Objeto:
Auditoría de Seguridad de la Información del Sistema Buenos Aires Compras (BAC).

Período auditado:
Entre el 6 de julio y el 21 de octubre de 2022.

Normativa relevante:
Constitución de la Ciudad Autónoma de Buenos Aires.
Leyes N° 70, N° 1.845, N° 2.095, N° 2.689, N° 6.292 y N° 6.347.
Decreto de Necesidad y Urgencia N° 1/20 y N° 5/22.
Decretos N° 1.000/99, N° 823/10, N° 463/19 y N° 74/21.
Resoluciones N° 424-MHGC/13, N° 177-ASINF/13, N° 239-ASINF/14, N° 46-ASINF/17 y N° 2.481-MEFGC/18.
Disposiciones N° 1.1990-DGCYC/18, N° 150-DGCYC/19 y N° 167-DGCYC/21.

Equipo auditor:
Emilse TEYO
Hugo CONTI
Alejandra SANCHEZ VALENCIA
Adrián GIROTTI
Morena PALACIOS GOÑI
José CARBALLO

Informe Ejecutivo

PROYECTO N° 26/22
Ministerio de Hacienda y Finanzas
Subsecretaría de Gestión Operativa
Dirección General de compras y Contrataciones

Alcance:

A fin de llevar adelante las tareas de auditoría, se realizaron reuniones de trabajo vía *MS Teams* con funcionarios de la Dirección General de Compras y Contrataciones (en adelante DGCyC) y el relevamiento del Sistema Buenos Aires Compras (en adelante "el sistema", "la aplicación" o "BAC") se realizó de manera remota.

Asimismo, y teniendo en cuenta que las tareas de desarrollo y mantenimiento del BAC, son llevadas a cabo por la Dirección General Unidad Informatica de Administración Financiera (en adelalante DGUIAF), se mantuvieron reuniones con personal de dicha dependencia, en las oficinas sitas en la calle Maipu 116, relativas a las tareas pertinentes relacionadas al BAC.

Limitaciones al alcance:
No existieron.

Principales hallazgos/observaciones:

a) Si bien la DGCyC tiene implementado un procedimiento de copias de resguardo de la información digital, la misma no se encuentra completamente alineada con los requisitos establecidos en las Políticas del Grupo PO0701 del Marco Normativo de TI.

   Entre los puntos que no se encuetran alineados las políticas indicadas, podemos mencionar los requerimientos mínimos de resgurado, copias realizadas sobre la información digital, copias que correspondan en *software* de aplicación, *software* de base y/o archivos de configuraciones, entre otros.

b) Si bien la DGCyC tiene un procedimeinto documentado ante la ocurrencia de un eventual incidente que pueda afectar la disponibilidad del BAC, el mismo no configuraría un Plan de Contingencia y Recuperación ante Desastres ya que dicho documento está desarrollado mediante una breve descripción, no pudiendo ser considerado un plan detallado. Falta la especificación de requerimientos tales como la asignación de roles y responsabilidades para cada actividad definida; la conformación de un comité de crisis para liderar la implementación y seguimiento del Plan de Contingencia; y el sitio de contingencia, entre otros puntos a tener en cuenta.

c) Del análisis efectuado a la documentación provista por el auditado, se comprobó

que el *software* del BAC no se encuentra inscripto a nombre del GCABA a efectos de proteger la propiedad intelectual del mismo de acuerdo con lo establecido en la Resolución N° 46-ASINF/17.

d) Del análisis realizado al *front-end* de la aplicación, se evidenció la existencia de cuatro (4) vulnerabilidades.

Respuesta del organismo al Informe de Auditoría:
Emitió opinión.

Conclusiones y principales recomendaciones:
En base a la información remitida por el auditado y al resultado de las tareas de fiscalización efectuadas por este Organismo de Control, se infiere que las principales fortalezas de la DGCYC respecto a la gestión general del sistema BAC radican en la constante evolución de sus funcionalidades con el fin de mejorar la experiencia de la compras y contrataciones que se llevan adelante en el ámbito del GCABA.

Los hallazgos que se mencionan en el presente Informe constituyen oportunidades de mejora para las tareas de seguridad y gestión del sistema BAC que la DGCYC lleva adelante, las cuales son realizadas con un profesionalismo adecuado, según surge de las evidencias obtenidas durante las tareas de fiscalización.

Por tanto, la DGCYC debe definir estrategias para mantener los logros alcanzados y documentar la Política de copias de resguardo y recuperación (PO0701), la Política de Registro eventos en servicios de TI (PO0803) y la Política de control de eventos en servicios de TI (PO0804), según Marco Normativo de TI.

A efectos de proteger la propiedad intelectual del GCABA respecto del sistema BAC, de acuerdo con lo establecido en la Resolución N° 46-ASINF/17, la Dirección General de Compras y Contrataciones debe arbitrar su inscripción en la Dirección Nacional del Derecho de Autor.

Respecto de los hallazgos referentes a la seguridad de la aplicación, estos corresponden a cuestiones de desarrollo que pueden ser subsanadas con la modificación del código de la aplicación, tal como el auditado ha expresado en su opinión.

Finalmente, se destaca la buena predisposición y colaboración de los funcionarios auditados durante el desarrollo de las tareas de auditoría.

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
"2022 - Año del 40° Aniversario de la Guerra de Malvinas. En homenaje a los veteranos y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

Hoja Adicional de Firmas
Informe externo Reservado

Número: IF-2022-45812328-GCABA-SGCBA

Buenos Aires, Miércoles 7 de Diciembre de 2022

Referencia: Informe Ejecutivo - Proyecto N° 26/22.

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

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.12.07 13:04:14 -03'00'

Mónica Freda
Sindico General
SINDICATURA GENERAL DE LA CDAD. AUTONOMA DE BS.AS.
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.12.07 13:04:15 -03'00'