RESO SAGYP N° 547/23

Buenos Aires, 6 de noviembre del 2023

VISTO:

El TEA A-01-00023609-4/2023 caratulado *"D.G.C.C. S/ PLAN INTEGRAL DE SEGURIDAD INFORMATICA"*, y

CONSIDERANDO:

Que por la Resolución SAGyP N° 516/2023, se aprobaron los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, como Adjuntos 148394/23 y 126252/23, , y se llamó a la Licitación Publica N° 2-0017-LPU23, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, para el día 8 de noviembre de 2023 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto administrativo.

Que en el marco del mentado proceso, la firma Point It S.R.L. efectúo una consulta dentro del plazo previsto (v. Adjunto 161678/23).

Que oportunamente, la Dirección General de Compras y Contrataciones dio intervención a la Dirección General de Informática y Tecnología, en su carácter de responsable técnico de la contratación de marras, a fin de brindar una respuesta técnica sobre la consulta formulada por la firma Point S.R.L. (V. Adjunto 161677/23).

Que en tal entendimiento, la Dirección General de Compras y Contrataciones, mediante Memo DGCC 2310/23, en su calidad de Unidad Operativa de Adquisición, manifestó

que, en función de la consulta efectuada por la firma Point IT SRL y la respuesta de la Dirección General de Informática y Tecnología, se elevó los presentes actuados acompañando el proyecto de Circular Con Consulta N° 1 (v. Adjunto 162026/23).

Que asimismo, la Dirección General de Compras y Contrataciones, debido al carácter modificatorio de la Circular Con Consulta N° 1, entendió necesario postergar la fecha para la presentación de ofertas y la apertura pública de ofertas para la presente contratación.

Que la Ley N° 6.302 al modificar la Ley N° 31 creó la Secretaría de Administración General y Presupuesto y estableció dentro de sus funciones la de ejecutar, bajo el control de la Comisión de Administración, Gestión y Modernización Judicial, el presupuesto anual del Poder Judicial de la Ciudad Autónoma de Buenos Aires (cfr. inc. 4 del art. 27 de la Ley N° 31 –texto consolidado según Ley N° 6.588-) y la de realizar las contrataciones de bienes y servicios (cfr. Inc. 6° del art. 27 de la Ley N°31 -texto consolidado según Ley N° 6.588-).

Que conforme lo dispuesto en el artículo 13 de la Ley N° 2.095 (texto consolidado según Ley N° 6.588) y de su mentada norma reglamentaria, corresponde a esta dependencia suscribir los actos administrativos que aprueben circulares aclaratorias y modificatorias de contrataciones. Asimismo, es dable destacar el valor de los informes técnicos y que las modificaciones planteadas surgen en pos de fortalecer la concurrencia al presente proceso licitatorio.

Que en cuanto a la postergación de la fecha del llamado a Licitación Pública N° 2-0017-LPU23, resulta pertinente poner de resalto que en el inciso b) del artículo 13 -referido a la formalidad de las actuaciones- de la Ley N° 2.095 (texto consolidado según Ley N° 6.588) prevé "*La suspensión o postergación de la fecha de apertura de ofertas*" como uno de los casos en que debe dictarse acto administrativo, con los requisitos establecidos en el artículo 7° de la Ley de Procedimientos Administrativos de la Ciudad Autónoma de Buenos Aires -Decreto N° 1.510/97 (texto consolidado según Ley N° 6.588).

Que en virtud de lo antedicho, en vista del estado del proceso licitatorio en cuestión, y atento a lo solicitado por la Dirección General de Informática y Tecnología y a lo recomendado por la Dirección General de Compras y Contrataciones, en su calidad de Unidad Operativa de Adquisiciones, corresponderá, aprobar la Circular Modificatoria Con Consulta N° 1 en el marco de la Licitación Publica Nº 2-0017-LPU23 y proceder con la postergación de la fecha de presentación y apertura pública de ofertas prevista para la mentada Licitación Pública para el día 21 de noviembre de 2023 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretar asueto.

Que finalmente, corresponderá instruir a la Dirección General de Compras y Contrataciones a efectos de que por su intermedio se realicen las tareas necesarias para realizar las publicaciones y notificaciones de este acto, junto a la Circular Modificatoria Con Consulta N° 1 que se apruebe, y proceder a la postergación de la fecha de presentación de ofertas y apertura en cuestión, y a realizar las publicaciones y notificaciones conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.588), su reglamentaria Resolución CM N° 276/2020 y en la Ley de Procedimientos Administrativos -Decreto 1.510/97- (texto consolidado según Ley N° 6.588). Asimismo, deberá comunicar la presente Resolución a todas las firmas que hubiesen realizado consultas o requerimientos o adquirido el pliego por la Licitación Pública N° 2-0017-LPU23.

Que por la Resolución CM N° 143/2023, el Plenario del Consejo de la Magistratura designó como reemplazo transitorio de la Secretaria de Administración General y Presupuesto del Poder Judicial a la Dra. Clara María Valdez, al amparo de lo dispuesto por el artículo 35 de la Ley N° 31 (texto consolidado según Ley N° 6.588).

Por lo expuesto y en el ejercicio de las atribuciones conferidas por las Leyes Nros. 31 y 2.095 (ambos textos consolidados según Ley N° 6.588), las Resoluciones CM Nros. 276/2020, 143/2023;

LA SECRETARIA DE ADMINISTRACIÓN GENERAL Y PRESUPUESTO DEL PODER JUDICIAL DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES

RESUELVE:

Artículo 1°: Apruébase la Circular Modificatoria Con Consulta N° 1 en el marco de la Licitación Pública N° 2-0017-LPU23 que como Adjunto 162026/22, forma parte de la presente Resolución

Artículo 2°: Postérgase la fecha límite para la presentación de ofertas y la apertura pública de ofertas de la Licitación Pública N° 2-0017-LPU23, para el día 21 de noviembre de 2023 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Artículo 3°: Instruyese a la Dirección General de Compras y Contrataciones para que realice la publicación y notificación de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.588) su reglamentaria Resolución CM N° 276/2020 y en la Ley de Procedimientos Administrativos - Decreto 1.510/97- (texto consolidado según Ley N° 6.588). Asimismo, deberá comunicar la presente Resolución a todas las firmas que hubiesen realizado consultas o requerimientos o adquirido el pliego por la Licitación Pública N° 2-0017-LPU23.

Artículo 4°: Publíquese en la página web del Consejo de la Magistratura y en el Boletín Oficial del Gobierno de la Ciudad Autónoma de Buenos Aires, comuníquese por correo electrónico oficial a los titulares de las Direcciones Generales de Informática y Tecnología y de Programación y Administración Contable. Pase a la Dirección General de Compras y Contrataciones para sus efectos.

Poder Judicial de la Ciudad de Buenos Aires
Consejo de la Magistratura

FIRMAS DIGITALES

Clara Valdez
SEC DE ADMIN GRAL Y PRESU DEL P JUD
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES

Poder Judicial de la Ciudad de Buenos Aires
Consejo de la Magistratura

CIRCULAR CON CONSULTA MODIFICATORIA Nº 1

LICITACIÓN PÚBLICA N° 2-0017-LPU23

Por la presente, la Dirección General de Compras y Contrataciones del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, en el marco de la Licitación Pública N° 2-0017-LPU23, referida al Plan Integral de Seguridad Informática, la cual tramita por el Expediente TEA N° A-01-00023609-4/2023, comunica la presente Circular Con Consulta Modificatoria N° 1, en función de la Consulta N° 1 efectuada a través de la plataforma JUC -juc.jusbaires.gob.ar-:

Consulta Nº 1:

Se realizan las consultas sobre el segundo punto del pliego de especificaciones técnicas: "ESPECIFICACIONES TÉCNICAS RENGLÓN 1"

Donde indica: "El adjudicatario deberá proveer tecnologías (con los respectivos equipamientos de corresponder) con la finalidad de implementar las siguientes soluciones de seguridad en Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires:

• AntiSpam.

• Antimalware Avanzado.

• SIEM.

• SOAR.

Si bien dentro del mismo punto se especifican las especificaciones técnicas requeridas para AntiSpam, Antimalware Avanzado y SIEM, no se indican las características técnicas de la solución de SOAR.

Podrán indicar las especificaciones técnicas requeridas para la tecnología de SOAR?

Aclaración N° 1:

Se amplía el detalle técnico tal como se describe a continuación

SOAR

1.1 Características Generales

- *La solución debe ser del tipo Virtual Appliance a implementarse en el esquema de virtualización provisto por el Consejo de la Magistratura de la Ciudad de Buenos Aires*
- *La solución deberá estar licenciada en modalidad suscripción permitiendo la administración de 3 operadores (concurrentes)*

1.2 Funcionalidades mínimas Requeridas

Características de Monitoreo

- *La solución debe tener un panel configurable dependiendo de la función del usuario.*
- *Las alertas que superan el período de tiempo del SLA deben resaltarse en la GUI.*
- *El tablero debe mostrar alertas y las tareas del analista.*
- *El ROI debe ser configurable con varios criterios: ahorro de costos, ahorro de tiempo.*
- *Las alertas deben estar ordenadas por gravedad.*
- *Cada analista debe tener su propia carga de trabajo.*
- *El tablero debe admitir la importación, exportación en formato JSON.*
- *El panel debe actualizarse automáticamente.*
- *Vista del panel de control de roles: analistas T1, T2 o nivel 1, nivel 2.*
- *La solución debe poder mostrar el tiempo medio para: Identificación, Confirmación, Contención, Erradicación, Recuperación o secuelas para la gestión de incidentes.*
- *La solución debe tener un panel dedicado para monitorear el estado / disponibilidad de cada integración y también el estado del sistema del motor SOAR.*
- *La solución debe proporcionar un marco de desarrollo de tablero basado en HTML / JSON / JS para permitir a los usuarios crear sus widgets de tablero personalizados e importarlos a la solución SOAR.*

Características de Reportes

- *Los informes deben ser personalizables mediante la interfaz de usuario.*
- *Los informes deben permitir la programación.*
- *El administrador debería poder exportar el informe con formatos PDF y CVS.*
- *Los informes deben enviarse por correo electrónico.*
- *El acceso a los informes depende del rol y se controla a través de RBAC.*
- *La solución debe admitir la recodificación de registros de auditoría para todos los informes descargados.*
- *Los informes deben tener métricas.*

Funcionalidades de Alertas Incidentes / Administración de Casos

- *Las alertas y los incidentes deben manejarse cada uno en un módulo de interfaz separado.*
- *Los campos de alerta deben cambiarse automáticamente al tipo de ataque relevante.*
- *Las alertas deben correlacionarse entre sí si comparten el mismo tipo de ataque, activo u otro componente aplicable.*
- *La pista de auditoría (no editable) debe estar disponible para cada caso.*
- *Las interfaces deben ser personalizables.*
- *El administrador debe poder ver registros sin procesar de consultas de datos analizados / normalizados.*
- *Los flujos de trabajo / playbooks deben establecer qué acciones de remediación puede tomar un investigador y prevenir acciones que harían cambios innecesarios o causarían pérdida de evidencia.*
- *El usuario debe poder buscar palabras clave en todos los campos de datos.*
- *Todas las actualizaciones, notas o acciones deben poder transferirse de la investigación a una plataforma de ticketing.*
- *El analista debe tener la capacidad de solicitar que se cree un nuevo ticket en la plataforma de ticketing con información relevante incluida.*
- *El administrador debe tener la capacidad de administrar los comentarios (agregar, editar / eliminar / eliminar) o adjuntos (agregar, editar / eliminar / eliminar, buscar).*
- *Los metadatos del ticket deben ofrecer información diversa sobre un ticket seleccionado (quién / cuándo, ID, estado, prioridad, cola).*
- *La gestión de casos debe admitir el acceso basado en roles (RBAC).*
- *La solución debe permitir escalar tickets basado en: prioridad, riesgo, impacto, años.*
- *La solución debe poder realizar un análisis de la causa raíz (RCA, relacionado con la causa del incidente).*
- *La solución debe ser capaz de realizar un análisis posterior al incidente (PIA, relacionado con el manejo de incidentes).*
- *La solución debe tener playbooks / flujos de trabajo personalizables sobre cómo manejar un incidente en diferentes incidentes (correo electrónico, web, infección de punto final).*
- *La solución debe poder realizar una búsqueda de texto completa en todos los incidentes para notas y descripción u otras palabras clave en los incidentes.*

- *La solución debe soportar el ciclo de vida de respuesta a incidentes (asignación / mapeo / escalamiento).*
- *La solución debe admitir el mapeo / etiquetado de tickets / incidentes en las fases de Cyber Kill Chain.*
- *La solución debe admitir el seguimiento y las alertas de SLA (acuerdos de nivel de servicio de seguimiento de incidentes).*
- *La solución debe administrar el archivo adjunto como parte de la administración de alertas / incidentes (agregar, editar / eliminar / eliminar, buscar).*
- *La solución debe ser compatible con las campañas Threat Hunting / Track.*
- *La solución debe admitir la búsqueda de las IOC agregadas en el sistema de gestión de registros.*
- *Solución Debe tener la capacidad de crear módulos personalizados desde dentro de la GUI web, un módulo es un subsistema como: Alertas, Incidencias, indicadores, etc.*
- *La solución debe proporcionar los registros necesarios relacionados con IOC específicos en los tickets (registros de red / sistemas de endpoint).*

Playbooks

- *La solución debe tener al menos 80 playbooks listos para usar.*
- *Las métricas de informes de los playbooks deben estar disponibles (tiempo de ejecución, punto de falla, etc.).*
- *La ejecución de playbooks debe crear una pista de auditoría en el caso.*
- *La solución debe tener la capacidad de enviar actualizaciones al sistema de tickets a partir de los pasos y resultados del playbook.*
- *El administrador debe tener la capacidad de exportar playbook, incluidas todas sus versiones guardadas (similar a SVN / GIT).*
- *La solución debe admitir la ejecución de varios playbooks al mismo tiempo.*
- *Las herramientas de depuración deben estar disponibles con la herramienta.*
- *La solución debe admitir la creación de playbooks con una interfaz visual.*
- *Los playbooks deben admitir acciones y tareas manuales.*
- *Los playbooks deben admitir toma de decisiones.*
- *Los playbooks deben admitir playbooks anidados.*
- *Los playbooks deben admitir ejecución de Python para scripts personalizados.*
- *Los playbooks deben admitir correos electrónicos de texto enriquecido.*

- *La herramienta debe tener al menos 6 tipos de iniciación de playbooks.*
- *La solución debe tener guías de ingestión de datos.*
- *La solución debe permitir activar informes de playbooks.*
- *La solución debe capturar errores y las razones de la falla.*
- *La solución debe controlar los playbooks a través de RBAC.*
- *La solución debe admitir el control de versiones de los playbooks.*
- *La solución debe admitir la exportación de un solo playbook.*
- *La solución debe admitir el reinicio del playbook desde el paso fallido.*

Características de los Conectores

- *El fabricante debe proporcionar actualización y soporte consistentes a los conectores suministrados.*
- *El proveedor debe proporcionar nuevos conectores mediante la liberación de nuevas versiones.*
- *El proveedor debe proporcionar documentación para configurar la integración con los conectores compatibles.*
- *La solución debe tener al menos una integración con 290 conectores.*
- *La solución debe enviar una notificación sobre la nueva actualización.*
- *El proveedor debe proporcionar el SDK del conector sin costo adicional.*
- *La solución debe tener un asistente de ingestión de datos para SIEM, Exchange, TIP y plataformas relacionadas.*
- *La solución debe mostrar el estado de salud de la integración / conector desde la página del conector sin ningún paso adicional.*

Características de IOC

- *La solución debe tener un módulo dedicado de indicadores, búsquedas y campañas.*
- *Los IoC deben correlacionarse entre diferentes incidentes / tickets.*
- *El analista debe poder agregar, editar, eliminar y buscar IOC.*
- *El IoC debe poderse agrupar por evento, campaña, atacante, vector, agrupación de sectores.*
- *El analista debe poder etiquetar los IOC en las fases de Cyber Kill Chain (etiqueta).*

Requerimientos de Auditoría

- *La solución debe registrar el seguimiento de auditoría de todos los pasos manuales y automatizados, acciones durante la ejecución de un playbook.*
- *La solución debe poder documentar automáticamente todo el flujo de trabajo del incidente, así como los pasos automatizados de todos los incidentes y de todas las acciones tomadas en un incidente.*
- *La solución debe monitorear su uso para mantener un log de auditoría completo del acceso al sistema, modificaciones del sistema, cambios de configuración, etc. Registros de auditoría granulares con detalles de "Quién, Qué, Cuándo, Dónde" con resultado de éxito / falla para todas y cada una de las actividades de usuarios.*
- *La solución debe incluir un módulo de cumplimiento listo para usar que ayude a las actividades de SoC a cumplir con el estándar.*

Administración de usuarios & RBAC

- *La solución debe admitir el control de acceso basado en roles para la segregación del tipo de alerta / incidente.*
- *La solución debe admitir un menú sencillo para que los administradores agreguen, modifiquen y eliminen usuarios y luego proporcionen acceso.*
- *El administrador debe poder limitar el acceso a componentes específicos (búsqueda, informes, ejecutar libros de jugadas, etc.).*
- *La solución debe admitir el inicio de sesión único y las autenticaciones de doble factor.*

Despliegue

- *La solución debe tener la capacidad de implementarse completamente local en modalidad on-premise.*
- *La solución se debe proporcionar en software OVA e implementarse en la infraestructura virtual.*
- *La solución debe transferir fácilmente la configuración a una versión actualizada.*

FIRMAS DIGITALES

Gabriel Robirosa
DIRECTOR GENERAL
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES