Objeto:
Auditoría de Misiones y Funciones Subgerencia Operativa Monitoreo, Prevención y Detección

Período auditado:
01 de junio de 2024 al 30 de junio de 2025

Normativa relevante:
Resolución N° 224-ASINF/18

Resolución N° 177-ASINF/13

Equipo auditor:

Auditora Interna:

Lic. Nadina MEZZA

Subgerente Operativo Soporte de Auditoría I (Sistemas):

Sr. Eduardo Ernesto, SPAHN

Subgerente Operativo Soporte de Auditoría II (Operacional):

Cra. Celina SIMONE

Equipo de Trabajo:

Lic. Verónica ACOSTA

Cra Natalia AMÁBILE

Cra. Fabiana LOPEZ

Cr. Juan Manuel VAZQUEZ

Informe Ejecutivo

PROYECTO N°010/25
F/N Agencia de Sistemas de Información (ASI). Ley Nº 2.689

Dirección General de Seguridad Informática

Alcance:
El presente informe corresponde al Proyecto N° 10-UAIASINF/25, contemplado en el Plan Anual de Auditoría del año 2025 para la Agencia de Sistemas de Información (en adelante ASI), aprobado por la Sindicatura General de la Ciudad Autónoma de Buenos Aires (en adelante SGCBA), mediante Resolución Nº 162-SGCBA/24. El período auditado abarca desde el 01 de junio de 2024 al 30 de junio de 2025 inclusive.

Limitaciones al alcance:
No surgieron limitaciones al alcance.

1. La Subgerencia Operativa de Monitoreo, Prevención y Control ha delegado funciones clave como la administración de equipos de seguridad e implementación de capacitaciones, generando una desconexión entre sus responsabilidades formales y su ejercicio práctico.
2. El proveedor limita su intervención a tareas de monitoreo, SOC 1, mientras que funciones críticas de SOC 2 son asumidas por personal interno. Esto reduce el alcance del servicio contratado.
3. Se identifican debilidades en variedad, profundidad y cobertura de reglas. Faltan reglas para orígenes relevantes. No hay protocolo sobre revisión y actualización de reglas. No se observa supervisión de las áreas que confeccionan las reglas en búsqueda de reglas integradas que alerten sobre incidentes complejos.
4. A pesar de la alta frecuencia de ciertos incidentes, no existen respuestas automatizadas.
5. Diversos dispositivos críticos no están conectados al SIEM, incluyendo equipos recientemente actualizados. También se detectan equipos desactivados que afectan la eficacia de correlación.
6. La actual plataforma de registro de incidentes (tickets NOC) no contienen ni todos los incidentes tratados, en particular algunos incidentes identificados por el área de infraestructura vía su sistema de monitoreo, ni las respuestas automatizadas del SOAR, dificultando la consolidación de información y el análisis de recurrencias.
7. No existe un procedimiento formal para el análisis forense, lo que impide verificar criterios, trazabilidad, responsabilidades y retroalimentación al SIEM.
8. No se evidencian capacitaciones obligatorias por parte del proveedor. Internamente, se limita a guías de pentesting sin formación continua sobre desarrollo seguro o configuración avanzada.
9. Las políticas vigentes no definen claramente qué constituye un incidente de seguridad. Incorporar esta definición permitiría establecer estándares técnicos, mejorar la trazabilidad, automatización y evaluación del desempeño del monitoreo.

Sr. Ariel VALDIVIEZO

Cdor. Juan Pablo BERTONE

Respuesta del organismo al Informe de Auditoría:
Emitió opinión.

Conclusiones y principales recomendaciones:
Del análisis de la configuración del sistema de seguridad informática diseñada por el área de responsable del monitoreo, prevención y detección de la Dirección General de Seguridad Informática surge que el área priorizó disponer de equipamiento de última generación, con alta capacidad de detección y tratamiento de incidentes. Efectivamente, tanto el SIEM-SOAR como los equipos que le proveen de registros están entre los de mayor eficacia disponible en el mercado. Sin embargo, resta implementar acciones que aseguren que el sistema sea efectivamente eficiente.
Es decir, debe avanzarse consolidando las capacidades de los recursos humanos, de modo de mejorar el ambiente de prevención de incidentes, más aún teniendo presente la gran proporción de aplicaciones operativas en ambiente productivo por excepción. A su vez, el área es un área chica, con poco personal, por lo cual se vuelve crucial que la empresa proveedora contratada para realizar tareas de SOC1 y SOC2 cumpla la totalidad de tareas para lo cual fue contratada.
El área debe avanzar en normar sus procedimientos. Debe mejorar sus procesos de supervisión de las funciones que ha delegado en otras subgerencias, de modo de asegurar la actualización del sistema generación de alertas tempranas, revisando reglas, integrando reglas para ataques complejos, buscando la automatización de la mayor cantidad de eventos posibles.
Esta auditoría interna entiende que debe fortalecerse el ambiente de control de esta subgerencia crítica dentro de la organización, resultando necesario atender las medidas detalladas en este informe, a fin de fortalecer la seguridad, garantizar la trazabilidad de los eventos y mitigar la posibilidad de que se materialicen amenazas que afecten la integridad, disponibilidad y confidencialidad de los datos institucionales.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

Hoja Adicional de Firmas
Informe externo Reservado

Número: IF-2025-41989213-GCABA-UAIASINF

Buenos Aires, Martes 30 de Septiembre de 2025

Referencia: Informe Ejecutivo - Proyecto N° 010/25.

El documento fue importado por el sistema GEDO con un total de 2 pagina/s.

Digitally signed by Comunicaciones Oficiales
Date: 2025.09.30 20:54:58 -03:00

Nadina Mezza
Titular
UNIDAD AUDITORIA INTERNA ASINF
MINISTERIO JEFATURA DE GABINETE

Digitally signed by Comunicaciones Oficiales
Date: 2025.09.30 20:54:59 -03:00