RESO SAGYP N° 552/24

Buenos Aires, 1 de noviembre del 2024

VISTO:

El TAE A-01-00027811-0/2024 caratulado *"D.G.C.C. S/ PROVISIÓN DE SOLUCIONES DE PREVENCION Y DEPURACIÓN DE DDOS"*

CONSIDERANDO:

Que por la actuación citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, por la provisión e implementación, soporte técnico, mantenimiento y garantía de soluciones informáticas de prevención y depuración de DDoS para el Poder Judicial de la Ciudad Autónoma de Buenos Aires. En tal sentido, la mentada Direccion propuso cláusulas para incorporar los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas (v. Nota DGIYT Nº 827/24 y Adjuntos 133359/24 y 133360/24).

Que, en ese marco, la Dirección General de Compras y Contrataciones entendió viable el llamado a Licitación Pública, de etapa única, bajo la modalidad de llave en mano, conforme lo dispuesto en los artículos 26, 28, 32, 33, 40, 45 y concordantes de la Ley Nº 2.095 (texto consolidado según Ley Nº 6.588), la Resolución CM Nº 276/2020 y la Resolución SAGyP N° 30/2021 (v. Adjunto 147653/24).

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 158554/24 y 158526/24 y estableció como presupuesto oficial la suma de dólares estadounidenses tres millones cuatrocientos mil (U$S 3.400.000.-). Asimismo, elevó lo actuado a esta Secretaría y recomendó que *"la adquisición de los Pliegos correspondientes proceda mediante el pago de la suma de Pesos Cuatrocientos Mil ($ 400.000.-), para participar en la*

Licitación Pública N° 2-0039-LPU24." (v. MDGCC 2041/24).

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

Que 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, vinculados como Adjuntos 158554/24 y 158526/24 , y llamar a Licitación Pública N° 2-0039-LPU24, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la provisión e implementación, soporte técnico, mantenimiento y garantía de soluciones informáticas de prevención y depuración de DDoS para el Poder Judicial de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses tres millones cuatrocientos mil (U$S 3.400.000.-), para el día 15 de noviembre de 2024 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° 2-0039-LPU24, y realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.588), su reglamentación y en la Ley de Procedimientos Administrativos -Decreto 1.510/97- (texto consolidado según Ley N° 6.588).

Que en cumplimiento de la Ley N° 70 (texto consolidado según Ley N° 6.588), la Dirección General de Programación y Administración Contable tomó conocimiento y realizó la

afectación y el compromiso presupuestario correspondiente para hacer frente la contratación de marras (v. Adjuntos 156499/24 y 156501/24)

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 13323/2024.

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

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, las cuales obran vinculados como Adjuntos 158554/24 y 158526/24, y forman parte de la presente Resolución, que regirán Licitación Pública N° 2-0039-LPU24, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la provisión e implementación, soporte técnico, mantenimiento y garantía de soluciones informáticas de prevención y depuración de DDoS para el Poder Judicial de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses tres millones cuatrocientos mil (U$S 3.400.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0039-LPU24, de etapa única, fijándose como fecha límite para la presentación de ofertas y la apertura pública de ofertas para el día 15 de noviembre de 2024 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° 2-0039-LPU24, será por un monto de pesos cuatrocientos mil ($ 400.000.-).

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0039-LPU24, a los Dres. Hernán Labate y Adrián Costantino como miembros titulares, y al Dr. Matías Vázquez y la Dra. Javiera Graziano 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° 2-0039-LPU24, 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° 6.588) su reglamentaria Resolución CM N° 276/2020 y en la Ley de Procedimientos Administrativos - Decreto 1.510/97- (texto consolidado según Ley N° 6.588).

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 los titulares de la Dirección General de Informática y Tecnología y de 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

FERRERO Genoveva Maria
SEC DE ADMIN GRAL Y PRESU DEL P JUD CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES

LICITACION PÚBLICA N° 2-0039-LPU24

PROVISIÓN DE SOLUCIONES DE PREVENCIÓN Y DEPURACIÓN DE DDOS

PLIEGO DE BASES Y CONDICIONES PARTICULARES

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 pública de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la provisión e implementación, soporte técnico, mantenimiento y garantía de soluciones informáticas de prevención y depuración de DDoS para el Poder Judicial 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 Tres Millones Cuatrocientos Mil (U$S 3.400.000.-)**, el cual se compone de la siguiente manera:

Renglón 1: Dólares Estadounidenses Un Millón Cien Mil (U$S 1.100.000,00).

Renglón 2: Dólares Estadounidenses Seiscientos Mil (U$S 600.000,00).

Renglón 3: Dólares Estadounidenses Cuarenta Mil (U$S 40.000,00).

Renglón 4: Dólares Estadounidenses un Millón Seiscientos Sesenta Mil (U$S 1.660.000,00).

4. RENGLONES A COTIZAR

Renglón 1: Provisión de una solución “on premise” de prevención de DDoS, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Provisión de una solución de depuración de DDoS en la nube, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 3: Provisión de servicios de implementación para 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 servicios de soporte técnico, mantenimiento y actualización tecnológica de 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.

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 Cuatrocientos Mil ($ 400.000.-)** 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 de la Contratación

La presente contratación tendrá un plazo máximo de vigencia de treinta y ocho (38) meses, contados a partir del perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

6.2 Plazo de Ejecución Renglones 1, 2 y 3

El adjudicatario deberá efectuar la provisión e implementación de las soluciones requeridas dentro de los sesenta (60) 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 provistas tendrán una vigencia de treinta y seis (36) meses, contados a partir del Parte de Recepción Definitiva del Punto 6.2.

6.4 Plazo de Ejecución del Renglón 4

Los servicios solicitados tendrán un plazo de treinta y seis (36) meses, contados a partir del Parte de Recepción Definitiva del Punto 6.2.

El plazo aludido podrá ser prorrogado en las mismas condiciones, a exclusivo juicio de este Consejo de la Magistratura, por un período igual o menor del contrato inicial, en los términos del artículo 111 de la Ley N° 2.095 (texto consolidado por Ley N° 6.588).

7. MODALIDAD DE LA CONTRATACIÓN

La contratación de lo requerido en el presente Pliego se efectúa bajo la modalidad llave en mano, de conformidad con lo dispuesto por el artículo 45 de la Ley N° 2.095 -según texto consolidado por Ley N° 6.588- 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 solicitado, de manera que los oferentes deberán cotizar una solución integral que satisfaga las necesidades del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

La solución propuesta deberá incluir todos los bienes, servicios y componentes solicitados y cumplir con los demás requerimientos técnicos y funcionales que se describan o se

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

8. 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 6.588)

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 6.588) 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.

9. 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.

10. 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.

11. 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.

12. 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 AFIP

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 AFIP.

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 AFIP. Con anterioridad a la emisión del Dictamen de Evaluación, se efectuará una nueva consulta.

13. 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 y 3:

13.1 Precio Total de cada Renglón, en Dólares Estadounidenses.

Renglón 4:

13.2 Precio Mensual del Renglón, en Dólares Estadounidenses.

13.3 Precio Total del Renglón, en Dólares Estadounidenses.

Monto Total:

13.4 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.

14. REPRESENTACIÓN OFICIAL. ANTECEDENTES COMERCIALES

14.1 Representación Oficial

Los oferentes deberán 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.

14.2 Antecedentes Comerciales

Se 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.

15. VISITA TÉCNICA

Los interesados deberán realizar una visita técnica a los sitios donde se desarrollarán las tareas objeto de la presente contratación, con el objeto de evaluar las condiciones en que los trabajos deberán ser efectuados, no pudiendo alegar posterior ignorancia y/o imprevisión en las condiciones en que se ejecutará y cumplirá el contrato.

Las visitas se facilitarán **hasta tres (3) días antes** de 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 11-4159-9006, a los efectos de coordinar el día y hora en que las mismas 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.

El Certificado de Visita deberá acompañarse obligatoriamente con la oferta, bajo apercibimiento de considerarse la misma como no admisible.

16. 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° 6.588-:

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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. PERFECCIONAMIENTO DEL CONTRATO

Conforme lo establecido por el artículo 24 del PCG.

23. 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 6.588-.
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.

24. PERSONAL DE LA ADJUDICATARIA

24.1 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

24.2 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.

24.3 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.

24.4 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.

25. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO

25.1 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.

25.2 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, 2 y 3:

El pago de lo solicitado se efectuará conforme lo indicado en el Pliego de Bases y Condiciones Generales.

Renglón 4:

El pago de lo solicitado se efectuará por anticipado, conforme lo indicado en el Pliego de Bases y Condiciones Generales.

En función de lo dispuesto en el párrafo precedente, el adjudicatario deberá integrar un seguro de caución por el total adjudicado, en garantía del pago anticipado; seguro que tendrá vigencia hasta la conformidad definitiva

26. PENALIDADES

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° 6.588- 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° 6.588- 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.

27. 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.

28. 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° 6.588) 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° 6.588) 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° 6.588) 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

LICITACIÓN PÚBLICA N° 2-0039-LPU24

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 PCP, a los edificios detallados a continuación:

SEDE	FECHA	FIRMA Y ACLARACIÓN AGENTE CERTIFICADOR
Avda. Julio A. Roca 530	/ /	
Hipólito Yrigoyen 932	/ /	

LICITACIÓN PÚBLICA N° 2-0039-LPU24

PROVISIÓN DE SOLUCIONES DE PREVENCIÓN Y DEPURACIÓN DE DDOS

PLIEGO DE ESPECIFICACIONES TÉCNICAS

PLIEGO DE ESPECIFICACIONES TÉCNICAS.

1. GENERALIDADES

Las presentes especificaciones indican las prestaciones mínimas que deberá brindar la tecnología ofrecida.

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.

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 Adjudicataria 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. CONSIDEERACIONES GENERALES

Dado que las tecnologías a proveer en la presente licitación deberán trabajar en forma integrada nativamente será requisito que sean de un único fabricante y que el soporte técnico posterior sea brindado en un único canal de comunicación y resolución.

Las tecnologías para proveer deberán tener una integración nativa con la infraestructura de Firewall de Aplicaciones Web (F5 Inc) actualmente en uso por el Consejo de la Magistratura de la Ciudad de Buenos Aires.

3. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 1

El oferente deberá proveer de una tecnología de DDoS On Premise que cuente con módulos para proteger ataques desde capa dos a capa 7.

Características del equipamiento

Se deberán proveer dos (2) equipos, a ser implementados uno de ellos en cada uno de los centros de cómputos que el Consejo de la Magistratura de la Ciudad de Buenos Aires defina.

La solución deberá 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 (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 4 sistemas conviviendo en el mismo appliance (Multitenant).
- Deberá soportar arquitectura de software de 64 bits.
- El storage deberá ser de al menos 480 GB SSD.
- La solución deberá incluir mínimo 45.000 TPS para llaves de 2K SSL.
- La solución deberá tener la capacidad de soportar al menos 25 Gbps de bulk encryption.
- Deberá 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, se deberá proveer el siguiente software:

- Módulo de Balanceo Global y Disponibilidad de DNS para los dos appliances.
- Módulo de Balanceo Local para los dos appliances.
- Módulo de Firewall y protección DDoS para los dos appliances.
- Módulo de Firewall de Aplicaciones para los dos appliances.

Módulo de Balanceo Global y Disponibilidad DNS

- La solución deberá soportar alta disponibilidad de aplicaciones distribuidas en dos o más data centers.
- Deberá funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio.
- Deberá poder redireccionar queries DNS utilizando un CNAME Pool.
- Deberá poder hacer forward traffic a otros DNS locales.
- Deberá permitir los siguientes métodos de balanceo estático y dinámico:
    - Estáticos:
        - Drop Packet
        - Fallback IP
        - Global Availability
        - Ratio
        - Return to DNS
        - Round Robin
        - Static Persist
        - Topology / Geolocalization
    - Dinámicos
        - Completion Rate
        - CPU
        - Hops
        - Kilobytes / Seconds
        - Least Connections
        - Packet Rate

  - QoS
  - Round Trip Time
  - Virtual Server Score
  - Virtual Server Capacity

- El método de QoS deberá contar con la posibilidad de determinar varios coeficientes, como mínimo:
  - RTT
  - Hit Ratio
  - Hops
  - Packet rate
  - Bits per second
  - Network Proximity / Geolocalization
  - Number of Nodes Up
  - User defined Ranking / Score
  - LCS
- Deberá manejar persistencia a nivel global, manteniendo a los usuarios en un mismo centro de cómputos por el transcurso de su sesión.
- Permitir balanceo de cargas entre centros de cómputos de acuerdo a la ubicación geográfica.
- Deberá permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico por topología que concuerde con la infraestructura interna.
- Deberá permitir monitoreo de la infraestructura y las aplicaciones, integrándose con otros equipos del mismo fabricante o de terceros.
- Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.
- Deberá permitir transferencia de zonas en caso de ser necesario.
- Deberá permitir la autenticación vía certificados SSL con los demás sistemas con los cuales se compartirá información.
- Deberá permitir la configuración de TTL en una respuesta “DNS NoError” y en códigos de retorno de falla.

- Deberá permitir la configurar de código de retorno (RCODE) a los clientes cuando la consulta de balanceo falle.
- Deberá permitir el análisis de dispositivos que participen en la cadena de servicio DNS y la recolección de estadísticas
- Deberá permitir realizar balanceo de servidores DNS.
- Deberá soportar DNSSEC, firmando digitalmente y cifrando las respuestas de queries DNS.
- Deberá poder integrarse con HSMs externos para la creación automática/manual de llaves para DNSSEC.
- Deberá incluir herramienta de administración gráfica para el manejo de zonas DNS.
- Deberá soportar registros AAAA para IPv6.
- Deberá soportar traducción entre DNS IPv4 y DNS Ipv6.
- Deberá tener una capacidad mínima de 2,300,000 Query DNS RPS con DNS Express
- Deberá integrarse con IP Anycast
- Deberá funcionar como firewall de DNS
- Deberá proveer protección contra DNS Flood Attacks.
- Deberá contar con validación de protocolo.
- Deberá proveer protección contra ataques de DdoS de DNS
- Deberá proveer protección contra ‘LDNS cache poisoning’
- Deberá proteger contra ataques de ampliación de DNS
- Proveer la posibilidad de utilizar “Response Policy Response”.
- Deberá Integrarse con servicios como SURBL o Spamhaus.
- Deberá integrarse con módulos de balanceo LTM del fabricante F5 a los efectos de poder utilizar los diversos monitores de salud que aquellos módulos poseen y poder determinar de una mejor manera la decisión de a que dispositivo redireccionar la consulta DNS.
- Permitir el uso de perfiles para resolución de DNS por caché:
    - Cache transparente
    - Hot Cache
    - Caching resolver
    - No Cache response

- Validating caching resolver

Módulo de Balanceo Local

- Deberá 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 deberá realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.
- La solución deberá 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.
- Deberá 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 deberá realizar el control de persistencia de las conexiones por:
    - Dirección IP origen
    - Dirección IP destino
    - Cookies

  - Hash
  - SIP: deberá permitir definir el campo SIP sobre el cual hacer persistencia
  - Sesiones SSL
  - Microsoft Remote Desktop

- Deberá permitir crear persistencia por cualquier valor del paquete por medio de reglas.
- Deberá 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, Postgre, 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 deberá 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 redireccionar la petición en caso que todos los servidores del pool estén caídos
- La administración de la solución deberá 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 permitirá, 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.
- Deberá 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 cpu’s 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 deberá 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 deberá 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.
- Deberá soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.

- Deberá contar con la capacidad de inspeccionar tráfico ssl para bloquear tráfico malicioso y aceptar tráfico adecuado.
- Deberá contar con funcionalidades para mejorar la performance al menos 2x en el usuario final sin cambiar nada en servidores, aplicaciones.
- Deberá 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

Módulo de Firewall y Protección DDoS

- Deberá incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables
- La solución de DDoS deberá contar con un sistema de protección basado en comportamiento (Behavioral) que permita la creación de firmas o vectores de ataque de manera dinámica.
- La solución deberá proteger contra ataques de denegación de servicio tanto en una topología en línea (inline deployment) como en una topología fuera de línea (TAP mode)
- Deberá bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks
- Deberá mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
- Deberá permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.
- Deberá permitir la creación de reglas globales.
- Deberá tener la opción de funcionar como un firewall statefull full-proxy y ser certificado por ICSA Labs como Network Firewall
- Deberá permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas.
    - Entre intervalos de tiempo
    - Hasta una fecha especifica
    - Después de una fecha específica.
    - Deberá permitir la creación de listas blancas (White lists) de direcciones IP
- Deberá permitir la configuración de túnel IPSEC Site-to-Site
- Deberá incluir funcionalidad de application delivery controller o integrarse con dispositivos de Application Delivery
- Deberá brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo

- Deberá brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo
- Deberá permitir personalizar los Logs y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.
- Deberá funcionar como un Proxy SSH para control de conexiones entre diferentes redes con el fin de dar visibilidad a las sesiones SSH y controlar las mismas
- Deberá soportar Port Misuse, evitando que servicios pasando a través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo, un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).
- Deberá soportar RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.

Módulo de Firewall de Aplicaciones WEB (WAF)

- La solución deberá incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no deberá ser un appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).
- La funcionalidad de WAF deberá 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.
- Deberá trabajar en un esquema proxy TCP reverso y/o transparente
- El WAF deberá poder construir automáticamente políticas basadas en el tráfico detectado
- Deberá 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.
- Deberá trabajar en modo de bloqueo o en modo informativo
- Deberá permitir diferentes políticas de seguridad para diferentes aplicaciones

- WAF deberá 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 deberá 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 deberá 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 deberá 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 deberá medir el estrés de la aplicación para una detección precisa
- WAF deberá 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 deberá 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 deberá 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 deberá tener la capacidad de agregar cookies para la persistencia del equilibrio de carga.
- El WAF deberá 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 deberá 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.
- Deberá permitir la creación de firmas personalizadas
- Deberá trabajar con modelos de seguridad positiva y negativa

- La solución deberá 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 deberá entregar una puntuación de riesgo de la violación recibida
- Deberá tener la capacidad de crear, modificar y eliminar políticas de WAF mediante API Rest.
- Deberá poder aprender el comportamiento de la aplicación automáticamente sin intervención humana
- El WAF deberá poder admitir la aplicación de políticas de seguridad para aplicaciones escritas en Google Web Toolkit (GWT)
- El WAF deberá 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 deberá permitir personalizar las páginas de bloqueo
- El WAF deberá 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 deberá 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.
- Deberá prevenir exponer el "OS fingerprinting"
- Deberá permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.
- El WAF deberá 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 deberá incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)
- El WAF deberá 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 deberá incluir protección contra Web Scraping

- Deberá 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).
- Deberá permitir verificar las firmas de ataque en las respuestas del servidor al usuario
- Deberá permitir el enmascaramiento de información sensible filtrada por el servidor
- Deberá poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.
- Deberá permitir la integración con servidores Antivirus por medio del protocolo ICAP
- Deberá brindar reportes respecto a la normativa PCI DSS 2.0
- Deberá integrarse con Firewall de Base de Datos:
- Oracle Database Firewall
- IBM InfoSphere Guardium
- Deberá 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.
- Deberá soportar tecnologías AJAX y JSON
- Deberá 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

- Deberá 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.
- Deberá permitir verificaciones de seguridad y validación a protocolos FTP y SMTP
- Deberá permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas
- Deberá incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.
- Deberá soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.
- Deberá ofrecer protección sobre tráfico basado en WebSockets
- El WAF deberá identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.
- Deberá proteger las aplicaciones contra ataques de denegación de servicio a nivel L7
- El WAF deberá 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 deberá permitir utilizar protección avanzada de credenciales en formularios de la aplicación web, haciendo cifrado de la data entrada en formularios. Este cifrado se deberá realizar usando un esquema de llave publica/privada. Este cifrado deberá 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 deberá realizar ofuscación de contenido HTTP, en particular de los nombres de cualquier parámetro dentro de la aplicación. Esta ofuscación de parámetros deberá 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 deberá 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 deberá 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 deberá soportar WebHook notifications, notificando a servicios de Continuous Integrations / Continuous Delivery (CI/CD) cuando hay cambios en la política o Eventos de Seguridad
- Deberá 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 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 deberá tener un mecanismo de reversión de políticas
- El WAF deberá 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)
- Deberá tener la capacidad de exportar e importar las políticas de WAF en formato XML y JSON.
- El WAF deberá 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 deberá incluir protección basada en comportamientos (Behavioral).

4. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 2

El oferente deberá proveer una tecnología que posea las características especificadas a continuación:

- La plataforma de DDoS en la nube deberá contar con un servicio del estilo Scrubbing Center (Centro de Depuración), que trabaje de manera nativa y en forma coordinada con la solución On Premise, con un soporte de hasta 500 Mbps para redireccionar tráfico limpio desde el Scrubbing Center hacia la plataforma del cliente.
- El rendimiento de la solución deberá ser extensible.
- La solución deberá contar con detector de Controladores, deberá ser responsable del análisis de tráfico, la visualización del tráfico, incluyendo la visualización de alertas sobre posibles ataques DDoS y también deberá ofrecer funcionalidad de informes para la capacidad y la planificación de decisiones de peering. La función deberá ser capaz de soportar BGP flowspec y con la interacción iBGP con los proveedores del enrutador de terceros (p.ej. Cisco IOS-XR) ser capaz de tráfico blackholing o shaping (usando BGP flowspec signalling).
- La solución deberá apoyar multigestión de inquilinos con un solo panel para gestionar múltiples bloques funcionales de detección e inteligencia de amenazas integrados en cualquier red o nubes privadas o públicas.
- La mitigación es una acción realizada por el dispositivo de limpieza para diferenciar el tráfico legítimo del tráfico de ataque y bloquear el segundo tráfico sospechoso observado por la función de detección. Si el volumen de DDoS está por encima de la capacidad definida que satura la capacidad de procesamiento o enlaces actualmente disponible, el tráfico puede ser desviado al servicio de mitigación de DDoS basado en la nube.
- La solución deberá contar con un motor de mitigación en línea (IME). El objetivo principal es analizar el tráfico y mitigar inmediatamente los ataques DDoS contra la infraestructura. Si el volumen de DDoS está por encima de la capacidad definida, el IME enviará una señal a la plataforma de mitigación para redirigir el tráfico al central de depuración y asumir la mitigación del ataque de alto volumen.

- El diseño de la plataforma DDoS deberá estar basada en una configuración de alta disponibilidad y geo-redundancia. Por lo tanto, la plataforma de defensa contra ataques DDoS deberá consistir en los dos centros de depuración central geo-redundantes independientes con motores de mitigación cuya capacidad debería ser extensible en servicio y controladores de detección geo-redundantes independientes.
- La protección DDoS basada en la nube global deberá iniciarse y hacerse cargo del ataque y limpiar el tráfico antes de que afecte a nuestros proveedores ascendentes.
- La protección DDoS basada en la nube global deberá garantizar la recepción de un mínimo de 500Mb de tráfico limpio, sin importar el volumen de ataque recibido.
- Los objetos de protección pueden estar no solo en la red del organismo, sino también en las nubes públicas. Se requiere una solución común para todos los casos de uso mediante el uso del Portal de Gestión con un solo panel.
- La solución deberá basarse en la acción de BGP de desviar el tráfico dirigido al Centro de Limpieza (en el lugar o en la nube). Para clientes específicos, se proporcionará la opción de solución de mitigación en línea.
- La solución deberá contar con contramedidas de lista negra/blanca que posibiliten las acciones de permitir o negar el tráfico basado en parámetros similares a ACL. Este filtro se realizará antes de otras contramedidas. Si un paquete coincide con la lista negra o blanca, no se aplican más contramedidas y los paquetes se descartan o reenvían adecuadamente.
- Debido a las ventajas de rendimiento, la solución deberá basarse en ACL en los enrutadores o filtrado a través de BGP Flowspec que proporciona un mayor rendimiento y por lo tanto deberá ser considerada como la opción principal para el filtrado básico. El Centro de Depuración Central se centrará en medidas más profundas.
- El centro de datos deberá detectar flujos sospechosos en la red basándose en umbrales.
- El tráfico que supere los umbrales (uno o más) deberá reaccionarse mediante la visualización de alerta a la interfaz de gestión gráfica y enviar SNMP trap/SYSLOG mensaje.

5. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 3

El oferente deberá brindar los servicios de implementación según los requerimientos técnicos especificados en el presente Pliego de Especificaciones Técnicas.

El oferente realizará la implementación de las soluciones propuestas 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 Ciudad de Buenos Aires.

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.

Las tareas deben incluir:

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

Se deberá presentar un Plan de Trabajo que especifique el detalle de las tareas a realizar y los plazos de implementación.

6. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 4

El oferente deberá proveer un servicio de soporte técnico, mantenimiento y actualización tecnológica, por el plazo de treinta y seis (36) meses.

Acuerdo de Nivel de Servicio

- Los servicios ofrecidos deben incluir un soporte técnico local en modalidad 7x24x365 para la resolución de incidencias técnicas.
- El soporte técnico local deberá ser brindado con personal especializado propio del adjudicatario.
- Se deberá contemplar el servicio de soporte técnico del fabricante en modalidad 7x24x365 para el escalamiento de incidencias técnicas.
- El servicio de soporte técnico deberá 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.
- 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 Ciudad de Buenos Aires.