RESO SAGYP N° 516/23

Buenos Aires, 24 de octubre del 2023

VISTO:

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

CONSIDERANDO:

Que por el TEA citado en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, que tiene por objeto la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires. En tal sentido, propuso cláusulas para incorporar en los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, y estimó que el presupuesto oficial asciende a la suma total de dólares estadounidenses cinco millones setecientos cincuenta y tres mil (U$S 5.753.000.-) (v. Nota DGIyT 649/23 y Adjuntos 114216/23 y 114249/23).

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, 45 y concordantes de la Ley Nº 2.095 (texto consolidado según Ley Nº 6.588), y su reglamentaria Resolución CM Nº 276/2020 y la Resolución SAGyP Nº 30/2021 (v. Adjunto 118473/23).

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 148394/23 y 126252/23. 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 Doscientos Mil ($ 200.000.-), para participar en la Licitación Pública N° 2-0017-LPU23"* (v. Memo DGCC 1833/23).

Que en cumplimiento de la Ley N° 70 (texto consolidado según Ley N° 6.588), la Dirección General de Programación y Administración Contable afectó la suma necesaria para hacer frente a la contratación de marras (v. Adjuntos 145080/23 y 145108/23).

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 12337/2023.

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, 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 148394/23 y 126252/23, y llamar a Licitación Pública N° 2-0017-LPU23, cuyo objeto es la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cinco millones setecientos cincuenta y tres mil (U$S 5.753.000.-), para el día 8 de noviembre de 2023 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

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° 2-0017-LPU23, 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 por la Resolución CM N° 143/2023, el Plenario del Consejo de la Magistratura designó como reemplazo transitorio de la Secretaria de Administración General y Presupuesto del Poder Judicial a la Dra. Clara María Valdez, al amparo de lo dispuesto por el artículo 35 de la Ley N° 31 (texto consolidado según Ley N° 6.588).

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

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

Artículo 1º: Apruébanse los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran como Adjuntos 148394/23 y 126252/23, y forman parte de la presente Resolución, que regirán la Licitación Pública N° 2-0017-LPU23, que tiene por objeto la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cinco millones setecientos cincuenta y tres mil (U$S 5.753.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0017-LPU23, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante,

servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, fijándose como fecha límite para la presentación de ofertas y la apertura pública de ofertas el 8 de noviembre de 2023 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Artículo 3º: Establézcase que la adquisición de los Pliegos necesarios para cotizar en la Licitación Pública Nº 2-0017-LPU23, será por un monto de pesos doscientos mil ($ 200.000.-)

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0017-LPU23, a los Dres. Hernán Labate y Matías Vázquez como miembros titulares, y a los Dres. Adrián Constantino y 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° 2-0017-LPU23 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 las Direcciones Generales de Informática y Tecnología y de Programación y Administración Contable. Pase a la Dirección General de Compras y Contrataciones para sus efectos.

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

FIRMAS DIGITALES

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

LICITACION PÚBLICA 2-0017-LPU23

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA

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 de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la contratación de un Plan Integral de Seguridad Informática, con su correspondiente implementación, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires.

3. PRESUPUESTO OFICIAL

El presupuesto oficial de la presente licitación pública asciende a la suma total de **Dólares Estadounidenses Cinco Millones Setecientos Cincuenta y Tres Mil (U$S 5.753.000.-),** el cual se compone de la siguiente manera:

Renglón 1: Dólares Estadounidenses Un Millón Seis Mil (U$S 1.006.000.-).

Renglón 2: Dólares Estadounidenses Dos Millones Trescientos Cuarenta y Ocho Mil (U$S 2.348.000.-).

Renglón 3: Dólares Estadounidenses Doscientos Treinta y Dos Mil (U$S 232.000.-).

Renglón 4: Dólares Estadounidenses Quinientos Cuarenta y Un Mil (U$S 541.000.-).

Renglón 5: Dólares Estadounidenses Trescientos Nueve Mil (U$S 309.000.-).

Renglón 6: Dólares Estadounidenses Setecientos Veintidós Mil (U$S 722.000.-).

Renglón 7: Dólares Estadounidenses Trescientos Treinta y Cuatro Mil (U$S 334.000.-).

Renglón 8: Dólares Estadounidenses Doscientos Sesenta y Un Mil (U$S 261.000.-).

4. RENGLONES A COTIZAR

Renglón 1: Provisión de Solución Antispam, Antimalware avanzado, SIEM y SOAR para el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Servicio de Soporte y Actualización Tecnológica de la solución provista en el Renglón 1, por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 3: Provisión de una Solución de Gestión de Vulnerabilidades para el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, a suscribirse por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 4: Servicio de Soporte y Actualización Tecnológica de la solución provista en el Renglón 3, por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 5: Provisión de una Solución de Gestión de Identidades y Privilegios para el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, a suscribirse por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 6: Servicio de Soporte y Actualización Tecnológica de la solución provista en el Renglón 5, por treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 7: Servicio de Implementación para las soluciones provistas en los renglones 1, 3 y 5, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 8: Servicio de Capacitación para las soluciones provistas en los renglones 1, 3 y 5, 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 Doscientos Mil ($ 200.000-)** y podrá abonarse mediante depósito en efectivo o por transferencia bancaria a la Cuenta Corriente N° 6/2, a nombre del Consejo de la Magistratura, en el Banco de la Ciudad de Buenos Aires, Sucursal Nº 68, sita en Av. Pte. Julio A. Roca 538, de esta Ciudad, CBU 0290068100000000000628, 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 Máximo de la Contratación:

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 Provisión e Implementación Renglones 1, 3, 5 y 7:

El plazo máximo de provisión e implementación de las soluciones solicitadas en los renglones 1, 3, 5 y 7 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, 2, 3, 4, 5 y 6:

Los servicios solicitados tendrán una duración de treinta y seis (36) meses, contados a partir de la fecha indicada en el parte de recepción definitiva de la instalación y puesta en funcionamiento del equipamiento solicitado.

6.4 Plazo de Ejecución Renglón 8:

Los servicios de capacitación se proveerán durante el referido plazo de treinta y nueve (39) meses.

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. REQUISITOS TÉCNICOS

8.1 Junto a las condiciones establecidas en los Pliegos de Bases y Condiciones Generales, de Bases y Condiciones Particulares y de Especificaciones Técnicas, los oferentes deberán acreditar su condición de Canal Certificado para la comercialización y soporte post venta de los productos ofertados mediante nota del fabricante.

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

8.3 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.

8.4 Los oferentes deberán contar con experiencia comprobable en implementaciones similares. Especificar al menos cinco (5) casos e incluir contactos de referencia por cada uno de los renglones.

9. CONDICIONES PARA SER OFERENTE

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

a) Sociedades regularmente constituidas por alguna de las modalidades previstas y habilitadas por la Ley de Sociedades Comerciales, con domicilio legal en la Ciudad Autónoma de Buenos Aires o Sucursal debidamente inscripta en la Inspección General de Justicia.

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

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

d) 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. IMPEDIMENTOS PARA SER OFERENTE

Complementando lo estipulado por artículo 90 de la Ley N° 2.095 (Texto consolidado por Ley N° 6.588), no podrán concurrir como oferentes a la presente licitación:

a) Las sociedades cuyos Directores, Representantes, Socios, Síndicos, Gerentes registren condenas firmes por la comisión de delitos penales económicos.

b) Las Sociedades integradas por personas humanas y/o jurídicas cuyos miembros del Directorio, Consejo de Vigilancia, Síndicos, Gerentes, Socios, Representantes o Apoderados sean Agentes y/o Funcionarios bajo cualquier forma de modalidad contractual, de la Administración Pública Nacional, la Administración Pública Provincial y/o la Administración Pública de la Ciudad Autónoma de Buenos Aires.

c) Las Sociedades irregulares o de Hecho.

d) Sociedades que hubieran sido sancionadas con la anulación o rescisión por incumplimiento de las obligaciones contractuales, en el marco de una relación contractual con la Administración Pública u Organismo Público de alguno de los Estados: Nacional, Provincial, o de la Ciudad Autónoma de Buenos de Buenos Aires, sea en el país o en el extranjero.

e) Sociedades que se encuentren suspendidas o inhabilitadas en el RIUPP o en su equivalente en cualquier Municipalidad o Provincia del país.

f) Sociedades que posean acciones de otra u otras sociedades oferentes.

g) Las personas jurídicas en estado de quiebra o liquidación. En el caso de aquellas en estado de concurso, pueden contratar siempre que mantengan la administración de sus bienes mediante autorización judicial. Las que se encuentran en estado de concurso preventivo pueden formular ofertas, salvo decisión judicial en contrario.

h) Los que se encuentren inhabilitados por cualquier Ley/Reglamentación vigente en cualquier jurisdicción de la República Argentina.

La totalidad de los impedimentos enumerados precedentemente son de aplicación en forma individual a las sociedades integrantes de las UT que se presenten en esta Licitación Pública.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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, 3, 5, 7 y 8:

15.1 Precio Total de cada Renglón, en Dólares estadounidenses.

Renglones 2, 4 y 6:

15.2 Precio Mensual de cada Renglón.

15.3 Precio Total de cada Renglón, en Dólares Estadounidenses.

Monto Total:

15.4 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.

16. VISITA TÉCNICA

Los interesados deberán realizar una visita técnica al Centro de Cómputos existente en el edificio sito en Av. Julio A. Roca 530, Piso 3, de esta Ciudad, en el que se instalará el hardware a proveer en la presente contratación, con el fin de tomar conocimiento de las condiciones en que las prestaciones deberán ser llevadas a cabo, no pudiendo alegar posterior ignorancia y/o imprevisión en las condiciones en que ejecutará y cumplirá el contrato.

Las visitas podrán ser efectuadas hasta tres (3) días con antelación a la fecha prevista para la apertura de las ofertas, debiendo comunicarse con la Dirección General de Informática y Tecnología, de lunes a viernes de 10.30 a 12.00 y de 14.30 a 17.00 horas, al teléfono 15-4159-9006, a los efectos de coordinar el día y hora en que las mismas serán efectuadas.

La Dirección General de Informática y Tecnología extenderá el correspondiente Certificado de Visita –que como Anexo IV forma parte del presente Pliego de Base y Condiciones Particulares-, con el que se acreditará el cumplimiento de la visita técnica solicitada.

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

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° 6.588-:

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.

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 Preadjudicación) 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 6.588-.

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.

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 al 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 cuatro millones ($ 4.000.000,00.-).

Invalidez Total y/o parcial permanente por accidente: pesos dos millones ($ 2.000.000,00.-).

Asistencia Médico Farmacéutica (AMF): pesos un millón ($ 1.000.000,00.-).

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.

El adjudicatario debe asegurar, en los casos en que corresponda, 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 cuatro millones ($ 4.000.000.-). 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.

Asimismo, deberá presentar la siguiente documentación:

- Nóminas de Personal
- Libretas Sanitarias

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, 3, 5 y 7:

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

Renglones 2, 4 y 6:

El pago se efectuará por anticipado, luego de la emisión del Parte de Recepción Definitiva correspondiente a los Renglones 1, 3, 5 y 7, de conformidad con lo dispuesto 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.

Renglón 8:

El pago 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.

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 la 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.

30.2 Particularidades

La Dirección General de Informática y Tecnología del Consejo de la Magistratura será la encargada del contralor del grado de cumplimiento contractual por parte del adjudicatario.

El primer incumplimiento de lo dispuesto en el apartado Niveles de Servicio –Punto 5 del Pliego de Especificaciones Técnicas-, dará lugar a la aplicación de una multa equivalente a diez mil (10.000) unidades de compra.

El segundo incumplimiento de lo dispuesto en aquel apartado, dará lugar a la aplicación de una multa equivalente a veinticinco mil (25.000) unidades de compra.

A partir del tercer incumplimiento, estos darán lugar a la aplicación de una multa equivalente a setenta y cinco mil (75.000) 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° 6.588) 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

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 30

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 31

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° 2-0017-LPU23

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 16 del PCP, a los edificios detallados a continuación:

SEDE	FECHA	FIRMA Y ACLARACIÓN AGENTE CERTIFICADOR
Avda. Julio A. Roca 530		

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

LICITACION PÚBLICA N° 2-0017-LPU23

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA

PLIEGO DE ESPECIFICACIONES TÉCNICAS

ÍNDICE:

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.

Asimismo, y complementariamente a lo expresado en el párrafo anterior, los errores o las eventuales omisiones que pudieran existir en la presente documentación y especificaciones técnicas no invalidarán la obligación de la empresa de ejecutar las tareas y proveer, instalar y poner en servicio

los materiales y equipos en forma completa y correcta, de acuerdo a los fines a los que están destinados.

El adjudicatario tendrá la obligación de verificar, antes de la ejecución, que los documentos suministrados por este Consejo de la Magistratura no contengan errores, omisiones o discrepancias que puedan ser normalmente detectados por un especialista. Si descubriera errores, omisiones o discrepancias, deberá señalarlas inmediatamente por escrito. Si no los señalara oportunamente, serán a su cargo los trabajos que fueran necesarios ejecutar para corregir las fallas, y esos trabajos no podrán justificar ampliaciones de plazo ni del precio total o cualquier otro costo.

2. ESPECIFICACIONES TÉCNICAS RENGLÓN 1

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

- AntiSpam.
- Antimalware Avanzado.
- SIEM.
- SOAR.

Se deberá proveer las diferentes soluciones por un plazo de treinta y seis (36) meses.

Requerimientos generales

- Será requisito que las tecnologías a proveer en el presente renglón 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.
- El fabricante de las soluciones deberá contar con un puntaje no menor a 4.2 en Gartner Peer Insights de las siguientes tecnologías.
  - Endpoint Protection Platform Reviews and Ratings.
  - Email Security Reviews and Ratings.
  - Security Orchestration, Automation and Response Solutions Reviews and Ratings.
  - Security Information and Event Management Reviews and Ratings.

Especificaciones técnicas antispam

Características del equipamiento

- La solución deberá ser del tipo Virtual Appliance (la infraestructura será provista por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires).
- La solución deberá ser licenciada sin importar el número de buzones que proteja. El licenciamiento es basado en el performance del hardware suministrado (correo por hora).
- La solución deberá poder enrutar al menos 875.000 Mails por hora.
- La solución deberá poder enrutar al menos 750.000 Mails por hora utilizando motores de antivirus y antispam.
- La solución deberá poder soportar 2000 casillas en modo servidor.
- La solución no deberá utilizar más de 4 virtual cores.
- La solución deberá poder integrarse a futuro a un sandbox del mismo fabricante.
- La solución deberá ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.
- La solución deberá ser capaz de actuar como Gateway, en calidad de MTA (Mail Transfer Agent).
- La solución deberá ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.
- La solución deberá ser capaz de desplegarse en modo transparente tanto en L2 (bridge) como en L3 (router). En cualquier caso, deberá poder dejar pasar la dirección IP original del cliente o server sin necesidad de agregar encabezados o headers especiales.
- Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist del dominio.
- La solución puede ser implementada como un cliente WCCP y recibir correo y analizar mediante este protocolo.
- La solución deberá soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP.
- Deberá tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación.

Características Generales

- La solución deberá soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema.
- La solución deberá permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus y antispyware.
- La solución deberá poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
- La solución deberá poder definir el reenvío de correo (relay) a una IP especifica con base a la IP origen del mensaje.
- La solución deberá proporcionar soporte para múltiples dominios de correo electrónico.
- La solución deberá ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente.
- La solución deberá ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.
- La solución deberá soportar cuarentena por usuario, permitiendo que cada usuario pueda gestionar sus propios mensajes en cuarentena, la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se deberá acceder a través de la página web y POP3.
- La solución deberá ser capaz de programar el envío de informes de cuarentena.
- La solución deberá ser capaz de realizar el almacenamiento de correo electrónico (Archivado/archiving), basado en el envío y recepción de políticas, con el apoyo también de almacenamiento remoto.
- La solución deberá ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega.
- La solución deberá ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.
- La solución deberá ser capaz de mantener listas de reputación del remitente sobre la base de:
    - Número de virus enviado.
    - La cantidad de correos electrónicos considerados correo no deseado.
    - La cantidad de destinatarios equivocados.
- La solución deberá ser compatible con el enrutamiento en IPv4 y IPv6.
- La solución deberá permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto.

- La solución deberá tener características antispam, antivirus, antispyware y anti-phishing.
- La solución deberá ser capaz de realizar la inspección del correo de Internet entrante y saliente.
- La solución deberá contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger.
- La solución deberá proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb.
- La solución deberá proporcionar un control DNS reverso para la protección contra los ataques spoofing.

Funcionalidades de AntiSpam

- La solución se deberá conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.
- La solución deberá poder detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.
- La solución deberá poder detectar si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante.
- La revisión de URLs deberá permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante.
- La solución deberá contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correos recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM.
- La solución deberá ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo al comportamiento del correo y así determinar si un correo es spam.
- La solución deberá ser capaz de realizar análisis Bayesiano para determinar si un correo es SPAM.
- La solución deberá ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter).
- La solución deberá contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su comportamiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos.
- La solución deberá ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje.

- La solución deberá ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).
- La solución deberá contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM.
- La solución deberá permitir crear lista blancas o negras de palabras.
- La solución deberá permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobrescribir el destinatario, archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado.
- La solución deberá ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM.
- La solución deberá ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL.
- La solución deberá ser compatible con la lista gris para las cuentas de correo electrónico en IPv4 e IPv6.
- La solución deberá ser capaz de detectar las direcciones IP falsificadas (Forged IP).
- La solución deberá permitir identificar imágenes que hagan alusión a contenido SPAM. Para ello debe soportar el análisis de las siguientes extensiones: GIF, JPEG, PNG.

Funcionalidades de Sesión

- La solución deberá poder validar si el destinatario del correo entrante es un buzón válido.
- La solución deberá ser compatible con Sender Policy Framework (SPF).
- La solución deberá ser compatible con Domain Keys Identified Mail (DKIM).
- La solución deberá ser compatible con Domain Based Message Authentication (DMARC).
- La solución deberá identificar altos volúmenes de conexiones y aplicar limites basado en senders e IPs.
- La solución deberá ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.

Funcionalidades de Gestión

- La solución deberá permitir su configuración a través del acceso web (HTTP, HTTPS).

- La solución deberá ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.
- La solución deberá ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only).
- La solución deberá permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como antispam, antivirus, autenticación, entre otros.
- La solución deberá soportar doble factor de autenticación para el login de usuarios administradores.

Funcionalidades de Alta Disponibilidad (HA)

- La solución deberá permitir esquemas de Alta Disponibilidad, tanto Activo-Activo como Activo-Pasivo.
- Cuando la solución se implemente para alta disponibilidad deberá ser capaz de controlar el estado del enlace.
- Cuando la solución se implemente para alta disponibilidad, deberá soportar la conmutación por falla de red.
- Cuando la solución se implemente para alta disponibilidad, deberá ser capaz de sincronizar los mensajes de e-mails en cuarentena.
- Cuando la solución se implemente para alta disponibilidad Activo/Pasivo debería ser posible sincronizar los mensajes de correo electrónico y configuraciones.
- Cuando la solución se implementa para alta disponibilidad deberá ser capaz de detectar y reportar el fallo de un dispositivo.
- El modo de Activo-Pasivo deberá soportar hasta 25 miembros en el clúster.

Funcionalidades de Modo Servidor

- La solución, estando en server mode, deberá poder sincronizar contactos y calendarios con clientes de correo (MUA).
- En modo server, deberá soportar los protocolos WebDAV y CalDAV para la publicación y sincronización de calendarios.
- La solución deberá contar con algún mecanismo para la fácil migración de buzones y cuentas desde un servidor a la nueva solución estando en server mode.

Funcionalidades de Malware

- La solución deberá contar con capacidades de evaluar, retener y/o bloquear correos que cuenten con amenazas avanzadas, del tipo Zero Day mediante el análisis de archivos con herramientas de sandboxing.
- Debe permitir integrar el análisis de sandboxing con soluciones on premise o en la nube.
- La solución deberá ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.
- La solución deberá ser capaz de ejecutar el análisis antivirus/antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ, and RAR.
- La solución deberá contar con una base de datos de malware suministrada por el fabricante y terceros aliados, la cual puede ser actualizada recurrentemente.
- Ante la detección de un malware, la solución deberá poder ejecutar las siguientes acciones: enviar un mensaje de notificación en lugar del correo, reenviar el correo y el malware a una cuenta definida, reescribir el destinatario.
- La solución deberá poder re escanear los correos que son liberados de la cuarentena de SPAM por el usuario en busca de contenido malicioso.
- Funcionalidades de Virus Outbreak.
- La solución deberá contar con una base de datos de malware basada en técnicas de sandboxing, sin necesidad de tener un sandbox habilitado, la cual es suministrada por el fabricante.
- La solución deberá poder analizar las imágenes en busca de tipos de imágenes inapropiadas con contenido para adultos.
- La solución deberá proporcionar una solución DLP para detectar la información sensible que puede estar llegando por e-mail.
- La funcionalidad DLP deberá permitir definir la información a detectar como palabras, frases y expresiones regulares.
- La funcionalidad DLP deberá tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros.
- La funcionalidad DLP deberá permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.
- La funcionalidad DLP deberá permitir la creación de filtros por tipos de archivos.

- La funcionalidad DLP deberá permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico.
- La funcionalidad DLP deberá permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado.

Funcionalidades de Cifrado

- Deberá soportar cifrado de mensajes basado en identidad (IBE- Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado.
- El cifrado de mensajes con IBE, deberá soportar tanto el método push como pull, donde el mensaje cifrado estará almacenado en la plataforma de correo para su acceso remoto autenticado, o bien sea enviado como un adjunto al destinatario.
- En ambos métodos de cifrado con IBE se deberá contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación.
- Deberá soportar cifrado de correo usando S/MIME.
- Deberá soportar cifrado SMTPS y SMTP over TLS.

Funcionalidades de Regulación

- La solución deberá analizar el contenido y adjuntos de un mensaje en busca de palabras que indiquen que el correo deba ser puesto en cuarentena, Cifrado, Archivado, Bloqueado, Taggeado, sobrescrito o reenviado a otro host.
- Deberá contar con Diccionarios predefinidos que permitan el cumplimiento de normativas como HIPAA, GLB, SOX. Estos diccionarios deberán identificar: Canadian SIN, US SSN, Credit card, ABA Routing, CUSIP, ISIN y poder definir diccionarios personalizados.
- Deberá poder inspeccionar archivos protegidos por contraseña, mediante password predefinidos, una lista de contraseñas o buscar en el cuerpo la palabra password.
- Deberá contar con la opción de remover o neutralizar contenido potencialmente malicioso y de reconstruirlos después. Por ejemplo, en archivos como MS Office y pdf que tengan macros, java o HTML con URLs maliciosas.

Funcionalidades de Log y Reporteria

- La solución deberá ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).
- La solución deberá permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.
- La solución deberá generar informes por demanda o programados a intervalos de tiempo específicos.
- La solución deberá generar y enviar informes en formato PDF o HTML.

Especificaciones técnicas antimalware avanzado

Características Generales

- Se deberán proveer cinco mil (5.000) licencias del antimalware a utilizar.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1, 10 y 11.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Windows Server 2003 SP2, R2 SP2, 2008 SP1, 2008 R2 SP2, 2012, 2012 R2, 2016, 2019, y 2022.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: macOS Versiones: El Capitán (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), y Monterey (12.x).
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.x, 7.x, y 8.x.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Linux Versiones: Ubuntu LTS 16.04.x, 18.04.x, 20.04.x server, 64-bit solamente.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Linux Versiones: Oracle Linux 6.10, 7.7+ and 8.2+.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Linux Versiones: Amazon Linux AMI 2.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Linux Versiones: SuSE SLES 15.1.
- La solución propuesta deberá ser compatible con los siguientes sistemas operativos: Ambientes Virtual Desktop Infrastructure (VDI) en VMware y Citrix, VMware Horizons 6 y 7, Citrix XenDesktop 7.

- La solución propuesta deberá tener un consumo máximo de 120MB de memoria RAM.
- La solución propuesta deberá tener un consumo promedio de menos de 2% de uso de CPU.
- La solución propuesta deberá tener un consumo menor a 20MB de espacio en disco.
- La solución propuesta deberá soportar el despliegue masivo a través de herramientas como MS System Center, JAMF y Satellite.
- La solución propuesta deberá tener la habilidad de actualizar el Endpoint sin interacción por parte del usuario y sin requerimiento de reinicio.
- La solución propuesta deberá tener protección "Anti-Tamper" en el Agente.
- La solución propuesta deberá trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos.
- La solución propuesta deberá poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos.
- La solución propuesta deberá contar con la opción de establecer contraseña para desinstalar el agente en el endpoint.
- La solución propuesta deberá poder generar un instalador de Windows Preconfigurado. Esta configuración deberá permitir la instalación sin requerir interacción ni configuración por parte de los usuarios.
- El colector que será instalado en los endpoint de la solución propuesta deberá poder trabajar detrás de un proxy.

- Detección de Malware:
  - La solución propuesta deberá poder funcionar en modalidad "offline" fuera de línea sin que el Agente se encuentre conectado a la red empresarial.
  - La solución propuesta deberá poder detectar procesos en ejecución, inicios de procesos, paradas de procesos e interacciones entre procesos.
  - La solución propuesta deberá poder detectar, eliminar y volver a su valor inicial cambios realizados por procesos maliciosos en el registro de las PC.
  - La solución propuesta deberá poder detectar solicitudes DNS enviadas desde el dispositivo.
  - La solución propuesta deberá poder detectar conexiones de red desde el dispositivo.
  - La solución propuesta deberá poder detectar actividad sospechosa asociada con archivos DLL.

- La solución propuesta deberá poder incorporar inteligencia de amenazas en el esquema de detección.
- La solución propuesta deberá poder incorporar las técnicas de MITRE ATT&CK en el esquema de detección y mostrar cuales de estas técnicas fueron utilizadas.
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como: nombre de archivo y hash de archivo, etc.
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Linux (Redhat y CentOS) utilizando indicadores de compromisos (IOC) tales como archivos, logs y comportamiento de red.
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionadas a archivos (Creación, Eliminación, Rename).
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relaciones a los procesos (Terminación de Proceso, Creación de Proceso, Carga de Ejecutable).
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al uso de red (Socket Connect, Socket Close, Socket Brind).
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada a las bitácoras de Windows (Event Log).
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al registro de Windows (Key Create, Key Delete, Value Set).
- La solución propuesta deberá tener la capacidad para realizar free text queries para filtrar la información disponible para threat hunting.
- La solución propuesta deberá tener la capacidad para almacenar búsquedas realizadas para ser reutilizadas en el futuro.
- La solución propuesta deberá tener la capacidad programar las búsquedas de indicadores de compromiso (IOC) almacenados.

- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al registro del uso del teclado (KeyLogging).
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionadas a la toma de "Screen Shots".
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionadas a las consultas generadas a DNS.
- La solución propuesta deberá identificar actividad maliciosa conocida.
- La solución propuesta deberá tener la capacidad de recibir actualizaciones diarias de inteligencia.
- La solución propuesta deberá tener la capacidad de categorizar los eventos detectados en diferentes categorías (Por Ejemplo: Malicioso, Sospechoso, No concluyente, Probablemente Seguro).
- La solución propuesta deberá tener la capacidad de convivir con otras soluciones de seguridad endpoint del tipo antivirus tradicional o de nueva generación.
- La solución propuesta deberá tener capacidad de crear excepciones a un archivo o a carpetas seleccionadas de la revisión por parte del motor de NGAV al momento de ejecutarse el archivo.

- Prevención de Malware:
  - La solución propuesta deberá tener la capacidad de prevención de ejecución de archivos maliciosos.
  - La solución propuesta deberá incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning".
  - La solución propuesta deberá tener capacidad de controlar dispositivos USB.
  - La solución propuesta deberá tener capacidad de crear excepciones a los dispositivos USB basado en el nombre del dispositivo.
  - La solución propuesta deberá tener capacidad de crear excepciones a los dispositivos USB basado en el vendor del dispositivo.
  - La solución propuesta deberá tener capacidad de crear excepciones a los dispositivos USB basado en el número de serie del dispositivo.

- La solución propuesta deberá tener capacidad de crear excepciones a los dispositivos USB basado en una combinación del: nombre del dispositivo, vendor, número de serie.
- La solución propuesta deberá tener capacidad de crear excepciones a un proceso conocido legitimo conocido de ser monitoreado por la plataforma de EDR.
- La solución propuesta deberá poder bloquear tráfico malicioso de exfiltración de datos.
- La solución propuesta deberá poder bloquear tráfico malicioso de comunicación hacia C&C (Command & Control).
- La solución propuesta deberá poder frenar brechas de seguridad e intentos de ransomware en tiempo real.
- La solución propuesta deberá poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.
- La solución propuesta deberá permitir que las políticas en la misma sean modificadas permitiendo varios estados como: Activa, Desactivada o solo crear "logs" para las reglas de seguridad contenidas en estas.
- La solución propuesta deberá poder ser configurada en modo de simulación donde no se realicen bloqueos pero toda actividad maliciosa es registrada.
- La solución propuesta deberá poder permitir la modificación de las reglas de detección de eventos maliciosos para que estas reglas solo almacenen un registro o estén en modo bloqueo.
- La solución propuesta deberá poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado.
- Requerimiento - Difusión (Post-Infección).
- La solución propuesta deberá permitir el aislamiento automático del tráfico de red de un dispositivo donde se ha encontrado una actividad causada por malware.
- La solución propuesta deberá permitir cambiar las políticas asignadas de un dispositivo donde se ha encontrado una actividad causada por malware.
- La solución propuesta deberá permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos.
- La solución propuesta deberá tener la capacidad de creación de excepciones para los procesos basados en la localización del archivo (File Path).
- La solución propuesta deberá tener la capacidad de creación de excepciones para los procesos basados en el destino del tráfico generado por el proceso.

- La solución propuesta deberá tener la capacidad de creación de excepciones para los procesos basados en usuario que ha ejecutado el proceso.
- La solución propuesta deberá tener la capacidad de crear excepciones para los falsos positivos de forma manual para marcar la actividad como falso positivo y evitar que ocurran bloqueos futuros.
- La solución propuesta deberá tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.
- La solución propuesta deberá permitir la creación de excepciones de eventos basados en direcciones IP, aplicaciones y protocolos.

- Respuesta a Incidentes:
  - La solución propuesta deberá permitir un histórico de los eventos por un mínimo de un (1) mes.
  - La solución propuesta deberá almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses.
  - La solución propuesta deberá permitir la integración con plataformas SIEMs (Security Information and Event Management) a través de un syslog.
  - La solución propuesta deberá tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria que permitan la realización de procesos forenses.
  - La solución propuesta deberá tener la capacidad de abrir tickets en plataformas de gestión tales como ServiceNow y JIRA.
  - La solución propuesta deberá permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tal como: Dirección IP, nombre de host, usuario, fecha/hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API.
  - La solución propuesta deberá tener la capacidad para terminar un proceso basado en la clasificación del mismo.
  - La solución propuesta deberá tener la capacidad para eliminar un archivo basado en la clasificación del mismo.
  - La solución propuesta deberá la capacidad para restaurar la configuración base del registro basada en la clasificación de actividad predefinida.
  - La solución propuesta deberá tener la capacidad para aislar dispositivos infectados de la red.

- La solución propuesta deberá tener la capacidad para restringir el acceso del dispositivo a la red de forma automática según la clasificación (Malicioso, Sospechoso, etc.) del proceso detectada.
- La solución propuesta deberá obtener visibilidad completa de la cadena de ataque y cambios maliciosos.
- La solución propuesta deberá permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos mientras mantiene el tiempo de disponibilidad del dispositivo.
- La solución propuesta deberá permitir la suscripción de servicios opcionales de detección y respuesta a incidentes (Ej.: Servicios gestionados de detección y respuesta).
- La solución propuesta deberá permitir el envío de ejecutables para su análisis a un sandbox , con la finalidad de determinar si son maliciosos o inofensivos.
- La solución propuesta deberá proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red.

- Control de Vulnerabilidades y Comunicación:
  - La solución propuesta deberá tener la capacidad para descubrir aplicaciones que se estén comunicando a través de la red y que estas representen riesgo al endpoint.
  - La solución propuesta deberá tener la capacidad para realizar un parche virtual, a través de la restricción de los accesos de comunicación en aquellas aplicaciones que sean vulnerables.
  - La solución propuesta deberá permitir la reducción de las superficies de ataque utilizando políticas proactivas de comunicación basadas en el riesgo de acuerdo a CVE y la calificación o reputación que puede tener una aplicación.
  - La solución propuesta deberá tener la capacidad para prevenir la comunicación a través de la red de cualquier aplicación no autorizada.
  - La solución propuesta deberá tener la capacidad para crear políticas que tengan la capacidad de prevenir la comunicación de aplicaciones de acuerdo con la versión de la aplicación instalada.
  - La solución propuesta deberá poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red.
  - La solución propuesta deberá poder entregar información sobre el uso de aplicaciones en red mostrando información como cuales dispositivos generan tráfico de una aplicación.

- La solución propuesta deberá poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos del tráfico generado por la aplicación.
- La solución propuesta deberá poder tener la capacidad de crear una lista de aplicaciones cuya ejecución será bloqueada. Esta lista deberá permitir la creación de políticas para su uso en grupos de estaciones de trabajo seleccionadas.

- Escenarios de Ataque:
  - La solución propuesta deberá identificar y prevenir los intentos de estalación de privilegios.
  - La solución propuesta deberá bloquear ataques de ransomware conocido.
  - La solución propuesta deberá detectar malware desconocidos como RAT (Remote Access Trojan) a través de las actividades del malware y no una firma.
  - La solución propuesta deberá proteger contra Scripts de Powershell maliciosos.
  - La solución propuesta deberá proteger contra Scripts de CScript maliciosos.
  - La solución propuesta deberá proteger contra macros de Office maliciosos.
  - La solución propuesta deberá tener control sobre dispositivos USB.
- IOT:
  - La solución propuesta deberá tener la capacidad de detectar dispositivos IOT no administrados en la red.
  - La solución propuesta deberá tener la capacidad de detectar dispositivos no administrados y protegidos por la solución con sistemas operativos macOS/Linux/Windows.
- Consola de Administración:
  - La solución propuesta deberá cumplir con los estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS).
  - La solución propuesta deberá cumplir con el estándar HIPAA.
  - La solución propuesta deberá cumplir con el estándar GDPR.
  - La consola de administración de la solución propuesta deberá permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.
  - La consola de administración de la solución propuesta deberá permitir el uso de autenticación de doble factor (2FA) para acceder a la misma.
  - La consola de administración de la solución propuesta deberá permitir la integración con SAML para la autenticación de los usuarios a la consola de gestión.

- La consola de administración de la solución propuesta deberá permitir el uso de roles granulares para los administradores.
- La consola de administración de la solución propuesta deberá permitir la gestión para ambientes Multi-inquilinos.
- La consola de administración de la solución propuesta deberá permitir la gestión a través de Full Restful API.
- La solución propuesta deberá poder ser gestionada en una arquitectura hibrida utilizando servicios en las premisas complementadas con otras en nube.
- La solución propuesta deberá poder ser gestionada en una arquitectura totalmente en las premisas del cliente con acceso a consultas a la base de inteligencia de amenazas en la nube sin necesidad de enviar archivos completos del organismo para su análisis.
- La solución propuesta deberá permitir la integración para realizar acciones en soluciones de terceros a través de scripts Python para accionar un API cuando ocurra un evento de seguridad.
- La consola de administración de la solución propuesta deberá permitir la visualización de los eventos registrados en los dispositivos que requieran atención.
- La consola de administración de la solución propuesta deberá permitir la visualización de la salud de los Agentes instalados.
- La consola de administración de la solución propuesta deberá permitir la desinstalación remota del Agente instalado en los dispositivos.
- La consola de administración de la solución propuesta deberá permitir la desactivación/activación remota del Agente instalado en los dispositivos.
- La consola de administración de la solución propuesta deberá permitir la actualización remota del Agente instalado en los dispositivos.
- La consola de administración de la solución propuesta deberá permitir la creación de reportes ejecutivos conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
- La consola de administración de la solución propuesta deberá permitir la creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás.
- La consola de administración de la solución propuesta deberá permitir la exportación de bitácoras locales generadas por los Agentes desde la misma consola.

- La consola de administración de la solución propuesta deberá permitir la creación de reportes de inventario sobre los Agentes desplegados conteniendo información como: Dirección IP, Hostname, Sistema Operativo, Dirección MAC, Versión de Agente instalada, Estado del Agente, último día visto por la consola.
- La consola de administración de la solución propuesta deberá permitir la visibilidad de eventos generados por los dispositivos o eventos de acuerdo con el proceso ejecutado.
- La consola de administración de la solución propuesta deberá permitir la integración de un SMTP externo para el envió de alertas a través de correo electrónico.
- La consola de administración de la solución propuesta deberá permitir las auditorías de cambios realizados por los administradores/operadores. Estas auditorías deberán poder ser además descargas en un formato CSV.
- La solución propuesta deberá requerir una contraseña para ser deshabilitado por una aplicación de tercero.
- La solución propuesta deberá permitir el aislamiento de un dispositivo a través de la integración de un NAC de acuerdo a la categoría del evento detectado.
- La solución propuesta deberá permitir agregar direcciones IP maliciosas detectadas en uno o más firewalls remotos integrados.
- La solución propuesta deberá permitir la configuración de perfiles sobre la información recolectada para la función de threat hunting.
- La solución propuesta deberá permitir exclusiones de información que no será recolectada dentro de la función de threat hunting.
- La solución propuesta deberá estar certificada por Microsoft como una solución de Antivirus y poder integrarse con Windows Security Center.
- La solución propuesta deberá permitir que los servicios en nube recategoricen la clasificación de un evento.
- La solución propuesta deberá permitir que los administradores deshabiliten las notificaciones de un evento de detección.
- La solución propuesta deberá permitir realizar funciones web filtering bloqueando el acceso a páginas web categorizadas como maliciosas.

Especificaciones técnicas SIEM

Características del equipamiento

- La solución deberá ser hardware appliance y soportar un total de 15.000 EPS.

- La solución deberá estar licenciada para al menos 6000 EPS, 1000 dispositivos.
- La solución deberá tener al menos 32GB de memoria.
- La solución deberá tener al menos 36TB de disco distribuido en no menos de 12 discos para HA.
- La solución deberá poseer como mínimo 4 interfaces con puertos GE RJ45.
- La solución deberá poseer la capacidad de desplegar nodos virtuales de recolección de eventos sin la necesidad de licenciamiento adicional. Permitiendo la virtualización en los siguientes hipervisores: VMware ESX, Microsoft Hyper-V, KVM.

Características Generales

- Debe tener una interfaz gráfica basada en WEB.
- Debe tener un control de acceso basado en roles enriquecidos para restringir el acceso a la GUI y datos en varios niveles.
- Debe tener toda la comunicación entre módulos protegida por HTTPS.
- Debe realizar un seguimiento completo de auditoría de la actividad del usuario.
- Debe tener autenticación de usuario flexible: local, externa a través de Microsoft AD y OpenLDAP, Cloud SSO SAML.
- Escaneo de red activo y pasivo.
- Inventario de activos.
- Inventario de servicios.
- La solución deberá tener la capacidad de realizar la integración nativa del tipo MESH con las soluciones de AntiMalware Avanzado, AntiSpam y SOAR que formen parte de la solución propuesta.

Funcionalidades mínimas Requeridas

- Gestión de vulnerabilidades:
  - Monitoreo continuo de vulnerabilidades.
  - Escaneo activo autenticado / no autenticado.
  - Verificación de remediación.
- Detección de Intrusiones:
  - Gestión de registros.
  - Visualización y análisis de las actividades de red NetFlow.
  - Supervisión de la disponibilidad del servicio.

- Análisis de protocolo de red/captura de paquetes.

- Gestión de eventos e incidentes:
  - Visualización de las actividades de registro.
  - Correlación de eventos.
  - Visualización de los incidentes.
  - Identificación de patrones de eventos que indiquen una posible amenaza o vulnerabilidad.
  - Determinar la magnitud del riesgo de los ataques o compromisos potencialmente dañinos.
  - Creación de informes con configuraciones del usuario.
- Panel de control:
  - Creación de dashboard con configuraciones del usuario.
  - Se requiere una plataforma del tipo Next Generation Security Information and Event Manager (Next Generation SIEM) que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura TI de la entidad.
  - La plataforma deberá colectar los eventos de seguridad de múltiples marcas para lo cual se deberá incluir el licenciamiento necesario para esto.
  - Debe tener una arquitectura que permita escalar la recolección de datos mediante la implementación de múltiples colectores.
  - Los colectores deberán poder almacenar eventos en el búfer cuando el Supervisor no está disponible.
  - Debe permitir el almacenamiento de logs en una base de datos de NoSQL o Elasticsearch con el fin de soportar grandes volúmenes de datos sin afectar la estabilidad de la solución.
  - Debe permitir el descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad. Esta información debe alimentar una base de datos de administración de configuraciones, la cual se debe mantener actualizada por medio de redescubrimientos programados.
  - La plataforma deberá tener la capacidad de comportarse como una herramienta del tipo CMDB.
  - Debe contar con un visor personalizado de log de tráfico.
  - Debe ser capaz de aprovechar una variedad de fuentes públicas y privadas de datos para enriquecer los datos fuente.

- Debe ser capaz de clasificar claramente los diferentes tipos de datos que recoge para ayudar en la analítica o consultas ad hoc por los analistas SOC. También Debe ser capaz de clasificar tales datos basados en su sensibilidad o protección requerida de seguridad/privacidad donde sea apropiado y también deberá ser capaz de agrupar datos similares.
- Debe proporcionar una capacidad nativa para recibir fuentes de inteligencia de amenazas de fuentes abiertas y comerciales.
- Debe ser capaz de realizar análisis en tiempo real basado en datos históricos dentro de la plataforma, y deberá proporcionar la capacidad de permitir el desarrollo de análisis personalizados y realizar análisis sin comprometer la velocidad o la estabilidad de la solución global.
- Debe ser capaz de generar alertas basadas en condiciones programadas de una variedad de análisis de seguridad, disponibilidad y rendimiento. También debe soportar varias maneras de comunicar estas alertas y proporcionar un flujo de trabajo para su investigación y confirmación.
- Debe proporcionar capacidades nativas para producir dashboards y análisis visuales predeterminados y personalizados para los consumidores típicos de SOC, así como proporcionar la capacidad de integrarse con soluciones de terceros que pueden proporcionar funciones similares a través de múltiples plataformas SOC.
- Debe proporcionar acciones correctivas manuales, secuenciadas y/o automatizadas sobre los controles de seguridad gestionados a través de la solución SIEM. Esto puede proporcionarse directamente a través del propio SIEM o a través de la integración con sistemas de gestión externos.
- Debe tener su propia herramienta de gestión de tickets y permitir la integración con herramientas de terceros: ConnectWise, ServiceNow, SalesForce y Remedy.
- Debe ser capaz de almacenar y administrar datos internos y de gestión de configuración dentro de las Bases de Datos de Gestión de Configuración (CMDB). Esto necesitará incluir una capacidad nativa pero también debe soportar la integración con plataformas CMDB de terceros.
- Debe incluir un análisis de anomalías en base a estadísticas y técnicas de aprendizaje automático.
- Debe poderse implementar de forma distribuida, de tal forma que los colectores sean independientes del motor de correlación, permitiendo que ante una caída del enlace que

comunica al motor de correlación, los eventos se puedan almacenar por un tiempo determinado.

- Debe tener la capacidad de correlacionar los eventos recibidos en memoria antes de escribir en disco, logrando así la capacidad de correlación en tiempo real.
- Debe contar con capacidad de monitoreo activo de disponibilidad de performance mediante el monitoreo contante de SNMP, servicios TCP, entre otros, de tal forma que permita generar estadificas de uso de recursos como CPU, memoria, tráfico de red, entre otros.

- Funcionalidades de monitoreo:
  - Debe tener la capacidad colectar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones.
  - Debe tener la capacidad de colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones.
  - Debe contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas.
  - Debe tener la capacidad de definir métricas customizadas.
  - Debe tener la capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada.
  - Debe monitorear las caídas e inicios de los sistemas vía Ping, SNMP, WMI, así como análisis del inicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage.
  - Debe hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos.
  - Debe proporcionar la capacidad de soportar solicitudes de información ad-hoc o programadas de la solución para satisfacer las necesidades de auditoría o cumplimiento.
  - Debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA 256.
  - Debe proporcionar reportes de auditoría y cumplimiento con plantillas de PCI, COBIT, SOX, ISO, ISO 27001, HIPPA, GLBA, FISMA, NERC, GPG13, SANS Critical Controls.
  - Debe proporcionar una arquitectura altamente escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en la producción.

- Debe soportar plataformas de desarrollo y lenguajes de programación para el desarrollo personalizado dentro de la solución y sus componentes tipo XML.
- Debe admitir el descubrimiento y la supervisión de estos servidores de aplicaciones: Apache, Tomcat, IBM WebSphere, Microsoft ASP.NET, Oracle GlassFish Server, Oracle WebLogic, RedHat JBOSS.
- Debe admitir la autenticación de los siguientes servidores para descubrimiento y monitoreo: Cisco Access Control Server (ACS), Cisco Identity Solution Engine (ISE), CyberArk Password Vault, CyberArk,.
- Debe admitir la configuración para enviar syslog en un formato específico para Fortinet FortiAuthenticator, Juniper Networks SteelBelted RADIUS, Microsoft Internet Authentication Server (IAS), OneIdentity Safeguard, Vasco DigiPass.
- Debe soportar las siguientes bases de datos para descubrimiento y monitoreo: IBM DB2 Server, Microsoft SQL Server, MySQL Server, Oracle Database Server.
- Debe soportar los siguientes servidores de DHCP y DNS para descubrimiento y monitoreo: Infoblox DNS/DHCP, ISC BIND DNS, Linux DHCP, Microsoft DHCP (2003-2008), Microsoft DNS (2003-2008).
- Debe soportar el siguiente servidor de directorio para descubrimiento y monitoreo: Microsoft Active Directory.
- Debe soportar el siguiente servidor de gestión de documentos para descubrimiento y monitoreo: Microsoft SharePoint.
- Debe soportar los siguientes servidores web de gestión para descubrimiento y monitoreo: Cisco Application Centric Infrastructure (ACI), Fortinet FortiManager.
- Debe soportar la siguiente aplicación de escritorio remoto para descubrimiento y monitoreo: Citrix Receiver (ICA).
- Debe soportar las siguientes herramientas de control de código fuente para la recopilación de registros a través de API: GitHub y GitLab.
- Debe soportar mínimamente los siguientes servidores VoIP para descubrimiento y monitoreo: Avaya, Cisco, Fortinet.
- Debe soportar los siguientes Servidores Web para descubrimiento y monitoreo: Apache Web Server, Microsoft IIS for Windows 2000 o 2003, Microsoft IIS for Windows 2008, Nginx Web Server.
- Debe soportar los siguientes servidores Blade para descubrimiento y monitoreo: Cisco UCS Server, HP BladeSystem.

- Debe soportar las siguientes aplicaciones Cloud para monitoreo: AWS Access Key IAM, Permissions and IAM Policies AWS CloudTrail API, AWS EC2, CloudWatch API, AWS RDS, Box.com, Cisco FireAMP Cloud, Google Apps Audit, Microsoft Azure Audit, Microsoft Office 365 Audit, Microsoft Cloud App Security, Microsoft Azure Advanced Threat Protection (ATP), Microsoft Windows Defender, Advanced Threat Protection (ATP), Okta, Salesforce CRM Audit.
- Debe soportar la siguiente consola de acceso de dispositivos para descubrimiento y monitoreo: Lantronix SLC Console Manager.
- Debe soportar las siguientes aplicaciones de antivirus y seguridad de host (HIPS) para descubrimiento y monitoreo: Cisco Security Agent (CSA), CloudPassage Halo, Crowdstrike, Digital Guardian, ESET NOD32 Anti- Virus, FortiClient, MalwareBytes, McAfee ePolicy Orchestrator (ePO), Sophos, Symantec, Trend Micro.
- Debe soportar los siguientes dispositivos para monitoreo: APC Netbotz Environmental Monitor, APC UPS, Generic UPS, Liebert FPC, Liebert HVAC, Liebert UPS.
- Debe soportar los siguientes Firewalls para descubrimiento y monitoreo: Cisco Adaptive Security Appliance (ASA), Dell SonicWALL Firewall, Fortinet FortiGate Firewall, Juniper Networks SSG Firewall, McAfee Firewall Enterprise (Sidewinder), Sophos UTM.
- Debe soportar los siguientes balanceadores de carga y firewalls de aplicaciones para descubrimiento y monitoreo: Citrix Netscaler Application Delivery Controller (ADC), F5 Networks Application Security Manager, F5 Networks Local Traffic Manager, F5 Networks Web Accelerator, Qualys Web Application Firewall.
- Debe ser compatible con las siguientes aplicaciones de monitoreo de gestión de cumplimiento de red: Cisco Network Compliance Manager, PacketFence Network Access Control (NAC).
- Debe soportar los siguientes sistemas de protección de intrusos IPS para descubrimiento y monitoreo: AirTight Networks SpectraGuard, Cisco FireSIGHT, Cisco Intrusion Protection System, Cisco Stealthwatch, Cylance Protect Endpoint Protection, Cyphort Cortex Endpoint Protection, FireEye Malware, Protection System (MPS), FortiDDoS, Fortinet FortiSandbox, IBM Internet Security Series Proventia, Juniper DDoS Secure, Juniper Networks IDP Series, McAfee IntruShield, McAfee Stonesoft IPS, Motorola AirDefense, Radware DefensePro, Snort Intrusion Protection System, Sourcefire 3D and Defense Center, TippingPoint Intrusion Protection System.

- Debe soportar los siguientes Security Gateways para descubrimiento y monitoreo: Barracuda Networks Spam Firewall, Blue Coat Web Proxy, Cisco IronPort Mail Gateway, Cisco IronPort Web Gateway, Fortinet FortiMail, Fortinet FortiWeb, McAfee Vormetric Data Security Manager, McAfee Web Gateway, Microsoft ISA Server, Squid Web Proxy, SSH Comm Security CryptoAuditor, Websense Web Filter.
- Debe soportar los siguientes servidores para descubrimiento y monitoreo: HP UX Server, IBM AIX Server, IBM OS400 Server, Linux Server, Microsoft Windows Server, Sun Solaris Server.
- Debe soportar los siguientes dispositivos de almacenamiento para descubrimiento y monitoreo: Brocade SAN Switch, Dell Compellant Storage, Dell EqualLogic Storage, EMC Clarion Storage, EMC Isilon Storage, EMC VNX Storage Configuration, NetApp Filer Storage, Nimble Storage, Nutanix Storage.
- Debe soportar detección de amenazas en ThreatConnect. Las siguientes fuentes de inteligencia de amenazas externas son soportadas: Emerging Threat, FortiGuard, FortiSandbox, Malware Domain, SANS, ThreatStream, ThreatConnect, TruSTAR, Zeus. En general cualquier fuente que provea un archivo CSV o que soporte STIC/TAXII standard.
- Debe soportar los siguientes servidores de virtualización para descubrimiento y monitoreo: HyperV, Hytrust CloudControl, VMware ESX.
- Debe soportar los siguientes VPN Gateway para descubrimiento y monitoreo: Cisco VPN 3000 Gateway, Cyxtera AppGate Software Defined Perimeter (SDP), Juniper Networks SSL VPN Gateway, Microsoft PPTP VPN Gateway, PulseSecure.
- Debe soportar los siguientes scanners de vulnerabilidades para descubrimiento y monitoreo: AlertLogic Intrusion Detection and Prevention Systems (IPS), McAfee Foundstone Vulnerability Scanner, Nessus Vulnerability Scanner, Qualys Vulnerability Scanner, Rapid7 NeXpose Vulnerability Scanner, Rapid7 InsightVM Integration, Tenable.io.
- Debe soportar los siguientes aceleradores de red WAN para descubrimiento y monitoreo: Cisco Wide Area Application Server, Riverbed SteelHead WAN Accelerator.
- Debe soportar los siguientes dispositivos de Wireless LAN para descubrimiento y monitoreo: Aruba Networks Wireless LAN, Cisco Wireless LAN, FortiAP, FortiWLC, Motorola WiNG WLAN AP.

3. ESPECIFICACIONES TÉCNICAS RENGLÓN 3

El adjudicatario deberá proveer una tecnología que posea las características especificadas a continuación para la detección y gestión de vulnerabilidades Web y de Infraestructura del Consejo de la Magistratura de la C.A.B.A.

Requerimientos generales

Será requisito que las tecnologías a proveer en el presente renglón 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.

El fabricante de las soluciones deberá contar con un puntaje no menor a 4.4 en Gartner Peer Insights de la tecnología denominada “Vulnerability Assessment”.

Cada oferente deberá contar con expresa autorización del fabricante para distribuir la solución y/o ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato.

Requerimientos de la solución

Características de licenciamiento

- Se requiere licenciamiento en modalidad suscripción por el período de treinta y seis (36) meses.
- La solución deberá ser provista en modalidad software, el cual será implementado en la infraestructura del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.
- Contar con la capacidad de realizar la detección y gestión de vulnerabilidades de hasta 2.000 activos.
- Contar con la capacidad de realizar la detección y gestión de vulnerabilidades en hasta 30 FQDNs.
- No deberá tener restricciones en la cantidad de motores de escaneo a desplegar.
- Capaz de instalar hasta 2.000 agentes en los hosts para la detección de vulnerabilidades.
- Capaz de permitir el descubrimiento ilimitado de activos en la red.

Características generales

- Capacidades de descubrimiento de activos, incluyendo servidores físicos y virtuales, dispositivos de comunicaciones, estaciones de trabajo, dispositivos móviles, sistemas en nube, etc.
- Análisis de vulnerabilidades cubriendo la inspección de más de 60.000 evaluaciones.
- Provisión de Informes y Análisis a nivel Dashboards, reportes prediseñados y personalizables.
- Ejecución de medidas a través del análisis de información de usuarios, configuración, activos y de red, registros de auditoría.
- Controles de configuraciones a efectos de validar violaciones de compatibilidad con estándares predefinidos.
- Consola de administración unificada para las características de infraestructura y web.
- Contar con motores de escaneo propios en la nube para la detección de vulnerabilidades desde entornos externos.
- Solución de gestión y escaneo en modalidad virtual appliance.
- Interfaz web de administración segura.
- Integración con sistemas del tipo LDAP para su autenticación.
- Administración de usuarios basados en roles. Mínimamente deberá proveer los siguientes roles:
    - Administrador Central.
    - Administrador de Organización.
    - Auditor.
    - Analista de Seguridad.
    - Analista de Vulnerabilidades.
    - Gestor de credenciales.
- Administración de Permisos. Mínimamente deberá proveer la gestión de los siguientes permisos:
    - Sobre el escaneo: creación de escaneos, políticas.
    - Sobre los activos.
    - Sobre el análisis: aceptación de riesgos, cambio en nivel de riesgos.
    - Sobre la organización que contiene activos a analizar.
    - Sobre los usuarios.
    - Sobre los reportes.
    - Sobre la actualización.

    - Sobre el flujo de trabajo.
- Integración con SMTP.
- Configuración de Proxy Web.
- Configuración de Syslog con niveles de Severidad, Información, Alarmas y Emergencias.
- Actualización programada de firmas y plugins de producto vía Web.
- Configuración de seguridad que incluya:
    - Timeout de sesión.
    - Intentos máximos de login.
    - Tamaño mínimo de password y complejidad.
    - Banner de inicio.
    - Deshabilitación de usuarios luego de un período de inactividad.
    - Compatibilidad con FIPS 140-2.
- Otras configuraciones:
    - Diagnóstico de sistema.
    - Logs de sistema.
    - Notificación de tareas a revisar en colas de trabajo.
    - Administración de llaves RSA/DSA para integración y autenticación entre las partes de la solución.
- Repositorios de bases de datos de vulnerabilidades ya sea local como externo.
- Integración con sistemas de Patch Management tales como:
    - Microsoft SCCM/WSUS.
    - Red Hat Network Satellite Server.
    - Symantec Altiris.
    - IBM TEM.
    - Dell Kace 1000.
- Provisión de cifrado mínimo de:
    - Credenciales locales en AES-256.
    - Comunicación entre scanners y consola de gestión SSL TLS 1.2.
    - Actualizaciones en SSL TLS 1.2.
- API de análisis para integrarse con otras tecnologías.

Descubrimientos de Activos y Escaneo de Vulnerabilidades

- Capacidad de uso mediante agentes instalados sobre los dispositivos a analizar o agent less (mediante scanner remoto).
- Gestión de activos descubiertos mediante organizaciones configurables. Las organizaciones podrán ser gestionadas por diversos administradores.
- Análisis de vulnerabilidades activo.
- Descubrimiento de vulnerabilidades sin credenciales.
- Descubrimiento de vulnerabilidades con credenciales, pudiendo usar para sistemas Windows:
    - Contraseñas.
    - Kerberos.
    - Hash LM/NTLM.
    - Password vaults de otros fabricantes (Cyberark/Thycotic).
- Descubrimiento de vulnerabilidades con credenciales, pudiendo usar para sistemas Linux/Unix/Cisco métodos SSH y posibilidades de configurar escalación de privilegios.
- Descubrimiento de vulnerabilidades con credenciales en bases de datos y uso de SNMP.
- Opciones de escaneo avanzadas:
    - Habilitación de chequeos que eviten impactar negativamente sobre los dispositivos a analizar.
    - Disminución de velocidad de análisis cuando se detecte congestión en el proceso.
    - Definición de chequeos máximos por host.
    - Definición de hosts máximos a analizar.
    - Definición de número de sesiones TCP concurrentes máximas por hosts.
    - Definición de numero de sesiones TCP concurrentes máximas por escaneo.
- Opciones de descubrimiento:
    - Uso de protocolos ARP, TCP, ICMP, UDP.
    - Validación de todos los puertos para encontrar servicios.
    - Habilitación/Deshabilitación de análisis sobre SSL.
    - Identificación de certificados próximos a expirar.
- Opciones de fuerza bruta:
    - Configuración de credenciales provistas por el usuario.
    - Uso de Hydra (www.thc.org) para análisis de fuerza bruta.
- Habilidad de escanear file system, especificando diferentes directorios como ser:
    - Systemroot.
    - ProgramFiles.

  - ProgramData.
  - UserProfiles.
  - Directorios Personalizados.
- Personalización de escaneos, incluyendo la posibilidad de calendarizarlos.
- Asignación de dispositivos a los escaneos en modalidad:
  - Dirección Ipv4/Ipv6.
  - Rango IP.
  - Subnet con nota CIDR.
  - Host a resolver.
  - Host a resolver con subnet.
  - Host a resolver con nota CIDR.
- Funciones programadas posteriores a la finalización de un escaneo, por ejemplo ejecutar reportes.
- Ventanas de tiempo donde se impide la ejecución de escaneos, por ejemplo horas productivas.
- Cobertura de diversos activos:
  - Dispositivos de redes: firewalls, routers, switches, printers, storage.
  - Auditoría de configuraciones de dispositivos de redes en modo offline.
  - Virtualización: VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server.
  - Sistemas Operativos: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries.
  - Bases de Datos: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB.
  - Aplicaciones Web: Web Servers, Web Services, vulnerabilidades OWASP.
  - Cloud: Escaneo de configuración de aplicaciones cloud como ser Salesforce, AWS, Azure, Rackspace.
  - Cumplimiento: auditoría de cumplimiento regulatorio.
- Provisión de políticas de base que posibiliten:
  - Descubrimiento de activos, hosts, servicios.
  - Escaneo de redes y puertos.
  - Auditoría de cumplimiento de políticas.
  - Auditorías del tipo SCAP y OVAL.
- Vistas de gestión de vulnerabilidades que contengan:

  - Vulnerabilidades acumuladas y mitigadas.
  - Sumario por IPs.
  - Sumario por activos.
  - Sumario CCE / CVE.
  - Sumario por DNS name.
  - Listas de Servicios, sistemas operativos, servidores SSH, clientes de mail, software, cliente web, server web.
  - Sumario boletines Microsoft.
  - Sumario de puertos, protocolos.
  - Sumario por severidad.
  - Lista de vulnerabilidades.
- Filtros de vulnerabilidades que contengan:
  - Riesgo aceptado.
  - Dirección IP.
  - Activo.
  - Archivo.audit.
  - ID CCE/CVE.
  - Score y Vector CVSS.
  - Referencia de vulnerabilidad.
  - Exploit disponible.
  - ID IAMV.
  - ID boletín Microsoft.
  - Mitigadas.
  - Parche publicado.
  - ID de vulnerabilidad.
  - Nombre de vulnerabilidad.
  - Tipo de vulnerabilidad.
  - Puerto/Protocolo.
  - Severidad STIG.
  - Política que la contiene.
- Gestión de vulnerabilidades mediante la aceptación del riesgo de las mismas, evitando así que las mismas sean desplegadas a nivel reportes.
- Análisis de score de riesgo basado en CVSS, 5 niveles de severidad.

- Priorización de resolución de vulnerabilidades basado en frameworks de exploit (Metasploit, Core Impact, Canvas, Exploit HUB).
- Análisis de vulnerabilidades sobre servers MDM del tipo ActiveSync, Apple Profile Manager, AirWatch, Good, Mobile Iron.
- Proveer mecanismos propios de priorización basados en información de inteligencia.

Escaneo de Vulnerabilidades Web

- Debe poder analizar vulnerabilidades en sitios que utilicen, al menos, los siguientes framworks:
    - HTML.
    - JavaScript.
    - AJAX.
    - HTML5.
    - SPA (Single-Page Application).
- Permitir la automatización de los escaneos de detección de vulnerabilidades web y minimizar el nivel de impacto en la aplicación.
- Brindar indicadores de ciber exposición con una visión externa.
- Identificar las vulnerabilidades de OWASP Top 10 y brindar recomendaciones para la mitigación del riesgo.
- Permitir la exclusión de funciones críticas de la aplicación por medio de URLs o extensiones de archivo.
- Permitir la detección de problemas de configuración:
    - Escaneo SSL/TLS para identificar certificados inválidos, vencidos o emitidos incorrectamente.
    - Auditoria de configuraciones en las respuestas a las llamadas HTTP para limitar la información proporcionada ante un reconocimiento.
- Permitir la exclusión de funciones críticas de la aplicación por medio de URLs o extensiones de archivo.
- Identificar vulnerabilidades en componentes de terceras partes, como pueden ser web servers o Content Management Systems (CMS).
- Permitir implementar mecanismos de autenticación:
    - Autenticación basada en formularios.
    - Autenticación basada en cookies.

- Autenticación basada en Selenium.
- NTLM.

Tableros, Reportes e Informes

- Proveer dashboards ejecutivos, técnicos y de tendencia.
- Posibilidad de gestionar los dashboards, editando los mismos y generando nuevos.
- Determinar reportes de seguridad evolutivos que brinden un estado general de toda la infraestructura, logrando así conocer la postura de seguridad con respecto a diferentes cuestiones, como ser:
  - Mantenimiento de inventario de software y hardware.
  - Resolución de vulnerabilidades y malas configuraciones.
  - Despliegue de una red en forma segura.
  - Búsqueda de malware e intrusos.
- Capacidad de agregar nuevos reportes de seguridad evolutivos.
- Reportes en formato, PDF, RTF y CSV.
- Proveer templates de reportes:
  - Ejecutivos.
  - De Monitoreo.
  - Tendencia.
  - Descubrimiento.
  - Cumplimiento y Control de Configuraciones.
  - Reportes CIS para MySQL, Microsoft SQL, Oracle, IIS, VmWare ESXi, Apple, Apache, IBM, Linux, Unix, RedHat, Microsoft Windows, JunOS, Docker, Cisco, CentOS.
- Posibilidad de generar reportes personalizados que incluya:
  - Tipo de Reporte (PDF, RTF).
  - Página de presentación, índice, encabezado y pie de página.
  - Cifrado de archivo PDF.
  - Gráficos de barras, tortas, líneas, aéreas, etc.
- Capacidad de importar y exportar reportes.

Análisis de Malware

- Escaneos de Malware, incluyendo detección de malware específicos. Escaneo de File System, búsqueda de hashes MD5, etc.

Ejecución de Medidas y Riesgos

- Posibilidad de aceptar el riesgo de una vulnerabilidad mediante reglas, a los efectos de que la misma en un futuro sea apartada de los análisis.
- Posibilidad de modificar el nivel de riesgo de una vulnerabilidad.
- Emisión de alertas mediante uso de flujos de trabajo que posibiliten:
    - Asignar un ticket a un usuario.
    - Enviar un mail.
    - Enviar mensaje a un syslog server.
    - Ejecutar un escaneo.
    - Crear un reporte.

Control de Configuraciones

- Capacidad de utilizar configuraciones de auditoría a los efectos de validar que los activos estén configurados de acuerdo con estándares de seguridad predefinidos (PCI, Sarbanes Oxley, NIST, etc) o personalizados.
- Capacidad de utilizar archivos SCAP para validar control de configuraciones.
- Ejecución de auditorías de cumplimiento mediante el análisis de la configuración de los siguientes sistemas:
    - Bluecoat.
    - Adtran.
    - Brocade.
    - Cisco IOS.
    - Checkpoint.
    - Citrix.
    - Databases.
    - Extreme.
    - FireEye.
    - FortiGate.
    - HP Procurve.
    - Huawei VRP.
    - IBM iSeries.
    - Juniper.
    - NetApp.

  - Palo Alto.
  - Red Hat.
  - Unix.
  - VmWare.
  - Windows/Windows File Contents.
- Cumplimiento con FISMA, CyberScope, GLBA, HIPAA, NERC, SCAP, SOX.
- Auditoría de configuraciones CERT, CIS, COBIT/ITIL, DISA, STIG, FDCC, ISO, NIST, NSA, PCI.
- Auditoría de contenido sensible.

4. ESPECIFICACIONES TÉCNICAS RENGLÓN 5

El adjudicatario deberá proveer una tecnología que posea las características especificadas a continuación para la gestión de identidades de usuarios y privilegios de éstos para las cuentas administradas por el Consejo de la Magistratura de la C.A.B.A.

Requerimientos generales

- Los oferentes deberán ser un canal debidamente aprobado por el fabricante, por lo que se requiere la presentación de una carta de autorización a presentar oferta.
- Será requisito que las tecnologías a proveer en el presente renglón 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.
- El fabricante de las soluciones deberá contar con un puntaje no menor a 4.5 en Gartner Peer Insights de las siguientes tecnologías:
  - Access Management.
  - Privileged Access Management.
- Los oferentes deberán contar con expresa autorización del fabricante para distribuir el equipamiento ofertado y ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato.

Requerimientos de la solución

Características de licenciamiento

- Se requiere licenciamiento en modalidad suscripción por el período de treinta y seis (36) meses.
- Administrar las identidades de cinco mil (5.000) usuarios internos del Consejo de la Magistratura de la C.A.B.A.
- Administrar las identidades de cinco mil (5.000) usuarios de organismos externos que se integran con el Consejo de la Magistratura de la C.A.B.A.
- Administrar las identidades de cincuenta mil (50.000) usuarios finales que consumen los servicios brindados por el Consejo de la Magistratura de la C.A.B.A.

Características de gestión del ciclo de vida de la Identidad

- Debe proporcionar no sólo la capacidad de autenticación, sino también el aprovisionamiento de identidades en aplicaciones SaaS, cubriendo al menos el aprovisionamiento con plantillas listas en el catálogo para:
    - Office 365.
    - G Suite.
    - Webex.
    - Adobe Sign.
    - Amazon Web Services.
    - Docusign.
    - Salesforce.
    - ServiceNow.
    - Zendesk.
- La solución deberá proporcionar una interfaz para la administración de identidades de dominio (SCIM) para la creación automatizada de identidades en el directorio nativo de la solución y proporcionar documentación detallada para ella. La interfaz deberá ofrecer mínimamente:
    - Operaciones de creación, lectura, actualización y ordenación en objetos de tipo de usuario.
    - Operaciones de creación, lectura, actualización y ordenación en objetos de grupo.
- La solución deberá tener la capacidad de realizar el aprovisionamiento en aplicaciones que admiten interfaces de administración de identidades de dominio a dominio (SCIM), el estándar de mercado para las aplicaciones entregadas en el modelo SaaS para el aprovisionamiento de identidades.

Características de autenticación adaptativa y simplificada (Single Sign On)

- La solución deberá proporcionar un catálogo de aplicaciones web con modelos de configuración de inicio de sesión único (SSO) que contengan al menos 1000 tipos de las aplicaciones más conocidas del mercado, con el fin de facilitar la configuración de estas integraciones.
- La solución deberá permitir la configuración de las aplicaciones web mínimamente a través de los siguientes protocolos y métodos:
    - SAML 2.0.
    - OpenID connect.
    - Oauth 2.0 modo client.
    - Oauth 2.0 modo server.
    - WS-Federation.
    - NTLM.
    - HTTP Basic.
    - Extensión en el navegador para capturar aplicaciones web que utilizan el formulario con el usuario y la contraseña y realizar la finalización automática del inicio de sesión y la contraseña de forma automatizada. Esta información deberá almacenarse de forma segura en la solución para la finalización automática en futuros inicios de sesión en estas aplicaciones.
- Admitir SSO a través de la autenticación integrada de Windows (IWA) que reutiliza el inicio de sesión de red para la autenticación en aplicaciones web, sin necesidad de introducir el usuario y la contraseña de nuevo.
- Permitir la personalización de respuestas SAML, como la asignación de atributos de directorio a atributos SAML, la capacidad de incluir lógica compleja para controlar las respuestas SAML y habilitar la visualización de la respuesta SAML configurada antes de su implementación.
- La solución deberá proporcionar un portal WEB para el usuario final con las siguientes características:
    - Después de iniciar sesión deberá presentar las aplicaciones web disponibles para realizar el SSO, a través de un conjunto de iconos donde cada uno representa una aplicación que el usuario tiene el derecho de realizar el SSO.
    - Realice cambios en los atributos de identidad, como el teléfono celular, el correo electrónico y la foto.

  - Compruebe sus actividades de identidad a través del panel de control con la siguiente información:
    - Total de inicios de sesión.
    - Total de errores de inicio de sesión.
    - Geolocalización de sus inicios de sesión.
    - Compruebe la geolocalización actual de sus dispositivos registrados.
    - Uso de aplicaciones.
    - Historial de eventos importantes, como una nueva aplicación agregada a su portal de SSO, errores de inicio de sesión, entre otros.

- Debe tener servicio de directorio para almacenar identidades en la solución, sin depender de la sincronización con otros servicios de directorio on-premise o en la nube de terceros.
- El servicio de directorio de soluciones deberá tener la capacidad de ampliar su esquema configurando atributos personalizados para satisfacer requisitos empresariales complejos.
- El servicio de directorio de soluciones deberá ser autoescalable para admitir millones de identidades y miles de atenciones simultáneas.
- Debe tener la capacidad de forzar la complejidad de las contraseñas mínimamente a los siguientes requisitos:
  - Tamaño mínimo.
  - Tamaño máximo.
  - Requiere dígitos mínimos.
  - Requiere letras mayúsculas y minúsculas.
  - Requiere una función especial (símbolo).
  - Limitar caracteres consecutivos.
  - Forzar la expiración de las contraseñas en función de su edad.
  - Guardar historial de contraseñas para evitar la reutilización.
- Proporcionar una notificación para la expiración de las contraseñas por correo electrónico.
- Capturar errores de inicio de sesión repetidos para el bloqueo de usuarios.
- La solución también deberá admitir la integración con los servicios de directorio en la nube y on-premises, lo que deberá admitir mínimamente:
  - Microsoft Active Directory.
  - Microsoft Azure AD.

  - Directorio de Google.
  - Directorios LDAP.

- Las integraciones con un directorio de terceros no deberán sincronizarse con estas bases de datos, es decir, cargar todo el directorio configurado en la nube, la solución deberá actuar como intermediario entre los servicios de directorio de terceros y la solución.
- La solución deberá integrarse con proveedores de identidad social con el fin de autenticar delegados a dichos proveedores y cumplir los requisitos empresariales potenciales, apoyando mínimamente a los siguientes proveedores:
  - Google.
  - Facebook.
  - Linkedin.
  - Microsoft.
- La solución deberá tener la capacidad de configurar LOS PROVEEDORES DE IDENTIDAD (IDP) de los terceros afines al Consejo de la Magistratura de la C.A.B.A. para dar acceso a identidades federadas en aplicaciones propias sin necesidad de crear una nueva identidad en la infraestructura, a través de la federación realizada a través del protocolo SAML.

Características de Autenticación Adaptativa y Multifactor (MFA) para Usuarios Internos (5.000)

- La solución deberá ser capaz de cumplir mínimamente los siguientes casos de uso para solicitar uno y más factores de autenticación:
  - Aplicaciones web integradas en la autenticación simplificada - funciones SSO.
  - En las pantallas de inicio de sesión y desbloqueo de los sistemas operativos Windows y MacOs.
  - Autenticación multifactor para soluciones VPN a través de RADIUS o SAML.
  - Cualquier dispositivo o sistema operativo que admita RADIUS.
  - Complemento para ADFS (IDP, proveedor de identidad), servicios de federación de Active Directory.
  - A petición mediante el protocolo Oauth y las API de REST.
  - Para realizar el restablecimiento de contraseña de servicio automático o desbloqueo de usuario.

- La solución deberá ser capaz de ofrecer mínimamente los siguientes métodos para múltiples factores de autenticación:
    - Usuario y contraseña de los directorios admitidos en la solución.
    - A través de la aplicación móvil iOS y Android, que ofrece soporte para:
    - Biometría FaceID.
    - Biometría a través del lector digital.
    - Inserción de smartphone (notificación para aprobar o rechazar una autenticación).
    - Geolocalización a través de GPS coordenadas e IDatabase.
    - Suporte tokens OATH OTP.
    - Autenticación en la pantalla de inicio de sesión a través de QRcode (Passwordless) sin necesidad de introducir el usuario y la contraseña, con la opción de forzar la biometría en el dispositivo móvil.
    - Llamada telefónica solicitando un PIN configurado previamente.
    - Mensaje de texto SMS que ofrece el código para la entrada manual y también una URL única presente en el mensaje de texto que ofrece la opción de aprobar o rechazar la autenticación sin la necesidad de introducir el código manualmente.
    - Confirmación de código por correo electrónico.
    - Clientes de Oath OTP (por ejemplo, Google Authenticator).
    - Autenticadores que admiten FIDO2/U2F, que admiten mínimamente:
        - Windows Hello.
        - Yubikey.
        - Google Titan Key.
        - MacOS TouchID.
    - Preguntas y respuestas previamente configuradas.
- Para cada caso de uso o conjunto de casos de uso de varios factores de autenticación citados, la solución puede identificar los atributos de contexto de cada autenticación para proporcionar los métodos mejor definidos para la autenticación, lo que admite mínimamente:
    - Direccionamiento IP.
    - Día de la Semana.
    - Fechas específicas.
    - Ventanas de tiempo entre dos fechas.

  - Ventanas de tiempo entre horas (por ejemplo, horario laboral).
  - Tipo de sistema operativo.
  - Tipo de navegador.
  - Perfiles configurados en la solución.
  - País de acceso.
  - Si es un dispositivo administrado.
  - Autenticación a través del certificado.
  - Nivel de riesgo de autenticación medido por un motor de análisis de comportamiento del usuario.

- La solución deberá ser capaz de detectar casos de uso y perfiles de autenticación ya validados por los usuarios y ya no solicitarlos durante un período de tiempo configurado por el administrador de la solución, evitando así validaciones repetidas en un corto período de tiempo.
- El conjunto de factores de autenticación disponibles deberá basarse en el acceso a través de las reglas especificadas en el elemento anterior y segregadas por:

  - Suite de aplicaciones.
  - Una sola aplicación.
  - Reglas para el restablecimiento de contraseña de autoservicio y el desbloqueo del usuario.
  - Portal de Administrador.
  - Portal de usuarios.

- La solución deberá proporcionar un portal WEB para el usuario final con las siguientes características:

  - Permitir al usuario realizar el registro automático de sus factores de autenticación, como preguntas y respuestas, tokens FIDO2, OATH OTP, establecer PIN para llamada telefónica, TouchID, FaceID, Windows Hello, entre otros.
  - Permitir que el usuario redirija la autenticación multifactor a otros usuarios (siempre y cuando se permita).
  - Permitir a los usuarios administrar sus dispositivos inscritos mínimamente:
  - Smartphones Android e IOS.
  - Sistemas operativos Windows y MacOS.

  - Para cada dispositivo registrado, los usuarios deberán tener las siguientes capacidades de administración:
  - Deshabilite SSO de forma remota.
  - Habilite SSO de forma remota.
  - Realizar el registro automático de nuevos dispositivos móviles.

- La solución deberá proporcionar una aplicación móvil para Android e IOS con las siguientes características:
  - Después de iniciar sesión presente las aplicaciones web disponibles para realizar el SSO, a través de un conjunto de iconos donde cada uno representa una aplicación que el usuario tiene el derecho de realizar el SSO ya integrado con los navegadores instalados en dispositivos móviles.
  - Proporcionar el inicio de sesión a través del análisis de QRcode en el portal web que deberá permitir SSO sin ID de usuario y contraseña (Passwordless).
  - Configure OATH OTP adicional de otras soluciones.
  - Configure OATH OTP para la autenticación multifactor en sistemas operativos Windows y MacOS (pantallas de inicio de sesión y bloqueo) cuando se desconectan de Internet.
  - Compruebe los dispositivos registrados (dispositivos móviles y sistemas operativos).
  - Integración nativa con FaceID, TouchID, lector biométrico de dispositivos móviles que los aprovechan para la autenticación biométrica durante el inicio de sesión en aplicaciones.
  - Reporte coodernadas GPS a sistemas que utilicen geolocalización.
  - Detectar ROOT en dispositivos Android y Jailbreak en dispositivos IOS con el propósito de detectar actividad maliciosa y como consecuencia la aplicación está deshabilitada para su uso.

- La aplicación deberá admitir la autenticación de tipo de inserción, donde el usuario tiene la opción de aceptar o rechazar el desafío, esta notificación contiene mínimamente:
  - Acceso a la IP de origen.
  - Fecha y hora.
  - Geolocalización ciudad/acceso.
  - Aplicación a la que se accede.

5. ESPECIFICACIONES TÉCNICAS RENGLONES 2, 4 Y 6

El oferente deberá proveer un servicio de garantía y soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en los renglones 1, 3 y 5, por el plazo de treinta y seis (36) meses desde la entrega e implementación de las soluciones.

Servicio de soporte técnico reactivo/proactivo

- El servicio de soporte técnico deberá brindarse al personal del Consejo de la Magistratura. El Consejo de la Magistratura, suministrará al adjudicatario una lista con la identificación de aquellas personas que se encuentran autorizadas a reportar incidentes o solicitar el soporte.
- Ante cada evento de soporte técnico el adjudicatario deberá realizar y presentar al Consejo de la Magistratura, si éste así lo requiriese, un informe que contendrá como mínimo la siguiente información:
    - Descripción detallada del problema, su causa y solución.
    - Documentación adjunta de los cambios hechos.
    - Recomendaciones.
    - Fecha y hora de resolución.
- Cada vez que se genere una solicitud de soporte técnico, según lo establecido en las cláusulas precedentes, el Adjudicatario deberá entregar un número de orden registrable por tal reclamo en el que deberá dejarse constancia cómo mínimo, de la fecha y horario en el que se realizó tal orden y el problema reportado.
- Las resoluciones a los problemas e incidentes reportados deberán ser informadas (por cualquier medio) al Consejo de la Magistratura por el personal del proveedor que brinde el soporte técnico en el menor tiempo posible. El personal del Consejo de la Magistratura verificará la solución propuesta por el proveedor y evaluará el resultado. Si el resultado es satisfactorio se considerará el incidente como solucionado, en caso contrario se considerará el incidente como pendiente de solución.
- El servicio de soporte técnico no podrá ser modificado bajo ningún concepto de forma tal que se vea afectado el nivel de los servicios exigidos en estas especificaciones y comprometidos en la oferta.
- Si alguno de los productos objeto del contrato tuviese fecha de discontinuidad o si alguno de los servicios contratados tuviese fecha de vencimiento de soporte durante la vigencia del contrato, el Adjudicatario deberá, además de informarlo en forma escrita al Consejo de la

Magistratura, asumir el compromiso de continuar con el servicio contratado, sin limitaciones o condicionantes, hasta la fecha de finalización del contrato.

- 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.
- Este servicio de garantía y soporte técnico deberá incluir como mínimo:
    - El reemplazo de equipos/partes que presenten fallas:
    - El soporte técnico local 7x24 para diagnóstico de fallas:
    - La posibilidad de actualizar el firmware/software a la última versión disponible.
    - 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.
    - La movilización del personal o cualquier costo asociado que surgiera del servicio a prestar correrá por exclusiva cuenta del adjudicatario para cada vez que se requiera.
    - Los requerimientos se podrán efectuar telefónicamente, por correo electrónico o vía web. 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.
    - No deberá existir un límite en el número de casos de soporte que puede solicitar el Consejo de la Magistratura de la C.A.B.A.
    - 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.
- Los Oferentes deberán presentar, para la solución que proponen, un contrato de nivel de servicio. Se deja constancia que éste último no forma parte del criterio de evaluación. A tales efectos se deberá tener presente los siguientes grados de severidad:
    - **Grados de severidad de la solicitud:** Las solicitudes se clasificarán en grados de severidad en función del impacto de las mismas sobre el funcionamiento del sistema.

SEVERIDAD 1	El software/hardware no está disponible presentando interrupción parcial o total de los servicios críticos (*).
SEVERIDAD 2	El software/hardware está disponible con una o más funcionalidades críticas (*) inoperantes.
SEVERIDAD 3	El software/hardware está disponible, pero con problemas no críticos en sus funcionalidades.
SEVERIDAD 4	El software/hardware está disponible, pero presenta problemas que no hay impacto significativo; dudas o consultas de la operación del sistema, módulo de emisión de reportes entre otros.

(*) Funcionalidades críticas son las que interfieren con los procesos de aseguramiento (atención de reclamos), provisión, relacionados en forma directa con el servicio comprometido con el cliente (SLA).

- **Tiempos de atención/resolución de las solicitudes**: En función del grado de Severidad de la solicitud se le asociará una prioridad relacionada con los tiempos de atención y resolución de la misma. En la siguiente tabla se detallan los tiempos que el proveedor deberá comprometer.

SLA	SEVERIDAD 1	SEVERIDAD 2	SEVERIDAD 3	SEVERIDAD 4
Tiempo de respuesta del registro de la Solicitud	15 minutos	30 minutos	60 minutos	60 minutos
Tiempo Solución Temporal	12 horas	24 horas	72 horas	--

Tiempo Solución Definitiva	40 horas	80 horas	1 mes	A convenir (por ejemplo: próximo releáse)

- **Niveles de Servicios:** Los niveles de servicio indican el porcentaje que los tiempos de atención se mantienen dentro de los límites estipulados para cada grado de severidad. A saber;

GRADOS DE SEVERIDAD		
Grado 1	**Grado 2**	**Grado 3 y 4**
90%	**85%**	**80%**

Servicio de actualización tecnológica

- Se entenderá que ha ocurrido una actualización tecnológica cuando se presente una nueva versión o release del/los mismo/s producto/s objeto de este contrato en el mercado, así como también reparaciones disponibles (en general denominadas comercialmente como patches, temporary fixes, etc.) para la generalidad de los clientes.
- Se deberán entregar sin cargo adicional todas las actualizaciones tecnológicas que, según se indica en la definición anterior, sean liberadas al mercado durante la vigencia del contrato.
- Las actualizaciones tecnológicas de los productos de software deberán estar disponibles para el Consejo de la Magistratura dentro de los treinta (30) días de liberadas al mercado.
- La obligación del adjudicatario en la entrega de actualizaciones tecnológicas surgidas dentro del período de contrato no se extinguirá con la finalización del mismo, sino hasta la efectiva entrega de las actualizaciones liberadas durante el período de contrato.

6. ESPECIFICACIONES TÉCNICAS RENGLÓN 7

Servicio de implementación

El adjudicatario deberá realizar la implementación 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.

7. ESPECIFICACIONES TÉCNICAS RENGLÓN 8

El adjudicatario deberá brindar el servicio de capacitación oficial de todas las soluciones provistas en los Renglones 1, 3 y 5, las 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 Ciudad Autónoma de Buenos Aires.

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.