.

Ilustración 5 Tablero de análisis de la Plataforma PAD para solicitudes de soporte técnico internas. Fuente DG Ciudadanía Digital (DGCIUD).

De la prestación Publica, son reclamos que ingresan directamente los vecinos, durante el 2024 han ingresado 17622 de las cuales fueron todas resueltas.

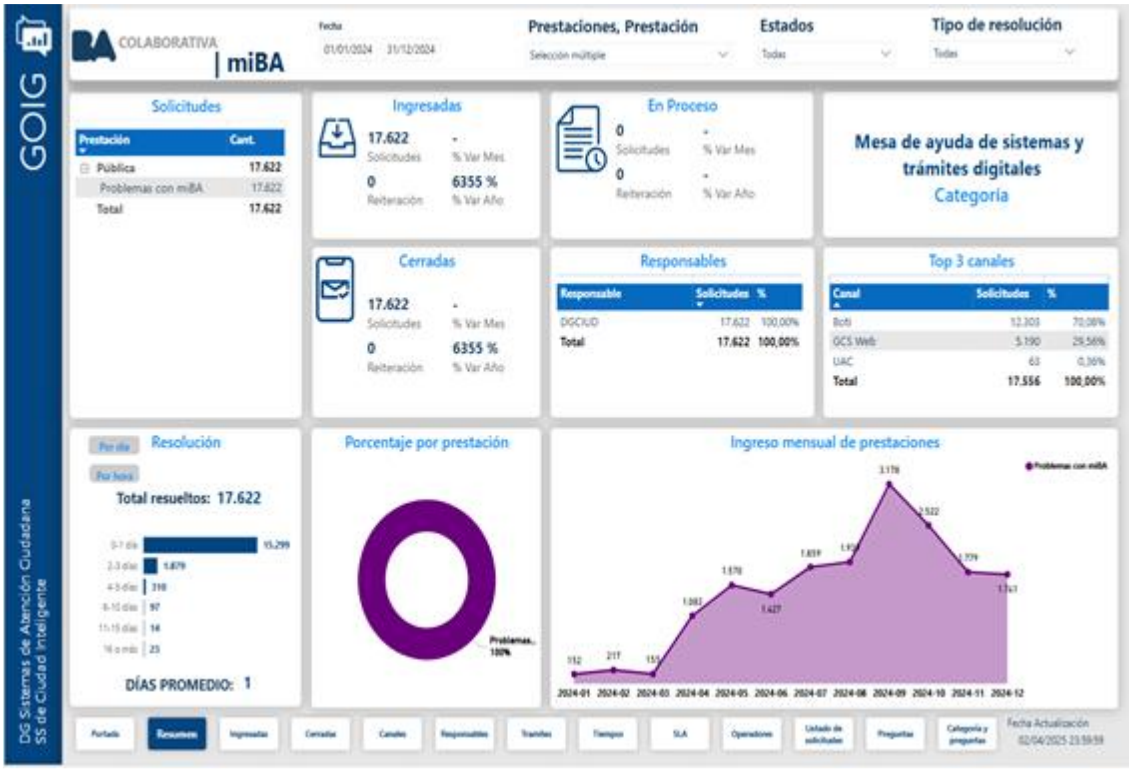


Ilustración 6 Tablero de análisis de la Plataforma PAD para solicitudes de soporte técnico del público (ciudadanos). Fuente DG Ciudadanía Digital (DGCIUD).

Los tableros de gestión permiten generar diversos reportes, entre ellos de volumen de tickets por categoría, tiempo promedio de resolución (TTR) y Top 10 de incidencias para la identificación de mejoras sistémicas.

Sin embargo, no se hallaron reportes o métricas de satisfacción del usuario (ej. CSAT) ni mecanismos documentados para incorporar formalmente el feedback ciudadano en el proceso de mejora continua.

Esta falencia motiva la Observación N° 6.

OBJETIVO ESPECÍFICO 6. Protección de datos personales.

El auditado manifiesta que la plataforma Login miBA garantiza la protección de los datos personales mediante diversas medidas de seguridad y procurando el cumplimiento de la normativa vigente. Entre las acciones implementadas, se informan:

- Almacenamiento seguro de la información en entornos protegidos y con acceso restringido.
- Cifrado de datos sensibles y uso de tecnologías de autenticación segura.
- Control de accesos que limita la información a personal autorizado.
- Monitoreo y auditorías periódicas orientadas a prevenir accesos indebidos.

Se cita como marco normativo de referencia la Ley N.º 25.326 de Protección de Datos Personales y la Política de Privacidad de miBA, publicada en el sitio oficial https://login.buenosaires.gob.ar, , bajo el enlace “Políticas de privacidad”.

En cuanto a los **datos recopilados**, el sistema Login miBA recolecta y procesa las siguientes categorías de datos personales:

Datos Obligatorios: para la validación de identidad, tales como nombre, apellido, tipo y número de documento, país emisor, fecha de nacimiento y correo electrónico.

Datos no obligatorios: como género, teléfono, dirección y código postal.

Datos biométricos: reconocimiento facial utilizado para la verificación de identidad digital de nivel 3. No se encuentra documentada la existencia de un flujo alternativo para usuarios que no deseen utilizar biometría.

Datos de Autenticación: contraseñas (hasheadas) y tokens de sesión (JWT).

Datos técnicos o comportamentales: información del dispositivo de la persona usuaria (modelo de equipo, versión del sistema operativo, identificadores únicos, datos de red móvil incluyendo número de teléfono), dirección IP, registros (logs) de acceso, cookies, geolocalización (si autorizada) e historial de autenticaciones. Estos datos son utilizados para optimizar los servicios y medir su desempeño.

El **propietario del dato** es el **ciudadano**, y el **custodio** del tratamiento es el **GCABA**.

La base de datos “Login miBA” se encuentra inscripta formalmente ante la autoridad de control, el Centro de Protección de Datos Personales (CPDP) de la

Defensoría del Pueblo de la CABA[70]. Dicho organismo otorgó el alta registral asignando la Clave Única de Identificación N° 241, mediante el dictado de la Disposición CPDP N° 04/19 (de fecha 29 de julio de 2019). De esta manera cumple con el requisito de inscripción obligatoria establecido por la Ley CABA N° 1845 de Protección de Datos Personales[71]. No obstante, no se encuentra registrada ante la Agencia de Acceso a la Información Pública (AAIP)[72] del Estado Nacional.

Sobre los derechos del titular de los datos, la DG de Ciudadanía Digital (DGCIUD) garantiza el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) [73] por parte de los titulares de los datos. A tal efecto, se han implementado mecanismos específicos:

En primer lugar, mediante el sistema de Autogestión Digital de la plataforma Login miBA, el ciudadano puede acceder a la rectificación de sus datos personales a través de las opciones de perfil de usuario. Asimismo, se garantiza el derecho de supresión —técnicamente instrumentado como “blanqueo de cuenta”— que permite la eliminación de los registros mediante los canales oficiales “Boti” o la plataforma “Buenos Aires Colaborativa”.

En segundo lugar, de conformidad con la Ley N° 1845 y el Reglamento aprobado por la Disposición CPDP N° 143/08, se ha constituido un domicilio formal para la recepción de solicitudes de ejercicio de derechos ARCO en el ámbito de la DG Ciudadanía Digital (DGCIUD), ubicado en Zavaleta 190, 2° piso.

En cuanto a la “Política de Privacidad” del sistema Login miBA, al tratar al almacenamiento, se advierte que contempla que los datos personales de las personas usuarias podrán ser almacenados “en servidores on premise del GCABA o en la nube, pudiendo o no encontrarse dentro de las regiones adecuadas” conforme la Disposición N° 60/2016 de la DNPDP[74]. Esta redacción introduce un riesgo de transferencia internacional de datos personales a países sin nivel adecuado de protección, lo que podría resultar incompatible con los artículos 12 y 25[75] de la Ley N° 25.326 y la normativa complementaria. No se evidenció documentación técnica o contractual que detalle las ubicaciones efectivas de los servidores ni los mecanismos de resguardo y cumplimiento aplicados en caso de almacenamiento fuera del territorio nacional.

Ello sin perjuicio de que, en la práctica, la totalidad de la información se encuentra alojada, custodiada y procesada en los servidores (Data Center) de la

[70] https://defensoria.org.ar/derechos/democracia-y-digitalidad/derechos-digitales-y-proteccion-de-datos-personales/registro-de-bases-de-datos/ [Accedido el 09/10/2025].
[71] En fecha pasado 12 de noviembre de 2025 (durante el periodo de esta auditoría) la DGCIUD ingresó en el CPDP un “Formulario de Actualización de Datos”, para poner al día los datos correspondientes a la Base de Datos.
[72] https://www.argentina.gob.ar/aaip/datospersonales/tramites [Accedido el 09/10/2025].
[73] Los Derechos ARCO se definen como Derecho de acceso, rectificación, cancelación y oposición de los Titulares sobre sus datos personales.
https://www.humanquality.com.mx/derechos-arco [Accedido el 09/10/2025].
[74] https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm [Accedido 9/10/2025]
[75] Estos artículos tratan sobre Transferencia internacional y la Prestación de servicios informatizados de datos personales

Agencia de Sistemas de Información (ASINF), lo que aseguraría que los datos permanecerían bajo jurisdicción local.

En cuanto a las condiciones del tratamiento de datos biométricos, se encuentran estipulados en el contrato con el proveedor S.D.C. S.R.L.[76], cuya adjudicación se realizó por medio de la Disposición DI-2025-44787928-GCABA-DGCIUD. Allí se establecen de manera expresa las condiciones técnicas y de seguridad aplicables a dicho tratamiento.

En materia de cifrado y resguardo de la información biométrica, se exige que todos los datos almacenados se encuentren protegidos mediante el algoritmo AES-256, considerado un estándar internacional de alta seguridad, así como que las imágenes utilizadas para la generación de los templates biométricos[77] se mantengan cifradas bajo el mismo esquema.

Finalmente, en cuanto al alcance del acuerdo de procesamiento de datos, se establecen obligaciones esenciales para el tratamiento de datos personales por parte del proveedor. Entre ellas se destacan la obligación de confidencialidad estricta, la prohibición de divulgar o reutilizar los datos, el reconocimiento de que la información continúa siendo propiedad del GCABA y la responsabilidad de implementar las medidas de seguridad adecuadas conforme la normativa vigente. Estos elementos dan cumplimiento a los requisitos propios de un Acuerdo de Procesamiento de Datos (DPA[78]).

No obstante las normativas, políticas, certificados y medidas técnicas declaradas, se detectan algunas brechas de cumplimiento normativo y documenta:

- No se evidencian medidas o prácticas activas de protección de datos personales.
- No se encuentra documentada una Evaluación de Impacto en la Protección de Datos (DPIA[79]), especialmente relevante por el uso de datos biométricos.

[76] La contratación se realizó bajo la modalidad de Orden de Compra Abierta para la prestación del "Servicio de Implementación y Mantenimiento Evolutivo y Correctivo de Software para la Validación de Identidad a través del Reconocimiento Biométrico (SaaS)", proceso de compra 2051-0801-LPU25, siendo la Disposición DI-2025-44787928-GCABA-DGCIUD el acto adjudicación.

[77] Una plantilla (template) biométrica es una representación matemática digital de los rasgos físicos o conductuales únicos de una persona, como una huella dactilar o un rostro. Se crea convirtiendo una muestra biométrica capturada (como un escaneo o una imagen) en un registro digital único. Es esta plantilla la que se almacena y utiliza para la comparación en un sistema biométrico, no los datos originales en sí.

[78] Un Data Processing Agreement (DPA) es un contrato legalmente vinculante entre un responsable del tratamiento y un encargado del tratamiento de datos que define sus respectivas funciones y responsabilidades en el manejo de datos personales. Describe cómo el encargado del tratamiento debe gestionar, proteger y utilizar los datos en nombre del responsable del tratamiento, garantizando el cumplimiento de las leyes de privacidad de datos, como el RGPD.
https://gdpr.eu/what-is-data-processing-agreement/ [Accedido el 09/10/2025]

[79] Un Data Protection Impact Assessment (DPIA), o Evaluación de Impacto sobre la Protección de Datos (EIPD), es un proceso para identificar y minimizar los riesgos del tratamiento de datos personales. Implica describir el tratamiento, evaluar su necesidad y proporcionalidad, e identificar y mitigar los posibles riesgos antes de iniciar el tratamiento de datos.
https://gdpr.eu/data-protection-impact-assessment-template/ [Accedido el 09/10/2025].

- No se evidencian evaluaciones de riesgo de privacidad ni medidas de mitigación formalmente aprobadas.
- No se acreditó la inscripción de la base de datos ante la Agencia de Acceso a la Información Pública (AAIP)[80], autoridad nacional de aplicación.

En síntesis, el sistema Login miBA incorpora medidas técnicas de seguridad acordes a su criticidad, aunque no se hallan evidencias de medidas o prácticas de cumplimiento efectivo en materia de protección de datos personales, y se carece de documentación formal sobre el tratamiento y la gestión integral de riesgos de privacidad. Ello resulta especialmente sensible considerando el procesamiento de datos biométricos.

Por lo expuesto, se formula la Observación N° 7.

OBJETIVO ESPECÍFICO 7. Auditorías y Control Interno.

OE7.1.- Informes de Auditoría Previos.

Desde el 1° de enero de 2020 a la fecha, no se han realizado auditorías, relevamientos ni seguimientos en las áreas de la DG de Ciudadanía Digital (GCIUD) por parte de la AGCBA, Sindicatura General de la Ciudad de Buenos Aires (SGCBA), la Unidad de Auditoría Interna (UAI) u otros organismos de control u entidades públicas o privadas. Tampoco se registran antecedentes anteriores que resulten pertinentes.

OE7.2 - Cambios y mejoras efectuadas en consecuencia a las observaciones.

Como consecuencia de la inexistencia de auditoría señalada en el punto anterior, no se han emitido observaciones ni recomendaciones, y por lo tanto no se implementaron cambios o mejoras derivados de informes.

OE7.3.- Control Interno.

El auditado reconoce que la Dirección General de Ciudadanía Digital no dispone de procedimientos de control interno formalizados ni de mecanismos sistemáticos de monitoreo o revisión periódica.

No se identifican políticas, metodologías ni marcos de referencia implementados (por ejemplo, COSO, COBIT o similares) que organicen o estructuren los controles internos al sistema Login miBA.

[80] https://www.argentina.gob.ar/aaip/datospersonales/tramites [Accedido el 09/10/2025].

Tampoco se evidenció la realización de pruebas de penetración (penetration tests) documentadas ni de auditorías de seguridad externas a cargo de terceros independientes.

Sí existen actualmente controles técnicos operativos (no formalizados como “control interno”), relevados en los puntos anteriores, tales como:

- Paneles de auditoría y tableros de control para el seguimiento de accesos y actividad del sistema.
- Gestión de identidades y sesiones mediante Keycloak.
- Generación de registros de auditoría y trazabilidad para todas las operaciones de autenticación y autorización.
- Monitoreo y detección de accesos inusuales, con alertas automáticas.
- Monitoreo de infraestructura con Dynatrace, PRTG y Kibana.
- Controles de acceso RBAC (Role-Based Access Control) y ABAC (Attribute-Based Access Control).
- Pruebas de calidad (QA) en ambientes no productivos.
- Control de versiones mediante GitLab.
- Análisis de Seguridad de Software (ASS) realizados por ASINF.
- Ejecución de pruebas de estrés.

No obstante, se destaca la ausencia de los siguientes componentes:

- Marco formal de control interno (COSO, COBIT u otro).
- Matriz de controles clave documentada.
- Segregación de funciones (SoD) formalizada.
- Proceso de autoevaluación de controles documentado.
- Gestión de riesgos de TI documentada o sistemática.

En conclusión, si bien el auditado dispone de herramientas técnicas que permiten ejercer ciertos controles sobre sus procesos y componentes tecnológicos, no se registran auditorías internas o externas (técnicas o de gestión), ni marcos formales de control ni documentación que respalde las prácticas de supervisión o evaluación continua.

Por ello se finaliza con la Observación N° 8.

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

VI.- OBSERVACIONES.

Las Observaciones halladas que se detallan a continuación son analizadas conforme a: los objetivos de gobierno y gestión establecidos para el Marco de Referencia COBIT 2019, las normas y recomendaciones establecidas por ASInf según la Resolución N°177/ASInf/13 y sus ampliaciones, el estándar NIST SP 800-63 (Digital Identity Guidelines) de la National Institute of Standards and Technology (NIST) y la referencia de buenas prácticas OWASP Top 10. Se organizan para cada Objetivo Específico:

Observaciones OE1: Seguridad de acceso: usuarios, contraseñas, sesiones.

COBIT 2019: Alinear, Planificar y Organizar (APO). APO13—Gestionar la seguridad.

Observación N° 1:

Se advierte que la política de contraseñas implementada en Login miBA no cumple con algunos de los requerimientos establecidos por los estándares internacionales actuales, como el NIST SP800-63B. En particular, no se impide el uso de identificadores del usuario como contraseña, no se conserva un historial que evite la reutilización, ni se realiza validación contra contraseñas comunes o previamente comprometidas, y el sistema no permite la autenticación con doble factor ni cuenta con dicha funcionalidad prevista.

Además, durante las pruebas realizadas se comprobó que el sistema acepta contraseñas débiles o comprometidas y presenta mensajes de error genéricos que dificultan la comprensión del motivo de rechazo. Asimismo, no envió correos electrónicos al usuario informando sobre la modificación de la contraseña.

En consecuencia, el esquema actual de contraseñas resulta parcialmente alineado con las buenas prácticas internacionales, pero requiere una revisión técnica integral que garantice niveles adecuados de seguridad y usabilidad.

Observación N° 2:

Se observó que no se encuentran documentadas ni implementadas de manera formal diversas prácticas de seguridad vinculadas a la autenticación y gestión de sesiones. En particular, no se evidencian evaluaciones de seguridad basadas en el estándar OWASP Top 10, escaneos automatizados de vulnerabilidades ni ejercicios orientados a la detección proactiva de fallas.

Asimismo, se detecta la ausencia de documentación técnica sobre configuraciones críticas del sistema de identidad Keycloak. Esta falta de evidencia limita la trazabilidad y dificulta la verificación de la robustez de los controles de seguridad implementados.

Observación N° 3:

Se observó que la versión de Java utilizada se encuentra discontinuada, sin actualizaciones de seguridad públicas y con vulnerabilidades (CVE) conocidas, mientras que la versión de Keycloak implementada es antigua, carece de soporte activo de la comunidad y presenta riesgos similares. Esta situación expone al sistema

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

a posibles fallas de seguridad no corregidas y limita la capacidad de aplicar actualizaciones o parches críticos para mantener la integridad y protección del entorno de autenticación.

Observación OE2: Complementación de Procesos productivos e Integración con otros sistemas.

COBIT 2019: Alinear, Planificar y Organizar (APO). APO09—Gestionar los acuerdos de servicio.

Observación N° 4:

Se constató la inexistencia de un marco formal de gobernanza de integraciones que establezca políticas, roles, métricas y responsabilidades para la administración y control de las conexiones activas entre sistemas. Asimismo, no se hallaron acuerdos de nivel de servicio (SLA) con los organismos externos involucrados —en particular con el RENAPER— ni con reparticiones del GCABA, especialmente la Agencia Gubernamental de Ingresos Públicos (AGIP). Tampoco se hallaron acuerdos operativos internos (OLA) entre las áreas internas responsables del mantenimiento y soporte de dichas integraciones. En consecuencia, no existen compromisos documentados sobre tiempos de respuesta, niveles de disponibilidad, protocolos de escalamiento ni procedimientos de gestión ante incidentes.

Observación OE3: satisfacción del usuario y cumplimiento de metas y objetivos.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA)- MEA01—Gestionar la monitorización del desempeño y la conformidad.

Observación N° 5:

Se identifica que, si bien los sistemas miBA y Login miBA cuentan con algunos mecanismos potenciales para relevar la satisfacción del usuario —como las calificaciones en tiendas de aplicaciones, los canales de soporte y las opciones internas de retroalimentación—, no existe un plan estratégico integral ni un sistema formalmente implementado para medir de manera sistemática el cumplimiento de metas, objetivos y el nivel de satisfacción de los usuarios.

Asimismo, no se aplican métricas estandarizadas de satisfacción como NPS (Net Promoter Score), CSAT (Customer Satisfaction Score) post-interacción, CES (Customer Effort Score), ni se realizan encuestas periódicas o análisis de comportamiento de los usuarios que permitan obtener información representativa y comparable a lo largo del tiempo. Esta situación limita la capacidad de la organización para evaluar objetivamente la experiencia de los usuarios, identificar áreas de mejora y verificar el cumplimiento de sus objetivos de servicio y calidad.

Observación OE5: Soporte técnico.

COBIT 2019: Entregar, Dar Servicio y Soporte (DSS). DSS02 — Gestionar las peticiones y los incidentes de servicio.

Observación N° 6:

El sistema cuenta con mecanismos de registro y análisis de casos a través del software Plataforma de Análisis de Datos (PAD), que permiten monitorear volúmenes, tiempos de resolución y principales incidencias. Sin embargo, no se relevan métricas de satisfacción del usuario ni procedimientos sistemáticos para incorporar el feedback ciudadano en la mejora continua del servicio, lo que limita la evaluación integral de la calidad del soporte técnico.

Observación OE6: Protección de datos personales.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA). MEA03 — Gestionar el cumplimiento de los requisitos externos.

Observación N° 7:

Si bien la plataforma Login miBA cuenta con normativa, políticas, un Acuerdo de Procesamiento de Datos (DPA) con su proveedor e implementa medidas técnicas de seguridad como cifrado de datos, autenticación segura y control de accesos; no se evidencian medidas o prácticas activas de protección de datos personales, no se constató la existencia de una Evaluación de Impacto en la Protección de Datos (DPIA), especialmente relevante por el uso de datos biométricos, ni se evidencian evaluaciones de riesgo de privacidad ni medidas de mitigación formalmente aprobadas.

Asimismo, se observa que la “Política de Privacidad” del, al tratar sobre almacenamiento, contempla la posibilidad de que los datos sean alojados “pudiendo o no encontrarse dentro de las regiones adecuadas” para el caso de transferencia internacional de datos. Ello sin perjuicio de que en la actualidad la totalidad de los datos personales se encuentran alojados en los data centers de la ASINF.

Por último, la Base de Datos se encuentra inscripta en el centro de Protección de Datos Personales (CPDP) de la Defensoría del Pueblo de la CABA conforme a Ley CABA N° 1.845 de Protección de Datos Personales, pero no se encuentra registrada ante la Agencia de Acceso a la Información Pública (AAIP), autoridad de aplicación nacional de la Ley N° 25.326 de Protección de Datos Personales.

Observaciones OE7: Auditoría y Control Interno.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA). MEA02 — Gestionar el sistema de control interno.

Observación N° 8:

La DG de Ciudadanía Digital (DGCIUD) no cuenta con procedimientos de control interno formalizados ni con mecanismos sistemáticos de monitoreo y revisión periódica aplicables al sistema Login miBA. No se identifican políticas, metodologías ni marcos de referencia (como COSO o COBIT) que estructuren los controles internos, ni se evidenció la realización de pruebas de penetración documentadas o auditorías de seguridad externas. Asimismo, se evidenció la inexistencia de auditorías internas o externas previas, técnicas o de gestión.

Aunque el sistema dispone de herramientas técnicas de control y monitoreo, estas prácticas operan de manera aislada y sin un marco formal de control. La ausencia de una estructura documentada de gestión de riesgos, matriz de controles

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

clave y procesos de autoevaluación limita la capacidad institucional de asegurar la eficacia y trazabilidad de los controles implementados.

VII.- RECOMENDACIONES.

Recomendaciones OE1: Seguridad de acceso: usuarios, contraseñas, sesiones.

COBIT 2019: Alinear, Planificar y Organizar (APO). APO13—Gestionar la seguridad.

Recomendación N° 1:

Se recomienda llevar adelante una revisión y actualización integral de la política de contraseñas de Login miBA con el fin de alinearla a los estándares internacionales vigentes, en particular al NIST SP800-63B. Esta actualización debería incluir mecanismos que impidan el uso de identificadores del propio usuario como contraseña, así como la implementación de un historial que evite la reutilización de claves previamente empleadas.

Asimismo, se sugiere incorporar validaciones automáticas que detecten y bloqueen el uso de contraseñas comunes, débiles o comprometidas. Resulta igualmente recomendable habilitar y promover el uso de autenticación en dos factores (2FA), poniendo a disposición la funcionalidad necesaria para fortalecer el proceso de acceso.

Por último, deberían ajustarse los mensajes de error para que brinden información clara sin comprometer la seguridad del sistema, al tiempo que se habilitan notificaciones automáticas al usuario ante cualquier modificación de su contraseña. Estas medidas contribuirán a mejorar la robustez del esquema de autenticación y reducir las vulnerabilidades asociadas a credenciales insuficientemente protegidas.

Recomendación N° 2:

Se recomienda formalizar y documentar las prácticas de seguridad vinculadas a los mecanismos de autenticación y gestión de sesiones del sistema Login miBA. Para ello, resulta necesario implementar evaluaciones de seguridad periódicas basadas en estándares reconocidos, como OWASP Top 10, junto con escaneos automatizados de vulnerabilidades y pruebas orientadas a la detección temprana de fallas. Estas actividades deberían quedar registradas de manera sistemática a fin de asegurar su trazabilidad y permitir un seguimiento efectivo de los hallazgos y acciones correctivas.

Asimismo, se sugiere elaborar y mantener actualizada la documentación técnica de las configuraciones críticas del sistema de identidad Keycloak, incluyendo parámetros de seguridad aplicados, políticas activas, y justificación de los valores adoptados. Contar con esta documentación resulta fundamental para garantizar la verificabilidad de los controles implementados, facilitar auditorías futuras y asegurar la continuidad operativa ante cambios de personal o evolución tecnológica.

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

Recomendación N° 3:

Se recomienda actualizar de manera prioritaria la versión de Java utilizada por el sistema Login miBA, dado que la versión actualmente desplegada se encuentra discontinuada, carece de soporte oficial y posee vulnerabilidades (CVE) conocidas que incrementan el riesgo de explotación. Del mismo modo, se sugiere actualizar la versión de Keycloak implementada, ya que la versión actual es antigua, no cuenta con soporte activo de la comunidad y presenta riesgos similares a los identificados para Java. En ambos casos, la adopción de una versión vigente permitirá recibir parches de seguridad, correcciones de fallas y mejoras funcionales necesarias para sostener un sistema de identidad robusto.

Finalmente, se aconseja que la DGCIUD establezca un procedimiento formal de gestión de actualizaciones y parches que contemple monitoreo continuo de CVE, evaluación del impacto de versiones nuevas.

Recomendación OE2: Complementación de Procesos productivos e Integración con otros sistemas.

COBIT 2019: Alinear, Planificar y Organizar (APO). APO09—Gestionar los acuerdos de servicio.

Recomendación N° 4:

Se recomienda a la DGCIUD formalizar un marco integral de gobernanza de integraciones que establezca de manera explícita las políticas, roles, métricas y responsabilidades aplicables a la administración y control de las conexiones activas entre sistemas.

Asimismo, se sugiere avanzar en la elaboración y firma de acuerdos de nivel de servicio (SLA) con los organismos externos involucrados —en particular con RENAPER— y con las distintas reparticiones del GCABA, especialmente la AGIP. Estos acuerdos deben contemplar compromisos concretos respecto de tiempos de respuesta, niveles de disponibilidad, mecanismos de soporte y protocolos de escalamiento.

Finalmente, se recomienda establecer acuerdos operativos internos (OLA) entre las áreas responsables del mantenimiento y soporte de las integraciones, a fin de documentar roles, actividades y compromisos internos que permitan una gestión coordinada. La inexistencia de estos instrumentos limita la capacidad de fijar expectativas claras y de asegurar una correcta gestión de incidentes, por lo que su formalización contribuirá al fortalecimiento del funcionamiento operativo del sistema.

Recomendación OE3: satisfacción del usuario y cumplimiento de metas y objetivos.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA)- MEA01—Gestionar la monitorización del desempeño y la conformidad.

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

Recomendación N° 5:

Se recomienda a la DGCIUD diseñar e implementar un plan estratégico integral para la medición de la satisfacción del usuario en relación con los sistemas Login miBA.

Asimismo, se sugiere adoptar métricas estandarizadas de satisfacción, tales como NPS (Net Promoter Score), CSAT (Customer Satisfaction Score) y CES (Customer Effort Score), así como implementar encuestas periódicas y mecanismos formales de retroalimentación post-interacción. Estas herramientas proporcionarían información representativa, comparable y orientada a identificar oportunidades de mejora continua.

Finalmente, se recomienda generar reportes periódicos que permitan evaluar el grado de cumplimiento de los objetivos de servicio y calidad establecidos. La incorporación de un sistema formal y sostenido de medición fortalecerá la capacidad de gestión, facilitará la toma de decisiones y contribuirá a una mejora continua en la experiencia de los usuarios.

Recomendación OE5: Soporte técnico.

COBIT 2019: Entregar, Dar Servicio y Soporte (DSS). DSS02 — Gestionar las peticiones y los incidentes de servicio.

Recomendación N° 6:

Se sugiere a la DGCIUD complementar los mecanismos actuales de registro y análisis de casos provistos por la Plataforma de Análisis de Datos (PAD) mediante la incorporación de métricas orientadas a evaluar la satisfacción del usuario con el soporte técnico brindado. La incorporación de indicadores específicos permitirá obtener una visión más completa del desempeño del servicio y de la percepción de los usuarios.

Recomendación OE6: Protección de datos personales.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA). MEA03 — Gestionar el cumplimiento de los requisitos externos.

Recomendación N° 7:

Se recomienda a la DGCIUD avanzar en la formalización e implementación de un marco integral de protección de datos personales aplicable a la plataforma Login miBA, Asimismo, se sugiere elaborar y aprobar una Evaluación de Impacto en la Protección de Datos (DPIA), especialmente necesaria dado el tratamiento de datos biométricos, así como documentar evaluaciones de riesgo de privacidad y las correspondientes medidas de mitigación.

En relación con la política de almacenamiento, se solicita revisar y actualizar la redacción a fin de eliminar ambigüedades respecto de la posibilidad de

transferencias internacionales a países sin nivel adecuado de protección. La política debería reflejar la normativa vigentes.

Por último, se aconseja regularizar la inscripción de la base de datos ante la Agencia de Acceso a la Información Pública (AAIP) —autoridad nacional de aplicación de la Ley N.º 25.326.

Recomendación OE7: Auditoría y Control Interno.

COBIT 2019: Monitorizar, Evaluar y Valorar (MEA). MEA02 — Gestionar el sistema de control interno.

Recomendación N° 8:

Se recomienda a la DGCIUD formalizar un marco de control interno para el sistema Login miBA, estableciendo políticas, metodologías y procedimientos alineados con estándares como COSO o COBIT. Este marco debe incluir una matriz de riesgos y controles clave, procesos de monitoreo periódico y mecanismos de autoevaluación que permitan verificar la eficacia de los controles implementados.

Asimismo, se sugiere incorporar evaluaciones independientes, tales como auditorías internas o externas y pruebas de penetración documentadas, a fin de obtener evidencia objetiva sobre el estado de la seguridad del sistema. Finalmente, se propone integrar las herramientas técnicas de monitoreo existentes dentro de un proceso formal y continuo que asegure la trazabilidad y consistencia del control interno.

VIII.- CONCLUSIÓN.

El sistema Login miBA constituye la plataforma central de autenticación e identidad digital del Gobierno de la Ciudad de Buenos Aires, permitiendo a la ciudadanía acceder de manera unificada y segura a múltiples servicios digitales. Su implementación representa un componente estratégico dentro del modelo de gobierno digital, al facilitar la trazabilidad de usuarios, la simplificación de trámites y la interoperabilidad entre organismos.

Durante la auditoría se identificaron fortalezas relevantes, entre ellas la existencia de mecanismos técnicos de seguridad como el uso de cifrado robusto, la autenticación segura y la integración con proveedores especializados para la verificación biométrica. Asimismo, se relevó la presencia de herramientas operativas de soporte, monitoreo y análisis que contribuyen al funcionamiento cotidiano del sistema.

No obstante, se advirtieron oportunidades de mejora significativas. En primer lugar, la política de contraseñas presenta debilidades en relación con estándares internacionales como NIST SP 800-63B, permitiendo contraseñas débiles o

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

previamente comprometidas y careciendo de mecanismos como historial, validación de listas prohibidas y autenticación multifactor.

En segundo término, se constató la ausencia de prácticas formalizadas de seguridad para la autenticación y gestión de sesiones, incluyendo la falta de evaluaciones basadas en OWASP Top 10, escaneos automatizados de vulnerabilidades y documentación técnica del sistema de identidad.

Finalmente, se verificó la inexistencia de un marco de gobernanza para las integraciones del sistema, con ausencia de políticas, roles, métricas, acuerdos de nivel de servicio (SLA) y acuerdos operativos internos (OLA), lo que limita la capacidad de asegurar la continuidad operativa y el funcionamiento coordinado con organismos internos y externos.

En síntesis, Login miBA constituye un sistema sólido desde el punto de vista operativo y con medidas técnicas adecuadas, pero requiere atender a las observaciones halladas en este informe.