RESO SAGYP N° 433/25

Buenos Aires, 30 de julio del 2025

**VISTO**:

El TAE A-01-00020209-2/2025 caratulado *"D. G. C. C. S/ PROVISIÓN Y PUESTA EN FUNCIONAMIENTO DE SOLUCIONES DE WAF Y DE VISIBILIDAD DE APIS"; y*

**CONSIDERANDO**:

Que por la actuación citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología para la contratación de la provisión de una solución WAF (Firewall de Aplicaciones Web Avanzado) y una solución de arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs, incluyendo los servicios de implementación, soporte técnico local y del fabricante, mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires. En tal sentido, la mentada Dirección propuso cláusulas para incorporar en los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas (v. Nota 2F DGIYT 552/25 y Adjuntos 106126/25 y 106153/25).

Que en ese marco, la Dirección General de Compras y Contrataciones entendió viable el llamado a Licitación Pública de etapa única, bajo la modalidad llave en mano, conforme lo dispuesto en los artículos 26, 28, 32, 33, 40, 45 y concordantes de la Ley Nº 2.095 (según texto consolidado por Ley Nº 6.764), la Resolución CM Nº 276/2020, modificada por la Resolución CM N° 248/2024, y la Resolución SAGyP N° 30/2021 (v. Adjunto 108115/25).

Que en tal entendimiento, la Dirección General de Compras y Contrataciones elaboró los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran vinculados como Adjuntos 116993/25 y 116998/25 y estableció como presupuesto oficial la suma de dólares estadounidenses cinco millones trescientos treinta mil (U$S 5.330.000.-). Asimismo, elevó lo actuado a esta Secretaría y recomendó que *"la adquisición de los Pliegos correspondientes proceda mediante el pago de la suma de pesos seiscientos mil ($ 600.000.-),*

*para participar en la Licitación Pública N° 2-0014-LPU25.”* (v. MDGCC 1619/25).

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° 6.764-) 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° 6.764-).

Que en atención a los antecedentes antes relatados, de acuerdo a lo actuado por la Dirección General de Compras y Contrataciones, a lo solicitado por la Dirección General de Informática y Tecnología, sobre la necesidad de impulsar la contratación de marras para garantizar el normal funcionamiento del Poder Judicial de la Ciudad Autónoma de Buenos Aires, y en línea con lo dictaminado por la Dirección General de Asuntos Jurídicos, corresponde aprobar los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran vinculados como 116993/25 y 116998/25, y llamar a Licitación Pública N° 2-0014-LPU25 para la contratación de la provisión de una solución WAF (Firewall de Aplicaciones Web Avanzado) y una solución de arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs, incluyendo los servicios de implementación, soporte técnico local y del fabricante, mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cinco millones trescientos treinta mil (U$S 5.330.000.-), para el día 14 de agosto de 2025 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Que en consecuencia, resulta oportuno instruir a la Dirección General de Compras y Contrataciones a efectos de que instrumente las medidas correspondientes para dar curso a la Licitación Pública N° 2-0014-LPU25, y realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.764), su reglamentación y en la Ley de Procedimientos Administrativos -Decreto 1.510/97- (texto consolidado según Ley N° 6.764).

Que en cumplimiento de la Ley N° 70 (texto consolidado según Ley N° 6.764), la Dirección General de Programación y Administración Contable, tomó conocimiento y realizó el informe presupuestario correspondiente para hacer frente la contratación de marras (v. Adjunto 119671/25).

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 14065/2025.

Que por la Resolución Presidencia N° 155/2024, ratificada por Resolución CM N° 63/2024, se 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° 6.764).

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° 6.764) y la Resolución CM N° 276/2020, modificada por la Resolución CM N° 248/2024 y la Resolución Presidencia 155/2024;

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

Artículo 1º: Apruébanse los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, que como Adjuntos 116993/25 y 116998/25 forman parte de la presente Resolución y regirán para la Licitación Pública N° 2-0014-LPU25, para la contratación de la provisión de una solución WAF (Firewall de Aplicaciones Web Avanzado) y una solución de arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs, incluyendo los servicios de implementación, soporte técnico local y del fabricante, mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cinco millones trescientos treinta mil (U$S 5.330.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0014-LPU25, de etapa única, bajo la modalidad de orden de llave en mano, fijándose como fecha límite para la presentación de ofertas y la apertura pública de ofertas para el día 14 de agosto de 2025 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Artículo 3º: Establézcase que la adquisición de los pliegos necesarios para cotizar en la Licitación Pública N° 2-0014-LPU25, será por un monto de pesos seiscientos mil ($ 600.000.-).

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0014-LPU25, a los Dres. Adrián Costantino y Hernán Labate como miembros titulares, y a los Dres. Javiera Graziano y Matías Vázquez como miembros suplentes de la Comisión de Evaluación de Ofertas que acompañarán al titular de la Unidad de Evaluación de Ofertas, Dr. Federico Hernán Carballo.

Artículo 5º: Instrúyase a la Dirección General de Compras y Contrataciones a implementar las medidas correspondientes para dar curso a la Licitación Pública N° 2-0014-LPU25, y para que realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.764) su reglamentaria Resolución CM N° 276/2020 y modificatoria, y en la Ley de Procedimientos Administrativos - Decreto 1.510/97- (texto consolidado según Ley N° 6.764).

Artículo 6°: 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 la Dirección General de Informática y Tecnología y a la Dirección General 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

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

# LICITACION PÚBLICA N° 2-0014-LPU25

## PROVISIÓN Y PUESTA EN FUNCIONAMIENTO DE SOLUCIONES INFORMÁTICAS DE WAF Y DE VISIBILIDAD DE APIS

## PLIEGO DE BASES Y CONDICIONES PARTICULARES

**31. CONSULTAS**

**32. COMUNICACIONES**

**ANEXO I - DECLARACIÓN JURADA DE APTITUD PARA CONTRATAR**

**ANEXO II - DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA**

**ANEXO III - DECLARACIÓN JURADA DE INCOMPATIBILIDAD**

**ANEXO IV – CERTIFICADO DE VISITA**

# PLIEGO DE BASES Y CONDICIONES PARTICULARES

## 1. GENERALIDADES

El presente Pliego de Bases y Condiciones Particulares (PCP) tiene por objeto completar, aclarar y perfeccionar las estipulaciones del Pliego Único de Bases y Condiciones Generales (PCG) aprobado por Resolución SAGyP N° 30/2021, para la presente licitación pública.

## 2. OBJETO DE LA CONTRATACIÓN

La presente es una licitación de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la provisión de una solución WAF (Firewall de Aplicaciones Web Avanzado) y una solución de arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs, incluyendo los servicios de implementación, soporte técnico local y del fabricante, mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires.

## 3. PRESUPUESTO OFICIAL

El presupuesto oficial para la presente contratación asciende a la suma total de **Dólares Estadounidenses Cinco Millones Trescientos Treinta Mil (U$S 5.330.000.-)**, el cual se compone de la siguiente manera:

Renglón 1: Dólares Estadounidenses Un Millón Seiscientos Doce Mil Quinientos (U$S 1.612.500.-).

Renglón 2: Dólares Estadounidenses Un Millón Ciento Setenta y Dos Mil Quinientos (U$S 1.172.500.-).

Renglón 3: Dólares Estadounidenses Dos Millones Cuatrocientos Ochenta y Cinco Mil (U$S 2.485.000.-).

Renglón 4: Dólares Estadounidenses Sesenta Mil (U$S 60.000.-).

## 4. RENGLONES A COTIZAR

**Renglón 1:** Provisión, implementación y puesta en funcionamiento de una solución WAF (Firewall de Aplicaciones Web Avanzado), incluyendo licencias y suscripciones, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

**Renglón 2:** Provisión, implementación y puesta en funcionamiento de una solución de arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs, conforme las

características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

**Renglón 3:** Provisión de suscripción a servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en los Renglones 1 y 2, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

**Renglón 4:** Provisión de suscripción a servicios de capacitación para la solución provista en el renglón 2, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

**5. PLIEGOS**

Sólo se tendrán en cuenta las propuestas presentadas por los oferentes que hayan abonado, previo a la apertura de las ofertas del acto licitatorio, el arancel correspondiente al valor de los pliegos.

El valor de los Pliegos asciende a la suma de **Pesos Seiscientos Mil ($ 600.000.-)** y podrá abonarse mediante depósito en efectivo o por transferencia bancaria a la Cuenta Corriente $ N° 000306800050213214, a nombre del Consejo de la Magistratura, en el Banco de la Ciudad de Buenos Aires, Sucursal Nº 52, sita en Av. Presidente Roque Sáenz Peña 541 de esta Ciudad, CBU 0290068100000502132146, CUIT 30-70175369-7.

Se estima conveniente establecer el valor de adquisición de los pliegos, dadas las características propias de la contratación, la magnitud de los valores involucrados, trascendencia, importancia y el interés público comprometido.

**Se deberá acompañar en forma obligatoria junto a la oferta el comprobante de compra del pliego licitatorio, conforme el artículo 3 del PCG.**

**6. PLAZOS DE LA CONTRATACIÓN**

**6.1 Plazo Contractual**

La presente contratación tendrá un plazo de vigencia de treinta y nueve (39) meses, contados a partir del perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

**6.2 Plazo de Ejecución Renglones 1 y 2:**

El plazo máximo de entrega, implementación y puesta en funcionamiento de las soluciones solicitadas no será superior a noventa (90) días corridos, contados a partir del perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

**6.3 Plazo de Vigencia Renglones 1 y 2:**

Las soluciones tendrán una vigencia de treinta y seis (36) meses, contados a partir de la fecha indicada en el parte de recepción definitiva de la implementación y puesta en funcionamiento de las soluciones solicitadas.

**6.4 Plazo de Ejecución Renglones 3 y 4:**

Los servicios requeridos tendrán una duración de treinta y seis (36) meses, contados a partir de la fecha indicada en el parte de recepción definitiva de la implementación y puesta en funcionamiento de las soluciones solicitadas.

## 7. MODALIDAD DE LA CONTRATACIÓN

La presente contratación se efectúa bajo la modalidad llave en mano, de conformidad con lo dispuesto por el artículo 40 inciso e) y 45 de la Ley N° 2.095 -según texto consolidado por Ley N° 6.764- y el Anexo I de la Resolución CM N° 276/2020, lo cual implica que se contratará a través de un único proveedor la realización integral del proyecto, de manera que los oferentes deberán cotizar una solución integral que satisfaga las necesidades del Poder Judicial.

En su propuesta el adjudicatario deberá incluir todos los bienes, servicios y componentes solicitados y cumplir con los requerimientos técnicos y funcionales que se describan o se soliciten en el presente Pliego de Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

## 8. GARANTÍA TÉCNICA, SOPORTE Y CANAL CERTIFICADO

La solución requerida deberá contar con treinta y seis (36) meses de garantía, contados a partir de la fecha de la provisión de las licencias y equipamiento.

El oferente deberá contar con servicio técnico en la Ciudad Autónoma de Buenos Aires, el que deberá cubrir el cumplimiento de la garantía.

El oferente deberá detallar en su oferta económica el procedimiento a realizar en caso de tener que reportar incidentes, tal como número de teléfono de asistencia, personas de contactos, etc.

Durante todo el plazo de vigencia de la garantía técnica, el Consejo de la Magistratura retendrá la garantía de adjudicación presentada a los efectos del afianzamiento de la misma.

El oferente deberá contar con expresa autorización del fabricante F5 Inc. para distribuir el equipamiento ofertado y ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato.

## 9. CONDICIONES PARA SER OFERENTE

Para concurrir como oferentes a la presente Licitación, se deberán reunir los siguientes requisitos:

1. En el caso de las personas humanas en forma individual, deberán cumplirse los requisitos contemplados en el Art. 89º de la Ley 2095 (Texto consolidado por Ley Nº 6.764)

2. En el supuesto de presentarse una sociedad, deberán cumplirse los requisitos contemplados en el Art. 89º de la Ley 2095 (Texto consolidado por Ley Nº 6.764) y los detallados a continuación:

a) Su objeto principal debe estar claramente relacionado con el objeto y naturaleza de los servicios que se licitan.

b) La vigencia de los Contratos Sociales de los Oferentes debe ser igual o superior al plazo previsto para esta contratación, más la eventual prórroga.

3. En el caso de las Uniones Transitorias (UT) que se constituyan a efectos de participar en la presente Licitación Pública, deberán estar integradas por un máximo de tres (3) sociedades comerciales, por lo menos una (1) de ellas deberá acreditar experiencia en el rubro conforme el presente Pliego.

La UT deberá estar inscripta o preinscripta en el RIUPP al momento de la presentación de la oferta, debiendo figurar inscripta al momento de la preadjudicación.

Las ofertas deberán contener, los documentos de constitución de la U.T., en los que deberán constar:

1. El compromiso de mantener la vigencia de la U.T., por un plazo superior a la duración de la contratación, incluyendo una eventual prórroga contractual.
2. El compromiso de mantener la composición de la U.T. durante el plazo mencionado en el inciso anterior, así como también de no introducir modificaciones en los estatutos de las empresas integrantes que importen una alteración de la responsabilidad, sin la previa aprobación del Consejo.
3. Designación de uno o más representantes legales que acrediten, mediante poder para actuar ante la administración pública, facultades suficientes para obligar a su mandante.
4. De los documentos por los que se confieran los poderes y por los que se constituya la U.T., deberá resultar que los otorgantes o firmantes lo hicieron legalmente, en ejercicio de las atribuciones que les corresponden como autoridades de cada una de las empresas en funciones, en el momento del acto respectivo.
5. Las empresas integrantes de la U.T. serán solidariamente responsables por el cumplimiento del

Contrato en caso de adjudicación. Cada una de las Sociedades Comerciales que integren la U.T., deberán presentar acta del órgano social correspondiente de la cual surja la decisión de presentarse a esta licitación pública por contrato asociativo de unión transitoria. A tal efecto, el Consejo intimará a los oferentes para que en el plazo perentorio de dos (2) días a contar desde el día siguiente al de la recepción de la intimación, se subsane la deficiencia, bajo apercibimiento de desestimarse la oferta.

**10. DECLARACIONES JURADAS**

Junto a la propuesta económica los proponentes deberán presentar las declaraciones juradas de Aptitud para Contratar, de Propuesta Competitiva y de Incompatibilidad establecidas en los Anexos I, II y III del presente pliego.

El Consejo de la Magistratura podrá verificar la veracidad de los datos volcados en las declaraciones juradas en cualquier etapa del procedimiento.

**11. INSCRIPCION EN EL REGISTRO INFORMATIZADO UNICO Y PERMANENTE DE PROVEEDORES DEL SECTOR PÚBLICO DE LA CIUDAD (RIUPP)**

Para que las ofertas sean consideradas válidas, los oferentes deberán estar inscriptos en el RIUPP o presentar constancia de inicio de trámite. Todo ello de conformidad con lo previsto en el artículo 5° del PCG.

Es condición para la preadjudicación que el proveedor se encuentre inscripto en el RIUPP, en los rubros licitados y con la documentación respaldatoria actualizada.

**12. CORREO ELECTRONICO Y CONSTITUCIÓN DE DOMICILIO**

Conforme el artículo 6 del Pliego de Bases y Condiciones Generales, se considerará como único domicilio válido el declarado por el oferente en calidad de constituido ante el RIUPP.

Asimismo, se considerará domicilio electrónico el declarado como correo electrónico por el administrador legitimado en el sistema, en oportunidad de inscribirse en el RIUPP, en el que se tendrán por válidas todas las notificaciones electrónicas que sean cursadas por el Consejo de la Magistratura.

Todo cambio de domicilio deberá ser comunicado fehacientemente al Poder Judicial de Ciudad Autónoma de Buenos Aires y surtirá efecto una vez transcurridos diez (10) días de su notificación. No obstante, el mismo deberá quedar establecido en el ámbito de la Ciudad Autónoma de Buenos Aires.

La Dirección General de Compras y Contrataciones (DGCC) constituye domicilio en la Av. Julio Argentino Roca Nº 530 piso 8vo, de la Ciudad Autónoma de Buenos Aires y domicilio electrónico en comprasycontrataciones@jusbaires.gob.ar.

Todas las notificaciones entre las partes serán válidas si se efectúan en los domicilios constituidos aquí referidos.

## 13. INFORMACIÓN SOCIETARIA Y HABILIDAD PARA CONTRATAR CON EL ESTADO

Los oferentes deberán cumplir con:

### 1. Información Societaria

En función de lo dispuesto por el artículo 5 de la Resolución CAGyMJ N° 106/2018, se deberán acompañar con la propuesta los estatutos sociales, actas de directorio, designación de autoridades y composición societaria de la firma oferente, así como toda otra documentación que permita constatar fehacientemente la identidad de las personas físicas que la componen.

El Consejo de la Magistratura requerirá a los organismos competentes en la materia los informes que resulten pertinentes respecto de dichas personas físicas.

### 2. Consulta ARCA

El Consejo de la Magistratura realizará la consulta sobre la habilidad de los oferentes para contratar con el Estado, mediante el servicio web de la ARCA.

Ante la eventualidad de que el resultado de la consulta arroje que la oferente registra deuda ante el organismo recaudador a la fecha de consulta, el Consejo de la Magistratura intimará vía correo electrónico a su subsanación ante la ARCA. Con anterioridad a la emisión del Dictamen de Evaluación, se efectuará una nueva consulta.

## 14. FORMA DE COTIZACION

Las propuestas económicas deberán ser formuladas electrónicamente, a través de la plataforma JUC -juc.jusbaires.gob.ar-, de conformidad con el artículo 12 del PCG y lo detallado a continuación:

**Renglones 1, 2, 3 y 4:**

14.1 Precio Total de cada Renglón, en Dólares Estadounidenses.

**Monto Total:**

14.2 Monto Total de la Oferta, en Dólares Estadounidenses.

Asimismo, en la oferta deberá consignarse expresamente y en detalle el equipamiento y servicios ofertados a fin de permitir su correcta evaluación.

No se admitirán cotizaciones en otras monedas a la indicada en las bases y condiciones establecidas para la presente contratación en la plataforma JUC. No se admitirán cotizaciones parciales, resultando obligatoria la presentación de propuestas por la totalidad de lo requerido.

En el precio el oferente debe considerar incluidos todos los impuestos vigentes, derechos o comisiones, movimientos dentro de los edificios, seguros, reparación de eventuales daños por culpa del adjudicatario, responsabilidad civil, beneficios, sueldos y jornales, cargas sociales, gastos de mano de obra auxiliar, gastos y costos indirectos, gastos y costos generales, costos de entrega, fletes, armado, medios de descarga y acarreo y todo otro gasto o impuesto que pueda incidir en el valor final de la prestación.

En caso de discrepancia entre la propuesta económica expresada en números y letras, prevalecerá esta última.

SE DEJA CONSTANCIA QUE EN CASO DE DIFERIR EL VALOR CONSIGNADO ENTRE LA PROPUESTA ECONOMICA CARGADA COMO DOCUMENTACIÓN ANEXA Y LA CARGADA EN JUC, SE ESTARÁ AL VALOR INGRESADO EN LA GRILLA DE JUC.

## 15. VISITA TÉCNICA

Los interesados deberán realizar una visita a los lugares donde se desarrollarán las tareas objeto de la presente contratación, con el fin de tomar conocimiento de las condiciones en que las prestaciones deberán ser llevadas a cabo y de evacuar todas las dudas que pudieran surgir del presente requerimiento, no pudiendo alegar posterior ignorancia y/o imprevisiones.

Las visitas se facilitarán **hasta el día anterior a** la fecha estipulada para la apertura pública de las ofertas, debiendo comunicarse con la Dirección General de Informática y Tecnología, de lunes a viernes de 10.30 a 12.00 horas y de 14.30 a 17.00 horas, al teléfono 15-4159-9006, a los efectos de coordinar el día y hora en que serán efectuadas.

La Dirección General de Informática y Tecnología del Consejo de la Magistratura extenderá el correspondiente Certificado de Visita, que como Anexo IV acompaña el presente Pliego.

**Los certificados de visita deberán acompañarse obligatoriamente con la oferta, bajo apercibimiento de considerarse la misma como no admisible.**

## 16. ANTECEDENTES COMERCIALES

El oferente deberá proveer al menos tres (3) referencias de implementaciones de características similares en organismos de gobierno de Argentina a los efectos de validar la implantación de la tecnología.

**17. CONSTITUCIÓN DE GARANTÍAS**

Para afianzar el cumplimiento de todas las obligaciones, los oferentes y adjudicatarios deben constituir las siguientes garantías de corresponder y sin límite de validez, conforme el artículo 93° de la Ley N° 2.095 -según texto consolidado por Ley N° 6.764-:

a) De impugnación de Pliegos: será del tres por ciento (3%) del presupuesto oficial de la presente Licitación Pública. Puede ser recibida hasta setenta y dos (72) horas antes de la fecha de apertura de ofertas y se tramita por cuerda separada.

La documentación que acredite la constitución de la garantía de impugnación deberá presentarse ante la Dirección General de Compras y Contrataciones del Consejo de la Magistratura, sita en Av. Pte. Julio A. Roca 538 Piso 8°, de esta

Ciudad, previo a formalizar la impugnación, completando el formulario electrónico correspondiente del sistema JUC, dentro del plazo legal establecido.

b) De Mantenimiento de Oferta: será del cinco por ciento (5%) sobre el valor total de la oferta. En caso de resultar adjudicatario esta garantía se prolongará hasta la constitución de la garantía de cumplimiento del contrato. Al momento de presentar sus propuestas, los oferentes deberán IDENTIFICAR e INDIVIDUALIZAR la garantía de mantenimiento de la oferta completando el formulario electrónico correspondiente del sistema JUC.

**En caso de tratarse de una póliza de caución que NO contenga firma digital o de otro tipo de garantía**, **ésta deberá ser entregada dentro del plazo de veinticuatro (24) horas** de formalizado el acto de apertura de ofertas, bajo apercibimiento de descarte de la oferta, en la Dirección General de Compras y Contrataciones, sito en Av. Julio Argentino Roca Nº 530 piso 8°, de la Ciudad Autónoma de Buenos Aires.

**En caso de tratarse de una póliza de caución con firma digital, la misma deberá ser cargada en JUC como archivo anexo, en su formato original generado por la compañía aseguradora.**

Los oferentes deberán mantener las ofertas por el término de treinta (30) días. Si el oferente no manifestara en forma fehaciente su voluntad de no renovar la garantía de mantenimiento de oferta con una antelación mínima de diez (10) días anteriores al vencimiento del plazo, aquella se considerará prorrogada automáticamente por un lapso igual al inicial.

c) De impugnación a la preadjudicación de las ofertas: será de cinco por ciento (5%) del monto de la

oferta del renglón o los renglones impugnados. Si el dictamen de evaluación para el renglón o los renglones que se impugnen no aconsejare la adjudicación a ninguna oferta, el importe de la garantía de impugnación se calculará sobre la base del monto de la oferta del renglón o renglones del impugnante. Esta garantía deberá integrarse en el momento de presentar la impugnación.

Conforme lo establecido en el artículo 20 del PCG, los interesados podrán formular impugnaciones a la preadjudicación dentro del plazo de tres (3) días de su publicación a través de JUC, previo depósito de la garantía pertinente.

La documentación que acredite la constitución de la garantía de impugnación deberá presentarse ante la Dirección General de Compras y Contrataciones del Consejo de la Magistratura, sita en Av. Pte. Julio A. Roca 538 Piso 8°, de esta Ciudad, previo a formalizar la impugnación, completando el formulario electrónico correspondiente del sistema JUC, dentro del plazo legal establecido.

d) De cumplimiento del contrato: será del diez por ciento (10%) del valor total de la adjudicación. El adjudicatario deberá integrar la garantía de cumplimiento de contrato, debiendo acreditar tal circunstancia mediante la presentación de los documentos en el Consejo de la Magistratura dentro del plazo de cinco (5) días de notificada la Orden de Compra o suscripto el instrumento respectivo. Vencido el mismo, se lo intimará a su cumplimiento por igual plazo.

**En caso de tratarse de una Garantía de Cumplimiento de Contrato mediante póliza de caución con firma digital, la misma deberá ser remitida por correo electrónico a la casilla comprasycontrataciones@jusbaires.gob.ar.**

Los importes correspondientes a las garantías de impugnación serán reintegrados a los oferentes solamente en el caso que su impugnación prospere totalmente.

**18. PRESENTACIÓN DE LAS OFERTAS**

Las ofertas deberán ser presentadas a través del sistema JUC -juc.jusbaires.gob.ar-, cumpliendo todos los requerimientos exigidos en el PCG, el PCP y el PET.

En este sentido, todos y cada uno de los documentos solicitados junto con la documentación adicional que el oferente adjunte electrónicamente, integrarán la oferta.

No se admitirán más ofertas que las presentadas en JUC, rechazándose las remitidas por correo o cualquier otro procedimiento distinto al previsto.

A fin de garantizar su validez, la oferta electrónicamente cargada deberá ser confirmada por el oferente, el cual podrá realizarla únicamente a través del usuario habilitado para ello.

El usuario que confirma la oferta es el administrador legitimado, dándole él mismo validez a todos los documentos que la componen, sin importar que no estén firmados por él.

Toda documentación e información que se acompañe, y que sea requerida en el presente Pliego deberá ser redactada en idioma castellano, a excepción de folletos ilustrativos, que podrán presentarse en su idioma original.

No se admitirán ofertas que no se ajusten a las condiciones establecidas en el artículo 12 del PCG. Los archivos en el sistema JUC, adjuntos a las ofertas deberán encontrarse en formato no editable.

**19. APERTURA DE LAS OFERTAS**

El acto de apertura se llevará a cabo mediante JUC, en la hora y fecha establecida en el respectivo Acto Administrativo de llamado, generándose, en forma electrónica y automática, el Acta de Apertura de Ofertas correspondiente.

Si el día señalado para la Apertura de Ofertas, fuera declarado inhábil para la Administración, el acto se cumplirá el primer día hábil siguiente, a través del mentado portal y en el horario previsto originalmente.

El Consejo de la Magistratura, se reserva la facultad de postergar el Acto de Apertura de Ofertas según su exclusivo derecho, notificando tal circunstancia en forma fehaciente a los adquirentes de los Pliegos y publicando dicha postergación en la página web del Consejo de la Magistratura y en el Boletín Oficial.

**20. CRITERIO DE EVALUACION Y SELECCION DE LAS OFERTAS**

La adjudicación se realizará a la oferta más conveniente a los intereses del Consejo de la Magistratura. Para ello, una vez apreciado el cumplimiento de los requisitos y exigencias estipulados en la normativa vigente y en los Pliegos de Condiciones Generales (PCG), de Condiciones Particulares (PCP) y de Especificaciones Técnicas (PET), se considerarán el precio y la calidad de los bienes y/o servicios ofrecidos, conjuntamente con la idoneidad del oferente y demás condiciones de la propuesta.

Cuando se estime que el precio de la mejor oferta presentada resulta inconveniente, la Comisión de Evaluación de Ofertas podrá solicitar al oferente mejor calificado una mejora en el precio de la oferta, a los fines de poder concluir exitosamente el procedimiento de selección conforme el artículo 99.7.4 del Anexo I de la Resolución CM Nº 276/2020.

**21. DICTAMEN DE LA COMISION EVALUADORA. ANUNCIO. IMPUGNACION**

El Dictamen de Evaluación de las Ofertas (Dictamen de Pre adjudicación) se comunicará a todos los oferentes a través de la plataforma JUC, se publicará en el Boletín Oficial y en la Web del Consejo de la Magistratura consejo.jusbaires.gob.ar/

Las impugnaciones al Dictamen de Evaluación se harán conforme el artículo 99.9º del Anexo I de la Resolución CM Nº 276/2020 y a los artículos 20 y 21 del PCG.

**Documentación Complementaria:**

La Comisión de Evaluación de Ofertas podrá requerir a los oferentes en forma previa a la emisión del Dictamen, aclaraciones sobre los documentos acompañados con su propuesta e información contenida en la misma, en el plazo que se fijará a tal efecto de acuerdo a la complejidad de la información solicitada. Asimismo, podrá requerir que se subsanen los defectos de forma de conformidad con lo establecido en el artículo 99.7.6 del Anexo I de la Resolución CM Nº 276/2020. En tal sentido, podrá solicitarse a los oferentes documentación faltante, en tanto su integración con posterioridad al Acto de Apertura de Ofertas no afecte el principio de igualdad entre oferentes.

## 22. ADJUDICACIÓN

La adjudicación de la presente contratación recaerá sobre un único oferente, motivo por el cual resulta obligatoria la presentación de propuestas por el total de lo solicitado.

## 23. PERFECCIONAMIENTO DEL CONTRATO

Conforme lo establecido por el artículo 24 del PCG.

## 24. CAUSALES DE EXTINCIÓN DEL CONTRATO

Son causales de extinción del contrato las siguientes:

a. Expiración del plazo término del contrato, y las respectivas prórrogas si las hubiere, y/o cumplimiento del objeto, según lo estipulado en el presente pliego.

b. Mutuo acuerdo.

c. Quiebra del adjudicatario.

d. Rescisión, conforme lo establecido en los artículos 122 al 127 de la Ley Nº 2.095 -según texto consolidado por Ley Nº 6.764-.

e. Presentación en concurso del adjudicatario, impidiendo dicha circunstancia el efectivo y total cumplimiento de las obligaciones emergentes de los Pliegos licitatorios.

f. Total cumplimiento de las obligaciones emergentes de los Pliegos licitatorios.

## 25. PERSONAL DE LA ADJUDICATARIA

**25.1 Nómina de Personal**

Previo a iniciar las prestaciones, el adjudicatario deberá presentar en la Dirección General de Informática y Tecnología la nómina del personal que efectuará los trabajos. En la información a brindar se consignarán los siguientes datos:

- Nombre y Apellido
- DNI
- Domicilio Actualizado
- Función que desempeña

**25.2 Responsabilidad por el Personal**

Todo el personal o terceros afectados por el adjudicatario de la Licitación al cumplimiento de las obligaciones y/o relaciones jurídico contractuales carecerán de relación alguna con el Consejo de la Magistratura y/o el Ministerio Público de la Ciudad Autónoma de Buenos Aires.

La adjudicataria asumirá ante el Consejo de la Magistratura y el Ministerio Público de la Ciudad Autónoma de Buenos Aires la responsabilidad total en relación a la conducta y antecedentes de las personas que afecten al servicio.

Estarán a cargo del adjudicatario todas las erogaciones originadas por el empleo de su personal, tales como jornales, aportes y contribuciones, licencias, indemnizaciones, beneficios sociales, otras erogaciones que surjan de las disposiciones legales, convenios colectivos individuales vigentes o a dictarse, o convenirse en el futuro y seguros.

El adjudicatario tomará a su cargo la obligación de reponer elementos o reparar daños y perjuicios que ocasionen al Consejo de la Magistratura y/o al Ministerio Público de la Ciudad Autónoma de Buenos Aires. por delitos o cuasidelitos, sean estos propios o producidos por las personas bajo su dependencia, o los que pudieron valerse para la prestación de los servicios que establece el pliego. El incumplimiento de lo establecido en esta cláusula dará motivo a la rescisión del contrato.

El adjudicatario se hará responsable de los daños y/o perjuicios que se originen por culpa, dolo o negligencia, actos u omisiones de deberes propios o de las personas bajo su dependencia o aquellas de las que se valga para la prestación de los servicios.

El adjudicatario adoptará todas las medidas y precauciones necesarias para evitar daños al personal que depende de él, al personal de este Poder Judicial, a terceros vinculados o no con la prestación del servicio, a las propiedades, equipos e instalaciones de esta Institución o de terceros, así puedan provenir esos daños de la acción o inacción de su personal o elementos instalados o por causas

eventuales.

**25.3 Daños a Terceros**

El adjudicatario implementará las medidas de seguridad que sean necesarias para dar cumplimiento a la legislación vigente en la materia, para evitar daños a las personas o cosas. Si ellos se produjeran, será responsable por el resarcimiento de los daños y perjuicios ocasionados.

**25.4 Exclusión**

El Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires se reserva el derecho de la Exclusión de cualquier personal, recurso, ayudante o coordinador mientras dure la relación contractual.

**26. SEGURIDAD E HIGIENE**

En los casos en que corresponda, la adjudicataria deberá dar cumplimiento a la normativa vigente en materia de "Seguridad e Higiene en el Trabajo" (Ley 19587 – Decreto 351/79 y otros vigentes).

La documentación a presentar ante la Dirección de Seguridad del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires antes del inicio de los trabajos será la siguiente:

1 - Presentación del responsable de Seguridad e Higiene de la empresa (es el responsable del cumplimiento de las normas de Seguridad e Higiene de la empresa por las tareas que ésta realice en el Consejo de la Magistratura).

2 - Certificado de cobertura de ART con cláusula de no repetición que accione a favor del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

3 - Plan de contingencias de la empresa por las tareas que son objeto de la presente contratación, conforme a las normativas vigentes en la materia, presentado y aprobado en la ART de la empresa que realice los trabajos.

4 - Constancias de capacitación al personal que realice los trabajos en los edificios en materia de Seguridad e Higiene en el Trabajo según normas vigentes en la materia.

5 - Constancias de entrega de elementos de protección personal a los trabajadores que realicen las tareas en los edificios que son objeto de la presente contratación, según normas vigentes en la materia.

Por otra parte, deberá presentar constancia de capacitación y/o matrícula habilitante del personal en las tareas que desarrollará.

6 - Formulario 931 AFIP de la totalidad de los meses del año en curso.

## 27. SEGUROS

### Coberturas de seguros a requerir

**Generalidades:**

A continuación, se detallan las coberturas de seguros a requerir para el ingreso y permanencia de terceros ajenos, sean proveedores y/o adjudicatarios que desarrollen tareas o presten servicios en ubicaciones pertenecientes al Consejo de la Magistratura y/o Ministerio Público de la Ciudad Autónoma de Buenos Aires tanto sean éstas en propiedad o en uso, así como las características mínimas de admisibilidad de las mismas. El adjudicatario deberá acreditar los contratos de seguros que se detallan y su vigencia durante todo el período contractual, mediante la presentación de copias de sus respectivas pólizas y los comprobantes de pago de las mismas. El adjudicatario no podrá dar comienzo a la prestación si los mismos no se han constituido.

Cada vez que el adjudicatario modifique las condiciones de póliza o cambie de compañía aseguradora, o cada vez que el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires lo solicite, se presentarán copias de las pólizas contratadas.

La contratación de los seguros que aquí se requieren es independiente de aquellos otros que deba poseer el adjudicatario a fin de cubrir los posibles daños o pérdidas que afecten a sus bienes o los de sus empleados, sean los mismos o no de carácter obligatorio.

Quedará a criterio del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, conforme a las actividades a realizar por terceros, la inclusión/incorporación/exclusión de cláusulas de cobertura, medida de la prestación y modificación de sumas aseguradas, durante la vigencia de las pólizas contratadas por el adjudicatario, los cuales deberán acreditar el endoso correspondiente a tales cambios.

**De las compañías aseguradoras:**

Las compañías aseguradoras con las cuales el adjudicatario/prestador o proveedor contrate las coberturas establecidas en el presente Artículo, deben ser de reconocida solvencia, radicadas en la C.A.B.A. o que posean filial administrativa local y autorizadas a tal fin por la Superintendencia de Seguros de la Nación para emitir contratos en los riesgos a cubrir.

El Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires se reserva el derecho de solicitar a su solo juicio el cambio de compañía aseguradora, si la contratada no alcanza con los indicadores generales, patrimoniales y de gestión en atención al riesgo asumido en el contrato de seguro.

**De las coberturas de seguro en particular:**

Las coberturas que el adjudicatario ha de acreditar aún cuando disponga de otros, son los que se detallan a continuación:

1) Seguros Laborales.

2) Seguro de Accidentes Personales. (En caso de corresponder)

3) Seguro de Responsabilidad Civil Comprensiva.

En los apartados siguientes se detallan las condiciones mínimas de los contratos de seguro. Los mismos deben cumplir con todos los requerimientos establecidos en las leyes vigentes para cada caso en particular.

**1) Seguros Laborales**

Seguro de Riesgos del Trabajo, cobertura de ART. El adjudicatario en cumplimiento de la legislación vigente, debe acreditar un seguro que cubra a la totalidad del personal que afecte al servicio contratado, el cual será suscripto con una "Aseguradora de Riesgos de Trabajo (ART)".

No se podrá afectar personal alguno cualquiera sea su índole, hasta que el mismo no cuente con su correspondiente cobertura por riesgo de accidentes de trabajo.

Se deberán presentar al Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, los certificados de cobertura de los trabajadores amparados, en los cuales estará incluido el siguiente texto:

"Por la presente, la A.R.T, renuncia en forma expresa a reclamar o iniciar toda acción de repetición, de subrogación o de regreso contra el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, sus funcionarios y/o empleados, sea con fundamento en el Art. N°39 ap. 5 de la Ley N°24.557, o en cualquier otra norma jurídica, con motivo de las prestaciones en especie o dinerarias que se vea obligada a abonar, contratar u otorgar al personal dependiente o ex dependiente del adjudicatario, amparados por la cobertura del contrato de afiliación N° XXXX, por acciones del trabajo o enfermedades profesionales, ocurridos o contraídas por el hecho o en ocasión de trabajo."

**2) Seguro de Accidentes Personales.** (En caso de corresponder)

En el caso que el adjudicatario contrate a personal y/o prestadores de servicio que no esté alcanzado por La Ley de Contrato de Trabajo, es decir, quienes no revistan el carácter de relación de dependencia con el mismo; se deberá contar con una póliza de seguros del ramo Accidentes Personales con las siguientes características:

Alcance de la Cobertura: Se deberá amparar a la totalidad del personal afectado durante la jornada

laboral incluyendo cobertura *in-itinere.*

Sumas mínimas a Asegurar:

Muerte: pesos veinte millones ($ 20.000.000,00.-).

Invalidez Total y/o parcial permanente por accidente: pesos ocho millones ($ 8.000.000,00.-).

Asistencia Médico Farmacéutica (AMF): pesos cuatro millones ($ 4.000.000,00.-).

La citada póliza deberá incluir el siguiente texto:

*"La compañía ……renuncia en forma expresa a realizar cualquier acción de repetición y/ó subrogación contra el* Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, *CUIT 30-70175369-7 del Consejo de la Magistratura de CABA, sus funcionarios y/o empleados."*

**3) Seguro de Responsabilidad Civil Comprensiva.**

En los casos en que corresponda, el adjudicatario debe asegurar, bajo póliza de responsabilidad civil, los daños que como consecuencia de tareas inherentes a su actividad que puedan ocasionar a personas, bienes o cosas de propiedad del Consejo de la Magistratura y/o del Ministerio Público de la Ciudad Autónoma de Buenos Aires o de terceros.

Suma Asegurada Mínima:

La misma será por un monto mínimo de pesos veinte millones ($ 20.000.000.-). Se detallan de manera enunciativa y no taxativa las coberturas adicionales a incluirse de corresponder en cada caso:

A) Responsabilidad Civil emergente de escapes de gas, incendio, rayo y/o explosión, descargas eléctricas.

B) Daños por caída de objetos, carteles y/o letreros

C) Daños por hechos maliciosos, tumulto popular.

D) Grúas, Guinches, auto elevador (de corresponder).

E) Bienes bajo cuidado, custodia y control.

F) Carga y descarga de bienes fuera del local del asegurado.

El contrato deberá contener un endoso en carácter de co-asegurado sin restricción de ninguna especie o naturaleza a favor del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires. Los empleados del Consejo de la Magistratura y del Ministerio Público de la Ciudad Autónoma de Buenos Aires deberán ser considerados terceros en póliza.

La citada póliza deberá incluir el siguiente texto:

*"La compañía ……. renuncia en forma expresa a realizar cualquier acción de repetición y/ó subrogación contra el* Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, *CUIT 30-70175369-7 del Consejo de la Magistratura de CABA, sus funcionarios y/o empleados."*

**28. PLAZO DE ENTREGA DE PÓLIZAS DE SEGUROS**

Las pólizas de seguro mencionadas en el Punto precedente, deberán ser presentadas en la Mesa de Entradas de este Consejo, sita en Av. Julio A. Roca 530, en un plazo de cinco (5) días desde la recepción de la Orden de Compra.

En este marco, será responsabilidad del adjudicatario asegurar la vigencia de las coberturas durante el plazo contractual.

**29. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO**

**29.1 Certificación de Conformidad**

A los efectos de otorgar la Conformidad Definitiva, el Consejo de la Magistratura emitirá el Parte de Recepción Definitiva.

Dicho Parte es el único documento interno para el trámite de pago e implica la aceptación de conformidad de los bienes recibidos y/o del servicio prestado.

El Consejo de la Magistratura emite los Partes por duplicado, conforme el siguiente detalle:

1. El original para el trámite de pago.
2. El duplicado para el proveedor.

Los Partes de Recepción Definitiva deberán ser suscriptos por los titulares de las reparticiones intervinientes.

**29.2 Pago**

Todos los pagos de la presente contratación se efectuarán en pesos. Todas las facturas que presente la adjudicataria se confeccionarán en pesos.

El tipo de cambio a considerar será el del dólar vendedor del Banco de la Nación Argentina, al cierre del día anterior al de la presentación de la factura.

**Renglones 1 y 2:**

Se abonará el treinta por ciento (30%) del monto total correspondiente a los Renglones 1 y 2 en concepto de anticipo financiero.

El adjudicatario deberá presentar un seguro de caución por el importe que se le anticipe, el cual tendrá vigencia hasta la recepción definitiva de los servicios adjudicados. El importe adelantado se descontará al liquidarse los montos facturados.

El monto restante se abonará en una única vez, conforme lo indicado en el Pliego de Bases y Condiciones Generales, luego de la emisión del Parte de Recepción Definitiva correspondiente a la implementación y puesta en funcionamiento de las soluciones requeridas.

**Renglones 3 y 4:**

El pago de lo solicitado se efectuará por anticipado, de conformidad con lo dispuesto en el Pliego de Bases y Condiciones Generales.

En tal sentido, el adjudicatario deberá integrar un seguro de caución por el total adjudicado en garantía del pago anticipado, seguro que tendrá vigencia durante toda la vigencia de la contratación (artículo 93° inciso c) de la Ley N° 2.095 -según texto consolidado Ley N° 6.764).

**30. PENALIDADES**

**30.1 Generalidades**

El incumplimiento en término y/o satisfactorio de las obligaciones contractuales coloca al adjudicatario en estado de mora y, por lo tanto, sujeto a la aplicación, previo informe de las áreas técnicas, de las penalidades establecidas en el Capítulo XII del Título VI de Ley N° 2.095 -según texto consolidado por Ley N° 6.764- y su reglamentación.

El Consejo de la Magistratura podrá aplicar penalidades y/o sanciones, aun cuando el contrato se encontrara extinguido y/o rescindido; ello en tanto el hecho motivador hubiera sido constatado durante la vigencia del contrato.

Sin perjuicio de la aplicación de las penalidades, los oferentes o co-contratantes pueden asimismo ser pasibles de las sanciones establecidas en el artículo 129 de la Ley N° 2.095 -según texto consolidado por Ley N° 6.764- y su reglamentación.

Toda mora en el cumplimiento del contrato coloca al adjudicatario en estado de mora automática, y por tanto innecesaria la constitución en mora de la contratista.

**30.2 Particularidades**

El primer incumplimiento de lo dispuesto en el apartado Niveles de Servicio del Pliego de Especificaciones Técnicas, dará lugar a la aplicación de una multa equivalente a diecisiete mil (17.000) unidades de compra.

El segundo incumplimiento de lo dispuesto en aquel apartado, dará lugar a la aplicación de una multa equivalente a cuarenta y dos mil seiscientos (42.600) unidades de compra.

A partir del tercer incumplimiento, estos darán lugar a la aplicación de una multa equivalente a ciento veintisiete mil ochocientos (127.800) unidades de compra en cada ocasión.

El Consejo de la Magistratura podrá rescindir el contrato de pleno derecho, cuando la suma de las penalidades aplicadas alcanzare en su monto el cinco por ciento (5%) del importe total del contrato.

**31. CONSULTAS**

Las consultas relacionadas con la presente contratación deberán efectuarse a través de la plataforma JUC -juc.jusbaires.gob.ar-, conforme lo establece el artículo 9º del PCG, hasta los tres (3) días previos a la fecha establecida para la apertura de ofertas.

Para consultas técnicas relativas al funcionamiento como proveedores en el sistema JUC, comunicarse con la Mesa de Ayuda JUC al Tel. 4008-0300, Whatsapp +549113151-0930 o enviar un correo electrónico a: meayuda@jusbaires.gob.ar.

Para consultas administrativas en relación a la participación de los interesados en el proceso de selección, como de su carga en la plataforma JUC, deberán enviar correo electrónico a utasc@jusbaires.gob.ar.

**32. COMUNICACIONES**

Todas las comunicaciones que se realicen entre el Consejo de la Magistratura y los interesados, oferentes y adjudicatarios, que hayan de efectuarse en virtud de las disposiciones de la Ley N° 2.095 (texto consolidado según Ley N° 6.764) y su reglamentación se entienden realizadas a través del envío de mensajería mediante JUC en forma automática, y a partir del día hábil siguiente al de su notificación.

No obstante, para aquellos casos en los que el mentado sitio no prevea una comunicación automática, podrán llevarse a cabo por cualquier medio de comunicación que responda a los principios de transparencia, economía y celeridad de trámites.

**ANEXO I**

**DECLARACION JURADA DE APTITUD PARA CONTRATAR**

El que suscribe (nombre y apellido, representante legal o apoderado)……..con poder suficiente para este acta DECLARA BAJO JURAMENTO, que (nombre y apellido o razón social)……CUIT N°……está habilitado/o para contratar con el PODER JUDICIAL DE LA CIUDAD AUTONOMA DE BUENOS AIRES, en razón de cumplir con los requisitos del artículo 89 de la Ley N° 2095 (según texto consolidado por Ley N° 6.764) y que no está incurso en ninguna de las causales de inhabilidad establecidas en los incisos a) a j) del artículo 90 del citado plexo normativo y del PCP.

FIRMA

…….

ACLARACION

…….

CARÁCTER

……

Ciudad de Buenos Aires, de… …de…….

**ANEXO II**

**DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA**

El que suscribe, (nombre y apellido, representante legal o apoderado)……..con poder suficiente para este acta, DECLARA BAJO JURAMENTO que la oferta realizada por la firma (nombre y apellido o razón social)……CUIT N°…… no ha sido concertada con potenciales competidores, de conformidad con lo establecido por el artículo 16 de la Ley N° 2.095 (texto consolidado según Ley N° 6.764) y modificatorias.

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

……

Ciudad de Buenos Aires, ……...de…..……. de……..

## ANEXO III

## DECLARACIÓN JURADA DE INCOMPATIBILIDAD

El que suscribe, (nombre y apellido representante legal o apoderado)……..con poder suficiente para esta acta, DECLARA BAJO JURAMENTO que los representantes legales, miembros y/o accionistas de la firma (nombre y apellido o razón social)……..……...……..……., CUIT N°……..……, no mantienen ni han mantenido durante el último año relación de dependencia, o contractual, con el Poder Judicial de la Ciudad Autónoma de Buenos Aires.

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

…….

Ciudad de Buenos Aires,……...de…..……. de……..

**ANEXO IV**
**CERTIFICADO DE VISITA**

Por la presente, se deja constancia de que el/la Sr./Sra. _____ en su carácter de _____ de la empresa _____, ha efectuado la visita obligatoria según cláusula 15 del Pliego de Bases y Condiciones Particulares, a los edificios detallados a continuación:

| **SEDE** | **FECHA** | **FIRMA Y ACLARACIÓN AGENTE CERTIFICADOR** |
|---|---|---|
| Avda. Julio A. Roca 530 | / / | |
| Hipólito Yrigoyen 932 | / / | |
| Suipacha 150 | / / | |

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

# FIRMAS DIGITALES

**DIAZ Gaston Federico**
DIRECTOR
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES

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

# LICITACIÓN PÚBLICA N° 2-0014-LPU25

## PROVISIÓN Y PUESTA EN FUNCIONAMIENTO DE SOLUCIONES INFORMÁTICAS DE WAF Y DE VISIBILIDAD DE APIS

## PLIEGO DE ESPECIFICACIONES TÉCNICAS

## 1. GENERALIDADES

Las presentes especificaciones indican las prestaciones mínimas que deberá brindar el equipamiento ofrecido.

En la oferta deberá quedar expresamente establecido el grado de cumplimiento de cada uno de los puntos exigidos en el Pliego de Condiciones Particulares y del presente Pliego de Especificaciones Técnicas. Se hace saber que no se admitirá especificar simplemente "según pliego" o "cumple" como identificación de los bienes ofertados ni de los requisitos cuya acreditación se exigen en la presente contratación.

El adjudicatario deberá realizar cualquier tipo de trabajo que, aunque no esté debidamente aclarado en los Pliegos, sea necesario ejecutar para la correcta y completa terminación de la encomienda y para que ésta responda a sus fines y objetivos, considerándose esos trabajos incluidos en los precios de su oferta.

Cuando las tareas a realizar debieran ser unidas o pudieran afectar en cualquier forma obras existentes, los trabajos necesarios al efecto estarán a cargo de la adjudicataria y se considerarán comprendidos sin excepción en la propuesta.

El adjudicatario proveerá todo lo necesario, ya sean elementos de infraestructura, hardware o software, para la instalación y puesta en marcha del equipamiento, aun cuando no fueran especificados en el presente Pliego.

En el caso que un oferente crea conveniente ofertar una solución de prestaciones superiores, la misma deberá cumplir en un todo con estas Especificaciones Técnicas.

El oferente deberá detallar ampliamente el sistema y equipamiento ofertado para realizar las funciones requeridas en el presente Pliego.

La empresa proveerá e instalará todos los elementos correspondientes a lo solicitado de acuerdo a lo detallado en el presente Pliego, además de la provisión y ejecución de todos los recursos y/o tareas para el perfecto funcionamiento, correcta terminación y máximo rendimiento del equipamiento provisto.

## 2. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 1

El oferente deberá proveer el reemplazo por obsolescencia de la tecnología actual -F5 Web Application Firewall i4800, con todas sus licencias y suscripciones- por el presente

equipamiento -cuatro (4) equipos marca F5 modelo Web Application Firewall R4800-.

Será requisito para los renglones 1 y 2 que las tecnologías a proveer en la presente licitación sean de un único fabricante, por lo siguiente:

- Deberán trabajar en forma integrada nativamente
- El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.

## 2.1 Equipamiento a proveer

Se deberán proveer cuatro (4) equipos, a ser implementados dos (2) de ellos en cada uno de los Centros de cómputos que el Consejo de la Magistratura de la Ciudad de Buenos Aires defina, los que deberán contar con las siguientes características:

- La solución debe ser del tipo Appliance.
- Cada Appliance deberá contar con la posibilidad de incorporar los siguientes puertos de conectividad:
    - Cuatro (4) puertos de 10 Gb de cobre.
    - Cuatro (4) puertos de 1/10/25 Gb de Fibra.
    - Deberá tener un (1) puerto 10/100/1000 Ethernet de Management.
    - Deberá contar con un puerto consola.
    - Deberá contar con un puerto USB 3.0.
- Throughput: 50 Gbps L4 / 40 Gbps L7.
- Conexiones por segundo L4: 750.000.
- Requerimientos por segundo L7: 1.800.000.
- Requerimientos por segundo L4 HTTP: 3.500.000.
- Conexiones concurrentes, máximo 38.000.000 L4.
- Fuentes de Poder Redundantes.
- Compresión por hardware: 30 Gbps.
- Deberá contar con la capacidad de tener al menos cuatro (4) sistemas conviviendo en el mismo appliance (Multitenant).
- Debe soportar arquitectura de software de 64 bits.
- El storage deberá ser de al menos 480 GB SSD.
- La solución debe incluir mínimo 45.000 TPS para llaves de 2K SSL.

- La solución debe tener la capacidad de soportar al menos 25 Gbps de bulk encryption.
- Debe soportar clúster Activo/Activo entre dos o más plataformas, no necesariamente del mismo modelo.
- La configuración será sincronizada entre todos los dispositivos del grupo pudiendo optar si la sincronización se realiza de manera automática o manual.
- Adicionalmente al equipamiento provisto, y a su respectivo licenciamiento de WAF Avanzado, se deberá proveer el siguiente software:
    - Módulo de Balanceo Local para los cuatro appliances.
    - Suscripciones IP Intelligence y Threat Campaigns.

## 2.2 Módulo de Balanceo Local

- Debe de incluir funcionalidad de Cache, Rate Shaping, Gateway de IPV6 sin costo adicional.
- Deberá contar con la capacidad de agregar funcionalidades al equipo sin necesidad de apagarlo o intervenirlo físicamente.
- La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web
- La solución debe permitir la definición de dirección IP y. puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
- Deberá poseer soporte para métodos de balanceo de carga estático y dinámico, con garantía de mantenimiento de sesión entre sistemas redundantes.
- Deberá asegurar la continuidad, seguridad y rendimiento correcto al interceptar, inspeccionar, transformar, y dirigir las solicitudes de las aplicaciones y los servicios Web basándose en valores encontrados en cualquier punto del paquete o “Payload”.
- Deberá proveer redundancia y fiabilidad a cualquier nivel, desde la red a la aplicación para asegurar una alta disponibilidad.
- Debe ser tecnología Full-Proxy, es decir, las conexiones de los usuarios terminan completamente en la solución, y se establecen nuevas conexiones hacia el

backend (servidores). Esto con la finalidad de poder establecer nuevas conexiones hacia los servidores con direccionamiento privado (mayor seguridad), al igual que filtrar cualquier tipo de información confidencial en los paquetes salientes (CURP, RFC, Datos Personales, etc.). De la misma manera esta tecnología full-proxy deberá de permitir hacer persistencia de conexiones hacia la aplicación en base a cualquier información contenido en cualquier parte del paquete completo, esto para poder adaptarse a las necesidades de diferentes aplicaciones.

- La solución debe realizar el control de persistencia de las conexiones por:
    - Dirección IP origen.
    - Dirección IP destino.
    - Cookies.
    - Hash.
    - SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia.
    - Sesiones SSL.
    - Microsoft Remote Desktop.
- Debe permitir crear persistencia por cualquier valor del paquete por medio de reglas.
- Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
- La solución deberá soportar los siguientes métodos de balanceo de carga: Adaptive Response, Fastest Server Response, Least Connections, Weighted Least Connections, Round Robin, Hash Address, Predictive, Ratio, Priority Group Activation (Failback Server Group).
- Deberá contar con monitores predefinidos y personalizables que permiten comprobar y verificar la salud y disponibilidad de cada componente de la aplicación y la red y una Arquitectura abierta para una integración completa con las aplicaciones y los equipos terceros. Los monitores como mínimo serán: Health Monitor, Performance Monitor, Diameter, DNS, FTP, ICMP, http, HTTPS, IMAP, Inband, LDAP, MSSQL, MySQL, NNTP, Oracle, POP3, Postgres, Radius, Real Server, RCP, SASP, SIP, SMB, SMTP, SNMP, SOACP, TCP, UDP, WAP, WMI.
- Dichos monitores deberán poder realizar chequeos sobre:

  - Conexiones transparentes o reversas.
  - Tiempo.
  - Salud y Performance.
  - Direcciones.
  - Aplicaciones.
  - Contenidos.
  - Servicios.
  - Recursos.
  - Locaciones Virtuales.
- Deberá contar con políticas:
  - En modo draft.
  - Con capacidad de clonación.
  - Usar operadores lógicos para condiciones y reglas.
  - Reusar los nodos y servicios en otras políticas.
- Deberá contar con perfiles de servicios para http que:
  - Trabajen en modo proxy explícito (DNS Resolver, Route Domain, Tunnel Name, Host Name, DNS Lookup Failed Message, Bad Request / Response Message).
  - Cuenten con seteos como:
    - Rewriting de redirecciones http.
    - Análisis de Header.
    - Seteo de aseguramiento sobre header.
- Deberá contar con perfiles de servicio de compresión http que:
  - Haga compresión de UR y Contenido.
  - Determine un mínimo tamaño de contenido para comprimir.
  - Cuente con un buffer.
- Deberá contar con otros perfiles de servicio a nivel protocolo como ser TCP, UDP, SCTP, IP, SSL, Authentication, Message Routing.
- Deberá contar con otros perfiles de servicio L7 como ser FTP, DNS, RTSP, ICAP, Radius, SMTP, SMTPS, Client nad Server LDAP, iSession, Rewrite, XMLS, HTTP2, SOCKS, FIX, GTP, Websocket, IPSec, Video Quality.

- La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
    - Ping.
    - Chequeo a nivel de TCP y UDP a puertos específicos.
    - Monitoreo http y https.
    - Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.
    - Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
    - Ejecución de scripts para determinar la respuesta emulando un cliente.
    - Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
    - Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma.
    - Monitoreo de aplicaciones de mercado:
        - LDAP.
        - FTP.
        - SMTP.
        - IMAP/POP3.
        - Oracle.
        - MSSQL.
        - MySQL.
        - RADIUS.
        - SIP.
        - Protocolo SASP.
        - SOAP.
        - WMI.
        - SNMP.

- La solución deberá permitir el balanceo de los siguientes protocolos haciendo una comprensión del contenido: HTTP (proxy con opciones limitadas para aumentar la performance, SCTP, Diameter / LDAP basado en mensajes en vez de conexiones, FTP, Tráfico IP que no sea TCP o UDP, Radius, RDP.
- La solución deberá soportar la capacidad de modificar, insertar o borrar encabezados de http y todo el paquete de datos (payload) en los request del cliente y las respuestas del server.
- La solución deberá soportar la capacidad de modificar, insertar o borrar encabezados y todo el paquete de datos (payload) en paquetes que no sean http.
- Deberá soportar certificados SSL de 4096 bits.
- La solución deberá contar con las siguientes características de compresión para alivianar el procesamiento de los servidores: Compresión diferenciada para tráfico JavaScript, Soportar al menos los métodos GZIP y Deflate, Seleccionar automáticamente el mejor algoritmo de compresión y la configuración adecuada dependiendo del tipo de tráfico.
- Deberá realizar cache de contenido HTTP en la memoria RAM del dispositivo para alivianar la carga de los servidores WEB.
- La solución deberá soportar la lectura, marcado y preservación de los tags de prioridad 802.1q.
- Deberá permitir la priorización del tráfico basado en criterios definidos por el administrador.
- Deberá soportar las siguientes características respecto del TOS (RFC 791) y DSCP (RFC 2475): Habilidad de especificar el valor basado en las políticas del dispositivo, Especificar que el sistema no modificará el valor del paquete, Especificar que el sistema defina el valor del paquete de salida al mismo valor que el paquete de entrada más reciente.
- La solución deberá re direccionar la petición en caso que todos los servidores del pool estén caídos.
- La administración de la solución debe ser basada en roles, donde dependiendo del rol se definen las acciones que el usuario puede hacer sobre la solución.
- La solución deberá autenticar los usuarios administrativos con los siguientes sistemas externos: LDAP, Kerberos, Active Directory, NTLM.

- Deberá permitir la creación de contenedores de objetos de configuración y asignar permisos de visualización, lectura y modificación a usuarios administrativos a esos contenedores.
- La solución de administración deberá permitir, como mínimo, lo siguiente:
    - Agregar, eliminar o modificar la configuración en un entorno gráfico.
    - Modificar las reglas de la solución, efectuar la configuración de los componentes de la solución.
    - Visualizar los registros de auditoría, eventos de balanceo y eventos de sistema.
- Deberá poder bloquear un usuario administrativo luego de una cierta cantidad de días sin uso.
- Debe proveer herramientas de logueo y monitoreo de estadísticas del sistema, las cuales deberán brindar información en tiempo real (del estado actual) como así también reportes históricos de como mínimo las siguientes estadísticas del sistema: Uso de CPU o de los CPUs para el manager y para los dispositivos gestionados por cada aplicación, Uso de memoria RAM por aplicación, Paquetes enviados y recibidos por interfaz física, Errores de transmisión y recepción por interfaz física, Ancho de banda utilizado por cada dispositivo gestionado, Ancho de banda utilizado para transmisión por cada interfaz.
- Deberá generar logs de auditoría por lo menos para los siguientes eventos: Login/Logout, Modificación de configuración, Aplicar los cambios de la configuración, Actividad del usuario, Modificación de Privilegios, Búsqueda o actualización de la base de datos, Modificación de la fecha.
- Soporte VLANs IEEE 802.1Q. Soporte de los 4096 ID VLANs IEEE 802.1Q
- La solución deberá sincronizar las conexiones entre ambos miembros del clúster.
- Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:
    - Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser

accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.
    - Soporte de API REST.
- La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:
    - Memoria cache.
    - Compresión tráfico HTTP.
    - Optimización de conexiones a la aplicación a nivel TCP.
    - Multiplexación de streams http.
- La solución debe contar con las siguientes características de Compresión de tráfico:
    - El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
- Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.
- Debe contar con la capacidad de inspeccionar tráfico SSL para bloquear tráfico malicioso y aceptar tráfico adecuado.
- Debe contar con funcionalidades para mejorar la performance al menos 2x en el usuario final sin cambiar nada en servidores, aplicaciones.
- Debe contar con funcionalidades de control de las aplicaciones mediante mecanismos de programación Node.js, los cuales permitirán extender el control de tráfico, la comunicación y la gestión de la disponibilidad.
- Deberá contar con templates predefinidos para aplicaciones, los cuales harán más sencillo el despliegue, gestión y visibilidad de las aplicaciones a balancear.
- Deberá incluir al menos los siguientes templates para las marcas / productos:
    - Adobe (Acrobat, Flash, Indesing).
    - Apache HTTP Server, Tomcat.
    - CA Siteminder.
    - Citrix XenApp, XenDesktop.
    - Cloud Connector.
    - Diameter Traffic Management.

- DNS Traffic Management.
- HTTP Applications.
- IBM Cognos, InfoSphere Guardim, Lotus, QRadar, Tivoli Maximo, Security Access Manager, Websphere.
- LDAP Traffic Management.
- Microsoft ADFS, AppV, Dynamics Exchange, FAST, IIS, Lync Server, Office 365, Office Web Apps, Remote Desktop, Sharepoint, Skype for Business, Virtualization.
- Nagios.
- Oracle Access Manager, Application Server, Database Firewall, E-Business Suite, Fusion Middleware, Hyperion, JD Edwards, PeopleSoft, Siebel, Weblogic.
- Radius traffic management.
- SAP Netweaver Enterprise Portal, ERP.
- SMTP Servers.
- SSL Intercept.
- VmWare Horizon, Site Recovery, Zimbra.

## 2.3 Módulo de Firewall de Aplicaciones WEB Avanzado (AWAF)

- La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).
- La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.
- Debe trabajar en un esquema proxy TCP reverso y/o transparente
- El WAF debe poder construir automáticamente políticas basadas en el tráfico detectado.
- Debe trabajar con políticas de seguridad por capas, donde se configura una política de seguridad base y las políticas de seguridad hijas heredan sus

configuraciones y permita que solo cambios específicos se apliquen a las políticas hijas.

- La creación automática de políticas deberá unificar múltiples URLs explicitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.
- Debe trabajar en modo de bloqueo o en modo informativo.
- Debe permitir diferentes políticas de seguridad para diferentes aplicaciones.
- WAF debe tener la capacidad de importar archivos de diccionario OpenAPI 3.0 (Swagger) para crear una política de protección de API automáticamente ajustada a su contenido. (Métodos, URL, Variables, etc.)
- El WAF debe tener la capacidad de realizar la firma antes de la implementación final. Durante el período de estadificación, los eventos falsos positivos se pueden administrar y ajustar para que coincidan con los datos de la aplicación del mundo real.
- El WAF debe tener la capacidad de retroceder a otro host en caso de que la aplicación protegida no esté disponible o devuelva códigos de error HTTP.
- El WAF debe tener la capacidad de multiplexación de nivel TCP para reducir la cantidad de conexiones L4 a servidores backend.
- WAF deberá filtrar los DDoS de nivel de aplicación antes de procesar sus políticas HTTP. La protección DDoS debe medir el estrés de la aplicación para una detección precisa.
- El WAF debe tener la capacidad de crear scripts de plano de datos (evento de tráfico) y plano de control (evento de gestión) para manejar eventos únicos que suceden en el entorno.
- El WAF debe tener la capacidad de detectar automáticamente el software utilizado en el backend para definir los conjuntos de firmas necesarios para la política WAF definida.
- Cada tipo de violación de WAF debe tener una configuración para activar la acción de Registro, Alarma o Bloquear o cualquier combinación de ellos.
- Para el modo de aprendizaje automático, las sugerencias deben aceptarse automáticamente en función de la probabilidad.
- El WAF debería tener soporte para el descifrado TLS 1.3.

- El WAF debe tener la capacidad de agregar cookies para la persistencia del equilibrio de carga.
- El WAF debe tener la capacidad de devolver el tráfico en modo proxy inverso a su puerto de origen y dirección MAC incluso si no se especifica una entrada de enrutamiento.
- WAF debe tener contextos administrativos con su propia configuración y diferentes usuarios permitidos para administrar estos contextos. De modo que varios grupos de administradores pueden trabajar con un sistema sin influencia en la configuración de los demás.
- Debe permitir la creación de firmas personalizadas.
- Debe trabajar con modelos de seguridad positiva y negativa.
- La solución debe tener la posibilidad de automatizar la creación de políticas de WAF desde los pipelines de desarrollo, a través de esquemas basados en modelos declarativos (archivos con sintaxis json). Esto podría hacerse desde herramientas como Jenkins, GitLab, postman, curl, ansible, terraform, cuya política de seguridad, se encuentre bajo dicho formato se mantenga en un repositorio u origen confiable privado, o público (github, por ejemplo).
- El WAF debe entregar una puntuación de riesgo de la violación recibida.
- Debe tener la capacidad de crear, modificar y eliminar políticas de WAF mediante API Rest.
- Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana.
- El WAF debe poder admitir la aplicación de políticas de seguridad para aplicaciones escritas en Google Web Toolkit (GWT).
- El WAF debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500 o responder con payloads JSON.
- El WAF debe permitir personalizar las páginas de bloqueo.
- El WAF debe admitir las siguientes técnicas de detección evasiva:
    - Decodificación de URL.
    - Terminación de cadena de bytes nulos.
    - Rutas de autorreferencia (es decir, uso de /./ y equivalentes codificados).

  - Referencias de ruta (es decir, uso de /./ y equivalentes codificados).
  - Caso mixto.
  - Uso excesivo de espacios en blanco.
  - Eliminación de comentarios (por ejemplo, convertir BORRAR / ** / DE a BORRAR DE).
  - Conversión de caracteres de barra invertida (compatibles con Windows) en caracteres de barra diagonal.
  - Conversión de codificación Unicode específica de IIS (% uXXYY).
  - Decodifique las entidades HTML (por ejemplo, c, & quot ;, & # xAA;).
  - Caracteres escapados (por ejemplo, \ t, \ 001, \ xAA, \ uAABB).
- El WAF debe proporcionar seguimiento de sesión con capacidades mejoradas de generación de informes y cumplimiento que toman en cuenta las sesiones de usuario HTTP y los nombres de usuario dentro de la aplicación. Esto le brinda al administrador más información sobre actividades sospechosas de la aplicación (por ejemplo, quién fue el usuario detrás de un ataque) y más flexibilidad para aplicar la política de seguridad (como impedir que un determinado usuario use la aplicación). Se puede configurar si el sistema realiza un seguimiento de las sesiones según el nombre de usuario, la dirección IP o el número de identificación de la sesión.
- Debe prevenir exponer el “OS fingerprinting”.
- Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.
- El WAF Debe soportar:
  - Restringir protocolo y versión utilizada.
  - Multi-byte language encoding.
  - Validar URL-encoded characters.
  - Restringir la longitud del método de request.
  - Restringir la longitud del URI solicitado.
  - Restringir el número de Encabezados (headers).
  - Restringir la longitud del nombre de los encabezados.
  - Restringir la longitud del valor de los encabezados.

  - Restringir la longitud del cuerpo (body) de la solicitud.
  - Restringir la longitud del nombre y el valor de las cookies.
  - Restringir el número de cookies.
  - Restringir la longitud del nombre y valor de los parámetros.
  - Restringir el número de parámetros.
- El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL).
- El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP, y presentar un dashboard de cumplimiento para cada una de las políticas creadas en la solución.
- El WAF debe incluir protección contra Web Scraping.
- Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario.
- Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento cross-domain, permitiendo evitar un CORS (Cross-Origin Resource Sharing).
- Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario.
- Debe permitir el enmascaramiento de información sensible filtrada por el servidor.
- Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.
- Debe permitir la integración con servidores Antivirus por medio del protocolo ICAP.
- Debe brindar reportes respecto a la normativa PCI DSS 2.0.
- Debe integrarse con Firewall de Base de Datos:
  - Oracle Database Firewall.
  - IBM InfoSphere Guardium.
- Debe proteger contra ataque DoS /DDoS de Capa 7.
- Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa.

- En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.
- Debe soportar tecnologías AJAX y JSON.
- Debe proteger como mínimo:
    - Ataques de Fuerza Bruta.
    - Entrada no validada.
    - Defectos de inyección OS.
    - Ataques de inyección NoSQL.
    - Cross-site scripting (XSS).
    - Cross Site Request Forgery.
    - SQL injection.
    - Parameter and HPP tampering.
    - Sensitive information leakage.
    - Session highjacking.
    - Buffer overflows.
    - Cookie manipulation.
    - Various encoding attacks.
    - Broken access control.
    - Forceful browsing.
    - Hidden fields manipulation.
    - Request smuggling.
    - XML bombs/DoS.
- Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.
- Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP.
- Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas.
- Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.
- Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.
- Debe ofrecer protección sobre tráfico basado en WebSockets.

- El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.
- Debe proteger las aplicaciones contra ataques de denegación de servicio a nivel L7.
- El WAF debe poder perfilar dinámicamente el tráfico y crear firmas de patrones de tráfico anómalos, deteniendo los ataques DoS de la capa 7 antes de que afecten a su aplicación, incluidos los ataques "Día Cero".
- EL WAF debe permitir utilizar protección avanzada de credenciales en formularios de la aplicación web, haciendo cifrado de la data entrada en formularios. Este cifrado se debe realizar usando un esquema de llave publica/privada. Este cifrado debe ser en tiempo real y no requerir modificaciones en la aplicación del lado del servidor o de la instalación de agentes en el servidor.
- Deberá de contar con una protección automática contra ataques DDoS, que analice el comportamiento de tráfico, usando técnicas como "Machine learning" y el análisis de datos.
- EL WAF debe realizar ofuscación de contenido HTTP, en particular de los nombres de cualquier parámetro dentro de la aplicación. Esta ofuscación de parámetros debe realizarse constantemente y los parámetros deben cambiar de nombre varias veces por minuto para evitar que estos parámetros sean objeto de ataques dirigidos.
- Deberá de monitorear constantemente la salud del servicio y su carga de trabajo, con el objetivo de validar las condiciones del servidor protegido, ataques y mitigaciones.
- El WAF debe prevenir contra keyloggers sobre el browser, evitando revelar los datos escritos sobre parámetros de la aplicación Web, bien sea cifrándolos o inyectando contenido “basura” en estos parámetros.
- La protección con base a comportamiento de tráfico deberá trabajar de la siguiente manera:
    - Aprender el comportamiento del tráfico normal.
    - Detectar el ataque basado en las condiciones actuales (salud del servidor).
    - Encontrar una anomalía en el comportamiento.
    - Mitigar, ralentizando a los clientes sospechosos.

- El WAF debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.
    - Scanners.
    - Exploits Windows.
    - Denial of Service.
    - Proxies de Phishing.
    - Botnets.
    - Proxies anónimos.
- Deberá de contar con los siguientes métodos de mitigación:
    - JavaScript challenge.
    - CAPTCHA challenge.
    - Request Blocking.
- El WAF debe soportar WebHook notifications, notificando a servicios de Continuous Integrations / Continuous Delivery (CI/CD) cuando hay cambios en la política o Eventos de Seguridad.
- Debe contar con soporte y Protección ante ataques a GraphQL:
    - GraphQL Content Profile and Policy Template.
    - Support JSON Content Type (POST).
    - Attack Signatures on GraphQL Traffic.
    - Query Depth Enforcement.
    - Introspection Query Enforcement.
    - Support GarphQL Batching.
    - Policy tunning with GraphQL violations.
    - DataGuard Support (sensitive data protection).
    - L7 Volumetric Behavioral DoS Protection Support.
- El WAF deberá contar con la posibilidad de mitigar ataques generados por BOTNETS o por Bots los cuales intentan suplantar el comportamiento de los usuarios, así mismo este deberá proveer la detección y el bloqueo de amenazas automatizadas a nivel de sesión.
- El WAF deberá contar con Soporte de API´s declarativa con capacidad de:
    - Autenticación Básica de referencias externas

  - Utilizar referencias externas para plantillas base,
  - Exportar políticas en formato declarativo JSON
- El WAF debe tener un mecanismo de reversión de políticas.
- El WAF debe ser extensible con una licencia complementaria para proporcionar la autenticación de API y admitir oAuth 2.0, permitiendo la importación de archivos swagger para la construcción de la política de protección (ya sea para las funcionalidades de autenticación, autorización de acceso, como también para la construcción de la política de WAF).
- Debe tener la capacidad de exportar e importar las políticas de WAF en formato XML y JSON.
- El WAF debe poder proporcionar listas blancas de direcciones IP unificadas para las direcciones IP de confianza de Policy Builder y listas blancas de anomalías (Prevención de ataques DoS, Prevención de ataques de fuerza bruta y Detección de web scraping) en una sola lista.
- La funcionalidad de protección contra ataques DDoS para aplicaciones debe incluir protección basada en comportamientos (Behavioral).

## 2.4 Implementación y Puesta en Funcionamiento

El adjudicatario deberá realizar la implementación y migración de la solución propuesta en modalidad “llave en mano”, por lo que se deberán proveer todos los elementos necesarios, realizar la instalación en sitio, puesta en marcha y configuración de acuerdo con las necesidades establecidas por el Consejo de la Magistratura de la C.A.B.A. La tecnología provista deberá implementarse utilizando la última actualización de software disponible por el fabricante.

La implementación deberá realizarse de acuerdo con las buenas prácticas recomendadas por el fabricante de la tecnología.

Los oferentes en su oferta deberán incluir un Plan de Implementación de toda la infraestructura requerida. Dicho Plan deberá contar con un esquema de trabajo enfocado en fechas, el cual no deberá superar los noventa (90) días corridos posteriores al perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

Las tareas deberán incluir:

- La instalación de la solución en un entorno de Pre-Producción.
- Pruebas y ajustes de la instalación.
- Pasaje a producción.
- Período de marcha blanca.

## 3. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 2

- La solución provista debe contar con una arquitectura virtual On Premise con soporte para el análisis de tráfico para la visibilidad de APIs.
- La solución debe brindar una consola en nube que se integre con la arquitectura virtual en premisas para una visión unificada del análisis de tráfico.
- La solución debe ser del mismo fabricante de la tecnología del Renglón 1 e integrarse de forma nativa con esta.
- La solución debe ser provista únicamente para el centro de datos primario y debe contar con capacidad de crecimiento para el centro de datos secundarios mediante la adición de nuevas máquinas virtuales con su respectivo licenciamiento.
- La solución deberá proporcionar una consola central SaaS para la administración centralizada de las configuraciones de red y seguridad, así como también acceso a herramientas de troubleshooting y dashboards donde se visualice la disponibilidad, estadísticas y el estado de los servicios/APIs.
- Debe permitir que la gestión se realice mediante clickops, API requests, Terraform o integrándose al pipeline CI/CD del Consejo de la Magistratura de la C.A.B.A.
- La solución de visibilidad de APIs basada en SaaS propuesta debe admitir cuentas de usuario de administración ilimitadas con RBAC.
- La solución de visibilidad de APIs propuesta debe admitir SSO para la gestión de acceso mediante OKTA, Google y Azure AD.
- La consola de administración de SaaS debe ser compatible con la autenticación multifactor.
- La solución deberá proporcionar al usuario del gestor centralizado la posibilidad de administrar sus servicios dentro de una consola unificada y donde se permita la colaboración de distintos equipos (SecOps, DevOps, entre otros).
- La solución de Visibilidad de APIs deberá ser full RESTful-API o API first:

  - Debe permitir realizar todas las configuraciones a través de su API, así como también, la petición de información de los dashboards.
  - Debe estar bien documentada y proveer de las configuraciones en JSON y YAML de cualquiera de los objetos que se definan.
  - Debe permitir la creación de credenciales por usuario, el uso de API token, certificados, así como la creación de usuarios API con RBAC.
- La plataforma de visibilidad de APIs SaaS debe permitir obtener el software del mismo fabricante para su instalación en cualquier ubicación del borde que prefiera sin restricciones. La instalación del software debe poder implementarse en cualquier de las siguientes opciones:
  - Implementación baremetal en hardware propietario del mismo proveedor.
  - Implementación baremetal en un servidor COTS certificado, con opción de certificar hardware si no figura en la lista del proveedor.
  - Implementación de máquinas virtuales en hipervisor (VMWare, KVM).
  - Implementación de máquinas virtuales en la nube pública (AWS, GCP, Azure).
  - Implementación de pods de contenedor en Kubernetes.
- La solución ofrecida por la plataforma SaaS debe permitir la exposición de la aplicación en cualquiera de los siguientes entornos:
  - Exposición en internet público.
  - Exposición a todas o a un conjunto de ubicaciones a través de la red interna.
- La plataforma de visibilidad de APIs SaaS debe poder conectar todos los modos y ubicaciones de implementación a la red troncal global de la nube del proveedor, creando una experiencia de nube distribuida única.
- La plataforma de visibilidad de APIs SaaS debe poder gestionar todos los modos y ubicaciones de implementación en una única consola y panel de control.
- La plataforma de visibilidad de APIs SaaS debe ser compatible con la implementación en premisas bajo un esquema de clúster de alta disponibilidad (HA).

- La plataforma SaaS debe ser compatible con un panel de Performance y seguridad.
- La solución SaaS deberá proporcionar visibilidad acerca de:
    - Salud de la aplicación.
    - Alertas activas.
    - Origin Servers/Backends.
    - Latencia de fin a fin.
    - Visitantes únicos.
    - Tipo de dispositivo.
    - Peticiones (Request Rate, Total Request, Error rate, total errors, drop rate, drop count).
    - Throughput.
    - ASN.
    - TLS Fingerprint.
    - TLS Ciphers y protocolos.
    - Códigos de error de HTTP.
    - Localización de clientes.
    - Top URLs.
- La solución deberá proporcionar integración con herramientas de logging de terceros.
- La sección de Performance también debe permitir el análisis detallado de cada request registrao a y realizar un seguimiento de las atribuciones de L3 a L7, así como verificar la latencia de extremo a extremo de los request registrados.
- La plataforma SaaS deberá proporcionar visibilidad sobre los cambios de configuración realizados por los usuarios del gestor centralizado durante un periodo de tiempo de 30 días.
- El sistema debe informar sobre alertas detalladas y errores en el procesamiento del servidor de origen o fallos en la sonda de estado.
- La solución deberá tener la capacidad de monitorear las APIs tan cerca del origen como sea posible. Además, la solución debe brindar esta capacidad utilizando el

mismo motor de protección tanto en la nube propia, como en nubes públicas/privados y en las premisas.

- La solución deberá contar con un mecanismo de análisis de comportamiento de las peticiones/request hacia cualquier de los API endpoints definidos, permitiendo la detección de anomalías por petición/request.
- La solución deberá contar con la capacidad de aprender/determinar todos los API endpoints que son accedidos, incluyendo petición y respuesta, y detectando información sensible. Además, debe proveer la vista de API endpoints en inventario, shadow y descubiertas y generar un Probability Distribution Function (PDF) para las métricas relacionadas a cada endpoint. Dicho análisis debe ser generado de forma periódica, y los PDFs ser actualizados de acuerdo con eso.
- La solución deberá contar con la capacidad de identificar y localizar la información sensible en las peticiones desde los clientes y en las respuestas de los API endpoints. Deberá identificar PII, tal como números de tarjeta de crédito e indicar el parámetro/campo donde la información está localizada.
- La solución deberá contar con un mecanismo que permita el descubrimiento dinámico de las APIs, determinar cuáles endpoints deberían ser utilizados y permitir únicamente estos API endpoints, obtener información de la utilización, como tamaño de las peticiones y frecuencia. Asimismo, la solución deberá proporcionar las siguientes métricas:
    - tamaño de la petición/respuesta.
    - latencia con datos y latencia sin datos.
    - frecuencia de peticiones.
    - frecuencia de errores.
    - troughput de las respuestas.
- La solución deberá aprender la estructura del esquema de las APIs, analizando los requests/peticiones y respuestas para cada una de ellas. Asimismo, deberá permitir la descarga del swagger file aprendido.
- La solución deberá permitir la importación de las especificaciones del API contenidas en un archivo Swagger.

- La solución debe contener sensores integrados para la detección de tipos de autenticación, y localización en las llamadas API. Una vez detectados, se deben asociar con un endpoint y mostrar un estado de autenticación.
- La solución deberá ser capaz de descubrir el header, payload y firma de JWTs así como la identificación de campos útiles para el cliente, permitiendo la identificación de datos sensibles en los payloads de JWT así como la definición del score de riesgo.
- La solución debe disponer de una función de descubrimiento de API que lea e identifique los API endpoints en el repositorio de código.
- La solución debe tener una función de descubrimiento de API que lea e identifique los endpoints de API de dominios externos.

**Implementación y Puesta en Funcionamiento:**

El adjudicatario deberá realizar la implementación y migración de la solución propuesta en modalidad "llave en mano", por lo que se deberán proveer todos los elementos necesarios, realizar la instalación en sitio, puesta en marcha y configuración de acuerdo con las necesidades establecidas por el Consejo de la Magistratura de la C.A.B.A. La tecnología provista deberá implementarse utilizando la última actualización de software disponible por el fabricante.

La implementación deberá realizarse de acuerdo con las buenas prácticas recomendadas por el fabricante de la tecnología.

Los oferentes en su oferta deberán incluir un Plan de Implementación de toda la infraestructura requerida. Dicho Plan deberá contar con un esquema de trabajo enfocado en fechas, el cual no deberá superar los noventa (90) días corridos posteriores al perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

Las tareas deberán incluir:

- La instalación de la solución en un entorno de Pre-Producción.
- Pruebas y ajustes de la instalación.
- Pasaje a producción.
- Período de marcha blanca.

## 4. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 3

El oferente deberá brindar por el período de treinta y seis (36) meses los servicios de soporte técnico local y del fabricante, mantenimiento proactivo y resolución de incidentes, según los requerimientos técnicos especificados en el presente documento, en un formato 7x24.

Los servicios descritos a continuación deben ser por el período de treinta y seis (36) meses:

- Los servicios ofrecidos deben incluir un soporte técnico local en modalidad 7x24x365 para la resolución de incidencias técnicas.
- El soporte técnico local debe ser brindado con personal especializado propio del adjudicatario.
- Se debe contemplar el servicio de soporte técnico del fabricante en modalidad 7x24x365 para el escalamiento de incidencias técnicas.
- El servicio de soporte técnico debe incluir el mantenimiento proactivo de la solución de forma tal de prevenir incidentes, asegurar el cumplimiento de las buenas prácticas del fabricante y optimizar el rendimiento de la tecnología.
- La movilización del personal o cualquier costo asociado que surgiera del servicio de soporte técnico a prestar correrá por exclusiva cuenta del adjudicatario para cada vez que se requiera.
- Los requerimientos de soporte técnico se podrán efectuar telefónicamente, por correo electrónico o vía web.
- Deberán considerarse incluidos dentro del servicio, la aplicación de parches, actualizaciones de software, etc. con el fin de mantener el estado de software de los dispositivos al día con su última actualización disponible por parte del fabricante.
- No deberá existir un límite en el número de casos de soporte que puede solicitar el Consejo de la Magistratura de la Ciudad de Buenos Aires.
- El servicio deberá contemplar el reemplazo parcial o total (RMA) de componentes de la solución que presenten fallas sin incurrir en gastos adicionales por parte del Consejo de la Magistratura de la C.A.B.A.

- El Oferente en su propuesta deberá tener presente que a lo largo de la vigencia del contrato deberá a su vez cumplir con los siguientes requisitos:
    - Deberá incluir un servicio de garantía y soporte técnico por un plazo de treinta y seis (36) meses. El oferente deberá explicar el alcance y detalle del mismo cubriendo software y hardware.
    - Deberá incluir dos (2) recursos full time con nivel SemiSenior, dedicados a la gestión de las soluciones ofertadas por el lapso del contrato, pudiendo trabajar en forma remota sobre la plataforma del Consejo de la Magistratura de la C.A.B.A.

## 5. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 4

El adjudicatario deberá brindar el servicio de capacitación oficial de todas las nuevas soluciones a proveer, específicamente del Renglón 2, que deberán contar al menos con las siguientes características:

- Cada una de las capacitaciones deberá ser brindada por el fabricante de la solución, en un esquema de horario laboral de 9 a 18 horas, de lunes a viernes, coordinando la ejecución de las mismas con el Consejo de la Magistratura de la C.A.B.A.
- La duración de las capacitaciones para cada una de las soluciones deberá contar con un mínimo de doce (12) horas.
- El Consejo de la Magistratura de la C.A.B.A. requerirá la participación de al menos cuatro (4) agentes de la Dirección General de Informática y Tecnología en dichas capacitaciones, las cuales deberán contar con partes teóricas y prácticas con el objetivo de conocer en forma pormenorizada la solución a gestionar.
- Si bien las capacitaciones pueden ser brindadas en forma virtual (mediante soluciones de colaboración tales como Zoom, Microsoft Teams, Google Meets, etc.), en caso de ser presenciales, las mismas deberán ser dictadas en la C.A.B.A.
- El oferente brindará un certificado de asistencia a las capacitaciones a cada uno de los agentes que participen en las mismas.
- El adjudicatario deberá brindar los elementos necesarios para el aprendizaje (manuales, acceso a plataformas web) a cada uno de los agentes participantes del Consejo de la Magistratura de la C.A.B.A.

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

# FIRMAS DIGITALES

**DIAZ Gaston Federico**
DIRECTOR
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES