



AUDITORÍA GENERAL
DE LA CIUDAD DE BUENOS AIRES

Informe Final de Auditoría
Con Informe Ejecutivo

Proyecto N° 10.26.01
SEGURIDAD DE LA INFORMACIÓN

Auditoría de Sistemas
Período 2025

BUENOS AIRES - OCTUBRE 2026

AUDITORIA GENERAL DE LA CIUDAD DE BUENOS AIRES

JEAN JAURES 220 - CIUDAD DE BUENOS AIRES

Presidenta

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: 10.26.01

Nombre del Proyecto Auditoría: Seguridad de la Información

Tipo de auditoría: Sistemas.

Organismo auditado: Dirección General de Seguridad Informática (DGSEI).

Objeto: Jurisdicción 21 - Entidad 270 - Unidad Ejecutora 687.

Objetivo: Evaluar los procesos implementados para la detección, clasificación, prevención y las acciones correctivas destinadas a los incidentes de seguridad de la información. Implementación de planes de concientización, prevención y divulgación. Impacto por la criticidad de los datos gestionados.

Alcance: Analizar los procedimientos establecidos para la gestión completa de los incidentes de seguridad, desde su identificación hasta las acciones correctivas, abarcando la revisión de los planes de concientización y la validación de la clasificación de la criticidad de la información administrada.

Período a Auditar: 2025

Supervisor: Mg. Hernán García

FECHA DE APROBACION DEL INFORME: 7 DE OCTUBRE DE 2026
APROBADO POR: UNANIMIDAD

INFORME EJECUTIVO

Lugar y fecha de emisión: Ciudad Autónoma de Buenos Aires, 7 de octubre de 2026

Código de Proyecto: 10.26.01

Denominación del Proyecto: Seguridad de la Información.

Tipo de Auditoría: Sistemas.

Dirección General: Dirección General Sistemas de Información.

Período bajo examen: 2025.

Objeto de la Auditoría: Jurisdicción 21 - Entidad 270 - Unidad Ejecutora 687.

Objetivo de la Auditoría: Evaluar los procesos implementados para la detección, clasificación, prevención y las acciones correctivas destinadas a los incidentes de seguridad de la información. Implementación de planes de concientización, prevención y divulgación. Impacto por la criticidad de los datos gestionados.

Alcance: Analizar los procedimientos establecidos para la gestión completa de los incidentes de seguridad, desde su identificación hasta las acciones correctivas, abarcando la revisión de los planes de concientización y la validación de la clasificación de la criticidad de la información administrada.

Limitaciones al Alcance: Sin limitaciones.

Observaciones:

- ✓ La Dirección General de Seguridad Informática carece de atribuciones operativas formalizadas para la toma de decisiones ante incidentes de seguridad. Ningún instrumento normativo identifica a los responsables de aprobar las acciones críticas.

Las disposiciones vigentes tampoco especifican qué autoridad aprueba la reasignación de los recursos económicos, ni definen los umbrales y los criterios de escalamiento técnico.

La falta de regulación incrementa la probabilidad de respuestas tardías o contradictorias frente a las contingencias. Cada decisión crítica se ejecuta según la interpretación del analista asignado.

- ✓ La DGSEI gestiona la seguridad de la información sin estrategia formalizada ni aprobación institucional vigente.

El funcionamiento del área se apoya en prácticas operativas sin objetivos estratégicos definidos ni planificación temporal que ordene sus acciones.

Las iniciativas de concientización no cuentan con responsables asignados ni cronogramas de ejecución, lo que debilita su implementación sostenida.

Las decisiones se adoptan sin indicadores documentados ni trazabilidad sobre los criterios utilizados, lo que restringe la verificación de la base de priorización aplicada.

- ✓ Los servicios que presta la DGSEI no tienen definición formal ni parámetros claros de medición.

La Dirección no asegura la trazabilidad de qué entrega, a quién y en qué condiciones, porque no establece alcance, responsables ni métricas de desempeño.

Las autoridades de control no disponen de evidencia suficiente para validar la ejecución, calidad ni los resultados.

- ✓ El organismo no incorpora requisitos de control de accesos en la planificación de sus contrataciones tecnológicas, ni asigna responsables de verificación del cumplimiento de las condiciones de seguridad pactadas con los proveedores.

Al no formalizar estos aspectos antes de la contratación, se reduce la posibilidad de exigirlos durante la ejecución del contrato.

- ✓ La Dirección General de Seguridad Informática no acredita, con evidencia documental, la aplicación efectiva de las medidas técnicas de protección de datos personales exigidas por el Estándar de Seguridad (ES0902). Tampoco demuestra la ejecución concreta de la verificación de seguridad prevista en su propio esquema de control.

El organismo no detalló las medidas técnicas de cifrado, gestión de roles, límites de sesión y monitoreo de accesos. No aportó informes de evaluación de seguridad ni ninguna otra evidencia de la aplicación de ese circuito de control.

Esa ausencia de evidencia expone al organismo a desviaciones no detectadas en los controles de seguridad de la información.

- ✓ La DGSEI implementa herramientas de seguridad sin documentación que acredite su selección, evaluación técnica e integración.

La auditoría no verificó evidencia de alineación con el Estándar tecnológico vigente. La falta de registros impide confirmar los criterios de selección, condiciones de integración y adecuación a la normativa técnica.

Sin este respaldo, el organismo pierde sustento para analizar el desempeño de las herramientas y decidir sobre su continuidad operativa.

- ✓ La Dirección General informa la aplicación de controles de seguridad sobre interfaces de programación y la ejecución de pruebas durante el período auditado.

La documentación presentada no describe los mecanismos de autenticación implementados ni detalla el alcance de los ensayos realizados. Tampoco

evidencia la adecuación a los estándares definidos por la Agencia de Sistemas de Información.

El área declara información que no coincide con la documentación disponible. Esta diferencia impide confirmar que los controles y las pruebas se ejecutan de manera efectiva. Los entornos de producción, además, no cuentan con validación técnica documentada.

- ✓ El inventario de recursos tecnológicos del área se mantiene desactualizado y no cuenta con roles de Propietario ni Custodio definidos oficialmente.

Los equipos de control biométrico, la plataforma de firma digital, los servidores de autenticación y los equipos perimetrales de seguridad presentan la misma falta de registro actualizado.

Esta condición limita la clasificación de los activos críticos y debilita la cadena de responsabilidad asociada a cada componente tecnológico.

Frente a incidentes en la infraestructura, la falta de inventario actualizado y de roles formalmente definidos disminuye la capacidad de identificar el activo afectado y su responsable, impactando en la oportunidad de respuesta y en la evaluación del impacto del incidente.

- ✓ Los resultados de evaluación presentados no contienen información técnica suficiente para verificar las modificaciones realizadas sobre los componentes que presentaban fallas de seguridad.

Los hallazgos son presentados como corregidos, sin que se adjunte la descripción de los cambios de configuración realizados ni la evidencia técnica que permita acreditar su corrección.

La entidad no dispone de un registro específico para documentar y auditar las correcciones implementadas sobre las configuraciones afectadas. El único respaldo disponible es el informe de evaluación de seguridad.

Esta falta de historial de cambios impide validar qué modificación puntual se aplicó a cada componente.

- ✓ El área no deja evidencia documentada de las verificaciones realizadas sobre los componentes críticos de la infraestructura de seguridad.

Esto limita la capacidad del organismo para acreditar, a través de registros verificables, el control de sus operaciones diarias y detectar fallas antes de que produzcan mayores consecuencias.

- ✓ La dependencia gestiona los incidentes de seguridad sin una guía formal que establezca las tareas de soporte técnico.

La ausencia de pautas de coordinación genera respuestas diferentes ante problemas informáticos idénticos según el sector interviniente, lo que afecta la trazabilidad de los cambios aplicados en las plataformas.

La falta de estandarización en la gestión de incidentes restringe la posibilidad de consolidar un historial confiable que permita diagnosticar y resolver incidentes de forma consistente y trazable.

- ✓ Las plataformas informáticas de la DGSEI operan sin planes de continuidad, esquemas de redundancia ni procedimientos formalizados de recuperación ante contingencias.

La Dirección no definió los tiempos máximos de interrupción ni los niveles tolerables de pérdida de datos frente a incidentes críticos.

No contar con esos umbrales interfiere en la evaluación del comportamiento de la infraestructura ante una interrupción real. Esta falta de parámetros deja sin sustento las pruebas de continuidad que el área pretenda acreditar ante terceros.

- ✓ La gestión de ciberseguridad en la Dirección se realiza sin un marco normativo que regule la interacción entre los dispositivos de detección, registro y respuesta automatizada.

El área no define criterios formales para validar las fuentes de datos ni para priorizar los eventos de seguridad. En ausencia de esos parámetros, los analistas responden de forma reactiva ante cada amenaza sin un marco que estructure sus decisiones.

El organismo no brinda cobertura integral de seguridad informática a la totalidad de las dependencias alcanzadas por la normativa vigente, pese a que la Resolución N°177/ASInf/13 establece la aplicación del marco de seguridad informática para todo el ámbito del GCBA.

La operación independiente de los dispositivos fragmenta la visibilidad del estado de seguridad y acota la capacidad del organismo para demostrar la coordinación entre herramientas.

- ✓ Las estadísticas de incidentes y las clasificaciones de impacto permanecen como información aislada dentro del organismo, ya que la entidad no incorpora métricas de respuesta técnica en la gestión del área.

La ausencia de un marco de control unificado resta valor a estos registros para la mitigación preventiva de los riesgos en ciberseguridad.

La DGSEI registra los incidentes, pero no evidencia que esa información haya sido utilizada para tomar decisiones de gestión ni que los controles se ajusten a los objetivos definidos durante el período auditado.

Conclusión/Dictamen: La Dirección General de Seguridad Informática opera las plataformas que detectan ataques, bloquean accesos indebidos y sostienen disponibles los servicios digitales del Gobierno de la Ciudad. También administra la infraestructura de monitoreo que sostiene esas tareas. El canal BA-CSIRT, por su parte, recibe y gestiona las denuncias de incidentes de seguridad que presentan los ciudadanos.

Aunque el organismo informó que esas herramientas operaron con normalidad durante el período analizado, el examen realizado identificó debilidades en la organización interna y en la documentación que respalda la gestión.

Ante un incidente crítico, no se encuentra definido quién aprueba la acción, quién autoriza los recursos económicos de emergencia ni bajo qué criterios se escala

el caso. La misma falta de definición aparece en otros aspectos de la gestión. Tampoco hay un plan estratégico aprobado ni acuerdos que determinen los servicios que el área presta a otras reparticiones del Gobierno.

El organismo no incorpora, en sus contrataciones de tecnología, la exigencia de garantías de control de accesos al proveedor. El organismo no acredita, con documentación propia, la verificación del estándar de protección de datos personales, la evaluación técnica de las herramientas de seguridad que incorpora ni los controles sobre sus interfaces de programación. El organismo no actualizó el inventario de sus equipos sensibles, como los sistemas de control biométrico y la plataforma de firma digital. La documentación aportada en el descargo solo permitió acreditar algunos aspectos, como determinadas cláusulas contractuales incorporadas en las contrataciones de servicios de seguridad.

En la operación diaria, el área no documenta las verificaciones que realiza sobre sus componentes críticos ni dispone de una guía común que indique cómo debe actuar cada sector técnico ante un mismo tipo de incidente. Tampoco definió los tiempos máximos de interrupción de un servicio ni el nivel de pérdida de información admisible. La forma en que interactúan los dispositivos de detección y respuesta no está definida en ningún documento.

El organismo no acreditó que la cobertura de seguridad alcance a todas las dependencias que la normativa vigente obliga a proteger, ni que la información obtenida de los incidentes se utilice para orientar decisiones de gestión. Estas deficiencias generan riesgos concretos: ante un incidente real, los distintos sectores podrían actuar sin coordinación y sin criterios comunes de respuesta.

Con el inventario actualizado y clasificado según su criticidad, el área podrá incorporar esos datos a la plataforma de respuesta automatizada y priorizar con mayor rapidez los sistemas más sensibles del Gobierno.

El equipo de auditoría cumplió con el objetivo previsto mediante los procedimientos aplicados, sin que se presentaran limitaciones que afectaran el desarrollo del examen.

Las tareas de auditoría culminaron en julio de 2026.

Palabras Claves: Agencia, seguridad, prevención, concientización.

Proyecto: 10.26.01	¡Error! Marcador no definido.
AUDITORÍA GENERAL.....	¡Error! Marcador no definido.
I. OBJETO DE AUDITORIA	12
II. OBJETIVO DE LA AUDITORIA	12
III. ALCANCE DEL EXAMEN	12
1. Marco Normativo	13
2. Procedimientos realizados.....	13
IV. LIMITACIONES AL ALCANCE	14
V. ACLARACIONES PREVIAS	14
1. Gobernanza, marco normativo y dirección estratégica.....	14
1.1. Marco normativo, estructura y competencias institucionales	14
1.2. Autoridad, atribuciones y roles institucionales.....	18
1.3. Estrategia de seguridad, objetivos formalizados y planificación institucional	19
1.4. Gestión de acuerdos de servicio y cobertura	20
1.5. Programas de formación y campañas de ciberseguridad	21
1.6. Estructura de personal, capacitación y modalidad operativa	27
2. Gestión de proveedores y seguridad operativa	28
2.1. Contrataciones y gestión de proveedores	28
2.2. Cumplimiento del Estándar de Seguridad ES0902 y supervisión	31
2.3. Ciclo de vida de los sistemas y trazabilidad documental.....	32
2.4. Desarrollo seguro, cambios y control del ciclo de vida.....	36
2.5. Análisis de vulnerabilidades y control de preproducción	37
3. Gestión de activos, identidad digital y administración de accesos.....	37
3.1. Inventario de activos, clasificación y roles de custodia	37
3.2. Controles de autenticación y acceso.....	40
3.3. Autenticación, identidad digital e interoperabilidad segura.....	41
3.4. Infraestructura y segmentación de seguridad	51
3.5. Coordinación técnica entre herramientas de seguridad	53
3.6. Comunicación y coordinación operativa.....	53
4. Gestión de incidentes, vulnerabilidades y operación de seguridad	54
4.1. Gestión y mitigación de vulnerabilidades	54
4.2. Operación y seguimiento de incidentes.....	55
4.3. Niveles de servicio y cumplimiento operativo	60
4.4. Análisis y respuesta ante incidentes	62

4.5. Resguardo y control de evidencias	63
5. Monitoreo, continuidad y gobernanza operativa	63
5.1. Continuidad y recuperación de servicios.....	63
5.2. Indicadores y control operativo	64
VI. OBSERVACIONES	68
Observación N°1	68
Observación N°2	68
Observación N°3	69
Observación N°4	69
Observación N°5	69
Observación N°6	70
Observación N°7	70
Observación N°8	70
Observación N°9	71
Observación N°10	71
Observación N°11	72
Observación N°12	72
Observación N°13	72
Observación N°14	73
VII. RECOMENDACIONES	74
Recomendación N°1	74
Recomendación N°2	74
Recomendación N°3	75
Recomendación N°4	75
Recomendación N°5	75
Recomendación N°6	76
Recomendación N°7	76
Recomendación N°8	77
Recomendación N°9	77
Recomendación N°10	78
Recomendación N°11	78
Recomendación N°12	78
Recomendación N°13	79
Recomendación N°14	79
VIII. CONCLUSIONES	81
ANEXO I	82

ANEXO II	83
ANEXO III	84
ANEXO IV	85
1. Dirección General de Seguridad Informática (DGSEI)	85
1.1. Gerencia Operativa Centro de Ciberseguridad	85
1.2. Gerencia Operativa Seguridad de la Información	86
1.2.1. Subgerencia Operativa Accesos e Infraestructura de Seguridad	87
1.2.2. Subgerencia Operativa Monitoreo, Prevención y Detección	87
1.2.3. Subgerencia Operativa Identidad Digital	87
ANEXO V	88
ANEXO VI	88
ANEXO VII	88
ANEXO VIII	89
ANEXO IX	89
ANEXO X	90
ANEXO XI	95

INFORME FINAL DE AUDITORÍA
“SEGURIDAD DE LA INFORMACIÓN”
PROYECTO N° 10.26.01

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 N°70 de la Ciudad Autónoma de Buenos Aires, y conforme a lo dispuesto en el artículo 135 de la Constitución de la Ciudad, la Auditoría General de la Ciudad de Buenos Aires ha procedido a efectuar una auditoría de sistemas en el ámbito de la Dirección General de Seguridad Informática.

I. OBJETO DE AUDITORIA

Jurisdicción 21 - Entidad 270 - Unidad Ejecutora 687.

II. OBJETIVO DE LA AUDITORIA

Evaluar los procesos implementados para la detección, clasificación, prevención y las acciones correctivas destinadas a los incidentes de seguridad de la información. Implementación de planes de concientización, prevención y divulgación. Impacto por la criticidad de los datos gestionados.

III. ALCANCE DEL EXAMEN

Analizar los procedimientos establecidos para la gestión completa de los incidentes de seguridad, desde su identificación hasta las acciones correctivas, abarcando la revisión de los planes de concientización y la validación de la clasificación de la criticidad de la información administrada.

1. Marco Normativo

El marco metodológico de la auditoría incluyó las Normas Básicas de Auditoría Externa de la AGCBA,¹ las Normas Básicas de Auditoría de Sistemas de la AGCBA,² la Ley N°70 CABA, la Ley N°325 CABA y sus normas complementarias, además de los Estándares de la Agencia de Sistemas de Información (ASInf).³

El equipo evaluó los sistemas informáticos específicamente bajo el Marco de Referencia COBIT 2019, Capítulo Buenos Aires.⁴ (ANEXO I)

2. Procedimientos realizados

El equipo de auditoría recopiló información de sitios oficiales del Gobierno de la Ciudad Autónoma de Buenos Aires relacionada con la Dirección General de Seguridad Informática (DGSEI).

Remitió comunicación formal a la DGSEI para informar el inicio del proyecto de auditoría.

Durante el relevamiento, entrevistó a personal de la DGSEI y a los especialistas encargados de aplicar los protocolos de seguridad

Se evaluaron las áreas y los sistemas de seguridad para establecer el marco operativo del proyecto de auditoría.

La información recopilada sirvió para estructurar el plan de trabajo y asignar los roles según la especialización de cada auditor.

Se efectuó un pedido de documentación relativa al marco normativo, la estructura jerárquica y el presupuesto detallado de la Dirección, incluyendo la matriz de responsabilidades, la composición del Comité de Seguridad y los funcionarios encargados de la aceptación formal de los riesgos.

Se solicitó el detalle del modelo de gobierno y gestión tecnológica, así como los objetivos estratégicos de los sistemas, comprendiendo las matrices de riesgos, métricas de desempeño y gestión, procesos de monitoreo y los estudios de factibilidad técnica que sustentan la operación actual.

Se requirió el detalle del capital humano afectado y de los servicios prestados, especificando perfiles técnicos, antecedentes, registros de capacitación y los mecanismos de interacción operativa con el Ministerio de Seguridad.

¹ Normas Básicas de Auditoría Externa de AGCBA. Obtenido el año 2024 en: <https://n9.cl/6um33> [Accedido el 3/3/26]

² Normas Básicas de Auditoría de Sistemas. Obtenido el mes de octubre del año 2000 en: <https://n9.cl/89yuy> [Accedido el 3/3/26]

³ Estándares de la Agencia de Sistemas de Información. Obtenido el año 2026 en: <https://n9.cl/uwqpb5> [Accedido el 3/3/26]

⁴ Normas COBIT 2019. Obtenido el año 2019 en: <https://www.isaca.org/resources/cobit> [Accedido el 3/3/26]

El equipo auditor pidió los registros vinculados a la integridad técnica y la capacidad de recuperación del área, comprendiendo auditorías realizadas, metodologías de desarrollo seguro, gestión de activos críticos, políticas de respaldo y acciones de concientización ciudadana.

Se requirió el aporte de los Acuerdos de Nivel de Servicio (SLA), destinados a establecer métricas de rendimiento, disponibilidad de los servicios tecnológicos y de los Acuerdos de Nivel Operativo (OLA), orientados a formalizar la articulación técnica entre las áreas internas para garantizar dichos niveles. También se solicitó la constancia de inscripción y actualización conforme a la Ley CABA de Protección de Datos Personales N°1.845/05.⁵

La auditoría solicitó que se especificaran los aspectos vinculados a la seguridad, contingencias, gestión de riesgos, administración de recursos, rendimiento y calidad de los sistemas.

Los datos relevados orientaron la selección de los procedimientos técnicos aplicados en las etapas siguientes.

El equipo auditor realizó una visita técnica presencial a la Dirección General de Seguridad Informática con el fin de complementar el análisis documental y las entrevistas efectuadas. La visita permitió obtener evidencia directa sobre el entorno de control. El análisis técnico específico se realizó por separado, a partir de la documentación relevada.

Las tareas de auditoría comenzaron en enero de 2026.

IV. LIMITACIONES AL ALCANCE

Sin limitaciones.

V. ACLARACIONES PREVIAS

Las secciones siguientes adoptan una estructura analítica común: presentación del marco regulatorio aplicable, descripción de lo informado por el organismo auditado, análisis de los elementos relevados y, cuando corresponde, remisión a la observación formal.

Esta organización facilita la lectura sistemática del informe y la verificación de la trazabilidad entre la evidencia y el hallazgo.

1. Gobernanza, marco normativo y dirección estratégica

1.1. Marco normativo, estructura y competencias institucionales

⁵ Ley N°1.845/05. Obtenido el día 24 de noviembre del año 2005 en: <https://n9.cl/is7bi> [Accedido el 3/3/26]

La Agencia de Sistemas de Información (ASInf) fue creada por la Ley N°2.689⁶ como entidad autárquica en el orden administrativo, funcional y financiero, en el ámbito de la Jefatura de Gabinete de Ministros de la Ciudad Autónoma de Buenos Aires, según el texto normativo vigente consolidado por la Ley N°6.764.⁷

El organismo fue creado con el propósito de ordenar la gestión tecnológica del Estado y garantizar el acceso ciudadano a la información.

La Agencia asumió el rol de órgano rector en Tecnologías de la Información y las Comunicaciones del Poder Ejecutivo de la Ciudad. Sus funciones incluyen coordinar la infraestructura informática, las telecomunicaciones y los sistemas utilizados por las dependencias del GCBA. x

La Agencia implementó medidas destinadas a ordenar la operación tecnológica y reforzar los controles de seguridad informática del Gobierno de la Ciudad.

La centralización de la infraestructura, la estandarización de compras y la publicación de normas técnicas constituyen los avances más relevantes del período.

Con relación a la remisión del cuerpo normativo y procedimental de seguridad de la información para el período 2025, la Dirección indicó que esta documentación se encuentra publicada en el sitio web oficial del Gobierno de la Ciudad Autónoma de Buenos Aires, en la sección de la Agencia de Sistemas de Información.⁸

La documentación define normas de seguridad, procesos administrativos y protocolos para el tratamiento de incidentes.

La publicación en línea evita que las áreas tengan que gestionar pedidos formales para acceder a los lineamientos vigentes.

En el año 2024, el Director Ejecutivo de la Agencia de Sistemas de Información, entidad autárquica con rango de organismo fuera de nivel en el ámbito de la Jefatura de Gabinete de Ministros, modificó su estructura organizativa mediante la Resolución N°118/ASInf/24.⁹

La nueva estructura entró en vigencia el 1° de junio de 2024, definió el organigrama y estableció las responsabilidades de cada área, dejando parcialmente sin efecto la Resolución N°17/ASInf/08,¹⁰ según lo previsto en el (ANEXO II).

⁶ Ley N°2.689/GCBA/08. Obtenido el día 21 de mayo del año 2008 en: <https://n9.cl/m2ub6> [Accedido el 3/3/26]

⁷ Ley N°6.764/GCBA/24. Obtenido el día 28 de noviembre del año 2024 en: <https://n9.cl/Oddm0v> [Accedido el 3/3/26]

⁸ Estándares y Procesos, Agencia de Sistemas de Información. Obtenido el día 3 de junio de 2025 en: <https://n9.cl/s2m1r> [Accedido el 3/3/26]

⁹ Resolución N°118/ASInf/24. Obtenido el día 5 de junio del año 2024 en: <https://n9.cl/6o9df> [Accedido el 3/3/26]

¹⁰ Resolución N°17/ASInf/08. Obtenido el día 8 de julio del año 2008 en: <https://n9.cl/za5exk> [Accedido el 3/3/26]

El organigrama, definido en el Anexo I de la Resolución N°118/ASInf/24, estableció la Dirección General de Seguridad Informática, la Dirección General Técnica, Administrativa y Legal, la Dirección General Infraestructura y la Dirección General Integración de Sistemas.

La Dirección General de Seguridad Informática tiene bajo su órbita a la Gerencia Operativa Centro de Ciberseguridad y a la Gerencia Operativa Seguridad de la Información. Esta última comprende la Subgerencia Operativa Accesos e Infraestructura de Seguridad, la Subgerencia Operativa Monitoreo, Prevención y Detección y la Subgerencia Operativa Identidad Digital, tal como se expone en el (ANEXO III).

En la Resolución recién mencionada, se detallan las responsabilidades primarias asignadas a la Dirección General de Seguridad Informática, así como a sus Gerencias y Subgerencias Operativas, en los términos previstos en el (ANEXO IV) de la citada resolución.

En el presupuesto correspondiente al año 2025, en las Planillas Anexas, se asigna a la Dirección General de Seguridad Informática, dependiente de la Agencia de Sistemas de Información, mediante la Jurisdicción 21, Entidad 270, Unidad Ejecutora 687, la suma de \$ 8.219.811.736¹¹ según consta en el (ANEXO V).

En cumplimiento de las directrices emanadas del Plan Plurianual de Inversiones Públicas para el trienio 2025-2027, se han programado y asignado a la citada Dirección General, dentro del presupuesto correspondiente al ejercicio fiscal 2025, recursos de inversión que alcanzan la cifra de \$ 3.937.806.057, de acuerdo con el (ANEXO VI).

Respecto del Proyecto de Presupuesto para el ejercicio 2025, la composición de recursos por Fuente de Financiamiento se detalla en el (ANEXO VII).

La asignación presupuestaria de la Jurisdicción 21 se distribuye en cuatro incisos, conforme a la normativa de los Presupuestos Jurisdiccionales:

- Gastos en personal: \$ 972.475.523.
- Bienes de consumo: \$ 51.069.985.
- Servicios no personales: \$ 7.041.175.037.
- Bienes de uso: \$ 155.091.191.

Lo que representa un presupuesto total asignado de \$ 8.219.811.736, conforme a la sumatoria de los incisos presupuestarios detallados en el (ANEXO VIII).

Las Planillas Anexas del Presupuesto 2025 de la Ciudad Autónoma de Buenos Aires detallan la Producción Pública por Proyecto. El documento especifica el producto y las unidades de medida asignadas a la Dirección General de Seguridad Informática. Esta información técnica se encuentra disponible para su consulta en el (ANEXO IX).

¹¹ Decreto N°12/GCBA/25. Distribución Administrativa de Créditos. Obtenido el día 7 de enero del año 2025 en: <https://n9.cl/p3fr6> [Accedido el 3/3/26]

La DGSEI aportó el detalle del presupuesto financiero para 2025. El crédito original aprobado ascendió a \$8.219.811.736, conforme las Planillas Anexas del Presupuesto.

El crédito vigente al cierre del ejercicio alcanzó \$8.686.880.456,75, cifra que refleja las modificaciones presupuestarias registradas durante el período, entre las cuales se informó una transferencia de \$38.000.000 efectuada por la Agencia de Sistemas de Información bajo el concepto de Caja Chica Especial de Certificados y Dominios, imputada a la Jurisdicción 21, Unidad Ejecutora N°687 y Beneficiario N°193.900.

El Cuadro N°1 detalla la clasificación presupuestaria por jurisdicción, entidad, unidad ejecutora, programa, inciso, concepto del gasto, crédito vigente y monto devengado.

Jur	Entidad	Unidad Ejecutora	Programa	Inc.	Descripción	Vigente	Devengado
21	270	687	98	1	Gastos en Personal	1.206.259.627	1.206.259.620,79
21	270	687	98	2	Bienes de Consumo	644.968	644.967,50
21	270	687	98	3	Servicios No Personales	7.413.490.650	7.413.490.646,93
21	270	687	98	4	Bienes de Uso	66.485.225	66.485.221,53
						8.686.880.470	8.686.880.456,75

Fuente: DGSEI

La Dirección General de Seguridad Informática responde directamente a la Dirección Ejecutiva de la Agencia de Sistemas de Información.

La Agencia establece las políticas y estándares técnicos del Poder Ejecutivo de la ciudad. Para ello, su personal técnico define los métodos de gestión de proyectos y las pautas de desarrollo de software aplicables. El organismo también coordina la infraestructura tecnológica y las telecomunicaciones con el fin de integrar los sistemas de forma segura, facilitando los trámites de los ciudadanos y la rendición de cuentas de la institución.

La Dirección General de Seguridad Informática informó que no posee bajo su custodia los esquemas de funcionamiento, la arquitectura ni los módulos funcionales de los sistemas informáticos de seguridad, ni participa en la generación de código fuente, en la elaboración de guías de usuario o en la ejecución de los controles automáticos de integridad de la información.

Su actuación se centra en definir políticas, lineamientos y criterios generales de seguridad, supervisar el cumplimiento normativo y gestionar los controles relacionados con el acceso, monitoreo y resguardo de los activos tecnológicos.

La documentación técnica, los diagramas de flujo y entidad-relación, así como la administración de integraciones entre sistemas y la gestión de infraestructuras administradas por terceros, corresponden a la Dirección General de Integración de Sistemas y otras áreas responsables del desarrollo, implementación y operación de los sistemas.

Estas áreas son responsables de definir la arquitectura, estructurar los módulos funcionales, gestionar los perfiles de usuario, garantizar la integridad de los datos y mantener disponible la documentación operativa y técnica.

Dado el objeto y alcance de la auditoría, el equipo no identificó desviaciones atribuibles a la DGSEI en estas actividades. La Dirección actúa como referente normativo, estableciendo criterios y marcos de seguridad que deben cumplir los entornos tecnológicos.

La Dirección General de Seguridad Informática define los requisitos y controles de seguridad aplicables a los procesos de integración entre sistemas, sin intervenir en su planificación, desarrollo ni administración operativa. Esas funciones corresponden a las áreas responsables de las soluciones tecnológicas dentro de la Agencia.

La Dirección General de Seguridad Informática comunica sus objetivos y lineamientos mediante la página oficial del GCBA (https://buenosaires.gob.ar/gcaba_historico/jefaturadegabinete/centro-de-ciberseguridad) y su cuenta institucional @bacsirt.

Por esos canales, el área difunde contenidos sobre sus actividades, alertas de seguridad, recomendaciones de prevención y acciones de concientización en seguridad de la información.

En colaboración con el equipo de comunicación de la Secretaría de Innovación y Transformación Digital, se desarrollan estrategias de comunicación dirigidas al personal del GCBA.

El objetivo declarado es que el personal del GCBA conozca y aplique medidas básicas de prevención ante incidentes.

El análisis no arrojó hallazgos en este aspecto dentro del período auditado.

1.2. Autoridad, atribuciones y roles institucionales

La Agencia de Sistemas de Información remitió la resolución de designación del Director General y la normativa que define las responsabilidades generales del área.

Las normas analizadas establecen competencias generales de seguridad informática y monitoreo, pero omiten la definición de atribuciones operativas para la gestión formal de incidentes.

El marco regulatorio vigente carece de delimitaciones explícitas respecto a la competencia jerárquica para la aprobación de decisiones críticas, la aceptación formal de riesgos latentes y la emisión de comunicaciones institucionales.

Se constató la ausencia de mecanismos formalizados para el escalamiento operativo y la priorización de recursos críticos en función de la severidad del impacto.

El análisis del cuerpo normativo no identificó definiciones expresas de atribuciones operativas para la gestión formal de incidentes. Los desvíos verificados se desarrollan en la Observación N°1.

En el descargo, la Dirección General de Seguridad Informática reiteró la normativa ya reseñada en el punto 1.1 y sostuvo que sus disposiciones delimitan las competencias y responsabilidades en materia de gestión de incidentes.

La Dirección aceptó, no obstante, la ausencia de una atribución formal para tomar decisiones ante incidentes de seguridad, tal como se señala en el punto 1.2, y se comprometió a avanzar con el acto administrativo correspondiente. El descargo no incorporó información sobre la autoridad para reasignar recursos económicos ni sobre los umbrales de escalamiento técnico.

1.3. Estrategia de seguridad, objetivos formalizados y planificación institucional

En lo referente a la estructura de gobierno y coordinación de la seguridad de la información, la Dirección General de Seguridad Informática manifestó que el Comité de Seguridad de la Información no se encuentra formalmente constituido como instancia permanente.

La gestión de seguridad se articula a través del BA-CSIRT.¹² Ante incidentes que lo exigen, el área convoca instancias de coordinación con participación de las áreas involucradas.

En este escenario operativo, el BA-CSIRT aplica protocolos de actuación auditados y respaldados por el Forum of Incident Response and Security Teams (FIRST).¹³

Se consultó al área quién estableció los objetivos estratégicos de los sistemas bajo su responsabilidad. El requerimiento buscó identificar si dichos objetivos fueron establecidos por el Gobierno de la Ciudad Autónoma de Buenos Aires, por la Agencia de Sistemas de Información o por la propia Dirección General de Seguridad Informática.

La Dirección informó que definió objetivos estratégicos junto con la Dirección Ejecutiva de la Agencia, aunque no aportó actas, planes, resoluciones ni documentación que permita verificar su aprobación formal, los responsables intervinientes o los criterios utilizados para su validación.

¹² BA-CSIRT (Buenos Aires Computer Security Incident Response Team) es el equipo del Gobierno de la Ciudad de Buenos Aires encargado de gestionar, analizar y responder ante incidentes de seguridad de la información que afecten sus sistemas y servicios tecnológicos.

¹³ Organización internacional que agrupa equipos de respuesta ante incidentes para mitigar ciberamenazas globales. Define estándares técnicos y audita protocolos de seguridad bajo normas globales para fortalecer la cooperación entre sus miembros.

Se indicó que esta definición se realizó con el fin de establecer la mejor estrategia para la protección de la información y de los activos tecnológicos del GCBA.

El material remitido menciona la intervención conjunta, pero el equipo no encontró documentación que respalde su formalización ni la aprobación institucional de los objetivos.

Además, no se presentó información que permita verificar cómo se alinean estos objetivos con los lineamientos estratégicos del Gobierno de la Ciudad Autónoma de Buenos Aires o con las políticas generales de la Agencia de Sistemas de Información en materia de seguridad de la información.

La definición y gestión de los objetivos de la Dirección General de Seguridad Informática se realiza a partir de la intervención del Director del área junto con la Dirección Ejecutiva de la Agencia de Sistemas de Información. Esas definiciones buscan garantizar el cumplimiento de los objetivos y responsabilidades primarias del área.

La evidencia presentada indica quiénes intervienen, pero omite cómo se establecen los objetivos y quién valida su aprobación. El equipo no encontró criterios de aceptación ni registros que respalden el proceso.

Durante el período analizado, el área desarrolló acciones de concientización y divulgación en seguridad de la información, con campañas y capacitaciones dirigidas a distintos públicos. Las iniciativas también difundieron prácticas de ciberseguridad entre la comunidad educativa y el personal del Gobierno.

Los registros disponibles no permiten confirmar la existencia de un plan de divulgación estructurado. Los lineamientos relevados se limitan a señalar la necesidad de actualizar los sistemas y ampliar las zonas de seguridad interna, sin precisar quién ejecuta cada acción, en qué plazo ni bajo qué criterios de evaluación.

El área informó actualizaciones, aunque no aportó documentación que permita verificar los cambios aplicados. Esa constatación origina la Observación N°2.

En el descargo, el organismo sostuvo que gestionó objetivos y líneas de acción propias durante el período auditado y detalló campañas de concientización, capacitaciones y fortalecimiento del monitoreo como parte de esa gestión.

Señaló también que siguió el avance de esas iniciativas con tableros de control e informes periódicos. La Dirección no acompañó actas, cronogramas ni indicadores que permitan verificar esas afirmaciones.

Reconoció que aún no cuenta con un instrumento formal de planificación estratégica y manifestó su compromiso de elaborarlo durante el segundo semestre del año, con aprobación de la Dirección Ejecutiva.

1.4. Gestión de acuerdos de servicio y cobertura

La Dirección General de Seguridad Informática no recibe servicios de seguridad de la información prestados por organismos externos al Gobierno de la Ciudad Autónoma de Buenos Aires.

No se registran acuerdos de colaboración, convenios interinstitucionales ni acuerdos de nivel de servicio vinculados a estas actividades. El alcance de los servicios de seguridad de la información queda así delimitado para el período auditado.

El material evaluado se concentra en acciones de comunicación y concientización, sin permitir identificar con precisión los servicios de seguridad informática brindados por la Dirección a las reparticiones del GCBA, los sistemas utilizados, las capacidades técnicas asociadas o los acuerdos de servicio vigentes para el año 2025.

El equipo formuló la Observación N°3 en función de esos desvíos.

En el descargo, la Dirección General de Seguridad Informática señaló que sus prestaciones se encuentran definidas y respaldadas por la Resolución N°118/ASInf/24, que fija las responsabilidades primarias del área y los procedimientos operativos aplicables.

Indicó también que los Acuerdos de Nivel de Servicio se encuentran formalmente parametrizados y administrados mediante el sistema de gestión de la Agencia, con categorías de atención, prioridades y plazos de respuesta y resolución.

La Dirección no acompañó documentación, reportes ni capturas de ese sistema que permitan verificar esas afirmaciones, por lo que la observación se mantiene. El organismo agregó que continuará trabajando para consolidar la documentación de sus servicios y de los niveles de servicio asociados.

1.5. Programas de formación y campañas de ciberseguridad

El área complementa los servicios operativos descriptos con acciones de concientización, capacitación y divulgación en ciberseguridad.

La documentación presentada expone las acciones de comunicación, capacitación y divulgación realizadas por el BA-CSIRT. Estas acciones incluyen campañas de concientización, talleres, jornadas de capacitación y participación en eventos de seguridad informática.

Las actividades apuntan a reducir incidentes de seguridad, fomentar prácticas seguras y difundir criterios básicos de ciberseguridad dentro del GCBA y hacia la ciudadanía.

Se utilizan diferentes medios para su difusión, tales como las redes sociales oficiales, sitios web institucionales, la plataforma BOTI y materiales audiovisuales en medios públicos.

En términos generales, estas iniciativas integran una serie de programas de comunicación, capacitación y divulgación orientados a la seguridad de la información, destacando las siguientes acciones:

- Servicios de comunicación, concientización y divulgación en ciberseguridad.

Durante el año 2025, el Centro de Respuesta ante Incidentes de Seguridad Informática de la Ciudad de Buenos Aires (BA-CSIRT), dependiente de la Dirección General de Seguridad Informática, brindó a distintas reparticiones del Gobierno de la Ciudad, servicios de concientización, divulgación y apoyo comunicacional en materia de seguridad de la información, en el marco de los acuerdos de servicio y de las funciones propias del Centro de Ciberseguridad.

Estos servicios tuvieron como objetivo prevenir incidentes de seguridad, fortalecer el uso seguro de las tecnologías y promover la cultura de la ciberseguridad tanto en el ámbito laboral como ciudadano.

- Campañas de concientización en ciberseguridad.

Se desarrollaron y difundieron campañas comunicacionales orientadas a empleados y ciudadanía, abordando temáticas vinculadas a buenas prácticas de seguridad, prevención de fraudes, protección de datos personales e ingeniería social.

Sistemas y canales involucrados:

- ✓ Redes sociales oficiales del BA-CSIRT.
- ✓ Redes sociales oficiales TecBA, utilizadas para la difusión de innovación, asistencia técnica y vinculación tecnológica empresarial.
- ✓ Plataforma BOTI, canal de atención y difusión.
- ✓ Sitio web institucional del BA-CSIRT.
- ✓ Sitios web institucionales.
- ✓ Cápsula de medios en televisión pública y de aire.

Capacidades técnicas: Producción de contenidos gráficos, audiovisuales y textos divulgativos. Adaptación del lenguaje técnico a formatos accesibles para públicos no especializados. Lineamientos editoriales y de tono comunicacional definidos por el BA-CSIRT.

Periodicidad: Continua, conforme a la planificación anual de campañas y a requerimientos específicos de las reparticiones.

- Capacitaciones, charlas y actividades de divulgación.

El BA-CSIRT brindó capacitaciones, talleres y charlas de concientización en ciberseguridad destinadas a empleados públicos, instituciones educativas y otros públicos específicos, en articulación con distintas reparticiones.

Sistemas involucrados:

- ✓ Plataformas de capacitación y materiales educativos.
- ✓ Presentaciones institucionales y contenidos multimedia.

Capacidades técnicas:

- ✓ Diseño de contenidos educativos en ciberseguridad.
- ✓ Ejecución de charlas presenciales y virtuales.
- ✓ Difusión de recomendaciones prácticas y preventivas.

Periodicidad: A demanda y según el cronograma anual de actividades de capacitación.

- Eventos y jornadas de ciberseguridad.

Se organizaron y coordinaron eventos y jornadas de ciberseguridad ciudadana, tales como CyberCity 2025¹⁴ y la participación del Centro de Respuesta ante Incidentes de Seguridad Informática de la Ciudad de Buenos Aires (BA-CSIRT) en eventos especializados, con el fin de ampliar el alcance de la concientización y promover la participación de distintos actores.

Sistemas y soportes involucrados:

- ✓ Materiales gráficos y audiovisuales.
- ✓ Canales digitales de difusión institucional.

Capacidades técnicas:

- ✓ Planificación de estrategias de comunicación del evento.
- ✓ Producción de piezas de difusión y contenidos educativos.
- ✓ Articulación con otras áreas y organismos.

Periodicidad: Según la planificación anual y cronograma de eventos.

- Lineamientos comunicacionales en seguridad.

El BA-CSIRT definió y aplicó lineamientos de tono, estilo y terminología para las comunicaciones vinculadas con ciberseguridad, con el objetivo de garantizar mensajes claros, preventivos y accesibles, alineados con la identidad institucional del Gobierno de la Ciudad Autónoma de Buenos Aires.

¹⁴ CyberCity 2025. Obtenido el día 30 de abril del año 2025 en: <https://n9.cl/kmzg3> [Accedido el 3/3/26]

Periodicidad: Permanente, como marco transversal de todas las acciones comunicacionales.

A continuación, se describen las acciones específicas vinculadas a la realización de eventos y actividades de divulgación.

Se realizaron eventos, jornadas y charlas de ciberseguridad ciudadana, orientadas a distintos públicos, con el fin de ampliar el alcance de la concientización y fomentar la participación de la comunidad.

Entre estas acciones se incluyen las jornadas y eventos de alcance masivo, así como actividades educativas y participativas.

Alcance del servicio:

- Divulgación y educación en ciberseguridad.
- Interacción directa con la ciudadanía.
- Promoción de la prevención y el reporte de incidentes.

Estas acciones corresponden a servicios de divulgación, no a la gestión directa de incidentes.

Como parte de las estrategias de prevención y fortalecimiento de capacidades en seguridad de la información, se llevaron adelante acciones de capacitación y divulgación en distintos ámbitos durante el año 2025.

Estas intervenciones abarcaron entornos educativos, con actividades dirigidas a familias y referentes pedagógicos, así como espacios sociales asociados a programas de acompañamiento a jóvenes, en articulación con el ámbito judicial. En el plano organizacional, se brindaron capacitaciones al personal de la Agencia de Sistemas de Información y sectores vinculados.

La documentación remitida describe actividades y registra comentarios favorables de los participantes, pero no incluye métricas de resultado.

La documentación indica que los asistentes valoraron la experiencia y manifestaron interés en ampliar los temas tratados.

Las actividades de concientización, prevención y divulgación se actualizan en función de la demanda operativa y de la planificación de las acciones a desarrollar, incorporando insumos derivados tanto de incidentes reales gestionados como de los resultados obtenidos en distintas instancias de evaluación.

Los talleres, capacitaciones y publicaciones incluyen los errores frecuentes detectados, patrones de comportamiento observados y recomendaciones específicas para usuarios, áreas del Gobierno de la Ciudad de Buenos Aires y la ciudadanía.

Para la elaboración de estos contenidos, se utiliza información estadística consolidada y actualizada al período inmediato anterior a cada actividad, lo que

permite alinear los mensajes con el contexto de amenazas vigentes y con las principales problemáticas detectadas.

El área declaró que utiliza la información relevada para ajustar los contenidos y enfoques de sus actividades de prevención. El criterio de priorización considera la recurrencia de los incidentes, su impacto y el nivel de exposición de los usuarios.

Por razones de seguridad operativa, la información se presenta de forma agregada.

Como componente específico de estos programas, la Dirección General de Seguridad Informática diseñó e implementó durante 2024 y 2025 campañas periódicas de simulación de suplantación de identidad orientadas a medir la exposición del factor humano, generar indicadores de riesgo, identificar niveles de vulnerabilidad por grupos de usuarios y definir acciones de capacitación y mejora continua.

Los resultados obtenidos, la metodología aplicada y las medidas de refuerzo implementadas se detallan a continuación.

- Contexto (2024 - 2025):
 - ✓ En 2024 se diseñó un Plan Integral de concientización interna orientado a reducir los riesgos asociados al factor humano.
 - ✓ Se definieron objetivos, indicadores, cronograma e incorporación de herramientas de simulación.
 - ✓ En 2025 se implementó el plan mediante campañas de simulación de suplantación de identidad y acciones de concientización, generando resultados medibles.
- Metodología y criterios técnicos:
 - ✓ Enfoque preventivo centrado en el comportamiento de los usuarios.
 - ✓ Definición de escenarios realistas de ataque.
 - ✓ Simulaciones con múltiples variantes para evitar el aprendizaje repetitivo.
 - ✓ Segmentación de usuarios por grupos.
 - ✓ Medición de indicadores como apertura, clic y nivel de riesgo.
 - ✓ Evaluaciones trimestrales.
 - ✓ Uso de resultados para orientar las capacitaciones.
- Objetivos e indicadores (2024):
 - ✓ Promover hábitos seguros en ciberseguridad.
 - ✓ Proteger activos digitales y datos sensibles.
 - ✓ Reducir incidentes y brechas de seguridad.
 - ✓ Mejorar estándares de seguridad.

- ✓ Indicadores previstos:
 - Reducción del 15% en incumplimientos de políticas y evaluaciones desaprobadas.
 - Reducción del 20% en apertura de correos maliciosos.
 - Adecuación al uso de correo institucional.
- Resultados (2025):
 - ✓ Las campañas iniciales de simulación de suplantación de identidad registraron niveles de riesgo humano que oscilaron entre el 4,6% y el 56,6%, evidenciando una dispersión significativa entre reparticiones. Esa disparidad demanda intervenciones diferenciadas, no campañas de concientización uniformes.
 - ✓ En el segundo semestre:
 - Tasas de apertura superiores al 50%, lo que indica que más de la mitad de los usuarios interactuó inicialmente con el correo simulado, evidenciando un nivel relevante de exposición ante intentos de suplantación de identidad.
 - Tasas de clic cercanas al 30%, reflejando que una proporción significativa de usuarios ejecutó la acción riesgosa (acceder al enlace), aumentando la probabilidad de compromiso de credenciales o ejecución de ataques.
 - Promedio anual de vulnerabilidad del 25%, calculado sobre el total de usuarios participantes en las simulaciones del período, representando el porcentaje que adoptó conductas inseguras e integrando los resultados de todas las reparticiones evaluadas.
- Impacto sobre activos críticos:
 - ✓ Enfoque preventivo orientado a reducir los accesos indebidos y compromiso de credenciales. Apunta a disminuir la probabilidad de que los usuarios otorguen acceso no autorizado, evitando el uso indebido de credenciales válidas por parte de los atacantes.
 - ✓ Identificación de conductas de riesgo que pueden afectar la confidencialidad, integridad y disponibilidad de la información.
 - ✓ No se realiza análisis técnico individual por activo.
- Acciones de refuerzo y capacitación:
 - ✓ Asignación de capacitaciones específicas a usuarios con conductas de riesgo.
 - ✓ Acciones generales de refuerzo para el resto de los usuarios.
 - ✓ Difusión de contenidos educativos.
 - ✓ Seguimiento de métricas para mejora continua.

Como parte de las acciones de concientización, el área ejecutó una campaña de simulación de suplantación de identidad dirigida al personal del Gobierno.

Esta iniciativa permitió analizar el comportamiento de los usuarios frente a correos electrónicos simulados y relevar información sobre los niveles de interacción, las respuestas observadas y los patrones de riesgo asociados al factor humano.

Finalizada la campaña, el área responsable elaboró informes técnicos en los que se consolidaron los resultados obtenidos. Estos documentos incluyeron el análisis de las conductas detectadas, la identificación de tendencias recurrentes y una evaluación general del nivel de exposición, lo que aportó insumos para el abordaje del riesgo vinculado al uso del correo electrónico y a las prácticas de los usuarios.

Los resultados fueron comunicados al Director General de Seguridad Informática, en su carácter de responsable de la gestión integral de los incidentes de seguridad de la información, mediante la remisión de reportes formales y la presentación de conclusiones en instancias de trabajo interno.

El área definió acciones de mejora orientadas a fortalecer la concientización del personal, basadas en los resultados de los informes.

Se impulsaron instancias de capacitación dirigidas a los usuarios, con el objetivo de mejorar la detección temprana de intentos de suplantación de identidad y promover prácticas más seguras en el uso de herramientas digitales. Estas actividades se iniciaron mediante una prueba piloto que validó los contenidos y la metodología, con previsión de extensión progresiva a otras áreas.

En forma complementaria, se dio continuidad a las campañas de simulación como mecanismo de evaluación periódica y mejora continua, orientando los recursos disponibles hacia el sostenimiento de estas iniciativas y al fortalecimiento de la cultura de seguridad.

Como respaldo documental, se cuenta con un informe unificado que consolida los informes técnicos y las presentaciones realizadas, en el cual se reúnen los principales resultados, conclusiones y lineamientos derivados del ejercicio, permitiendo evidenciar la comunicación de los hallazgos y su tratamiento en el ámbito directivo.

Los datos técnicos se exponen sin el nivel de detalle que podría facilitar la identificación de los vectores de ataque.

La documentación examinada no permitió identificar incumplimientos verificables dentro del alcance definido para este apartado.

1.6. Estructura de personal, capacitación y modalidad operativa

El Director General coordina la planificación estratégica con la Dirección Ejecutiva de la Agencia. La DGSEI cuenta con una estructura que asigna roles para la gestión y supervisión de la seguridad de la información, con funciones

que abarcan la conducción, coordinación y supervisión técnica del entorno tecnológico del GCBA.

La estructura incluye los siguientes puestos: Director General de Seguridad Informática; Gerente Operativo del Centro de Ciberseguridad; Gerente Operativo de Seguridad de la Información; Subgerente Operativo de Accesos e Infraestructura de Seguridad; Subgerente Operativo de Monitoreo, Prevención y Detección; y Subgerente Operativo de Identidad Digital. La asignación de cada puesto está formalizada mediante resoluciones de la Agencia de Sistemas de Información que determinan las designaciones y responsabilidades dentro del área.

Las actividades del personal se desarrollan bajo una modalidad combinada de trabajo presencial y remoto.

Para la gestión de las tareas y la comunicación interna se utilizan canales formales institucionales, entre ellos la plataforma NOC, disponible en <https://noc-mesa.buenosaires.gob.ar/>,¹⁵ empleada para la registración, seguimiento y coordinación de solicitudes y requerimientos operativos del área.

Durante el período 2022-2025, el personal participó en instancias de capacitación vinculadas con sus funciones, tanto a través del Instituto Superior de la Carrera como por iniciativa individual.

Algunas de esas actividades integran los programas de formación obligatoria establecidos para el personal del GCBA. La evaluación de competencias se realiza con periodicidad anual, a partir del seguimiento de tareas, el cumplimiento de objetivos y el avance en las metas definidas para cada agente.

Durante el año 2025, parte del personal participó en un entrenamiento técnico de tipo "red team", modalidad que consiste en la simulación controlada de ataques informáticos para evaluar y fortalecer las capacidades de detección, análisis y respuesta frente a amenazas.

La actividad abordó seguridad en aplicaciones web y móviles, gestión de identidades y directorios, e infraestructura tecnológica. La Dirección indicó que ese entrenamiento fortaleció los criterios técnicos del equipo para identificar amenazas y priorizar acciones de mitigación.

El equipo de auditoría tomó conocimiento de la información descripta en el presente apartado. El análisis de este contenido no generó observaciones.

2. Gestión de proveedores y seguridad operativa

2.1. Contrataciones y gestión de proveedores

En el (ANEXO X) se detallan los proveedores externos que brindan servicios de seguridad informática, licencias de software y soporte técnico especializado. La información suministrada permite identificar las contrataciones vinculadas con la

¹⁵ NOC. Sistema de tickets del GCBA. Obtenido el año 2022 en: <https://noc-mesa.buenosaires.gob.ar/> [Accedido el 27/5/26]

protección del perímetro, gestión de vulnerabilidades y monitoreo de la infraestructura digital.

Para cada registro se especifica el número de expediente, la modalidad de contratación y el proceso de compra aplicado. Se informa la descripción del servicio, la Dirección requirente y el documento contractual asociado con su respectiva fecha. Se consigna el importe del compromiso, la fecha de vencimiento del vínculo y la razón social del proveedor involucrado.

El (ANEXO XI) presenta las contrataciones de servicios de ciberseguridad y la adquisición de hardware gestionadas por la DGSEI durante el año 2025. El esquema identifica a los proveedores, el objeto de la prestación y la modalidad de contratación aplicada.

La estructura permite visualizar el número de expediente, el proceso de compra y el documento contractual asociado. Cada registro especifica el importe comprometido y la fecha de vencimiento de la obligación.

La nómina incluye licencias de software y la compra de equipos mediante la modalidad de Convenio Marco, mecanismo de adquisición a través de proveedores previamente adjudicados en el catálogo electrónico BAC que agiliza las compras y estandariza las condiciones de contratación.

La tabla integra la identificación de los procesos dentro de la plataforma Buenos Aires Compra (BAC)¹⁶ para verificar el estado de ejecución y validar cada contratación.

Cuando interviene ante proveedores, la Dirección General de Seguridad Informática se limita a la seguridad operativa: monitoreo, protección de sistemas y definición de los lineamientos técnicos.

La Dirección opera con plataformas de seguridad provistas por terceros, detalladas en las contrataciones indicadas en los apartados anteriores.

En el plano normativo, los contratos con proveedores críticos deben contemplar condiciones formalmente establecidas para la gestión de incidentes de seguridad, incluyendo niveles de servicio y mecanismos de actuación. Estas definiciones permiten reducir los riesgos y ordenar la respuesta ante eventos que afecten los sistemas.

La Dirección indicó que los pliegos contemplan niveles de servicio asociados a incidentes y obligaciones de confidencialidad. La Dirección General desarrolla funciones técnicas vinculadas a la seguridad, mientras que la gestión contractual se ubica en niveles superiores de gobierno tecnológico dentro del Gobierno de la Ciudad Autónoma de Buenos Aires.

La DGSEI interviene en la definición del marco normativo y de las políticas de seguridad, alineadas con estándares internacionales y mantiene los lineamientos obligatorios para el desarrollo de las aplicaciones.

¹⁶ Es el portal oficial de compras y contrataciones del Gobierno de la Ciudad Autónoma de Buenos Aires. El sistema permite la concurrencia de los proveedores en cada proceso. <https://www.buenosairescompras.gob.ar/>

Estos lineamientos se formalizan mediante resoluciones y estándares específicos, como el Estándar de Seguridad ES0902,¹⁷ y se aplican en instancias clave como el pasaje a producción, donde se requiere la validación de controles de seguridad.

La auditoría constató la ausencia de registros documentales que acrediten la integración de requerimientos de seguridad informática en las fases iniciales de adquisición tecnológica.

El equipo no encontró criterios de seguridad documentados para las fases de adquisición tecnológica. Se integra en la Observación N°4.

En el descargo, la Dirección General de Seguridad Informática sostuvo que interviene en la definición de las especificaciones técnicas, los requerimientos funcionales y las condiciones de seguridad de los bienes y servicios que contrata.

Remitió al (ANEXO X) y (ANEXO XI), incluidos en este informe, como respaldo de las contrataciones de componentes críticos de ciberseguridad ejecutadas en el período. Entre ellas figuran el Firewall, el Sistema de Gestión de Eventos e Información de Seguridad (SIEM), el Sistema de Orquestación, Automatización y Respuesta de Seguridad (SOAR), la Detección y Respuesta en Puntos Finales (EDR), el Cortafuegos de aplicaciones web (WAF), la protección contra ataques de denegación de servicio distribuido (DDoS), la gestión de vulnerabilidades, la microsegmentación y la seguridad de Active Directory.

La Dirección aportó el texto de referencia que incorpora en sus Especificaciones Técnicas Particulares (PET) para fijar niveles de servicio de soporte técnico.

El Cuadro N°2 detalla los tiempos de respuesta exigidos según la criticidad del problema.

Tipología	Criterio	Tiempo de respuesta
Crítico	Cuando la imposibilidad del personal de ASInf para efectuar una implementación o configuración afecta la prestación del servicio de la Agencia en su conjunto.	El plazo no deberá exceder de cuatro (4) horas y comenzará a contabilizarse a partir del llamado del GCBA al Centro de Atención del Proveedor.

¹⁷ Estándar de Seguridad (ES0902). Agencia de Sistemas de Información. Obtenido el mes de agosto del año 2025 en: <https://n9.cl/7yadd> [Accedido el 13/8/26]

Tipología	Criterio	Tiempo de respuesta
Mayor	Cuando la imposibilidad del personal de ASInf para efectuar una implementación o configuración afecta la calidad o continuidad del servicio prestado por la Agencia.	El tiempo de respuesta no deberá exceder de ocho (8) horas, contadas a partir del llamado del GCBA al Centro de Atención del Proveedor.
Menor	Cuando la imposibilidad del personal de ASInf para efectuar una implementación o configuración no genere riesgos ni afecte la prestación del servicio por parte de la Agencia.	No deberá exceder de setenta y dos (72) horas, contadas a partir del llamado del GCBA al Centro de Atención del Proveedor.

Fuente: Dirección General de Seguridad Informática (ASInf)

Sobre las contrataciones de servicios específicos de seguridad, la Dirección señaló que exige a los proveedores el cumplimiento de los estándares publicados en el portal de la Agencia de Sistemas de Información.

Indicó que las Especificaciones Técnicas Particulares (PET) de este tipo de contrataciones incorporan cláusulas específicas para establecer los niveles de servicio exigidos a los adjudicatarios.

Citó la cláusula 11.1, de Confidencialidad de la Información, que obliga al adjudicatario a resguardar los datos a los que accede durante la ejecución del contrato, bajo pena de resolución contractual por incumplimiento.

También mencionó la cláusula 11.3, de Estándares Tecnológicos, que remite a la Resolución N°177/ASInf/13 y a su complementaria N°239/ASInf/14 como marco de cumplimiento obligatorio para los proveedores.

La documentación aportada acredita que el organismo formaliza los requisitos de tratamiento de la información y de disponibilidad del servicio en sus contrataciones de ciberseguridad. No cubre, en cambio, el control de accesos ni la asignación de responsables de verificación, que quedan sin evidencia.

2.2. Cumplimiento del Estándar de Seguridad ES0902 y supervisión

El modelo definido asigna a las áreas de desarrollo la implementación de las medidas técnicas establecidas en el Estándar de Seguridad ES0902 versión 6.2, mientras que la Dirección General de Seguridad Informática debe verificar su cumplimiento durante las evaluaciones de seguridad.

Este estándar contempla aspectos críticos como la protección de los datos personales, la autenticación y autorización de usuarios, el control de los accesos, la integridad de la información y la seguridad en interfaces públicas.

No se identifican mecanismos formales que permitan a la DGSEI ejercer esta función de verificación de manera sistemática. La Observación N°5 recoge ese hallazgo.

En el descargo, la Dirección General de Seguridad Informática presentó el Proceso de control de cambios en software de aplicación provisto por Organismos (PC0901).¹⁸ Ese documento establece una separación de funciones entre el área de calidad de la Dirección General Integración de Sistemas (DGISIS), responsable de las pruebas funcionales en el ambiente de prueba (QA) y el área de seguridad, responsable de las pruebas específicas de seguridad.

Según lo informado por el organismo, el área de seguridad documenta los resultados en un informe de evaluación de seguridad de la aplicación en QA y, cuando detecta vulnerabilidades, informa su criticidad, solicita su corrección y repite las evaluaciones hasta verificar que hayan sido corregidas.

El descargo no incluyó, sin embargo, ningún informe de evaluación de seguridad concreto, ni el detalle de las medidas técnicas de cifrado, gestión de roles, límites de sesión y monitoreo de accesos aplicadas en los sistemas relevados.

2.3. Ciclo de vida de los sistemas y trazabilidad documental

Las actividades vinculadas al ciclo de vida del software permanecen bajo responsabilidad de otras áreas, mientras que la DGSEI interviene en la validación de los controles de seguridad y condiciones de pasaje a producción.

La Dirección General de Seguridad Informática informó que su intervención no incluye la gestión del ciclo de vida del software.

En función de esta definición, las actividades vinculadas con la planificación de necesidades, la adquisición, el mantenimiento y la gestión de las licencias y actualizaciones se encuentran bajo la órbita de otras áreas.

Esta delimitación de responsabilidades ubica a la Dirección en un rol acotado dentro del proceso, centrado en aspectos específicos de seguridad, sin intervención directa en las etapas formales del ciclo de vida del software.

Las actividades relacionadas con el control de cambios y el versionado de software quedan fuera del ámbito de responsabilidad de la Dirección General de Seguridad Informática, según las misiones y funciones asignadas.

El análisis del marco normativo indica que la gestión integral de cambios, el versionado de aplicaciones y la administración del ciclo de vida del software corresponden a las áreas de desarrollo o a los organismos titulares de los sistemas, en su carácter de responsables funcionales y técnicos de las soluciones implementadas.

Dentro de este esquema, la intervención de la Dirección se limita a la definición de los lineamientos de seguridad, a la validación de las condiciones para el

¹⁸ Proceso de control de cambios en software de aplicación provisto por Organismos (PC0901). Obtenido el año 2014 en: <https://n9.cl/6hqt8> [Accedido el 13/8/26]

pasaje a producción y al establecimiento de los controles que resguarden la integridad, confidencialidad y disponibilidad de la información en los entornos bajo su alcance.

El área indica que el estándar ES0902 se desarrolla y actualiza de forma periódica, con el propósito de definir lineamientos para el desarrollo de aplicaciones en el ámbito del Gobierno de la Ciudad Autónoma de Buenos Aires.

El análisis no arrojó elementos verificables sobre la implementación del estándar en producción. El área tampoco aportó reportes de cumplimiento, resultados de vulnerabilidades ni registros de excepciones.

Sin controles documentados, no es posible confirmar que los lineamientos se aplican en los sistemas en producción.

La Dirección analiza el desempeño y las vulnerabilidades de las soluciones tecnológicas mediante ensayos de concepto previos a su despliegue. El organismo también licita la adquisición de sus herramientas informáticas para asegurar la concurrencia de oferentes y la adopción de plataformas validadas en el mercado.

A pesar de estas prácticas, la DGSEI no documenta formalmente los criterios de selección de los sistemas, ni presenta estudios de factibilidad técnica, ni evaluaciones de recursos humanos y tecnológicos que respalden los objetivos estratégicos definidos.

Tampoco acredita la alineación de estas decisiones con los lineamientos estratégicos del Gobierno de la Ciudad Autónoma de Buenos Aires.

El relevamiento no identificó registros que documenten la justificación, aprobación y relación de las decisiones tecnológicas con los objetivos estratégicos.

La Dirección General de Seguridad Informática forma parte de la estructura de la Agencia de Sistemas de Información y tiene asignadas, entre otras, las siguientes responsabilidades:

- Intervenir en la definición de esquemas de seguridad para software, datos y comunicaciones, así como en programas de prevención y planes de contingencia.
- Definir, implementar y administrar la identidad de los usuarios del Gobierno de la Ciudad Autónoma de Buenos Aires.
- Administrar y controlar la operación de los sitios web, el servicio de correo electrónico y el acceso a internet.
- Definir mecanismos de monitoreo y alertas, y supervisar sistemas y redes para detectar accesos no autorizados.

En paralelo, el área incorporó soluciones de software, hardware y servicios según las necesidades operativas de cobertura y protección.

Estas soluciones sustentan los procesos operativos y los objetivos de seguridad, pero el área no presentó documentación que permita analizar su ciclo de vida.

La falta de registros impide verificar objetivos de creación, instancias de aprobación y etapas de desarrollo. Tampoco se evidencia el inicio de pruebas, la puesta en producción ni su alineación con los objetivos institucionales.

El análisis realizado sobre el período 2024-2025 incluyó la evaluación de las pruebas aplicadas al Proceso de Gestión de Incidentes de Seguridad y su efectividad operativa.

El análisis abarcó los mecanismos de pruebas periódicas, la intervención de los equipos operativos, la cobertura de incidentes y el seguimiento de hallazgos y acciones correctivas.

La revisión permitió identificar el nivel de formalización del proceso, las responsabilidades definidas y las limitaciones que afectan su funcionamiento operativo.

1. Estado de formalización de pruebas.

Durante el período auditado, la DGSEI no realizó pruebas formales, periódicas ni documentadas del Proceso de Gestión de Incidentes de Seguridad.

- No se realizaron simulacros integrales ni ejercicios de validación de procesos (simulaciones o pruebas prácticas).
- Carece de un plan de pruebas periódicas para evaluar las tareas vigentes.

2. Validación operativa mediante incidentes reales.

Aunque la DGSEI no realizó pruebas formales del proceso, el área informó que valida su funcionamiento mediante la atención diaria de incidentes y requerimientos de servicio.

El informe no incorpora métricas, muestras ni indicadores que permitan verificar la efectividad de esa validación operativa:

- PROC 1.1 - Gestión de Incidentes y Requerimientos de Servicio.
- PROC 2.1 - Gestión de Incidentes por Categoría.

Estos procedimientos definen:

- Circuitos administrativos, técnicos y de cierre.
- Aplicación sistemática en la operación diaria.

La ejecución de estos procedimientos recae en un esquema de roles formalmente distribuidos.

“2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires”

A fin de exponer la distribución de responsabilidades en la gestión de incidentes de seguridad de la información, el Cuadro N°3 detalla la matriz RACI¹⁹ utilizada por la Dirección General de Seguridad Informática, identificando los roles intervinientes y su nivel de participación en cada etapa del proceso.

Gestión de incidentes									
	Gerencia Operativa Seguridad Informática	Gerencia Operativa CSIRT	Gerencia Operativa Ciberseguridad	Recepción	Comunicaciones	Subgerencia Operativa Análisis Forense	Subgerencia Operativa SOC	Subgerencia Operativa Identidad	Dirección General Infraestructura
Detección	I	A	I	R	I	I	I	I	I
Análisis	I	I	A	I	I	R	C	C	C
Respuesta	C	A	R	I	I	R	C	C	C
Comunicación	C	A	I	I	R	C	C	C	C
Cierre	I	A	I	R	C	I	I	I	I

Fuente: DGSEI

R (Responsable): Es el agente encargado de ejecutar la tarea o actividad para completar el trabajo.

A (Responsable final): Es el actor que debe rendir cuentas sobre el éxito o fracaso de la tarea y quien tiene la autoridad final.

C (Consultado): Son los especialistas o interesados a quienes se les solicita opinión o información antes de realizar la acción.

I (Informado): Son las personas que deben ser notificadas sobre los avances o la finalización de la actividad.

3. Alcance y escenarios evaluados.

La revisión operativa abarca incidentes reales de distintas categorías:

- Código y software malicioso.
- Intrusiones y accesos no autorizados.
- Incidentes de disponibilidad y fallas críticas.
- Fraudes y otros eventos de seguridad.

Se evalúan los mecanismos de:

- Detección.
- Análisis.
- Respuesta.
- Comunicación.
- Cierre.

4. Frecuencia de validación.

¹⁹ Herramienta de gestión que asigna responsabilidades mediante cuatro roles clave: la ejecución, la aprobación, la consulta y la información.

- La validación se realiza de manera continua, integrada a la gestión diaria de incidentes y requerimientos reportados por los canales institucionales.

5. Participantes y responsabilidades.

- Equipos operativos de la Dirección General de Seguridad Informática, según la matriz RACI vigente.
- Subgerencias Operativas responsables según la tipología del incidente.
- Supervisión directa de la Dirección General.

6. Resultados, desvíos y acciones de mejora.

Si bien no se generaron reportes específicos de pruebas de proceso, los hallazgos detectados durante la operación diaria se gestionan mediante:

- Ajustes operativos en procedimientos existentes.
- Actualización de criterios técnicos de análisis y respuesta.
- Refuerzos en concientización y capacitación interna.

La Dirección informó ajustes operativos derivados de la experiencia de gestión, aunque no aportó evidencia documental de pruebas estructuradas del proceso.

La revisión no encontró esquemas de prueba periódica que validen la eficacia del proceso. El área no cuenta con un esquema de pruebas periódicas que valide el proceso de gestión de incidentes ni con un plan documentado que permita evaluar la eficacia de los procedimientos y coordinar los roles.

Los incumplimientos advertidos en la revisión de este apartado quedan consignados en la Observación N°6.

2.4. Desarrollo seguro, cambios y control del ciclo de vida

La solicitud y aprobación de nuevos desarrollos permanece bajo responsabilidad de las áreas encargadas de la gestión tecnológica.

La intervención se limita a evaluar el cumplimiento de los estándares de seguridad de la información definidos por la Agencia de Sistemas de Información, que establecen lineamientos obligatorios para el diseño, desarrollo e implementación de las aplicaciones.

Estos estándares incluyen la protección de la información, la gestión de los accesos, el tratamiento de las vulnerabilidades y la incorporación de controles de seguridad desde etapas tempranas del desarrollo.

La validación funcional de los desarrollos corresponde a otras áreas, mientras que la DGSEI verifica los controles de seguridad antes de la puesta en producción.

La protección del código fuente reduce riesgos asociados a accesos no autorizados y vulnerabilidades. Sobre este aspecto, se informó que la Subgerencia Operativa de Monitoreo, Prevención y Detección ejecuta

evaluaciones de seguridad y análisis estático del código en el marco de sus funciones.

La respuesta describe los controles técnicos implementados sobre las aplicaciones. La Dirección General de Seguridad Informática carece de atribuciones funcionales sobre las condiciones contractuales y legales del sistema. Esta separación de funciones determina el alcance de la información analizada.

La revisión realizada no identificó desvíos verificables bajo la responsabilidad del área auditada.

2.5. Análisis de vulnerabilidades y control de preproducción

El Gobierno de la Ciudad Autónoma de Buenos Aires establece pautas estrictas para el desarrollo de sistemas informáticos seguros. El organismo indicó que los desarrollos deben ajustarse a los lineamientos del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) y a los estándares de desarrollo definidos por el Gobierno de la Ciudad.

En la etapa de preproducción, la Subgerencia Operativa de Prevención dependiente de la Dirección General de Seguridad Informática realiza un análisis de las vulnerabilidades y verifica la corrección de las debilidades detectadas.

La información relevada muestra que la DGSEI interviene en la validación de los controles de seguridad previos a la puesta en producción. La validación funcional y la aceptación de los cambios permanecen fuera del alcance operativo de la DGSEI.

Estas tareas corresponden al Propietario del Sistema y a las áreas responsables del desarrollo y validación funcional de las aplicaciones. La DGSEI verifica los controles de seguridad y el cumplimiento de los estándares antes del pasaje a producción.

El examen de este punto no produjo hallazgos atribuibles a la gestión del área.

3. Gestión de activos, identidad digital y administración de accesos

3.1. Inventario de activos, clasificación y roles de custodia

La Política de Clasificación de la Información (PO0402)²⁰ regula el proceso de clasificación de la información del GCBA mediante criterios de confidencialidad, integridad y disponibilidad.

La norma asigna al Propietario la responsabilidad de mantener actualizado el inventario de activos de información, documentar su clasificación y definir los permisos de acceso. El instrumento también establece niveles de criticidad y medidas de tratamiento orientadas a proteger la información según su sensibilidad.

²⁰ Resolución N°177/ASInf/13. Política de Clasificación de la Información (PO0402). Obtenido el año 2026 en: <https://n9.cl/oqscb> [Accedido el 3/3/26]

La DGSEI puso a disposición herramientas para registrar activos de información y asignar responsabilidades conforme a la política vigente.

No se remitió un inventario actualizado ni evidencia que permita verificar la integridad, completitud o vigencia de los activos de información registrados, lo que comprende los equipos de control biométrico y la plataforma de firma digital, los servidores de autenticación y los equipos perimetrales de seguridad.

La DGSEI informó que la política vigente exige utilizar plantillas estandarizadas para su documentación, pero no precisó la fecha de la última actualización de los activos ni el área responsable de su mantenimiento.

La documentación remitida no permite verificar la clasificación ni los roles de custodia asociados a los activos.

El equipo auditor examinó las herramientas y controles de seguridad mediante análisis documental y visitas técnicas. La instancia aportó evidencia contextual sobre los controles y capacidades operativas.

A continuación, se detallan las principales herramientas y soluciones de seguridad identificadas, agrupadas según la Subgerencia Operativa responsable de su implementación y gestión.

1. Subgerencia Operativa de Accesos (SGO Accesos).

- Firewall: Equipos de seguridad perimetrales y red troncal con funciones de control de acceso en capas 3 (red), 4 (transporte) y 7 (aplicación) del Modelo OSI (Interconexión de Sistemas Abiertos).
- Microsegmentación: Infraestructura de microsegmentación orientada a limitar el alcance de incidentes dentro de la red.
- Sistema de Orquestación, Automatización y Respuesta de Seguridad (SOAR): Ejecuta acciones automáticas ante eventos detectados, contribuyendo a la respuesta operativa.

2. Subgerencia Operativa de Prevención (SGO Prevención).

- Sistema de Prevención de Intrusiones (IPS): Monitorea el tráfico y bloquea las actividades maliciosas o vulnerabilidades detectadas.
- Anti DDoS: Solución de defensa multicapa, capas 3, 4 y 7 del modelo OSI, que mitiga los ataques volumétricos y sofisticados. Bloquea el tráfico malicioso, como la saturación de solicitudes HTTP (Protocolo de Transferencia de Hipertexto utilizado por sitios web), DNS (Sistema de Nombres de Dominio) y redes de bots (botnets), garantizando la disponibilidad de las aplicaciones y servicios de la red.
- Firewall de Aplicaciones Web (WAF): Permite la generación de reglas de seguridad en la capa 7 del modelo OSI.

- Sistema de Gestión de Eventos e Información de Seguridad (SIEM): La solución permite monitorear los eventos de seguridad y generar alertas ante comportamientos anómalos.
- Infraestructura de Prevención de Vulnerabilidades: Herramienta que analiza las vulnerabilidades en los desarrollos de software y aplicaciones.
- Inteligencia de Amenazas: Sistema de vigilancia externo que genera alertas sobre riesgos de la organización, incluyendo la fuga de credenciales, suplantación de marca y exposición de información sensible.

3. Subgerencia Operativa de Identidad (SGO Identidad)

- EDR (Detección y Respuesta en Puntos Finales): La herramienta permite detectar y responder incidentes sobre estaciones de trabajo y servidores.
- Active Directory (Directorio Activo): Administrador central de usuarios y políticas de acceso para estaciones de trabajo y servidores, asegurando el control de identidad y permisos.

El material analizado no acredita un esquema de seguridad consistente. Para los controles biométricos y la videovigilancia, el área no presentó documentación que defina procedimientos, responsables ni registros de actividad.

La identificación de las bases de datos integradas, sus responsables técnicos y su registración conforme la Ley N°1.845/05 corresponden al organismo que genera y utiliza la información, en su carácter de titular de los datos. No se aportó evidencia suficiente para verificar la definición de los responsables y la registración formal de las bases de datos relevadas.

Por su parte, la Dirección interviene en la protección de los datos mediante la implementación de controles de seguridad sobre la infraestructura tecnológica, como el monitoreo, la detección de accesos no autorizados y la gestión de incidentes.

El área no acreditó que sus mecanismos de protección operen sobre información crítica real, la Observación N°8 desarrolla esta limitación.

En la información provista en el descargo, la DGSEI señaló que la titularidad, custodia y registración de los activos tecnológicos están distribuidas entre distintos organismos del Gobierno de la Ciudad, conforme a la Política PO0402, que asigna al Propietario del Activo la responsabilidad de mantener el inventario actualizado.

El organismo informó que trabajó junto con la Sindicatura General de la Ciudad de Buenos Aires para impulsar el cumplimiento de esa política en otros organismos. Manifestó, además, que procederá a revisar y actualizar el inventario de los activos bajo su administración directa, identificando para cada uno el área responsable, el nivel de criticidad y la fecha de revisión.

3.2. Controles de autenticación y acceso

Sobre autenticación, el área indicó que el mecanismo principal de acceso a los sistemas consiste en la combinación de usuario y contraseña. Informó la implementación de un esquema de inicio de sesión basado en OpenID,²¹ gestionado mediante la herramienta Keycloak.²²

El segundo factor de autenticación se encuentra disponible, aunque su uso no resulta obligatorio. Esa modalidad reduce su efectividad como medida de protección transversal.

El esquema implementado incorpora controles básicos para verificar la identidad de los usuarios y contribuye a la protección de los sistemas y la información, aunque presenta oportunidades de mejora en la extensión y obligatoriedad de los mecanismos de autenticación reforzada.

La Dirección General de Seguridad Informática define los lineamientos de seguridad lógica y los criterios generales de acceso. Las áreas responsables de infraestructura tecnológica y comunicaciones determinan los medios de acceso habilitados y las ubicaciones autorizadas.

A partir de la información relevada, la Dirección General indicó que aplica mecanismos de seguridad sobre las interfaces de programación de aplicaciones, incluyendo el análisis del tráfico entre servicios y la validación de los procesos de autenticación.

También informó la realización de pruebas de penetración y evaluaciones sobre los datos intercambiados, cuyos resultados remite a los equipos de desarrollo para su tratamiento.

El equipo de auditoría no encontró documentación que identifique los métodos de autenticación y autorización implementados ni que acredite su adecuación al Estándar de la Agencia de Sistemas de Información.

La documentación presentada no acredita los resultados obtenidos ni precisa el alcance de las pruebas realizadas. Esta limitación da lugar a la Observación N°7.

En el descargo, la Dirección General de Seguridad Informática citó el procedimiento PC0901 y el Estándar ES0902 como marco normativo del circuito de control entre los ambientes de desarrollo, calidad, homologación y producción.

De acuerdo con lo expresado por el organismo, las configuraciones de autenticación, autorización y demás controles de seguridad dependen de la arquitectura, la criticidad y las características de cada solución. Su verificación surge del análisis de la documentación técnica: documentos de arquitectura, requerimientos funcionales e informes de evaluación de seguridad elaborados para cada caso.

²¹ OpenID es un estándar de autenticación descentralizado que permite a los usuarios identificarse en diversos sistemas mediante una única cuenta digital, sin necesidad de crear credenciales nuevas en cada aplicación.

²² Keycloak es una herramienta de software, una plataforma que gestiona el acceso de los usuarios, centraliza el proceso de inicio de sesión y administra las credenciales de forma segura.

El organismo no identificó ni adjuntó ninguno de esos documentos en particular.

3.3. Autenticación, identidad digital e interoperabilidad segura

El personal del Gobierno de la Ciudad Autónoma de Buenos Aires debe cumplir con los lineamientos de la Dirección General de Seguridad Informática.

Los agentes deben bloquear sus pantallas al ausentarse, actualizar los sistemas operativos y utilizar contraseñas complejas y únicas.

La normativa restringe la instalación de software no autorizado y prohíbe modificar las configuraciones de seguridad. Los empleados deben notificar cualquier comportamiento extraño del equipo a la mesa de ayuda técnica.

La Agencia de Sistemas de Información autoriza las aplicaciones móviles y obliga a usar redes privadas virtuales para accesos remotos. Los dispositivos deben registrarse en los inventarios oficiales, activar las políticas de seguridad corporativas y evitar las redes inalámbricas públicas.

Los sistemas críticos requieren autenticación multifactor, una gestión de permisos documentada y herramientas de detección en el puesto de trabajo.

La administración renueva las claves periódicamente y audita los registros de ingreso a las plataformas.

Los funcionarios de la DGSEI no explicaron si la habilitación de la red privada virtual exige validar previamente la seguridad del dispositivo del usuario. La respuesta no aclara si el uso de la red privada virtual incluye controles de seguridad que mitiguen la ejecución de software malicioso en dispositivos sin protección propia.

La Dirección tampoco especificó cómo operan los controles en las reparticiones con administración de usuarios autónoma. Finalmente, el texto no define el límite de la responsabilidad del GCBA ante incidentes de seguridad remotos.

La clasificación de la información permite categorizar los datos según su importancia, sensibilidad y uso, y constituye la base para evaluar su criticidad dentro de la gestión de los incidentes de seguridad.

El auditado informó que no existen revisiones periódicas de dicha clasificación. La Dirección no actualiza la clasificación de los datos cuando cambian su uso o importancia dentro de las operaciones.

Los servicios prestados se detallan a continuación, especificando su alcance operativo.

a) Gestión directa de incidentes de ciberseguridad.

BA-CSIRT brindó gestión directa de incidentes de seguridad informática reportados por ciudadanos, incluyendo la recepción, análisis y asistencia ante incidentes tales como fraudes digitales, accesos indebidos, suplantación de identidad y otros eventos de ciberseguridad.

Canales de atención habilitados:

- Correo electrónico institucional de BA-CSIRT.
- Sitio web oficial de BA-CSIRT.
- Plataforma BOTI (atención vía WhatsApp con derivación a operadores).
- Atención telefónica en días y horarios hábiles.

Alcance del servicio:

- Recepción y análisis de reportes de incidentes.
- Asistencia y orientación a los ciudadanos afectados.
- Gestión directa de incidentes cuando corresponde al ámbito de competencia del BA-CSIRT.
- Asesoramiento en los casos que no constituyen incidentes técnicos formales.

Este servicio incluye la gestión directa de incidentes, conforme a las funciones del BA-CSIRT como centro de respuesta a incidentes de seguridad.

b) Derivación de incidentes.

En aquellos casos en que los incidentes reportados exceden el alcance técnico o jurisdiccional del BA-CSIRT, se realiza la derivación correspondiente a otros organismos competentes, fuerzas de seguridad u organismos especializados, brindando previamente orientación al ciudadano.

Alcance del servicio:

- Evaluación preliminar del reporte recibido.
- Derivación a organismos externos cuando corresponde.
- Información clara al ciudadano sobre los pasos a seguir.

El servicio contempla la derivación del incidente al área competente. El equipo del BA-CSIRT no gestiona de forma directa los casos ajenos a su competencia institucional.

c) Planes de concientización y divulgación en ciberseguridad.

BA-CSIRT desarrolló e implementó planes de concientización y divulgación dirigidos a la ciudadanía, con el objetivo de prevenir incidentes y promover el uso seguro y responsable de las tecnologías digitales.

Principales acciones desarrolladas:

- Campañas de difusión en redes sociales oficiales.
- Contenidos educativos y preventivos en el sitio web institucional.
- Difusión de mensajes de concientización a través de BOTI y otros canales digitales.

- Producción de materiales gráficos y audiovisuales con enfoque divulgativo.

Alcance del servicio:

- Divulgación de buenas prácticas de seguridad informática.
- Prevención de fraudes, estafas digitales e ingeniería social.
- Promoción de la cultura de la ciberseguridad ciudadana.

Este servicio corresponde exclusivamente a acciones de divulgación y concientización, sin gestión directa de incidentes.

La Resolución N°177/ASInf/13²³ establece que la Política General de Seguridad Informática resulta de aplicación obligatoria para todo el ámbito del GCBA y alcanza los recursos tecnológicos y actividades vinculadas a sus dependencias. Asigna a la Agencia de Sistemas de Información responsabilidades relacionadas con la definición e implementación de controles para la protección de la información y los servicios tecnológicos.

La cobertura efectiva de los servicios de seguridad informática no alcanza a la totalidad de las dependencias comprendidas dentro del ámbito definido por la normativa vigente.

Ciertas dependencias del Poder Ejecutivo del GCBA no reciben protección de la Dirección General de Seguridad Informática. Esto incluye al Ministerio de Seguridad, las empresas públicas y la Administración Gubernamental de Ingresos Públicos (AGIP).

También quedan excluidos el personal escolar y los alumnos del Ministerio de Educación con dominio edu.ar, cuyo acceso y seguridad se gestionan mediante un entorno tecnológico independiente.

La Dirección concentra su resguardo en las estaciones de trabajo registradas dentro del patrimonio informático del Poder Ejecutivo. Para ello, distribuye herramientas informáticas que protegen los dispositivos conforme a las políticas de seguridad aprobadas por el Gobierno.

El personal técnico analiza las evidencias mediante auditorías forenses cuando ocurren incidentes dentro del perímetro de la red institucional.

La documentación disponible no define con precisión las responsabilidades operativas frente a las fallas originadas en dispositivos no homologados.

Tampoco describe con detalle las situaciones excluidas de la cobertura de los servicios de seguridad ni las limitaciones de la prestación. La información suministrada no especifica con precisión el alcance de la responsabilidad del área frente a los incidentes que se generen fuera de la red institucional o en dispositivos que incumplen las normas vigentes.

²³ Resolución N°177/ASInf/13. Obtenido el día 6 de noviembre del año 2013 en: <https://n9.cl/ogscb> [Accedido el 3/3/26]

El equipo de auditoría solicitó detallar la relación técnica entre la clasificación de los activos, que permite asignar niveles de valor y criticidad a la información y los sistemas y la matriz de priorización de incidentes, a fin de conocer los criterios aplicados para definir la urgencia y la secuencia de tratamiento de los eventos de seguridad.

La descripción de los procedimientos que aportó el área determina cómo BA-CSIRT clasifica los incidentes. El documento también fija los plazos de resolución según la gravedad de cada evento.

A continuación, se detalla el procedimiento estructurado del documento suministrado:

- **Prioridad del incidente:** La prioridad surge del cruce directo entre el impacto del evento y la urgencia declarada por el usuario.
- **Matriz de prioridad:** El sistema utiliza una escala numérica del uno al cuatro. La categoría uno representa la prioridad crítica y la categoría cuatro representa la prioridad baja.
- **Definición de prioridad:** La categoría crítica prioriza la recuperación inmediata ante la pérdida total del servicio. La prioridad alta busca evitar afectaciones severas que comprometan la disponibilidad de la plataforma. La prioridad media comprende fallas que no interrumpen el servicio, pero requieren atención en el corto plazo. La prioridad baja agrupa eventos que pueden resolverse de forma diferida.
- **Criterios de urgencia:** La urgencia se categoriza en alta, media y baja en función del impacto y la criticidad del servicio afectado.
- **Criterios de impacto:** El impacto se mide por las consecuencias negativas sobre el servicio prestado. El manual pondera tres ejes: el daño legal o de imagen pública, la interrupción de las tareas laborales y el volumen de los usuarios afectados. Se toma siempre la mayor afectación observada.
- **Complejidad técnica:** La complejidad se calcula según el esfuerzo horario y el personal técnico requerido para la reparación. Se tipifica en alta (veinticuatro horas de trabajo), media (ocho horas de trabajo) y baja (una hora de trabajo).
- **Compromiso de tiempo de resolución:** Los plazos de cierre de los tickets varían entre una hora, para incidentes de baja prioridad y baja complejidad, y setenta y dos horas, para casos de prioridad media y alta complejidad. Para los incidentes de prioridad cuatro, la resolución se define según la evaluación caso por caso.

El documento proporcionado detalla prioridades, matrices y tiempos de resolución. No incluye, en cambio, el método técnico utilizado para determinar la criticidad de los activos, entendida como la evaluación del valor e importancia de los datos y sistemas para la operación y la seguridad de la organización.

Tampoco explica su relación con la clasificación de la información, que categoriza los datos según su sensibilidad, confidencialidad y valor operativo. La

documentación no evidencia cómo se aplica esta vinculación en incidentes concretos ni incluye registros que acrediten su utilización.

Los administradores de bases de datos y sistemas informáticos operan bajo controles de seguridad estrictos debido a sus privilegios de acceso elevados.

La Dirección General analiza las herramientas de software para validar la identidad de cada dispositivo que solicita conexión física o inalámbrica a la infraestructura.

Las plataformas de monitoreo envían los datos de uso al gestor de eventos para unificar el análisis de incidentes en un único repositorio. Los analistas de soporte intervienen ante los desvíos detectados para sanear el software afectado y contener las posibles intrusiones en la red.

El informe suministrado no contiene un flujo de trabajo aprobado que describa la gestión de los incidentes en los accesos remotos por redes virtuales privadas.

El equipo de auditoría no logró identificar las pautas establecidas en el bloqueo automático, la asignación de los responsables ni las metodologías de corrección del software desactualizado en las estaciones de trabajo.

El área responsable elabora los borradores del procedimiento, pero el documento no cuenta con la aprobación formal de las autoridades superiores de la institución.

Durante la auditoría se revisaron los mecanismos implementados por la Dirección General de Seguridad Informática para la detección y gestión de amenazas externas e internas.

Se analizó la integración de herramientas tecnológicas, la priorización de los incidentes y el uso de la información aplicada a la inteligencia para la prevención y respuesta operativa.

Seguidamente, se exponen los mecanismos tecnológicos identificados y las debilidades detectadas en su integración y uso operativo.

- Herramientas y servicios utilizados:
 - ✓ Servicio de inteligencia de amenazas externas: Reporta riesgos provenientes del entorno exterior para anticipar posibles ataques.
 - ✓ Sistema de Gestión de Eventos e Información de Seguridad (SIEM): Centraliza y correlaciona registros de distintas fuentes tecnológicas para generar alertas ante incidentes.
 - ✓ Plataforma de Orquestación, Automatización y Respuesta de Seguridad (SOAR): Ejecuta acciones automáticas ante eventos detectados y coordina la respuesta operativa inicial.

La Dirección General opera con fuentes de inteligencia cuyo origen y nivel de integración con las herramientas de monitoreo no se encuentran documentados.

Tampoco dispone de un procedimiento formal que respalde la priorización de los incidentes según la criticidad de los activos.

La evaluación no expuso elementos verificables sobre la integración de las fuentes de inteligencia ni sobre los criterios de priorización de incidentes según el riesgo asociado a los activos.

Los controles criptográficos protegen la confidencialidad, integridad y disponibilidad de la información sensible. El estándar ES0902 versión 6.2 establece los lineamientos mínimos para la administración de claves criptográficas, algoritmos de cifrado y firmas digitales dentro de la Agencia de Sistemas de Información.

Para la transmisión de datos se utilizan Certificados de Capa de Conexión Segura (SSL), cuya gestión contempla la generación, custodia y renovación de las claves conforme al ciclo de vida definido por dicho estándar.

El cifrado se implementa mediante el algoritmo Advanced Encryption Standard (AES),²⁴ que transforma la información en un formato inaccesible para usuarios no autorizados. Para ello, se emplean claves de 256 bits, lo que proporciona un nivel adecuado de protección tanto en almacenamiento como en transmisión.

La verificación de integridad se realiza a través del algoritmo SHA256 (Secure Hash Algorithm 256),²⁵ el cual genera un valor único asociado a los datos. Cualquier modificación no autorizada altera dicho valor, lo que permite detectar cambios en la información.

Los controles implementados se ajustan a los estándares técnicos vigentes de la Agencia.

El estándar ES0902 versión 6.2 define los lineamientos de seguridad que deben ser implementados por las áreas de desarrollo, mientras que la Dirección General de Seguridad Informática interviene en su verificación durante las evaluaciones de seguridad.

La Dirección General no exhibió evidencia de las medidas técnicas aplicadas en los sistemas ni de los mecanismos que garantizan la protección de los datos personales frente a los accesos indebidos. Tampoco describió los procedimientos de validación del cumplimiento del estándar.

La evaluación del control sobre los sistemas queda incompleta ante la falta de información sobre medidas técnicas y mecanismos de validación.

En la respuesta sobre la Política de Prevención contra Software Malicioso y los ciclos de actualización de firmas y parches, se indicó la implementación de una herramienta de Detección y Respuesta en Endpoints (EDR).

²⁴ Estándar criptográfico de cifrado simétrico adoptado internacionalmente para la protección de la información, el cual permite asegurar la confidencialidad de los datos tanto en almacenamiento como durante su transmisión.

²⁵ Es un algoritmo criptográfico, un conjunto de reglas matemáticas para proteger la información. Genera un código de 256 bits para los datos, permitiendo detectar cualquier alteración no autorizada y verificar la integridad de la información. No cifra los datos, sino que asegura que no se modifiquen.

Esta herramienta permite el monitoreo en tiempo real de los equipos. Identifica las actividades sospechosas, contiene amenazas activas y previene la ejecución del software malicioso mediante el análisis continuo de eventos y patrones de ataque.

La DGSEI señala que se mantiene actualizada de forma automática, lo que contribuye a mejorar su capacidad de detección frente a nuevas amenazas.

La información exhibida resulta insuficiente para comprender el marco de gestión que respalda su funcionamiento. No se detalló la política de prevención contra software malicioso ni los procedimientos asociados, lo que impide conocer cómo se organiza y ejecuta el control.

En la misma línea, no se especificaron los ciclos de actualización de firmas ni la gestión de parches, ni se identificaron los controles, frecuencias, responsables o mecanismos de verificación. La validación del correcto funcionamiento de la herramienta implementada no se encuentra descripta ni respaldada.

La gestión de usuarios en el Gobierno de la Ciudad Autónoma de Buenos Aires se rige por el Marco Normativo de Tecnologías de la Información, aprobado por la Resolución N°177/ASInf/13, anteriormente mencionada, y por la Política General de Seguridad Informática, de cumplimiento obligatorio en todo el ámbito del GCBA y para terceros vinculados mediante contratos o convenios.

La administración de identidades debe realizarse mediante procedimientos formales, con autoridades explícitamente designadas, garantizando la legalidad, trazabilidad y vigencia de las autorizaciones.

Seguidamente, se describen los roles y responsabilidades definidos para la gestión de usuarios.

Cargos jerárquicos y roles institucionales autorizados.

1. Áreas de Servicio / DGTAL de cada organismo.

Las Áreas de Servicio, dependientes de las Direcciones Generales Técnicas Administrativas y Legales (DGTAL) de cada organismo, son responsables formales de la administración de los usuarios.

Sus funciones incluyen:

- Solicitar altas, bajas y modificaciones (ABM) de usuarios internos.
- Validar la documentación respaldatoria.
- Ejecutar las gestiones a través del sistema ABM oficial.

2. Operadores ABM designados.

Cada organismo designa formalmente operadores ABM, quienes:

- Actúan en representación del organismo.
- Ejecutan las solicitudes en el sistema de ABM.

- Operan bajo la responsabilidad funcional de la DGTAL.

La designación de estos operadores se formaliza internamente y queda documentada conforme a los procedimientos de Identidad Digital.

3. Autoridades jerárquicas solicitantes / referentes.

En casos específicos (principalmente usuarios externos), la solicitud requiere la intervención de un referente institucional con rango no inferior a Gerente Operativo, quien:

- Avala la necesidad del acceso.
- Asume la responsabilidad sobre la vigencia del usuario.
- Figura expresamente en la solicitud o en copia.

4. Proceso de formalización de la autoridad.

La designación de operadores ABM se formaliza mediante comunicación oficial emitida por la DGTAL correspondiente. Esta comunicación constituye el acto administrativo habilitante mediante el cual la máxima autoridad administrativa del organismo:

- Designa formalmente a los operadores ABM.
- Define el alcance de las atribuciones delegadas.
- Asume la responsabilidad institucional sobre las gestiones de identidad solicitadas.

La información expuesta omite los controles de validación de identidad, los criterios de revisión periódica de roles y los mecanismos para identificar accesos innecesarios u obsoletos.

Esta omisión impide verificar la existencia de controles efectivos sobre la vigencia y legitimidad de los accesos.

En el ámbito del GCBA, la gestión de identidades digitales se organiza a partir de un modelo centralizado sustentado en un Directorio Activo (Active Directory, AD). Bajo este esquema, los usuarios se clasifican en categorías como internos, técnicos, de aplicación y externos, lo que permite segmentar los accesos según los distintos perfiles operativos.

La información técnica relevada no especifica los atributos de identidad asociados a cada categoría ni los protocolos aplicables en función de los estándares vigentes.

La DGSEI no presentó evidencia documental que respalde la gestión de altas, bajas y modificaciones de usuarios ni explicó cómo se asignan los perfiles en la práctica.

El equipo no encontró evidencia que acredite la correcta administración de identidades, el cumplimiento de las políticas de seguridad ni los controles efectivos sobre los accesos.

Sobre la gestión de accesos, el área precisó que su intervención se limita a la autenticación. La autorización de cada recurso corresponde al servicio o aplicación responsable.

La Dirección señaló que el principio de mínimo privilegio se aplica por defecto, pero no aportó el procedimiento ni los controles técnicos que lo sostienen en la práctica. La información aportada describe los mecanismos de autenticación sin explicar los controles de autorización requeridos, por lo que el equipo no pudo verificar cómo se otorgan los perfiles.

La Dirección General de Seguridad Informática informa que el Gobierno de la Ciudad Autónoma de Buenos Aires define y administra una matriz de roles y permisos centralizada, implementada sobre la plataforma Directorio Activo (Active Directory, AD), en concordancia con el Marco Normativo de Tecnologías de la Información.

También indica que la asignación de los roles se realiza en función de la categoría de usuario y de las responsabilidades operativas, utilizando grupos de seguridad y mecanismos de autenticación delegada.

En relación con las categorías de usuarios, se detalla:

1. Usuarios internos: Acceden a recursos corporativos básicos y a los sistemas habilitados según su función, tales como el correo electrónico, intranet y aplicaciones institucionales.
 - Los permisos se asignan en función de la pertenencia organizativa y del rol definido.
 - No cuentan con privilegios elevados por defecto.

Cada acceso se otorga según el rol y la posición del usuario en la estructura organizativa, de modo que ningún agente dispone de permisos por encima de lo que sus tareas requieren, conforme al criterio antes descripto.

2. Usuarios técnicos/administradores: Desempeñan funciones de administración técnica sobre plataformas, sistemas y servicios informáticos.
 - Disponen de permisos elevados acotados a su ámbito de responsabilidad técnica.
 - El acceso se encuentra segmentado según funciones específicas, incluyendo la administración del Directorio Activo (Active Directory, AD), políticas de grupo (Group Policy Objects, GPO) y otras plataformas.

Los privilegios administrativos se otorgan de forma restringida, controlada y justificada, bajo el mismo criterio restrictivo.

3. Usuarios de aplicación: Utilizan sistemas específicos sin interacción directa con otros recursos institucionales.
 - La autenticación se realiza obligatoriamente contra el Directorio Activo (Active Directory, AD).
 - No disponen de acceso a otros sistemas o recursos fuera del ámbito de la aplicación correspondiente.

Cada perfil de acceso queda restringido al sistema correspondiente, sin habilitación sobre entornos adicionales.

4. Usuarios externos: Corresponden a personas físicas o jurídicas ajenas a la organización que requieren acceso a determinados servicios.
 - El acceso se limita a servicios específicos previamente definidos. Se aplican restricciones por sistema, rol asignado y período de vigencia.

La administración de accesos restringe las autorizaciones a las tareas indispensables para la operatoria. Cada responsable de sistema o aplicación define el otorgamiento, uso y revocación de accesos privilegiados en servidores, mientras que la Dirección General de Seguridad Informática canaliza las solicitudes mediante una herramienta de tickets que exige justificación y aprobación jerárquica.

La revisión realizada determinó que el área no conserva registros de actividad vinculados con accesos privilegiados ni ejecuta monitoreos continuos o revisiones periódicas sobre su utilización. Tampoco implementa controles de segregación de funciones ni mecanismos orientados a detectar acciones indebidas.

A esta situación se suma la ausencia de lineamientos operativos que regulen de manera integral el ciclo de gestión de accesos privilegiados.

La Dirección General de Seguridad Informática utiliza una plataforma de Gestión de Eventos e Información de Seguridad para analizar los sucesos en tiempo real mediante nodos distribuidos que recopilan información de distintos activos tecnológicos.

El almacenamiento de registros depende de requerimientos puntuales y de la intervención manual de otra área técnica. La administración tampoco estableció reglas formales para resguardar la integridad y disponibilidad de esos registros, situación desarrollada en la Observación N°13.

El organismo, en su descargo, describió las funciones que tiene asignadas: el monitoreo de eventos, generación y gestión de alertas, correlación de eventos, prevención y detección de intrusiones, gestión de vulnerabilidades y la administración de las plataformas de seguridad.

Aclaró que existen integraciones operativas mediante APIs y servicios web entre Detección y Respuesta en Endpoints (EDR), Sistema de Gestión de Eventos e Información de Seguridad (SIEM), Sistema de Orquestación, Automatización y Respuesta de Seguridad (SOAR), sistemas de control de acceso, directorios institucionales y mecanismos de protección perimetral.

El organismo detalló que la gestión de incidentes se apoya en dos niveles de atención dentro del Centro de Operaciones de Seguridad (SOC). El primer nivel clasifica y prioriza las alertas. El segundo investiga el incidente con mayor profundidad y prioriza la respuesta según el impacto y la urgencia.

Precisó que la evaluación de vulnerabilidades sigue metodologías como el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), el catálogo de tácticas y técnicas de atacantes desarrollado por MITRE, y el estándar para evaluar y gestionar riesgos de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

Manifestó que su ámbito de actuación se limita a los organismos del Poder Ejecutivo administrados por la Agencia de Sistemas de Información y que los organismos con autonomía funcional quedan fuera de su intervención directa.

El organismo no adjuntó, sin embargo, la documentación que respalde los procedimientos de atención por niveles dentro del SOC, las integraciones entre plataformas ni la aplicación concreta de las metodologías citadas.

La Dirección se comprometió a documentar los estándares, metodologías y criterios utilizados para el análisis de las vulnerabilidades, la categorización de riesgos y la respuesta ante incidentes.

3.4. Infraestructura y segmentación de seguridad

La Dirección General de Seguridad Informática opera una infraestructura tecnológica distribuida en múltiples entornos. Los componentes se agrupan según su ámbito de aplicación.

1. Centro de datos.

- Cortafuegos (Firewall): Controlan el tráfico entrante y saliente según reglas predefinidas. Los equipos operan en el perímetro y en el núcleo de la red, con cobertura en distintos niveles de segmentación.
- Sistema de prevención de intrusiones (IPS): Inspecciona el tráfico en tiempo real y bloquea actividades maliciosas de forma automática, incluida la desconexión de sesiones comprometidas.
- Cortafuegos de aplicaciones web (WAF): Filtra las solicitudes dirigidas a aplicaciones web y neutraliza los ataques a nivel de aplicación antes de que alcancen los servidores.
- Microsegmentación: Divide la red en segmentos aislados para contener la propagación de incidentes y proteger los activos de forma específica.

- Sistema de gestión de eventos de seguridad (SIEM): Centraliza y correlaciona los eventos provenientes de múltiples fuentes para detectar comportamientos anómalos y generar alertas.
- Sistema de automatización y respuesta de seguridad (SOAR): Automatiza las acciones de respuesta ante eventos definidos, coordinando la actuación entre distintos sistemas de seguridad.

2. Infraestructura de análisis de vulnerabilidades.

- Herramientas de análisis de vulnerabilidades: Identifican debilidades en sistemas y desarrollos de software antes de su explotación.
- Directorio Activo (AD): Gestiona de forma centralizada los usuarios, credenciales y políticas de acceso en estaciones de trabajo y servidores.
- Ubicación: La infraestructura se aloja en las sedes de Av. Independencia 635 y Uspallata 3160, Ciudad Autónoma de Buenos Aires.

3. Entorno de internet.

- Protección contra ataques de denegación de servicio (Anti DDoS): Mitiga los ataques que buscan saturar los servicios y garantiza su disponibilidad.
- Inteligencia de amenazas: Monitorea el entorno digital externo para detectar filtraciones de credenciales, suplantaciones de identidad corporativa y actividades sospechosas en la red.

4. Red interna y centro de datos.

- Detección y respuesta en dispositivos finales (EDR): Monitorea de forma continua los equipos y servidores para identificar y contener amenazas mediante el análisis del comportamiento de los procesos.

Segmentación de red.

La red utiliza rangos IP públicos y privados. Los segmentos privados se distribuyen en cuatro ámbitos:

- Centro de datos: Aloja los servidores y servicios críticos del organismo.
- Red MAN: Conecta las sedes y oficinas del Gobierno de la Ciudad.
- VPN: Habilita el acceso remoto seguro mediante el cifrado del tráfico en redes públicas.
- VPC: Aloja servicios en entornos de nube aislados lógicamente, con control administrativo sobre los niveles de acceso.

Por razones de seguridad, no se publican los rangos IP exactos ni su asociación a cada ambiente.

El equipo de auditoría no detectó contradicciones entre la documentación examinada y el alcance definido en el presente apartado.

3.5. Coordinación técnica entre herramientas de seguridad

La DGSEI utiliza diversas Interfaces de Programación de Aplicaciones (API)²⁶ y servicios web (Web Services)²⁷ para integrar y automatizar los controles de seguridad en sus plataformas.

Las herramientas integran los sistemas y automatizan los controles de seguridad, sin exponer datos confidenciales en el proceso.

Entre las APIs utilizadas se destacan:

- API de EDR (Detección y Respuesta en Dispositivos Finales): Esta interfaz integra la Detección y Respuesta en Dispositivos Finales con los sistemas de monitoreo, correlaciona eventos y automatiza la respuesta inicial ante amenazas detectadas.
- API de acceso: Gestiona el control biométrico del personal del Gobierno de la Ciudad de Buenos Aires. Esta herramienta integra los sistemas de acceso físico con los directorios de usuarios de la organización. El proceso utiliza el Directorio Activo para asegurar la autenticación de cada agente. Esta integración garantiza que solo el personal autorizado ingrese a las dependencias oficiales.
- API de firewall: Integra la plataforma de Orquestación, Automatización y Respuesta de Seguridad (SOAR) con el sistema de defensa. El componente gestiona las alertas de seguridad de forma automatizada y centralizada. La interfaz permite la aplicación directa de políticas de protección en el perímetro de la red. Este mecanismo acelera la respuesta ante incidentes y optimiza la administración de los recursos tecnológicos.
- API de SIEM (Gestión de Información y Eventos de Seguridad): Integra múltiples fuentes de datos para consolidar la información de seguridad de la organización. El sistema facilita el análisis centralizado de los registros y la detección de amenazas en tiempo real. La interfaz automatiza la generación de reportes sobre incidentes y eventos críticos para la operación. Este mecanismo mejora la capacidad de respuesta ante las vulnerabilidades detectadas en la infraestructura.

3.6. Comunicación y coordinación operativa

La Dirección General de Seguridad utiliza canales institucionales definidos para gestionar y hacer seguimiento de los requerimientos de seguridad informática con otras áreas del Gobierno de la Ciudad.

²⁶ Conjunto de reglas y protocolos que habilita la comunicación e intercambio de información segura entre distintos sistemas y aplicaciones.

²⁷ Conjunto de protocolos y herramientas que permiten que distintas aplicaciones se comuniquen e intercambien información de manera automática y segura a través de internet o redes internas.

La operatoria diaria se administra a través del portal <https://noc-mesa.buenosaires.gob.ar/>, utilizado para registrar incidencias, canalizar solicitudes técnicas y efectuar el seguimiento de las intervenciones realizadas. El sistema centraliza las gestiones operativas y facilita el control de los tiempos de respuesta entre las áreas intervinientes.

Las comunicaciones de carácter formal y normativo se tramitan mediante el módulo de Comunicaciones Oficiales (CCOO), integrado al Sistema de Administración de Documentos Electrónicos (SADE).²⁸ Este circuito registra las actuaciones institucionales y conserva la evidencia documental de las comunicaciones emitidas con validez jurídica.

La definición técnica, administración y evolución de estos mecanismos responden a lineamientos transversales del Gobierno de la Ciudad Autónoma de Buenos Aires, cuya rectoría corresponde a niveles superiores de gobierno tecnológico. El esquema implementado formaliza la derivación de los requerimientos y mantiene la trazabilidad sobre las actuaciones realizadas.

4. Gestión de incidentes, vulnerabilidades y operación de seguridad

4.1. Gestión y mitigación de vulnerabilidades

El equipo de seguridad ejecuta pruebas de penetración y evaluaciones de vulnerabilidades antes de publicar las aplicaciones. Los técnicos simulan ataques controlados y revisan las configuraciones de seguridad para detectar fallas técnicas en los sistemas y componentes tecnológicos.

Luego, los analistas derivan los hallazgos a los equipos responsables para aplicar las correcciones correspondientes en los entornos de desarrollo. Estas actividades buscan reducir la exposición de los activos tecnológicos antes de su implementación en producción.

La documentación describe actividades de detección y corrección de vulnerabilidades. Los procedimientos que regulan el registro, seguimiento y validación de los cambios sobre configuraciones afectadas están ausentes.

Los informes examinados tampoco definen criterios homogéneos de priorización, responsables de tratamiento ni mecanismos de verificación sobre las correcciones implementadas. El equipo de auditoría no encontró registros que acrediten el seguimiento técnico de los cambios realizados ni la validación de su cierre.

Para las notificaciones internas, el área utiliza el módulo de Comunicaciones Oficiales y las casillas institucionales autorizadas. Los canales institucionales del Gobierno de la Ciudad centralizan las comunicaciones con ciudadanos y proveedores externos.

La documentación examinada no detalla los circuitos de escalamiento, validación técnica ni mecanismos de comunicación asociados al tratamiento de

²⁸ Sistema de Administración de Documentos Electrónicos. Obtenido el día 1 de julio del año 2009 en: <https://n9.cl/jbodz> [Accedido el 27/5/26]

configuraciones vulnerables y a la implementación de correcciones sobre los activos tecnológicos.

Las debilidades observadas en el control, seguimiento y validación de los cambios vinculados con vulnerabilidades dan lugar a la Observación N°9.

La Dirección General de Seguridad Informática, en el descargo, aportó informes de evaluación de seguridad con distinto versionado. Ese detalle exhibe que el estado de seguridad varió de una instancia a otra.

El organismo informó que los hallazgos y las correcciones se gestionan mediante el sistema institucional de tickets, Comunicaciones Oficiales cuando corresponde y el procedimiento PC0901. No se adjuntaron registros específicos que permitan verificar su aplicación. La documentación aportada tampoco detalla la corrección realizada en cada hallazgo ni el cambio de configuración puesto en práctica.

4.2. Operación y seguimiento de incidentes

La Dirección General de Seguridad Informática rige sus operaciones en la Gestión de Incidentes de Seguridad de la Información y Concientización del Centro de Ciberseguridad (BA-CSIRT), mediante los siguientes procedimientos vigentes:

1. Procedimiento de Gestión de Incidentes y Requerimientos de Servicio de BA-CSIRT-PROC 1.1 (versión vigente).

Objeto: Estandarizar el ingreso, registro y gestión administrativa de los incidentes de seguridad de la información y de los requerimientos de servicio recibidos por el BA-CSIRT.

Alcance: Aplica a la totalidad del personal que cumple funciones de gestión de incidentes y requerimientos de servicio en el ámbito del BA-CSIRT.

Circuito administrativo formal: El procedimiento establece el siguiente flujo obligatorio:

1. Ingreso del incidente o requerimiento por los canales institucionales habilitados.
2. Registro obligatorio en el sistema de gestión de incidentes institucional mediante plantilla normalizada.
3. Gestión y seguimiento del caso, documentando las acciones realizadas.
4. Cierre administrativo del ticket una vez finalizada la intervención.

Autoridad de aprobación: Dirección General de Seguridad Informática.

2. Procedimiento de Gestión de Incidentes por Categoría-PROC 2.1 (versión vigente).

Objeto: Definir el tratamiento técnico y administrativo de los incidentes y requerimientos de servicio una vez registrados en el sistema de gestión de incidentes institucional.

Clasificación formal de incidentes: El procedimiento establece un esquema de categorización propio del BA-CSIRT, que incluye, entre otras, las siguientes categorías:

- Código malicioso.
- Disponibilidad.
- Obtención de información.
- Intrusiones.
- Compromiso de la información.
- Fraude.
- Contenido abusivo.
- Política de seguridad.
- Otros.

El circuito administrativo de tratamiento es el siguiente:

1. Recepción del ticket registrado en el sistema.
2. Clasificación del incidente según la categoría definida.
3. Análisis y tratamiento conforme a la tipología correspondiente.
4. Registro de las acciones realizadas y resguardo de la evidencia asociada.
5. Cierre administrativo del incidente en el sistema.

Autoridad de aprobación: Dirección General de Seguridad Informática.

La Dirección General informó la existencia de la Política de Clasificación de la Información (PO0402), que define criterios de categorización y asigna roles y responsabilidades para su tratamiento. El equipo no encontró controles que acrediten su integración efectiva en los procesos de detección, análisis y respuesta ante incidentes.

La DGSEI monitorea sus sistemas en forma ininterrumpida las 24 horas, los 7 días de la semana. El personal interno supervisa y gestiona los eventos de seguridad entre las 07:00 y las 23:00 horas, mientras que un Centro de Operaciones de Seguridad (SOC) tercerizado asume la detección y respuesta ante incidentes en el horario nocturno.

Dentro del esquema, el primer nivel del Centro de Operaciones de Seguridad (SOC N1) efectúa el monitoreo inicial, analiza los eventos básicos, filtra falsos positivos y registra los incidentes.

Aquellos casos que requieren un análisis más profundo se escalan al segundo nivel del Centro de Operaciones de Seguridad (SOC N2), donde se realiza la evaluación técnica, se analiza la evidencia y se determinan las acciones de contención.

El modelo de dos niveles sostiene la vigilancia continua y ordena la respuesta según la complejidad de cada evento.

De acuerdo con lo manifestado por el área y la documentación exhibida, la organización cuenta con herramientas destinadas al seguimiento de incidentes y a la conservación de los eventos.

La entidad gestiona la correlación de los datos mediante una plataforma de seguridad que unifica la vigilancia del perímetro y la infraestructura.

Este sistema unificado procesa la información originada en los diferentes dispositivos de control de accesos de la red. Los analistas gestionan los eventos de seguridad informática a través de un sistema centralizado de registro de requerimientos de servicio.

La base de datos almacena la cronología del caso, los canales de reporte oficiales y la tipificación del incidente. El personal técnico asienta allí todas las actividades de diagnóstico ejecutadas y la resolución final del problema reportado.

Las autoridades del sector indicaron que no se registraron incidentes de seguridad con afectación de datos personales durante 2025. La información disponible no incluye los reportes anuales de disponibilidad de registros ni los elementos que permitan analizar la trazabilidad de los eventos.

Los datos aportados no permiten analizar el tratamiento de los eventos ni sus acciones de mitigación.

Frente a eventos de seguridad, la Dirección informó que usa distintas herramientas y canales de interacción para notificaciones automáticas y generación de alertas.

En particular, se identificaron los siguientes componentes:

- Herramientas de detección y respuesta:
 - ✓ Sistema de Gestión de Información y Eventos de Seguridad (SIEM).
 - ✓ Centro de Operaciones de Seguridad (COS).
 - ✓ Plataforma de Orquestación, Automatización y Respuesta de Seguridad (SOAR).
- Canales de interacción con la ciudadanía:
 - ✓ Sitio web oficial.
 - ✓ Línea telefónica 147.
 - ✓ Asistente virtual.

Los umbrales de criticidad para alertas, los tiempos de escalamiento y los canales formales de notificación no están definidos en la documentación aportada.

El área cuenta con herramientas de monitoreo y detección, pero no define los parámetros operativos ni los circuitos de actuación necesarios para evaluar su efectividad.

El análisis del proceso de detección y gestión de incidentes permitió identificar los siguientes componentes, esquemas de escalamiento y debilidades.

- Herramientas de detección temprana:
 - ✓ Sistema de Gestión de Eventos e Información de Seguridad (SIEM): Centraliza el análisis de registros en tiempo real, detecta amenazas mediante la correlación de los datos y emite alertas ante comportamientos anómalos.
 - ✓ Servicio de inteligencia de amenazas: Identifica patrones atípicos y riesgos potenciales en la infraestructura para anticipar ataques, mitigar vulnerabilidades y fortalecer la resiliencia operativa.

- Escalamiento de incidentes:

El proceso de escalamiento consiste en derivar cada evento al área operativa correspondiente según el tipo de incidente identificado.

- ✓ Subgerencia Operativa Identidad: Gestiona los incidentes vinculados con la identidad digital, las estaciones de trabajo y el correo electrónico para asegurar la integridad de las credenciales.
- ✓ Subgerencia Operativa Accesos: Administra las conexiones por redes privadas virtuales y los perfiles administrativos en los controladores de dominio. El sector gestiona las alertas por accesos no autorizados.
- ✓ Subgerencia Operativa Prevención: Mitiga ataques de denegación de servicio distribuido e intrusiones en la capa de aplicación mediante reglas de filtrado y políticas de seguridad.

En este circuito, el sector no ha formalizado internamente los parámetros de clasificación ni los plazos máximos de resolución jurisdiccionales. Esta omisión impide aplicar categorías de impacto homogéneas durante la gestión diaria de incidentes.

Aunque el Gobierno de la Ciudad establece tiempos de respuesta para la atención de incidentes, el área no utiliza estos indicadores como parte de su seguimiento operativo. El proceso de reporte no se encuentra integrado al flujo de trabajo del sector.

El área no define criterios formales para clasificar los incidentes ni establece niveles de severidad y tiempos de respuesta. Además, el sector carece de un esquema estructurado de cierre que incluya el análisis de causa raíz.

El Gobierno de la Ciudad Autónoma de Buenos Aires utiliza tres categorías para clasificar los incidentes operativos según el nivel de afectación del servicio.

Estas categorías abarcan los niveles crítico, mayor y menor, donde el proveedor debe responder en plazos de cuatro, ocho o setenta y dos horas respectivamente.

El cómputo del tiempo comienza en el instante en que la jurisdicción reporta la falla al centro de atención telefónica.

La normativa interna asigna la toma de decisiones finales al Director General de Seguridad Informática.

Para los mensajes internos, el área usa el módulo CCOO y casillas institucionales autorizadas. Los circuitos de escalamiento y las notificaciones formales hacia la conducción no tienen un procedimiento que los regule.

Como parte de la revisión del marco de continuidad operativa y del Plan de Recuperación ante Desastres, el equipo de auditoría solicitó información sobre la infraestructura centralizada de la Agencia, los simulacros realizados y las pruebas de recuperación ejecutadas durante 2024-2025.

También requirió evidencia sobre el seguimiento de las desviaciones identificadas y las medidas adoptadas para su corrección. La aplicación de estos planes resulta necesaria para mantener la disponibilidad de los servicios esenciales y establecer mecanismos de recuperación frente a los eventos críticos.

Adicionalmente, se solicitó al área detallar la relación entre la gestión de incidentes de seguridad y el plan de continuidad operativa. Los responsables no aportaron evidencia que demuestre esta vinculación ni documentación que establezca mecanismos de coordinación, condiciones de activación y comunicaciones entre los equipos responsables.

Esa ausencia impide validar la capacidad de respuesta ante escenarios críticos. Ese hallazgo queda documentado en la Observación N°11.

La Dirección General de Seguridad Informática mencionó en el descargo los procedimientos PROC 1.1, PROC 2.1 y una matriz RACI de gestión de incidentes.

Los procedimientos regulan el circuito de atención de denuncias ciudadanas ante BA-CSIRT, las vías de ingreso, el registro en la mesa de ayuda y la derivación según la categoría de incidente.

La matriz RACI asigna, para las etapas de detección, análisis, respuesta, comunicación y cierre de un incidente, la responsabilidad de ejecución, aprobación, consulta e información de cada tarea. Involucra a las áreas de Seguridad Informática, CSIRT, Ciberseguridad, Centro de Operaciones de Seguridad, Análisis Forense, Identidad e Infraestructura.

Esta matriz está identificada con el número IF-2026-10751301-GCABA-DGSEI y fue firmada el 2 de marzo de 2026, fecha posterior al período auditado.

Ninguno de estos documentos cubre la falta de una guía formal de soporte técnico ni la ausencia de un historial de incidentes trazable y homogéneo entre sectores.

4.3. Niveles de servicio y cumplimiento operativo

La entidad bajo examen remitió datos técnicos sobre los plazos de resolución para las prestaciones a otras dependencias.

El área clasifica las tareas según la gravedad del impacto que las fallas generan en la continuidad del negocio. El equipo de auditoría pidió los documentos de acuerdos de nivel de servicio y los acuerdos operativos internos asociados.

La respuesta oficial consignó que la Gerencia no firma los protocolos operativos internos para regular sus actividades habituales. El reporte técnico posterior enumera los tiempos límite establecidos para resolver los eventos de seguridad y completar el análisis de las vulnerabilidades. Esos parámetros documentados sirvieron para medir el cumplimiento de las metas del sector examinado.

A efectos de sistematizar los parámetros informados para la prestación de servicios y su cumplimiento operativo, el Cuadro N°4 detalla los tipos de requerimiento relevados, su nivel de prioridad, los plazos de atención establecidos, los resultados registrados y las observaciones asociadas.

Tipo de requerimiento	Prioridad	Acuerdo de Nivel de Servicio (plazo de atención)	Resultado	Observaciones
Incidente de seguridad	Crítico	Hasta 4 horas	Cumplido	Impacto total en la prestación del servicio
Incidente de seguridad	Mayor	Hasta 8 horas	Cumplido	Degradación del servicio
Incidente de seguridad	Menor	Hasta 72 horas	Cumplido	No afecta significativamente el servicio
Requerimiento de servicio	-	Hasta 48 horas hábiles	Cumplido	Solicitudes operativas generales
Evaluación de seguridad	-	5 días hábiles	Cumplido	Actividades de evaluación de seguridad

Fuente: DGSEI

El área auditada no gestiona Acuerdos de Nivel Operativo (OLA). Estos acuerdos internos entre sectores establecen responsabilidades, tiempos y criterios de coordinación para asegurar la prestación consistente de los servicios.

En el relevamiento efectuado no se identificó documentación que formalice estos acuerdos en relación con los servicios de seguridad de la información brindados a otras dependencias del Gobierno de la Ciudad.

La información disponible se limita a la definición de los plazos de respuesta, sin evidencia de validación, comunicación formal ni mecanismos de control asociados a su cumplimiento. El análisis del período auditado derivó en la Observación N°10.

En el descargo, el auditado indicó que las actividades vinculadas a la infraestructura de seguridad están asignadas a áreas especializadas. Esas áreas

cubren la instalación, configuración, administración, operación, el mantenimiento y la actualización de las plataformas de seguridad, junto con la correlación de eventos, la detección temprana de amenazas y la prevención de intrusiones y vulnerabilidades.

Agregó que la Dirección General de Seguridad Informática opera y administra las herramientas de seguridad, y sostiene el monitoreo continuo mediante personal propio y el Centro de Operaciones de Seguridad (SOC). Las alertas y los eventos generados por las distintas soluciones se centralizan y correlacionan en el Sistema de Gestión de Eventos e Información de Seguridad (SIEM).

Esto permite identificar amenazas, incidentes o comportamientos anómalos, y coordinar la respuesta, ya sea con controles automatizados o con intervención de los equipos técnicos.

También señaló que cuando un escenario de amenaza requiere intervención manual, el equipo analiza las acciones ejecutadas. Cuando resulta viable, incorpora esas acciones como flujos automatizados de respuesta en el Sistema de Orquestación, Automatización y Respuesta de Seguridad (SOAR), cuyo objetivo es reducir los tiempos de detección, contención y solución ante eventos similares en el futuro.

Sobre la plataforma SIEM, el auditado indicó que concentra los registros y eventos generados por los distintos componentes de la infraestructura central y perimetral. Señaló también que cuenta con tableros de monitoreo en tiempo real para visualizar los eventos detectados, las alertas generadas y las acciones de mitigación.

El auditado aportó la matriz de controles que se presenta en el Cuadro N°5.

Control	Periodicidad	Responsable	Evidencia
Supervisión de alertas SIEM	Continua (24x7)	Equipo SOC	Alertas, logs, tickets
Verificación de fuentes de eventos (logs)	Diaria	Equipo SOC	Paneles de monitoreo, registros de conectividad
Revisión de reglas de correlación	Periódica según necesidad operativa	Equipo SOC / Administradores SIEM	Registro de cambios y configuraciones
Control de ejecución de playbooks (acciones automatizadas predefinidas para un tipo de incidente) SOAR	Diaria	Equipo SOC	Historial de ejecuciones, correos automáticos y auditoría de playbooks

Control	Periodicidad	Responsable	Evidencia
Validación de integraciones SOAR	Periódica	Administradores SOAR	Logs de integración y reportes de estado
Seguimiento de incidentes generados por SIEM/SOAR	Continua	Equipo SOC	Tickets, informes y registros de atención

Fuente: Dirección General de Seguridad Informática

La información aportada describe el esquema de controles vigente sobre la infraestructura de seguridad, pero no presenta registros concretos de las verificaciones realizadas sobre ciertos componentes, como logs exportados, tickets cerrados o informes con fecha y responsable.

4.4. Análisis y respuesta ante incidentes

El Centro de Ciberseguridad gestiona los incidentes mediante un protocolo con fases definidas. El esquema comprende las etapas que se detallan a continuación:

- **Preparación:** Asegura la disponibilidad de las herramientas de análisis. El sector revisa periódicamente las capacidades operativas a partir de las experiencias previas.
- **Detección:** Identifica, confirma y categoriza el incidente. El proceso utiliza criterios definidos para determinar la naturaleza del evento de forma temprana.
- **Contención:** Ejecuta acciones inmediatas para limitar el impacto y evitar la propagación. El personal aplica medidas de estabilización para resguardar la infraestructura en el corto plazo.
- **Erradicación:** Elimina la causa raíz que originó el incidente. Esta fase contempla la subsanación integral de los sistemas comprometidos para garantizar su integridad.
- **Recuperación:** Restaura los sistemas y servicios afectados por la falla. El objetivo principal consiste en restablecer el funcionamiento normal de la red y las aplicaciones.
- **Lecciones aprendidas:** Analiza el incidente de forma posterior para elaborar los informes técnicos. El sector revisa los controles para fortalecer la capacidad de respuesta ante futuros ataques.

En relación con la gestión de incidentes de seguridad, se solicitó informar si los resultados de los análisis de causa raíz y las lecciones aprendidas se integran en la mejora continua de los procesos, controles técnicos y acciones de concientización.

Según lo informado, la organización incorpora de manera sistemática los resultados obtenidos, aplicándolos en los siguientes aspectos:

- Ajuste de procedimientos operativos y circuitos de notificación, con el objetivo de optimizar la respuesta ante incidentes.
- Refuerzo de controles técnicos, en función de las debilidades detectadas de forma recurrente.
- Actualización de contenidos de concientización, orientados a mitigar las conductas de riesgo identificadas.

Adicionalmente, los análisis de causa raíz permiten clasificar el origen de los incidentes, lo que facilita la definición de las acciones específicas:

- Falta de conocimiento o nivel insuficiente de concientización.
- Deficiencias en los procesos operativos.
- Debilidades técnicas o configuraciones inadecuadas.

Identificar la causa permite al área diseñar respuestas diferenciadas según el tipo de problema detectado.

4.5. Resguardo y control de evidencias

Se solicitó describir el procedimiento de preservación de evidencias digitales en el marco de los incidentes de seguridad. La Dirección aclaró que la evidencia se almacena en el Storage BA-CSIRT, ubicado en el Centro de Datos de la Agencia de Sistemas de Información.

El acceso está restringido a operadores autorizados mediante credenciales personales, desde la red del Gobierno de la Ciudad o por red privada virtual.

Cada incidente genera una carpeta identificada con el número de ticket del Centro de Operaciones de Red, donde se resguarda la información disponible.

Los archivos sospechosos se almacenan sin ejecución y su tratamiento queda documentado para el análisis posterior.

5. Monitoreo, continuidad y gobernanza operativa

5.1. Continuidad y recuperación de servicios

El área auditada informó que sus plataformas de seguridad operan bajo esquemas de alta disponibilidad; sin embargo, la documentación remitida omite describir las soluciones técnicas implementadas y los mecanismos de redundancia adoptados.

Se constató la ausencia de parámetros formales clave como el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO). El análisis del período auditado originó la Observación N°12.

La Dirección General de Seguridad Informática, en su descargo, señaló que opera múltiples herramientas de protección perimetral y monitoreo, y que los componentes críticos de su infraestructura cuentan con esquemas de alta disponibilidad y redundancia.

Reconoció que aún no formalizó el Tiempo Objetivo de Recuperación (RTO) ni el Punto Objetivo de Recuperación (RPO) de las plataformas bajo su administración directa.

El organismo se comprometió a definir, documentar y formalizar esos parámetros junto con las áreas de infraestructura tecnológica, Centros de Datos, comunicaciones y recuperación ante desastres. Preciso que el trabajo considerará la criticidad de cada servicio, sus dependencias tecnológicas y los mecanismos de revisión periódica.

5.2. Indicadores y control operativo

La auditoría analizó la disponibilidad y uso real de los tableros de control. El objetivo fue verificar si el área mide su rendimiento y corrige desvíos con base en datos concretos.

La Dirección informó que el seguimiento de los objetivos estratégicos de seguridad de la información se realiza mediante un esquema de gestión de proyectos, con etapas definidas de ejecución y control.

La documentación presentada remite a tableros de seguimiento por hitos y al monitoreo del avance de iniciativas en curso.

Algunos proyectos reciben seguimiento por parte de la Jefatura de Gabinete, que solicita informes mensuales con el estado de avance e indicadores asociados a cada iniciativa. Este esquema se orienta al control de ejecución de proyectos, sin detallar su vinculación con los objetivos estratégicos de seguridad.

El material aportado describe el seguimiento de iniciativas, aunque no establece cómo se mide el cumplimiento de los objetivos estratégicos de seguridad de la información. La Dirección no definió métricas ni indicadores formales para el control de procesos ni presentó un procedimiento documentado para la gestión de las acciones correctivas ante desvíos.

La Dirección General de Seguridad Informática indicó el uso de herramientas como el Sistema de Gestión de Información y Eventos de Seguridad (SIEM), la solución de monitoreo de red Paessler (PRTG)²⁹ y distintas consolas de análisis para la obtención de información operativa.

No se informaron los tipos de reportes generados ni su utilización en procesos de análisis, monitoreo o toma de decisiones. Tampoco se precisaron mecanismos de visualización ni criterios de interpretación de la información disponible.

²⁹ Herramienta de monitoreo que supervisa en tiempo real el estado, la disponibilidad y el rendimiento de las redes, dispositivos y servicios tecnológicos mediante sensores y alertas.

El equipo de auditoría no identificó evidencia que respalde el uso de estos datos en instancias de control o decisión. La disponibilidad de herramientas no acredita su aplicación efectiva en procesos de seguimiento y gestión.

Los estándares emitidos por la Agencia de Sistemas de Información son de cumplimiento obligatorio para todas las dependencias del Gobierno de la Ciudad Autónoma de Buenos Aires.

En el ámbito de sus competencias, la Dirección General de Seguridad Informática debe impulsar su aplicación y desarrollar mecanismos periódicos de control y seguimiento.

La auditoría consultó al área sobre el cumplimiento de estas obligaciones y solicitó la evidencia correspondiente. La Dirección indicó que estos aspectos se verifican durante las revisiones de seguridad.

En ese contexto, se informaron antecedentes de auditorías realizadas entre 2022 y 2025 por la Agencia de Sistemas de Información, en las que se ejecutaron proyectos vinculados con seguridad de la información, incluyendo relevamientos, seguimientos y evaluaciones de procesos.

Para el año 2025 se mencionó el Proyecto N°10-UAIASInf/25, incluido en el Plan Anual de Auditoría de la Agencia de Sistemas de Información aprobado por la Sindicatura General de la Ciudad Autónoma de Buenos Aires mediante Resolución N°162-SGCBA/24.³⁰

El período auditado abarca desde el 1 de junio de 2024 hasta el 30 de junio de 2025, identificado en el sistema de expedientes electrónicos mediante el documento IF-2025-40608420-GCBA-UAIASInf.

A su vez, se indicó el Proyecto N°20/25 vinculado con el proceso de definición, implementación y administración de la identidad de los usuarios del Gobierno de la Ciudad de Buenos Aires, identificado mediante el documento IF-2025-24803147-GCBA-GGAJISGCBA, junto con su respuesta registrada mediante la Nota NO-2025-26096084-GCBA-DGSEI.

Respecto de años anteriores, se mencionó para el año 2024 el Proyecto N°10-UAIASINF/24 referido al análisis de la gestión de licencias Microsoft, identificado mediante la Nota NO-2024-37207879-GCBA-UAIASInf.

Para el año 2023 se indicó el Proyecto N°08-UAIASInf/23 denominado "Análisis de Gestión de Incidentes de Seguridad Informática", identificado mediante la Nota NO-2023-13664254-GCBA-UAIASInf.

Para el año 2022 se informó el Proyecto N°8-UAIASInf/22 denominado "Análisis de implementación de firma digital", identificado mediante la Nota N°NO-2022-16441100-GCBA-UAIASInf.

La información suministrada se restringe a enumerar los proyectos de auditoría y a indicar las referencias de los expedientes electrónicos relacionados. La evidencia disponible no permite corroborar el contenido ni los resultados de los

³⁰ Resolución N°162-SGCBA/24. Obtenido el día 18 de diciembre de 2024 en: <https://n9.cl/gx71iz> [Accedido el 27/5/26].

informes referenciados. El estado de las recomendaciones anteriores no fue acreditado por el área.

El equipo solicitó información sobre el mecanismo de gestión de excepciones en los planes de capacitación obligatoria. La Dirección respondió que no dispone de un procedimiento formalizado, las excepciones se resuelven caso por caso con criterios internos no documentados. Esa práctica no garantiza la uniformidad ni la trazabilidad en las decisiones.

Durante el ejercicio 2025, la Dirección General recopiló datos estadísticos sobre el tratamiento de eventos de seguridad. Esta información permite visualizar la actividad del sector y los tiempos de resolución generales.

La distribución de los 2.419 incidentes informados es la siguiente:

- **Tiempos de respuesta:** La mayor parte de los eventos se resolvió en un plazo de seis horas. El resto de las intervenciones se distribuyó en periodos de 24, 48 y 72 horas según la complejidad del caso.
- **Clasificación por impacto:** Los registros muestran una predominancia de incidentes de impacto medio y bajo. Durante el periodo analizado, no se reportaron eventos categorizados como críticos.
- **Indicadores de riesgo:** El sector presentó un modelo de referencia para el análisis de aplicaciones. Ese modelo funciona como guía de evaluación y no constituye un mecanismo formal para medir los riesgos.

El equipo de auditoría no encontró evidencia de un sistema formal de indicadores de desempeño. El organismo no segmenta las métricas por criticidad de activos ni genera informes periódicos que demuestren el uso analítico de los datos relevados.

La Agencia organiza la evidencia digital en repositorios vinculados a los tickets del Centro de Operaciones de Red. Esta estructura permite seguir cada caso y resguardar los archivos maliciosos de forma segura. Estas medidas buscan evitar la ejecución directa de amenazas y preservar la integridad del entorno tecnológico durante las tareas de análisis forense.

El área ejecuta funciones operativas sobre los registros, pero no define criterios de conservación, eliminación ni cumplimiento normativo para la información almacenada.

La Dirección General no estableció indicadores de gestión para evaluar el rendimiento. El área tampoco registra los desvíos identificados ni documenta las decisiones de la conducción.

Estas omisiones impiden que la supervisión cuente con evidencias objetivas para validar los procesos. El equipo formuló la Observación N°14 a partir de ese análisis.

En su descargo, el organismo planteó que sus registros, estadísticas, indicadores operativos y reportes forman parte de un esquema de gestión, seguimiento y control de incidentes, evaluaciones de seguridad y proyectos vinculados a la protección de los activos tecnológicos. Esa información, según

indicó, se usa para monitorear la evolución de los incidentes, evaluar tendencias, medir el desempeño de los controles y respaldar las decisiones en materia de ciberseguridad.

El organismo agregó que dispone de tableros de control y avance, informes mensuales de incidentes remitidos a la Jefatura de Gabinete de Ministros, informes periódicos sobre los proyectos estratégicos, reportes de evaluación de seguridad, y registros de versionado y evaluación de hallazgos.

Mencionó que aplica criterios de resguardo sobre la información que pueda revelar incidentes específicos, vulnerabilidades detectadas o medidas técnicas adoptadas para mitigarlas, de acuerdo con la sensibilidad de cada antecedente.

El área no adjuntó ninguno de los instrumentos mencionados, ni propuso un mecanismo de acceso restringido para que la auditoría pudiera verificarlos.

VI. OBSERVACIONES

La evaluación se realizó conforme a las normas y lineamientos aplicables de la Agencia de Sistemas de Información (ASInf) y al marco COBIT 2019. Estos criterios guiaron el análisis de los procesos de detección, clasificación, prevención y respuesta frente a incidentes de seguridad de la información. También comprendieron las acciones de concientización, divulgación y protección, en función de la criticidad de los datos gestionados.

A continuación, se exponen los desvíos verificados durante el examen, ordenados según el proceso al que corresponden.

Objetivos de gestión

Organización, estrategia y actividades de apoyo para la tecnología y la información.

Observación N°1

Alinear, planificar y organizar - APO 01

- ✓ Gestionar el marco de I&T.

La Dirección General de Seguridad Informática carece de atribuciones operativas formalizadas para la toma de decisiones ante incidentes de seguridad. Ningún instrumento normativo identifica a los responsables de aprobar las acciones críticas.

Las disposiciones vigentes tampoco especifican qué autoridad aprueba la reasignación de los recursos económicos, ni definen los umbrales y los criterios de escalamiento técnico.

La falta de regulación incrementa la probabilidad de respuestas tardías o contradictorias frente a las contingencias. Cada decisión crítica se ejecuta según la interpretación del analista asignado.

Observación N°2

Alinear, planificar y organizar - APO 02

- ✓ Gestionar la estrategia.

La DGSEI gestiona la seguridad de la información sin estrategia formalizada ni aprobación institucional vigente.

El funcionamiento del área se apoya en prácticas operativas sin objetivos estratégicos definidos ni planificación temporal que ordene sus acciones.

Las iniciativas de concientización no cuentan con responsables asignados ni cronogramas de ejecución, lo que debilita su implementación sostenida.

Las decisiones se adoptan sin indicadores documentados ni trazabilidad sobre los criterios utilizados, lo que restringe la verificación de la base de priorización aplicada.

Observación N°3

Alinear, planificar y organizar - APO 09

- ✓ Gestionar los acuerdos de servicio.

Los servicios que presta la DGSEI no tienen definición formal ni parámetros claros de medición.

La Dirección no asegura la trazabilidad de qué entrega, a quién y en qué condiciones, porque no establece alcance, responsables ni métricas de desempeño.

Las autoridades de control no disponen de evidencia suficiente para validar la ejecución, calidad ni los resultados.

Observación N°4

Alinear, planificar y organizar - APO 10

- ✓ Gestionar los proveedores.

El organismo no incorpora requisitos de control de accesos en la planificación de sus contrataciones tecnológicas, ni asigna responsables de verificación del cumplimiento de las condiciones de seguridad pactadas con los proveedores.

Al no formalizar estos aspectos antes de la contratación, se reduce la posibilidad de exigirlos durante la ejecución del contrato.

Observación N°5

Alinear, planificar y organizar - APO 12

- ✓ Gestionar el riesgo.

La Dirección General de Seguridad Informática no acredita, con evidencia documental, la aplicación efectiva de las medidas técnicas de protección de datos personales exigidas por el Estándar de Seguridad (ES0902).³¹ Tampoco demuestra la ejecución concreta de la verificación de seguridad prevista en su propio esquema de control.

El organismo no detalló las medidas técnicas de cifrado, gestión de roles, límites de sesión y monitoreo de accesos. No aportó informes

³¹ Estándar de Seguridad (ES0902). Agencia de Sistemas de Información. Obtenido el mes de agosto del año 2025 en: <https://n9.cl/7yadd> [Accedido el 13/8/26]

de evaluación de seguridad ni ninguna otra evidencia de la aplicación de ese circuito de control.

Esa ausencia de evidencia expone al organismo a desviaciones no detectadas en los controles de seguridad de la información.

Observación N°6

Alinear, planificar y organizar - APO 13

- ✓ Gestionar la seguridad.

La DGSEI implementa herramientas de seguridad sin documentación que acredite su selección, evaluación técnica e integración.

La auditoría no verificó evidencia de alineación con el Estándar tecnológico vigente. La falta de registros impide confirmar los criterios de selección, condiciones de integración y adecuación a la normativa técnica.

Sin este respaldo, el organismo pierde sustento para analizar el desempeño de las herramientas y decidir sobre su continuidad operativa.

Definición, adquisición, implementación de soluciones e integración de los procesos del organismo.

Observación N°7

Construir, adquirir e implementar - BAI 03

- ✓ Gestionar la identificación y construcción de soluciones.

La Dirección General informa la aplicación de controles de seguridad sobre interfaces de programación y la ejecución de pruebas durante el período auditado.

La documentación presentada no describe los mecanismos de autenticación implementados ni detalla el alcance de los ensayos realizados. Tampoco evidencia la adecuación a los estándares definidos por la Agencia de Sistemas de Información.

El área declara información que no coincide con la documentación disponible. Esta diferencia impide confirmar que los controles y las pruebas se ejecutan de manera efectiva. Los entornos de producción, además, no cuentan con validación técnica documentada.

Observación N°8

Construir, adquirir e implementar - BAI 09

- ✓ Gestionar los activos.

El inventario de recursos tecnológicos del área se mantiene desactualizado y no cuenta con roles de Propietario ni Custodio definidos oficialmente.

Los equipos de control biométrico, la plataforma de firma digital, los servidores de autenticación y los equipos perimetrales de seguridad presentan la misma falta de registro actualizado.

Esta condición limita la clasificación de los activos críticos y debilita la cadena de responsabilidad asociada a cada componente tecnológico.

Frente a incidentes en la infraestructura, la falta de inventario actualizado y de roles formalmente definidos disminuye la capacidad de identificar el activo afectado y su responsable, impactando en la oportunidad de respuesta y en la evaluación del impacto del incidente.

Observación N°9

Construir, adquirir e implementar - BAI 10

- ✓ Gestionar la configuración.

Los resultados de evaluación presentados no contienen información técnica suficiente para verificar las modificaciones realizadas sobre los componentes que presentaban fallas de seguridad.

Los hallazgos son presentados como corregidos, sin que se adjunte la descripción de los cambios de configuración realizados ni la evidencia técnica que permita acreditar su corrección.

La entidad no dispone de un registro específico para documentar y auditar las correcciones implementadas sobre las configuraciones afectadas. El único respaldo disponible es el informe de evaluación de seguridad.

Esta falta de historial de cambios impide validar qué modificación puntual se aplicó a cada componente.

Entrega y soporte de servicios para la tecnología y la información.

Observación N°10

Entregar, dar servicio y soporte - DSS 01

- ✓ Gestionar las operaciones.

El área no deja evidencia documentada de las verificaciones realizadas sobre los componentes críticos de la infraestructura de seguridad.

Esto limita la capacidad del organismo para acreditar, a través de registros verificables, el control de sus operaciones diarias y detectar fallas antes de que produzcan mayores consecuencias.

Observación N°11

Entregar, dar servicio y soporte - DSS 02

- ✓ Gestionar las peticiones y los incidentes de servicio.

La dependencia gestiona los incidentes de seguridad sin una guía formal que establezca las tareas de soporte técnico.

La ausencia de pautas de coordinación genera respuestas diferentes ante problemas informáticos idénticos según el sector interviniente, lo que afecta la trazabilidad de los cambios aplicados en las plataformas.

La falta de estandarización en la gestión de incidentes restringe la posibilidad de consolidar un historial confiable que permita diagnosticar y resolver incidentes de forma consistente y trazable.

Observación N°12

Entregar, dar servicio y soporte - DSS 04

- ✓ Gestionar la continuidad.

Las plataformas informáticas de la DGSEI operan sin planes de continuidad, esquemas de redundancia ni procedimientos formalizados de recuperación ante contingencias.

La Dirección no definió los tiempos máximos de interrupción ni los niveles tolerables de pérdida de datos frente a incidentes críticos.

No contar con esos umbrales interfiere en la evaluación del comportamiento de la infraestructura ante una interrupción real. Esta falta de parámetros deja sin sustento las pruebas de continuidad que el área pretenda acreditar ante terceros.

Observación N°13

Entregar, dar servicio y soporte - DSS 05

- ✓ Gestionar los servicios de seguridad.

La gestión de ciberseguridad en la Dirección se realiza sin un marco normativo que regule la interacción entre los dispositivos de detección, registro y respuesta automatizada.

El área no define criterios formales para validar las fuentes de datos ni para priorizar los eventos de seguridad. En ausencia de esos parámetros, los analistas responden de forma reactiva ante cada amenaza sin un marco que estructure sus decisiones.

El organismo no brinda cobertura integral de seguridad informática a la totalidad de las dependencias alcanzadas por la normativa vigente,

pese a que la Resolución N°177/ASInf/13 establece la aplicación del marco de seguridad informática para todo el ámbito del GCBA.

La operación independiente de los dispositivos fragmenta la visibilidad del estado de seguridad y acota la capacidad del organismo para demostrar la coordinación entre herramientas.

Monitoreo del rendimiento tecnológico y objetivos de control interno.

Observación N°14

Monitorear, evaluar y valorar - MEA 01

- ✓ Gestionar la monitorización del desempeño y la conformidad.

Las estadísticas de incidentes y las clasificaciones de impacto permanecen como información aislada dentro del organismo, ya que la entidad no incorpora métricas de respuesta técnica en la gestión del área.

La ausencia de un marco de control unificado resta valor a estos registros para la mitigación preventiva de los riesgos en ciberseguridad.

La DGSEI registra los incidentes, pero no evidencia que esa información haya sido utilizada para tomar decisiones de gestión ni que los controles se ajusten a los objetivos definidos durante el período auditado.

VII. RECOMENDACIONES

Las recomendaciones que se presentan a continuación se formulan a partir de los desvíos identificados durante el examen y tienen por finalidad contribuir al fortalecimiento de los controles y procesos involucrados.

Para su elaboración se consideraron los objetivos y prácticas de gestión establecidos en COBIT 2019 y las normas, políticas y lineamientos aplicables de la Agencia de Sistemas de Información (ASInf), procurando que cada recomendación mantenga correspondencia directa con la observación a la que se encuentra asociada.

Objetivos de gestión

Organización, estrategia y actividades de apoyo para la tecnología y la información.

Recomendación N°1

Alinear, planificar y organizar - APO 01

- ✓ Gestionar el marco de I&T.

Formalizar las atribuciones de la Dirección General de Seguridad Informática para la gestión y resolución de incidentes de seguridad e incorporarlas al marco normativo y operativo vigente del área.

Definir en el procedimiento los niveles de autoridad para gestionar incidentes, incluyendo la aprobación de acciones críticas y la utilización o reasignación de recursos, con responsabilidades asignadas a roles o funciones.

Incorporar criterios de severidad y escalamiento técnico, junto con los canales formales de comunicación con las autoridades superiores cuando la situación requiera decisiones que excedan las atribuciones de la Dirección.

La atención de los incidentes debe contar con registros que permitan identificar las decisiones, responsables, acciones y aprobaciones, así como con revisiones periódicas para mantener actualizadas las atribuciones ante cambios organizativos o funcionales.

Recomendación N°2

Alinear, planificar y organizar - APO 02

- ✓ Gestionar la estrategia.

Elaborar y aprobar formalmente un plan estratégico de seguridad de la información que establezca su alineación con las directrices del Gobierno de la Ciudad Autónoma de Buenos Aires y las políticas de la Agencia de Sistemas de Información.

Partir de un diagnóstico de la situación actual del área para identificar los desvíos existentes entre sus capacidades y los objetivos que el

organismo se propone alcanzar en materia de seguridad de la información.

La planificación requiere responsables y cronogramas para cada iniciativa de concientización y divulgación, junto con instancias de seguimiento que permitan verificar su avance durante la ejecución de las actividades.

Incorporar indicadores y valores de referencia para evaluar el cumplimiento de los objetivos y resultados de las campañas, junto con una revisión periódica de la estrategia y el registro de los criterios utilizados para definir prioridades y decisiones.

Recomendación N°3

Alinear, planificar y organizar - APO 09

- ✓ **Gestionar los acuerdos de servicio.**

Definir y formalizar Acuerdos de Nivel Operativo para los servicios de seguridad tecnológica que la Dirección General de Seguridad Informática presta a las reparticiones del Gobierno de la Ciudad Autónoma de Buenos Aires, especificando el alcance, responsables y condiciones técnicas de cada servicio.

Establecer categorías de atención, prioridades y plazos de respuesta y resolución, de acuerdo con las características de cada servicio.

La gestión de los servicios requiere registros de desempeño y mecanismos de seguimiento que permitan verificar su cumplimiento, calidad y resultados.

Recomendación N°4

Alinear, planificar y organizar - APO 10

- ✓ **Gestionar los proveedores.**

Incorporar en las Especificaciones Técnicas Particulares de las contrataciones tecnológicas requisitos formales de control de accesos, alineados con la naturaleza del bien o servicio contratado.

Asignar en cada contratación un responsable de verificar el cumplimiento de las condiciones de seguridad pactadas durante la ejecución del contrato.

Las verificaciones requieren documentación que permita acreditar el cumplimiento de las condiciones de seguridad ante los organismos de control.

Recomendación N°5

Alinear, planificar y organizar - APO 12

- ✓ Gestionar el riesgo.

Detallar, para cada sistema comprendido en su ámbito de control, las medidas técnicas de protección de datos personales exigidas por el Estándar de Seguridad (ES0902) definido por la Agencia de Sistemas de Información. Esto incluye autenticación, cifrado, límites de sesión, gestión de roles y monitoreo de accesos.

Incorporar el informe de evaluación de seguridad correspondiente a cada sistema, junto con el registro de correcciones exigidas y su verificación posterior.

Mantener esta documentación disponible como evidencia de la aplicación efectiva de las medidas técnicas y del circuito de revisión previsto en el Proceso de control de cambios en software de aplicación provisto por Organismos (PC0901).³²

Recomendación N°6

Alinear, planificar y organizar - APO 13

- ✓ Gestionar la seguridad.

Diseñar un procedimiento de selección y evaluación técnica de herramientas de seguridad. Este instrumento verifica la alineación de cada componente con el estándar de seguridad vigente, asigna los responsables de la evaluación, fija los criterios técnicos de aceptación y registra las condiciones de integración con la infraestructura existente.

El procedimiento debe definir también los parámetros de desestimación, para que quede documentado por qué una herramienta evaluada no avanza hacia su implementación y no solo el fundamento de las que sí se incorporan.

Una instancia de revisión periódica tiene que confirmar la vigencia de esos criterios frente a los cambios tecnológicos o normativos y evaluar si las herramientas ya implementadas siguen cumpliendo los requisitos técnicos exigidos al momento de su incorporación.

Definición, adquisición, implementación de soluciones e integración de los procesos del organismo.

Recomendación N°7

Construir, adquirir e implementar - BAI 03

- ✓ Gestionar la identificación y construcción de soluciones.

³² Proceso de control de cambios en software de aplicación provisto por Organismos (PC0901).
Obtenido el año 2014 en: <https://n9.cl/6hgt8> [Accedido el 13/8/26]

El área es responsable de instaurar un procedimiento formal de pruebas sobre las interfaces de programación. El plan de ensayos debe fijar el alcance y la metodología según el nivel de criticidad de cada interfaz.

La documentación de cada ensayo debe incluir los mecanismos de autenticación evaluados y los resultados obtenidos. Antes de la aprobación, corresponde que un sector distinto del que desarrolló el componente aplique una instancia de aseguramiento de calidad.

Resulta necesario que un responsable del área valide que la información declarada coincida con la documentación técnica disponible. Sin esa validación registrada, el pasaje a producción no debe habilitarse y la misma exigencia rige para los entornos ya existentes.

Recomendación N°8

Construir, adquirir e implementar - BAI 09

- ✓ Gestionar los activos.

La Dirección necesita implementar un mecanismo de actualización periódica del inventario de recursos tecnológicos, con alcance sobre los equipos de control biométrico, la plataforma de firma digital, los servidores de autenticación, los equipos perimetrales de seguridad y el resto de los componentes bajo administración directa del área.

Cada activo debe quedar registrado con su propietario y custodio asignados, conforme a la Política de Clasificación de la Información (PO0402), con la periodicidad de revisión y el área responsable de ejecutarla.

Según su nivel de criticidad, queda a cargo del área identificar y priorizar dentro del inventario los activos clave para su funcionamiento. El organismo tiene que asegurar que cada activo cuente con seguimiento durante todo su ciclo de vida, desde la incorporación hasta la baja y con controles que mantengan identificada la responsabilidad sobre su gestión.

Recomendación N°9

Construir, adquirir e implementar - BAI 10

- ✓ Gestionar la configuración.

La información contenida en los informes de evaluación de vulnerabilidades requiere detallar la corrección aplicada a cada hallazgo, el cambio de configuración realizado y el componente afectado. También debe incorporar la evidencia técnica que permita verificar dicha corrección.

Complementar el circuito de tickets con un registro formal del historial de cambios de configuración asociado a cada vulnerabilidad detectada, que facilite la consulta de las modificaciones realizadas y documente su revisión.

Entrega y soporte de servicios para la tecnología y la información.

Recomendación N°10

Entregar, dar servicio y soporte - DSS 01

- ✓ Gestionar las operaciones.

Los registros correspondientes a las verificaciones periódicas de la infraestructura de seguridad deberán incluir la fecha, el responsable y el resultado obtenido en cada revisión.

Cada verificación debe dejar constancia del estado operativo, las actualizaciones de los componentes críticos y la coincidencia entre la configuración vigente y la configuración autorizada para cada equipo.

Esta documentación permitirá dejar constancia de los controles realizados sobre las operaciones diarias.

Recomendación N°11

Entregar, dar servicio y soporte - DSS 02

- ✓ Gestionar las peticiones y los incidentes de servicio.

Una guía escrita debe establecer las tareas de soporte técnico correspondientes a cada tipo de incidente de seguridad y definir su aplicación para todos los sectores intervinientes.

El registro centralizado de cada caso tendrá que identificar el sector que intervino, el diagnóstico realizado, la acción aplicada sobre la plataforma y el resultado obtenido.

Recomendación N°12

Entregar, dar servicio y soporte - DSS 04

- ✓ Gestionar la continuidad.

Es pertinente que la Dirección defina y formalice, para cada plataforma de seguridad y según su nivel de criticidad, el tiempo máximo admisible de interrupción del servicio (RTO) y el volumen máximo de datos que podría perderse frente a un incidente (RPO).

La continuidad operativa de cada plataforma crítica requiere un plan formalizado por escrito, con procedimientos de recuperación específicos, pasos a seguir, responsables de ejecución y criterios

para definir cuándo el servicio ha sido restablecido ante una interrupción.

La documentación de los esquemas de redundancia y alta disponibilidad ya implementados debe incorporar diagramas de arquitectura y registros de las pruebas de recuperación realizadas, para demostrar la continuidad operativa con evidencia respaldatoria.

Recomendación N°13

Entregar, dar servicio y soporte - DSS 05

- ✓ Gestionar los servicios de seguridad.

El área tiene que definir un marco normativo escrito que regule la interacción entre los dispositivos de detección, registro y respuesta automatizada, con criterios formales para validar las fuentes de datos y priorizar los eventos de seguridad.

Para todas las dependencias alcanzadas por la Resolución N°177/ASInf/13, corresponde acreditar la cobertura de seguridad informática. Un relevamiento debe identificar cuáles cuentan con cobertura y cuáles aún no.

La Dirección General de Seguridad Informática necesita respaldar con evidencia verificable la coordinación entre los dispositivos de seguridad, detección, registro y respuesta: diagramas de integración, registros de eventos compartidos entre plataformas y reportes que comprueben su funcionamiento conjunto. Así evita una gestión aislada por herramienta.

Monitoreo del rendimiento tecnológico y objetivos de control interno.

Recomendación N°14

Monitorear, evaluar y valorar - MEA 01

- ✓ Gestionar la monitorización del desempeño y la conformidad.

Elaborar un marco de control unificado que integre las estadísticas de incidentes, las clasificaciones de impacto y las métricas de respuesta técnica y establezca cómo esa información se utiliza para la toma de decisiones de gestión y el ajuste de los controles vigentes.

Los tableros de control, informes y reportes que el organismo declara utilizar requieren encontrarse disponibles para su verificación por parte de la auditoría, con acceso restringido cuando la sensibilidad de la información lo justifique, sin que las medidas de protección de los datos impidan acreditar su utilización efectiva ante el órgano de control.

Los objetivos de control del área deben quedar documentados para cada período, junto con los resultados alcanzados, de manera que

“2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires”

pueda comprobarse si los controles implementados responden a lo previsto.

VIII. CONCLUSIONES

La Dirección General de Seguridad Informática opera las plataformas que detectan ataques, bloquean accesos indebidos y sostienen disponibles los servicios digitales del Gobierno de la Ciudad. También administra la infraestructura de monitoreo que sostiene esas tareas. El canal BA-CSIRT, por su parte, recibe y gestiona las denuncias de incidentes de seguridad que presentan los ciudadanos.

Aunque el organismo informó que esas herramientas operaron con normalidad durante el período analizado, el examen realizado identificó debilidades en la organización interna y en la documentación que respalda la gestión.

Ante un incidente crítico, no se encuentra definido quién aprueba la acción, quién autoriza los recursos económicos de emergencia ni bajo qué criterios se escala el caso. La misma falta de definición aparece en otros aspectos de la gestión. Tampoco hay un plan estratégico aprobado ni acuerdos que determinen los servicios que el área presta a otras reparticiones del Gobierno.

El organismo no incorpora, en sus contrataciones de tecnología, la exigencia de garantías de control de accesos al proveedor. El organismo no acredita, con documentación propia, la verificación del estándar de protección de datos personales, la evaluación técnica de las herramientas de seguridad que incorpora ni los controles sobre sus interfaces de programación. El organismo no actualizó el inventario de sus equipos sensibles, como los sistemas de control biométrico y la plataforma de firma digital. La documentación aportada en el descargo solo permitió acreditar algunos aspectos, como determinadas cláusulas contractuales incorporadas en las contrataciones de servicios de seguridad.

En la operación diaria, el área no documenta las verificaciones que realiza sobre sus componentes críticos ni dispone de una guía común que indique cómo debe actuar cada sector técnico ante un mismo tipo de incidente. Tampoco definió los tiempos máximos de interrupción de un servicio ni el nivel de pérdida de información admisible. La forma en que interactúan los dispositivos de detección y respuesta no está definida en ningún documento.

El organismo no acreditó que la cobertura de seguridad alcance a todas las dependencias que la normativa vigente obliga a proteger, ni que la información obtenida de los incidentes se utilice para orientar decisiones de gestión. Estas deficiencias generan riesgos concretos: ante un incidente real, los distintos sectores podrían actuar sin coordinación y sin criterios comunes de respuesta.

Con el inventario actualizado y clasificado según su criticidad, el área podrá incorporar esos datos a la plataforma de respuesta automatizada y priorizar con mayor rapidez los sistemas más sensibles del Gobierno.

El equipo de auditoría cumplió con el objetivo previsto mediante los procedimientos aplicados, sin que se presentaran limitaciones que afectaran el desarrollo del examen.

Las tareas de auditoría culminaron en julio de 2026.

ANEXO I

El marco COBIT 2019 organiza el gobierno y la gestión de la información y tecnología organizacional mediante un conjunto de principios que orientan su diseño y aplicación.

Estos principios se dividen en dos grupos: seis principios aplicables al sistema de gobierno de la organización, que establecen las características que debe cumplir un sistema de gobierno efectivo y tres principios aplicables al propio marco de referencia, que guían su estructura, flexibilidad y capacidad de adaptación a las necesidades de cada organización.

Sobre la base de este enfoque, COBIT 2019 define objetivos de gobierno y gestión que permiten alcanzar los resultados esperados para que la información y la tecnología contribuyan al cumplimiento de los objetivos organizacionales.

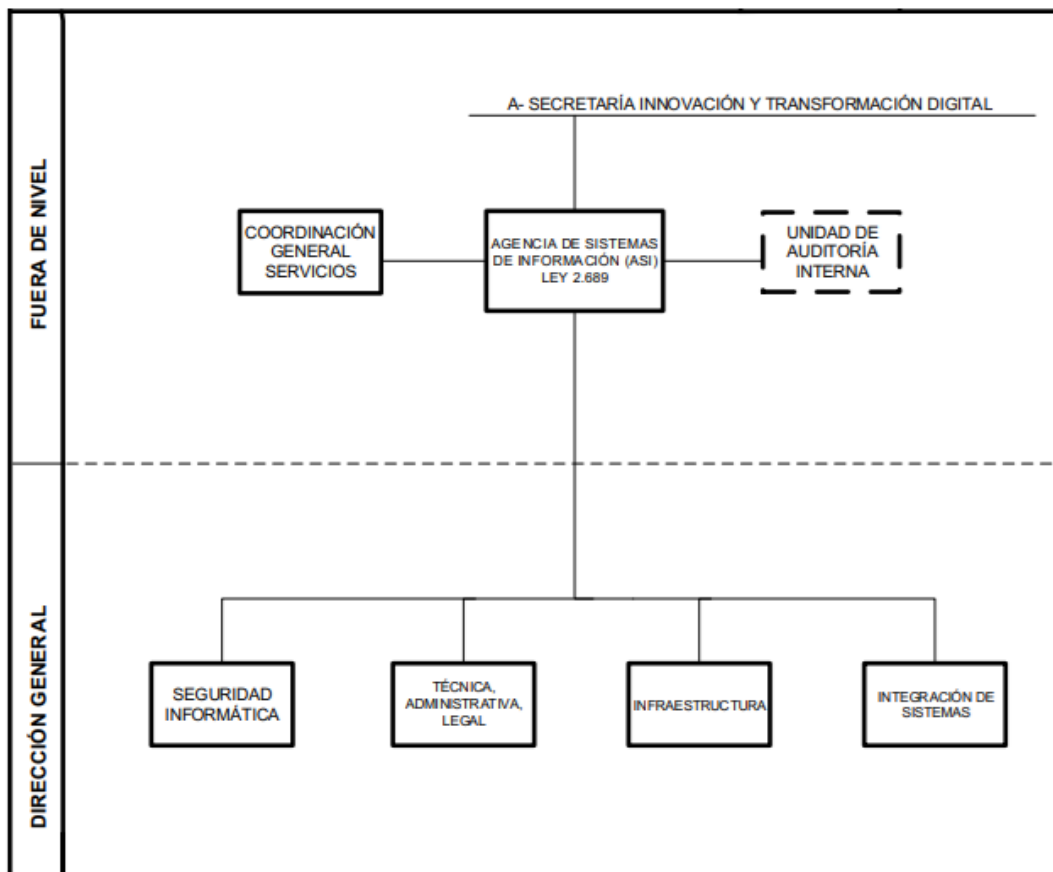
El modelo establece cinco objetivos de gobierno y treinta y cinco objetivos de gestión, cada uno asociado con componentes del sistema de gobierno que permiten su implementación y operación.

Estos objetivos se logran mediante la interacción de los componentes del sistema de gobierno, que proporcionan los elementos necesarios para diseñar, implementar y mantener un sistema de gobierno integral. Los componentes contemplados por COBIT 2019 son: procesos; estructuras organizativas; principios, políticas y procedimientos; información; cultura, ética y comportamiento; personas, habilidades y competencias; y servicios, infraestructura y aplicaciones.



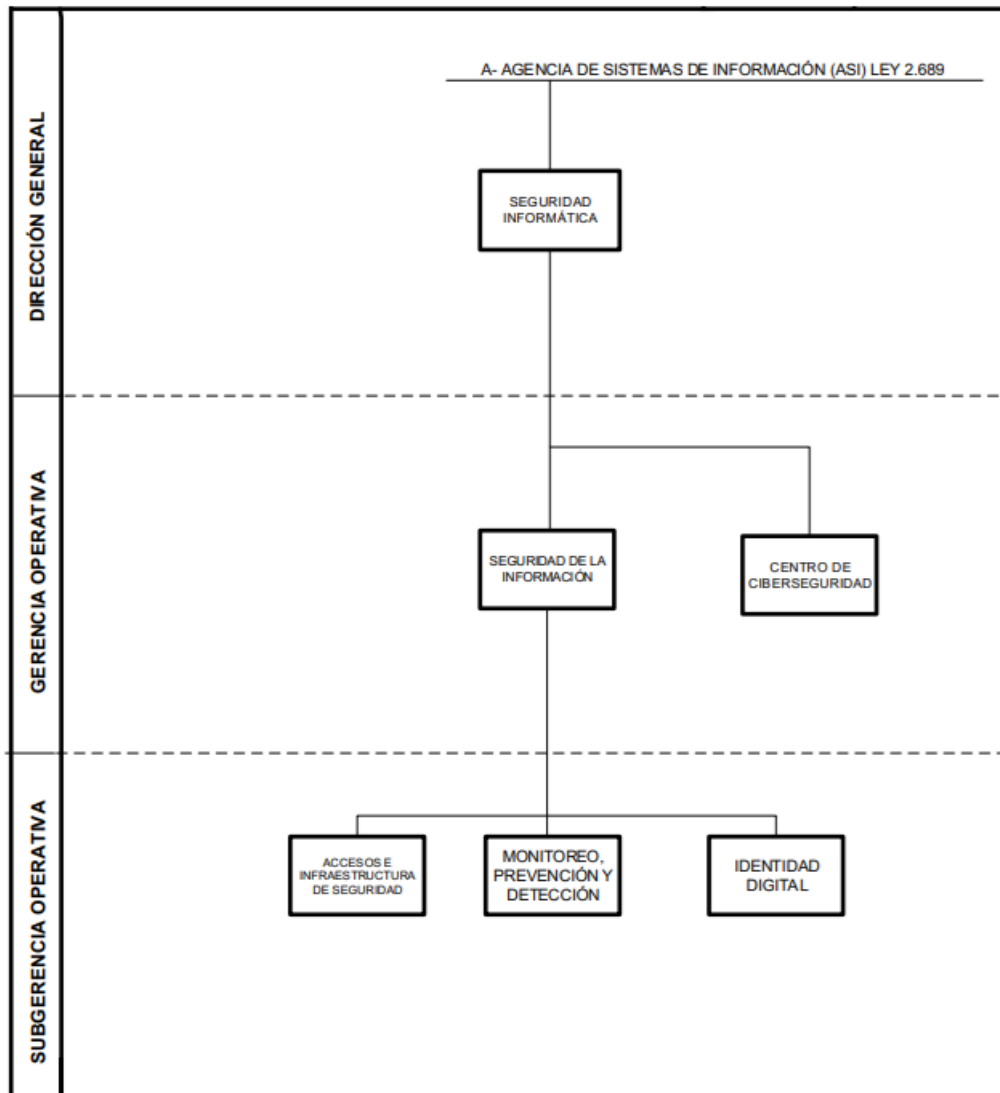
Fuente: Asociación de Auditoría y Control de Sistemas de Información

ANEXO II



Fuente: GCBA

ANEXO III



Fuente: GCBA

ANEXO IV

Responsabilidades Primarias.

Con el fin de entender las funciones y tareas asignadas, se detallan las responsabilidades primarias asignadas a la Dirección General de Seguridad Informática.

1. Dirección General de Seguridad Informática (DGSEI)

"Elaborar y/o aprobar las pautas, políticas y normas de seguridad física y lógica de sistemas, equipos informáticos, datos y comunicaciones del Gobierno de la Ciudad de Buenos Aires."

"Intervenir en las definiciones de los esquemas de seguridad del software, datos y comunicaciones, de los programas de prevención y control de seguridad, y de los planes de contingencia."

"Definir, implementar y administrar la identidad de los usuarios del Gobierno de la Ciudad de Buenos Aires."

"Administrar la infraestructura de firma digital del Gobierno de la Ciudad de Buenos Aires y gestionar los certificados digitales para las plataformas y aplicativos webs."

"Administrar y controlar la operatividad de los sitios de internet, el servicio de correo electrónico y el servicio de acceso a internet."

"Administrar y controlar los procedimientos de seguridad lógica de acceso a los componentes del software de base y aplicativo de los servidores bajo responsabilidad de la Agencia de Sistemas de Información."

"Definir los mecanismos de alarmas y monitoreo de sistemas y las redes de comunicaciones para detectar intentos de acceso no autorizados al software aplicativo, así como a los datos almacenados en los servidores bajo responsabilidad de la Agencia de Sistemas de Información."

"Elaborar y ejecutar proyectos relacionados con la asistencia a la ciudadanía en temáticas de seguridad de la información."

"Definir y elaborar planes de capacitación para usuarios del gobierno y para la ciudadanía en general, con el objetivo de entrenar, informar y concientizar en materia de seguridad informática."

Las responsabilidades primarias de las áreas bajo la órbita de la Dirección General de Seguridad Informática, vinculadas con la seguridad de la información y consideradas relevantes para el alcance de la auditoría, son las siguientes:

1.1. Gerencia Operativa Centro de Ciberseguridad

"Asistir a la Dirección General en la elaboración, implementación y ejecución de proyectos relacionados con asistencia a la ciudadanía en temas de seguridad de la información."

"Asistir a la Dirección General en la planificación de las capacitaciones y entrenamientos en materia de seguridad informática en coordinación con otras áreas de gobierno."

"Recibir, clasificar y gestionar reportes de incidentes de seguridad de la información."

Proponer y gestionar acuerdos de colaboración con otras áreas de gobierno, y entidades afines, con el propósito de agilizar y mejorar los procesos de detección de amenazas de seguridad informática y facilitar lazos de colaboración y de asistencia técnica."

"Diseñar y ejecutar acciones de concientización, prevención y divulgación para promover el uso seguro y responsable de las TICs."

1.2. Gerencia Operativa Seguridad de la Información

"Definir e implementar el software relacionado con el análisis de riesgo y pruebas de vulnerabilidad de los servidores, detección de ataques en tiempo real y acceso no autorizado a las redes, telecomunicaciones, aplicativos y sistemas bajo la responsabilidad de la Agencia de Sistemas de Información."

"Definir el nivel de seguridad requerido para el pasaje a producción de las aplicaciones que se encuentren bajo responsabilidad de la Agencia de Sistemas de Información."

"Analizar y generar informes de los incidentes y/o ataques que pudieran afectar la prestación de servicios y elevarlos al titular de la Dirección General de Seguridad Informática."

"Definir el software para contener y resguardar la identidad de los usuarios del Gobierno de la Ciudad de Buenos Aires."

"Implementar un sistema de antimalware en las estaciones de trabajo del Gobierno de la Ciudad de Buenos Aires y en los servidores bajo responsabilidad de la Agencia de Sistemas de Información."

"Definir las políticas de seguridad en estaciones de trabajo e identidad digital de los usuarios."

"Administrar y controlar la implementación de los sistemas de autenticación y autorización de usuarios y servicios a los recursos informáticos de la red del Gobierno de la Ciudad Autónoma de Buenos Aires."

"Definir la arquitectura e infraestructura de los activos de seguridad informática."

"Investigar, analizar y definir las pautas de seguridad informática en los proyectos del Gobierno de la Ciudad Autónoma de Buenos Aires."

"Asistir a la Dirección General en la elaboración de políticas y normas de seguridad física y lógica de sistemas, equipos."

1.2.1. Subgerencia Operativa Accesos e Infraestructura de Seguridad

"Configurar y operar el sistema de correlación de eventos que proveen los equipos de seguridad."

"Instalar, configurar y operar el hardware y el software de los equipos informáticos utilizados para el análisis y testeo de penetración de aplicaciones web, aplicaciones móviles y activos de red."

"Mantener actualizados los firmwares, firmas de detección y sistemas operativos de los activos de seguridad bajo la responsabilidad de la Gerencia Operativa."

"Diseñar, mantener y actualizar la plataforma de seguridad de la información."

"Administrar y autorizar los accesos remotos a la red del Gobierno de la Ciudad de Buenos Aires."

1.2.2. Subgerencia Operativa Monitoreo, Prevención y Detección

"Administrar los sistemas de alertas tempranas de incidentes de seguridad informática."

"Implementar y controlar los procesos que garanticen el nivel de seguridad requerido para el pasaje a producción de las aplicaciones que se encuentren bajo responsabilidad de la Agencia de Sistemas de Información."

"Realizar capacitaciones sobre herramientas de detección de vulnerabilidades y capacitar a desarrolladores respecto de programación segura."

"Administrar los equipos de seguridad para la prevención de intrusiones y vulnerabilidades."

"Realizar los análisis de seguridad en búsqueda de las causas de un ataque informático detectado y/o reportado."

"Realizar diagnósticos que permitan detectar brechas de seguridad en las aplicaciones publicadas y definir su riesgo."

1.2.3. Subgerencia Operativa Identidad Digital

"Administrar el software para contener y resguardar la identidad de los usuarios del Gobierno de la Ciudad de Buenos Aires."

"Administrar el sistema de antimalware de las estaciones de trabajo del Gobierno de la Ciudad de Buenos Aires y de los servidores bajo responsabilidad de la Agencia de Sistemas de Información."

"Proveer, mantener y actualizar la plataforma para el despliegue automatizado de sistemas operativos para estaciones de trabajo cumpliendo las normas de seguridad preestablecidas."

“2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires”

ANEXO V

ADMINISTRACIÓN GUBERNAMENTAL DEL GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES DISTRIBUCIÓN ADMINISTRATIVA DE CRÉDITOS - EJERCICIO 2025 - En Pesos

Juris	SubJuris	Entidad	UE	Programa	SubPrograma	Descripción	Crédito Sanción
21	0	270	687			Dirección General de Seguridad Informática	8.219.811.736

Fuente: GCBA

ANEXO VI

ADMINISTRACION DEL GOBIERNO DE LA CIUDAD DE BUENOS AIRES PLAN PLURIANUAL DE INVERSIONES PUBLICAS 2025-2027 (en pesos)

Jur	Og	UE	Pg	Sg.	Py.	Ac.	Ob	FF	Denominación	Inversiones		
										2025	2026	2027
270									AGENCIA SISTEMAS DE INFORMACION	28.825.529.464	0	0
		682							DIRECCIÓN GENERAL DE INFRAESTRUCTURA	22.042.051.747	0	0
			96						INFRAESTRUCTURA INFORMÁTICA	22.042.051.747	0	0
				61					INFRAESTRUCTURA	8.502.149.137	0	0
					0	1	11		MANTENIMIENTO FIBRA OPTICA	4.273.966.998	0	0
					0	2	11		MANTENIMIENTO CONECTIVIDAD	4.228.182.138	0	0
						62			INFRAESTRUCTURA DC	13.539.902.610	0	0
					0	1	11		MANTENIMIENTO INFRAESTRUCTURA DC	3.862.116.014	0	0
					0	2	11		MANTENIMIENTO INTEGRAL DE CENTRALES TELEFÓNICAS GCBA	792.749.438	0	0
					0	3	11		PLATAFORMA Y APLICATIVOS	88.508.525	0	0
					0	5	11		UPGRADE DE TRÁFICO DE INTERNET	748.907.643	0	0
					0	8	11		RENOVACION INTEGRAL DE EQUIPAMIENTO EN DATA CENTER	8.047.820.870	0	0
		683							DIRECCIÓN GENERAL DE INTEGRACIÓN DE SISTEMAS	2.945.671.686	0	0
			94						DES. Y CALIDAD DE APLIC.	2.945.671.686	0	0
				61					INT. DE SISTEMAS	2.945.671.686	0	0
					0	1	11		MANTENIMIENTO PLATAFORMA Y APLICATIVOS GCBA	2.945.671.686	0	0
		687							DIRECCIÓN GENERAL DE SEGURIDAD INFORMÁTICA	3.937.806.057	0	0
			96						SEGURIDAD INFORMÁTICA	3.937.806.057	0	0
				62					SEGURIDAD INFORMÁTICA	3.937.806.057	0	0
					0	3	11		PLATAFORMA DE SEGURIDAD Y SOC	3.586.388.758	0	0
					0	5	11		FIRMA DIGITAL	339.407.298	0	0

Fuente: GCBA

ANEXO VII

ADMINISTRACION GUBERNAMENTAL DEL GOBIERNO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES PROGRAMA POR FUENTE DE FINANCIAMIENTO PROYECTO DE PRESUPUESTO 2025

Jur	Sjur	Ent	UE	Prog	iprog	Descripción	Fte11	Fte12	Fte13	Fte14	Fte15	Fte22	TOTAL
21	0	270				AGENCIA SISTEMAS DE INFORMACION	63.446.845.066	0	0	0	0	0	63.446.845.066
21	0	270	682			Dirección General de Infraestructura	35.528.390.620	0	0	0	0	0	35.528.390.620
21	0	270	682	96		Infraestructura Informática	35.528.390.620	0	0	0	0	0	35.528.390.620
21	0	270	682	96	0	Infraestructura Informática	35.528.390.620	0	0	0	0	0	35.528.390.620
21	0	270	683			Dirección General de Integración de Sistemas	10.124.296.579	0	0	0	0	0	10.124.296.579
21	0	270	683	94		Desarrollo y Calidad de Aplicaciones	10.124.296.579	0	0	0	0	0	10.124.296.579
21	0	270	683	94	0	Desarrollo y Calidad de Aplicaciones	10.124.296.579	0	0	0	0	0	10.124.296.579
21	0	270	686			Coordinación General de Servicios	2.958.933.697	0	0	0	0	0	2.958.933.697
21	0	270	686	97		Estandarización de Aplicación y Tecnología	2.958.933.697	0	0	0	0	0	2.958.933.697
21	0	270	686	97	0	Estandarización de Aplicación y Tecnología	2.958.933.697	0	0	0	0	0	2.958.933.697
21	0	270	687			Dirección General de Seguridad Informática	8.219.811.736	0	0	0	0	0	8.219.811.736
21	0	270	687	98		Seguridad Informática	8.219.811.736	0	0	0	0	0	8.219.811.736
21	0	270	687	98	0	Seguridad Informática	8.219.811.736	0	0	0	0	0	8.219.811.736
21	0	270	8056			Agencia de Sistemas de Información	6.615.412.434	0	0	0	0	0	6.615.412.434
21	0	270	8056	7		Actividades Comunes	6.615.412.434	0	0	0	0	0	6.615.412.434
21	0	270	8056	7	0	Actividades Comunes	6.615.412.434	0	0	0	0	0	6.615.412.434

Fuente: GCBA

“2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires”

ANEXO VIII

Programa: 98 Seguridad Informática	
Unidad Ejecutora: Dirección General de Seguridad Informática	
Jurisdicción: 21.JEFATURA DE GABINETE DE MINISTROS	
Finalidad: Administración Gubernamental	
Función: Dirección ejecutiva	
PRESUPUESTO FINANCIERO	
Inciso Principal	IMPORTE
Gastos en personal	972.475.523
Personal Permanente	299.413.270
Personal Transitorio	656.272.862
Asignaciones familiares	2.520.878
Asistencia social al personal	14.041.478
Gabinete de autoridades superiores	227.035
Bienes de consumo	51.069.985
Productos alimenticios, agropecuarios y forestales	50.037.588
Productos químicos, combustibles y lubricantes	1.032.397
Servicios no personales	7.041.175.037
Mantenimiento, reparación y limpieza	909.084.050
Servicios profesionales, técnicos y operativos	131.001.609
Servicios Especializados, Comerciales y Financieros	5.931.133.388
Pasajes, viáticos y movilidad	1.047.228
Otros servicios	68.908.762
Bienes de uso	155.091.191
Maquinaria y equipo	129.242.659
Activos intangibles	25.848.532
TOTAL	8.219.811.736

Fuente: GCBA

ANEXO IX

ADMINISTRACIÓN GUBERNAMENTAL DEL GOBIERNO DE LA CIUDAD AUTONOMA DE BUENOS AIRES
 PRODUCCION PÚBLICA POR PROYECTO - EJERCICIO 2025

Juris	OGESE	UE	Programa	SubPrograma	Proyecto	Actividad	Obra	Descripción	Producto	Unidad de medida	Total
21	270	687						Dirección General de Seguridad Informática			
21	270	687	98					Seguridad Informática			
21	270	687	98	0				Seguridad Informática			
21	270	687	98	0	62			SEGURIDAD INFORMATICA			
21	270	687	98	0	62	0		Plataforma de Seguridad y SOC			
21	270	687	98	0	62	0	3	Plataforma de Seguridad y SOC	Respuesta Ataques Informáticos al GCABA	Firewall	3.200.000
21	270	687	98	0	62	0		Firma Digital			
21	270	687	98	0	62	0	5	Firma Digital	Mantenimiento Plataforma Digital - Certificados Emitidos	Certificado	2.160

Fuente: GCBA

ANEXO X

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
46465547/23	Licitación pública	8056-1990-LPU23	Renovación de licencias, actualizaciones y soporte de 9 equipos Firewall Fortinet y 1 licencia FortiAnalyzer (u\$s 647.830)	DGSEI	8056-1558-OC24	1/3/2024	\$ 525.843.611	03/03/25	KRUGG TECHNOLOGIES S.A.
4262913/24	Licitación pública	8056-0046-LPU24	Renovación suscripción licencias QRadar SIEM, Qradar SOAR y playbook de SOAR (u\$s 527.000)	DGSEI	8056-1902-OC24	7/3/2024	\$ 437.726.200	07/03/25	TECNOLOGIA, COMUNICACIONES Y NEGOCIOS S.A.
7868218/24	Licitación pública	8056-0231-LPU24	OC Abierta - Adquisición de componentes para la solución integral de hardware y software y servicio de soporte técnico del control de acceso y presentismo para diferentes edificios del GCBA (u\$s 534.510,82)	DGSEI	8056-0010-OCA24	5/4/2024	\$ 452.463.409	04/04/26	CLAUDIO OSCAR FREDA
45635660/22	Prórroga	8056-1887-LPU22	Prórroga x 12 meses (mar-may/24) OC 8056-1841-OC23 - Servicio SOC Nivel 1 y 2	DGSEI	8056-3996-OC24	16/4/2024	\$ 23.232.000	03/03/25	RAN INGENIERIA DE SISTEMAS SRL
14720483/24	Licitación pública	8056-0575-LPU24	Renovación de Licencias, Actualizaciones y Soporte de cinco equipos Firewall Fortinet hasta el 31/10/24 (u\$s 483.600)	DGSEI	8056-6223-OC24	22/5/2024	\$ 408.450.000	31/10/24	POINT IT SRL
14491250/24	Licitación pública	8056-0561-LPU24	Adquisición de Solución de Seguridad Avanzada del Endpoint (u\$s 187.250)	DGSEI	8056-6555-OC24	28/5/2024	\$ 163.469.250	27/05/25	RAN INGENIERIA DE SISTEMAS SRL
EX-2024-18917840-GCBA-ASInf	Licitación pública	8056-0797-LPU24	Renovación de licencias, actualizaciones y soporte de software Acunetix y Burp	DGSEI	8056-8649-OC24	28/6/2024	\$ 148.039.790	28/06/25	KRUGG TECHNOLOGIES S.A.
EX-2024-14491250-GCBA-ASInf	Ampliación	8056-0561-LPU24	Ampliación OC 8056-6555-OC24 - Adquisición de Solución de Seguridad Avanzada del Endpoint para SBASE (u\$s 3.745)	DGSEI	8056-9869-OC24	18/7/2024	\$ 3.269.385	27/05/25	RAN INGENIERIA DE SISTEMAS SRL

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2024-19920956-GCBA-ASInf	Licitación pública	8056-0841-LPU24	OC Abierta - Adquisición de kits de identificación de firma digital	DGSEI	8056-0080-OCA24	13/8/2024	\$ 17.033.686	19/08/25	IDENTIMAX S.A.
EX-2024-33438758-GCBA-ASInf	Licitación pública	8056-1555-LPU24	Código estático - Ciudad 3D Open Source	DGSEI	8056-16404-OC24	23/10/2024	\$ 16.855.760	3/3/2025	RAN INGENIERIA DE SISTEMAS SRL
EX-2024-33258922-GCBA-ASInf	Licitación pública	8056-1551-LPU24	Adquisición de una Plataforma de concientización y evaluación de usuarios sobre seguridad informática	DGSEI	8056-16756-OC24	25/10/2024	\$ 46.248.000	24/10/25	ZESTDATA SAS
EX-2024-31315631-GCBA-ASInf	Licitación pública	8056-1457-LPU24	Renovación de Infraestructura de Firewall de Aplicaciones WEB F5, licencias asociadas y soporte técnico	DGSEI	8056-16919-OC24	28/10/2024	\$ 463.412.851	31/10/25	KRUGG TECHNOLOGIES S.A.
EX-2024-31256764-GCBA-ASInf	Licitación pública	8056-1451-LPU24	Renovación de una solución para la protección DDoS de F5 en sitio y nube	DGSEI	8056-17231-OC24	31/10/2024	\$ 187.513.040	31/10/25	TWA SRL.
EX-2024-31256839-GCBA-ASInf	Licitación pública	8056-1452-LPU24	Renovación de la Solución de Gestión e Inspección Continua de Vulnerabilidades (Tenable), implementación y soporte técnico x 12 meses	DGSEI	8056-16988-OC24	1/11/2024	\$ 275.420.600	28/10/25	POINT IT SRL
EX-2024-36106053-GCBA-ASInf	Licitación pública	8056-1691-LPU24	Renovación de Licencias, Actualizaciones y Soporte de equipos FIREWALL FORTINET y FORTIANALYZER	DGSEI	8056-17854-OC24	13/11/2024	\$ 608.170.950	28/02/25	POINT IT SRL
EX-2024-37000067-GCBA-ASInf	Licitación pública	8056-1754-LPU24	Renovación de Servicios de Mantenimiento, soporte Técnico y actualizaciones para la solución de prevención de intrusiones y protección de perímetro para el Centro de Datos	DGSEI	8056-18668-OC24	1/12/2024	\$ 544.124.115	30/11/25	KRUGG TECHNOLOGIES S.A.

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2024-39591447-GCBA-ASnf	Licitación pública	8056-1888-LPU24	Renovación de la Suscripción y Soporte Técnico de un Servicio de Monitorización y Remediación	DGSEI	8056-19516-OC24	5/12/2024	\$ 84.737.610	05/12/25	RAN INGENIERIA DE SISTEMAS SRL
EX-2024-39434018-GCBA-ASnf	CD x Exclusividad	8056-2024-CDI24	Servicio Profesional de Soporte y Mantenimiento de la Plataforma de Firma Digital (PKI)	DGSEI	8056-19544-OC24	5/12/2024	\$ 205.987.200	09/12/25	MS ARGENTINA SRL
EX-2024-42357062-GCBA-ASnf	Licitación pública	8056-2029-LPU24	Solución de Seguridad para Active Directory	DGSEI	8056-19950-OC24	10/12/2024	\$ 291.015.000	09/12/25	POINT IT SRL
EX-2024-42174345-GCBA-ASnf	Licitación pública	8056-2015-LPU24	Suscripción Solución de Microsegmentación de redes, servidores y aplicaciones	DGSEI	8056-20299-OC24	13/12/2024	\$ 300.203.550	15/12/25	AVANTI TECHNOLOGY SRL
EX-2024-04262913-GCBA-ASnf	Prórroga	8056-0046-LPU24	TCN Renovación suscripción licencias QRadar SIEM, Qradar SOAR y playbook de SOAR	DGSEI	8056-21451-OC24	23/12/2024	\$ 437.726.200	08/02/26	TECNOLOGIA, COMUNICACIONES Y NEGOCIOS S.A.
EX-2024-48245631-GCBA-ASnf	Licitación pública	8056-2263-LPU24	Renovación de Licencias, Actualizaciones y Soporte de equipos Firewall Fortinet y Fortianalyzer	DGSEI	8056-1257-OC25	1/3/2025	\$ 1.436.126.149,44	28/2/2026	POINT IT SRL
EX-2025-06797201-GCBA-ASnf	Licitación pública	8056-0157-LPU25	Servicio SOC Niveles 1 y 2	DGSEI	8056-2319-OC25	13/3/2025	\$ 138.869.640,00	28/2/2027	RAN INGENIERIA DE SISTEMAS SRL
NO-2025-11822952-GCBA-DGSEI	Ampliación	8056-2029-LPU24	Suscripción de Licencias de la Solución de Seguridad para Active Directory	DGSEI	8056-3092-OC25	25/3/2025	\$ 58.203.000,00	25/3/2025	POINT IT SRL
EX-2025-12746799-GCBA-ASnf	Licitación pública	8056-0418-LPU25	Servicio para la Evaluación de la Seguridad de Aplicaciones Web Móviles	DGSEI	8056-0111-OCA25	25/4/2025	\$ 366.118.494,00	24/4/2026	RAN INGENIERIA DE SISTEMAS SRL
EX-2025-15580379-GCBA-ASnf	Licitación pública	8056-0569-LPU25	Adquisición de una Solución de seguridad avanzada del Endpoint	DGSEI	8056-6961-OC25	26/5/2025	\$ 926.544.000,00	26/5/2027	POINT IT SRL

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requerente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2025-14109598-GCBA-ASInf	Licitación pública	8056-0481-LPU25	Renovación de licencias, actualizaciones y soporte de software Acunetix y Burp	DGSEI	8056-7496-OC25	2/6/2025	\$ 195.953.000,00	29/6/2026	Krugg Technologies S.A.
EX-2024-33258922-GCBA-ASInf	Prórroga	8056-1551-LPU24	Adquisición de una Plataforma de concientización y evaluación de usuarios sobre seguridad informática	DGSEI	8056-10729-OC25	17/7/2025	\$ 46.248.000	25/10/2026	ZESTDATA SAS
EX-2024-31256839-GCBA-ASInf	Prórroga	8056-1452-LPU24	Renovación de la Solución de Gestión e Inspección Continua de Vulnerabilidades (Tenable), implementación y soporte técnico x 12 meses	DGSEI	8056-10722-OC25	17/7/2025	\$ 275.420.600	31/10/2026	POINT IT SRL
EX-2025-15580379-GCBA-ASInf	Ampliación	8056-0569-LPU25	Suscripción y Renovación de una Solución de seguridad avanzada del Endpoint para Sbase	DGSEI	8056-11062-OC25	23/7/2025	\$ 926.544.000	26/5/2027	POINT IT SRL
EX-2024-37000067-GCBA-ASInf	Prórroga	8056-1754-LPU24	Renovación de Servicios de Mantenimiento, soporte Técnico y actualizaciones para la solución de prevención de intrusiones y protección de perímetro para Centro de Datos	DGSEI	8056-11265-OC25	30/7/2025	\$ 544.124.115	1/12/2026	Krugg Technologies S.A.
NO-2025-35764961-GCBA-DGSEI	Prórroga	8056-1451-LPU24	Renovación de una solución para la protección DDoS de F5 en sitio y nube	DGSEI	8056-13689-OC25	29/8/2025	\$ 187.513.040	1/11/2026	TWA SRL.
EX-2024-42357062-GCBA-ASInf	Prórroga	8056-2029-LPU24	Solución de Seguridad para Active Directory AD original	DGSEI	8056-14527-OC25	12/9/2025	\$ 349.218	10/12/2026	POINT IT SRL
NO-2025-38071337-GCBA-DGSEI	Prórroga	8056-1457-LPU24	Renovación de Infraestructura de Firewall de Aplicaciones WEB F5, licencias asociadas y soporte técnico	DGSEI	8056-14553-OC25	12/9/2025	\$ 463.412.851	31/10/2026	Krugg Technologies S.A.

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2024-42357062-GCBA-ASInf	Ampliación	687-1067-AMP25	Suscripción de Licencias de la Solución de Seguridad para Active Directory	DGSEI	8056-16426-OC25	13/10/2025	\$ 58.203.000,00	10/12/2026	POINT IT SRL
EX-2025-40463922-GCBA-ASInf	Licitación pública	8056-1613-LPU25	Suscripción y Renovación de Software como Servicio de Respaldo	DGSEI	8056-18161-OC25	6/11/2025	\$ 432.480.000,00	5/11/2027	AVANZIT TECNOLOGÍA S.A.
EX-2024-39434018-GCBA-ASInf	Prórroga	8056-2024-CDI24	Servicio Profesional de Soporte y Mantenimiento de la Plataforma de Firma Digital (PKI)	DGSEI	8056-15011-OC25	10/12/2025	\$ 205.987.200	10/12/2026	MS ARGENTINA SRL
EX-2024-39637387-GCBA-ASInf	Licitación pública	8056-1986-LPU25	Servicio de Consultoría para entrenamiento de prácticas ofensivas para personal de la DGSEI de la Agencia de Sistemas de Información (Red Team)	D-GSEI	8056-21692-OC25	15/12/2025	\$ 99.750.000,00	14/1/2026	INFOBYTE S.A.
EX-2024-42174345-GCBA-ASInf	Prórroga	8056-2015-LPU24	Suscripción Solución de Microsegmentación de redes, servidores y aplicaciones	DGSEI	8056-14935-OC25	16/12/2025	\$ 300.203.550	16/12/2026	AVANTI TECHNOLOGY SRL
EX-2025-48525152-GCBA-ASInf	Licitación pública	8056-1911-LPU25	Renovación de la Suscripción y Soporte Técnico de un Servicio de Monitorización y Remediación	DGSEI	8056-21913-OC25	16/12/2025	\$ 109.012.500	15/12/2026	BIWARES SRL
EX-2024-42174345-GCBA-ASInf	Ampliación	8056-2015-LPU24	Ampliación 50% Suscripción Anual de licencias para Solución de Microsegmentación de Redes, Servidores y Aplicaciones	DGSEI	8056-22639-OC25	22/12/2025	\$ 150.101.775	16/12/2026	AVANTI TECHNOLOGY SRL

Fuente: DGSEI

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

ANEXO XI

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2024-48245631-GCBA-ASInf	Licitación pública	8056-2263-LPU24	Renovación de Licencias, Actualizaciones y Soporte de equipos FIREWALL FORTINET y FORTIANALYZER	DGSEI	8056-1257-OC25	1/3/2025	1.436.126.149,44	28/2/2026	POINT IT SRL
EX-2025-06797201-GCBA-ASInf	Licitación pública	8056-0157-LPU25	Servicio SOC Niveles 1 y 2	DGSEI	8056-2319-OC25	13/3/2025	138.869.640	28/2/2027	RAN INGENIERIA DE SISTEMAS SRL
NO-2025-11822952-GCBA-DGSEI	Ampliación	8056-2029-LPU24	Suscripción de Licencias de la Solución de Seguridad para Active Directory	DGSEI	8056-3092-OC25	25/3/2025	58.203.000	25/3/2025	POINT IT SRL
EX-2025-12746799-GCBA-ASInf	Licitación pública	8056-0418-LPU25	Servicio para la Evaluación de la Seguridad de Aplicaciones Web Móviles	DGSEI	8056-0111-OCA25	25/4/2025	366.118.494	24/4/2026	RAN INGENIERIA DE SISTEMAS SRL
EX-2025-15580379-GCBA-ASInf	Licitación pública	8056-0569-LPU25	Adquisición de una Solución de seguridad avanzada del Endpoint	DGSEI	8056-6961-OC25	26/5/2025	926.544.000	26/5/2027	POINT IT SRL
EX-2025-14109598-GCBA-ASInf	Licitación pública	8056-0481-LPU25	Renovación de licencias, actualizaciones y soporte de software Acunetix y Burp	DGSEI	8056-7496-OC25	2/6/2025	195.953.000	29/6/2026	Krugg Technologies S.A.
EX-2024-33258922-GCBA-ASInf	Prórroga	8056-1551-LPU24	Adquisición de una Plataforma de concientización y evaluación de usuarios sobre seguridad informática	DGSEI	8056-10729-OC25	17/7/2025	\$ 46.248.000	25/10/2026	ZESTDATA SAS
EX-2024-31256839-GCBA-ASInf	Prórroga	8056-1452-LPU24	Renovación de la Solución de Gestión e Inspección Continua de Vulnerabilidades (Tenable), implementación y soporte técnico x 12 meses	DGSEI	8056-10722-OC25	17/7/2025	\$ 275.420.600	31/10/2026	POINT IT SRL

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requerente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2025-15580379-GCBA-ASInf	Ampliación	8056-0569-LPU25	Suscripción y Renovación de una Solución de seguridad avanzada del Endpoint para SBASE	DGSEI	8056-11062-OC25	23/7/2025	\$ 926.544.000	26/5/2027	POINT IT SRL
EX-2024-37000067-GCBA-ASInf	Prórroga	8056-1754-LPU24	Renovación de Servicios de Mantenimiento, soporte Técnico y actualizaciones para la solución de prevención de intrusiones y protección de perímetro para Datacenter	DGSEI	8056-11265-OC25	30/7/2025	\$ 544.124.115	1/12/2026	Krugg Technologies S.A.
NO-2025-35764961-GCBA-DGSEI	Prórroga	8056-1451-LPU24	Renovación de una solución para la protección DDoS de F5 en sitio y nube	DGSEI	8056-13689-OC25	29/8/2025	\$ 187.513.040	1/11/2026	TWA SRL.
EX-2024-42357062-GCBA-ASInf	Prórroga	8056-2029-LPU24	Solución de Seguridad para Active Directory AD original	DGSEI	8056-14527-OC25	12/9/2025	\$ 349.218	10/12/2026	POINT IT SRL
NO-2025-38071337-GCBA-DGSEI	Prórroga	8056-1457-LPU24	Renovación de Infraestructura de Firewall de Aplicaciones WEB F5, licencias asociadas y soporte técnico	DGSEI	8056-14553-OC25	12/9/2025	\$ 463.412.851	31/10/2026	Krugg Technologies S.A.
EX-2024-42357062-GCBA-ASInf	Ampliación	687-1067-AMP25	Suscripción de Licencias de la Solución de Seguridad para Active Directory	DGSEI	8056-16426-OC25	13/10/2025	\$ 58.203.000	10/12/2026	POINT IT SRL
EX-2025-40463922-GCBA-ASInf	Licitación pública	8056-1613-LPU25	Suscripción y Renovación de Software como Servicio de Respaldo	DGSEI	8056-18161-OC25	6/11/2025	\$ 432.480.000	5/11/2027	AVANZIT TECNOLOGÍA S.A.
EX-2024-39434018-GCBA-ASInf	Prórroga	8056-2024-CDI24	Servicio Profesional de Soporte y Mantenimiento de la Plataforma de Firma Digital (PKI)	DGSEI	8056-15011-OC25	10/12/2025	\$ 205.987.200	10/12/2026	MS ARGENTINA SRL
EX-2024-39637387-GCBA-ASInf	Licitación pública	8056-1986-LPU25	Servicio de Consultoría para entrenamiento de prácticas ofensivas para personal de la DGSEI de la ASI (Red Team)	DGSEI	8056-21692-OC25	15/12/2025	\$ 99.750.000	14/1/2026	Infobyte S.A.

"Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Expediente	Modalidad	Proceso de compras	Descripción	Dirección Requirente	Documentación contractual	Fecha doc.	Importe (\$)	Vencimiento	Proveedor
EX-2024-42174345-GCBA-ASInf	Prórroga	8056-2015-LPU24	Suscripción Solución de Microsegmentación de redes, servidores y aplicaciones	DGSEI	8056-14935-OC25	16/12/2025	\$ 300.203.550	16/12/2026	Avanti Technology SRL
EX-2025-53092396-GCBA-ASInf	Convenio Marco	—	Notebook	DGSEI	687-21136-OC25	16/12/2025	\$ 11.490.000	30/12/2025	AP SUPPLIER GROUP S.A.
EX-2025-48525152-GCBA-ASInf	Licitación pública	8056-1911-LPU25	Renovación de la Suscripción y Soporte Técnico de un Servicio de Monitorización y Remediación	DGSEI	8056-21913-OC25	16/12/2025	\$ 109.012.500	15/12/2026	BIWARES SRL
EX-2025-54359102-GCBA-ASInf	Convenio Marco	—	8 Monitores	DGSEI	687-22038-OC25	17/12/2025	\$ 1.590.082	30/12/2025	CONGRESO INSUMOS SA
EX-2024-42174345-GCBA-ASInf	Ampliación	8056-2015-LPU24	Ampliación 50% Suscripción Anual de licencias para Solución de Microsegmentación de Redes, Servidores y Aplicaciones	DGSEI	8056-22639-OC25	22/12/2025	\$ 150.101.775	16/12/2026	Avanti Technology SRL
EX-2025-54785732-GCBA-ASInf	Convenio Marco	—	Adquisición de Smart TV para DGTAL y DGSEI	DGSEI	687-22987-OC25	26/12/2025	\$ 1.402.245	30/12/2025	APM GROUP SRL.

Fuente: DGSEI