

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.

IF-2026-00023390-AGCBA-DTACO

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

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

IF-2026-00023390-AGCBA-DTACO

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.

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

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

IF-2026-00023390-AGCBA-DTACO

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

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.

- Se encuentra embebido el Informe Final -



Auditoría de la Ciudad de Buenos Aires
"2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma
de Buenos Aires"

Hoja Adicional de Firmas
Informe Gráfico

Número: IF-2026-00023390-AGCBA-DTACO

Buenos Aires,
Miércoles 7 de Octubre de 2026

Referencia: IF 10.26.01 - Seguridad de la Información

El documento fue importado por el sistema GEDO con un total de 5 pagina/s.

Digitally signed by sade.agcba.gob.ar
Date: 2026.10.07 13:04:26 -03:00

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

Digitally signed by sade.agcba.gob.ar
Date: 2026.10.07 13:04:27 -03:00