RESO SAGYP N° 536/24

Buenos Aires, 24 de octubre del 2024

VISTO:

El TAE A-01-00023603-5/2024 caratulado *"Plan integral de seguridad informática segunda etapa" y;*

CONSIDERANDO:

Que por la actuación TAE citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, por la contratación de la Segunda Etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, 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, la mentada Dirección General propuso cláusulas para incorporar en los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, además de acompañar el cuadro de presupuesto oficial (v. Nota Dirección DGIYT 660/24 y Adjuntos 115801/24, 115804/24 y 115807/24).

Que, en ese marco, la Dirección General de Compras y Contrataciones entendió viable el llamado a Licitación Pública, de etapa única, bajo la modalidad de llave en mano, conforme lo dispuesto en los artículos 26, 28, 32, 33, 40 y 45 y concordantes de la Ley Nº 2.095 (texto consolidado según Ley Nº 6.588), la Resolución CM Nº 276/2020 y la Resolución SAGyP N° 30/2021 (v. Adjunto 124028/24).

Que en tal entendimiento, la Dirección General de Compras y Contrataciones elaboró los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran vinculados como Adjuntos 154207/24 y 154209/24 y estableció como presupuesto oficial la suma de dólares estadounidenses cinco millones ochocientos siete mil (U$S 5.807.000.-). Asimismo,

elevó lo actuado a esta Secretaría y recomendó que *"la adquisición de los Pliegos correspondientes proceda mediante el pago de la suma de Pesos Cuatrocientos Mil ($ 400.000.-), para participar en la Licitación Pública N° 2-0036-LPU24"* (v. Memo DGCC 1980/24).

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

Que en atención a los antecedentes antes relatados, de acuerdo a lo actuado por la Dirección General de Compras y Contrataciones, a lo solicitado por la Dirección General de Informática y Tecnología sobre la necesidad de impulsar la contratación de marras para garantizar el normal funcionamiento del Poder Judicial de la Ciudad Autónoma de Buenos Aires, y en línea con lo dictaminado por la Dirección General de Asuntos Jurídicos, corresponde aprobar los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, vinculados como Adjuntos 154207/24 y 154209/24, y llamar a Licitación Pública N° 2-0036-LPU24, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la contratación de la Segunda Etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, 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 ochocientos siete mil (U$S 5.807.000.-), para el día 8 de noviembre de 2024 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Que en consecuencia, resulta oportuno instruir a la Dirección General de Compras y Contrataciones a efectos de que instrumente las medidas correspondientes para dar curso a la Licitación Pública N° 2-0036-LPU24, y realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.588), su reglamentación y en la Ley de Procedimientos Administrativos -Decreto 1.510/97- (texto consolidado según Ley N° 6.588).

Que en cumplimiento de la Ley N° 70 (texto consolidado según Ley N° 6.588), la Dirección General de Programación y Administración Contable tomó conocimiento y realizó la afectación y compromiso presupuestario correspondiente para hacer frente la contratación de marras (v. Adjunto 151700/24 y 151707/24)

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 13304/2024.

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

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

Artículo 1º: Apruébanse los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, que como Adjuntos 154207/24 y 154209/24 forman parte de la presente Resolución, que regirán la Licitación Pública N° 2-0036-LPU24, de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la contratación de la Segunda Etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, 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 ochocientos siete mil (U$S 5.807.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0036-LPU24, de etapa única, bajo la modalidad de llave en mano, fijándose como fecha límite para la presentación de ofertas y la apertura pública de ofertas para el día 8 de noviembre de 2024 a las 11:00 horas, o el día hábil siguiente a la misma hora si resultara feriado o se decretara asueto.

Artículo 3º: Establézcase que la adquisición de los pliegos necesarios para cotizar en la Licitación Pública N° 2-0036-LPU24, será por un monto de pesos cuatrocientos mil ($400.000.-)

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0036-LPU24, al Dr. Matías Vázquez y la Dra. Javiera Graziano como miembros titulares, y a los Dres. Hernán Labate y Adrián Costantino 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° 2-0036-LPU24, y para que realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.588) su reglamentaria Resolución CM N° 276/2020 y en la Ley de Procedimientos Administrativos - Decreto 1.510/97- (texto consolidado según Ley N° 6.588).

Artículo 6°: Publíquese en la página web del Consejo de la Magistratura y en el Boletín Oficial del Gobierno de la Ciudad Autónoma de Buenos Aires, comuníquese por correo electrónico oficial a los titulares de las Dirección 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

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

LICITACION PÚBLICA 2-0036-LPU24

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA SEGUNDA ETAPA

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 la Segunda Etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, 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 para la presente contratación asciende a la suma total de **Dólares Estadounidenses Cinco Millones Ochocientos Siete Mil (U$S 5.807.000.-)**, el cual se compone de la siguiente manera:

Renglón 1: Dólares Estadounidenses Un Millón Doscientos Cuarenta y Cinco Mil (U$S 1.245.000.-).

Renglón 2: Dólares Estadounidenses Dos Millones Trescientos Cuarenta Mil (U$S 2.340.000.-).

Renglón 3: Dólares Estadounidenses Doscientos Mil (U$S 200.000.-).

Renglón 4: Dólares Estadounidenses Cuatrocientos Treinta y Dos Mil (U$S 432.000.-).

Renglón 5: Dólares Estadounidenses Doscientos Treinta Mil (U$S 230.000.-).

Renglón 6: Dólares Estadounidenses Quinientos Setenta y Seis Mil (U$S 576.000.-).

Renglón 7: Dólares Estadounidenses Treinta Mil (U$S 30.000.-).

Renglón 8: Dólares Estadounidenses Cincuenta y Cuatro Mil (U$S 54.000.-).

Renglón 9: Dólares Estadounidenses Quinientos Mil (U$S 500.000.-).

Renglón 10: Dólares Estadounidenses Doscientos Mil (U$S 200.000.-).

4. RENGLONES A COTIZAR

Renglón 1: Provisión de soluciones de threat intelligence, sandboxing, NGN Firewall y ampliación de la solución antimalware avanzado FortiEDR conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Provisión de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en el Renglón 1, 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 para la detección y gestión de vulnerabilidades en ambientes de Directorio Activo y ampliación de la solución de gestión de vulnerabilidades de Infraestructura Tenable SC, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 4: Provisión de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en el Renglón 3, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 5: Provisión de tecnología para ambiente de testing/laboratorio de gestión de identidades de usuarios del fabricante CyberArk y privilegios de éstos para las cuentas administradas por el Consejo de la Magistratura de la C.A.B.A., conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 6: Provisión de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones

provistas en el Renglón 5, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 7: Provisión de tecnología para una solución de resguardo de configuraciones de dispositivos de seguridad y comunicaciones multimarca, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 8: Provisión de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en el Renglón 7, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 9: Provisión de servicio de implementación para las soluciones provistas en los renglones 1, 3, 5 y 7, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 10: Provisión de servicio de capacitación para las soluciones provistas en los renglones 1, 3, 5 y 7, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

5. PLIEGOS

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

El valor de los Pliegos asciende a la suma de **Pesos Cuatrocientos Mil ($ 400.000.-)** y podrá abonarse mediante depósito en efectivo o por transferencia bancaria a la Cuenta Corriente $ N° 000306800050213214, a nombre del Consejo de la Magistratura, en el Banco de la Ciudad de Buenos Aires, Sucursal Nº 52, sita en Av. Presidente Roque Sáenz Peña 541 de esta Ciudad, CBU 0290068100000502132146, CUIT 30-70175369-7.

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

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

6. PLAZOS DE LA CONTRATACIÓN

6.1 Plazo 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 Ejecución Renglones 1, 3, 5 y 7:

El plazo máximo de provisión 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 Ejecución Renglón 9:

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

6.4 Plazo de Ejecución Renglones 2, 4, 6, 8 y 10:

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 de las soluciones solicitadas.

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. REPRESENTACIÓN OFICIAL. GARANTÍA TÉCNICA

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.

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

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

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

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

9. CONDICIONES PARA SER OFERENTE

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

1. En el caso de las personas humanas en forma individual, deberán cumplirse

los

requisitos contemplados en el Art. 89º de la Ley 2095 (Texto consolidado por Ley Nº 6.588)

2. En el supuesto de presentarse una sociedad, deberán cumplirse los requisitos contemplados en el Art. 89º de la Ley 2095 (Texto consolidado por Ley Nº 6.588) y los detallados a continuación:

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

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

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

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

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

1. El compromiso de mantener la vigencia de la U.T., por un plazo superior a la duración de la contratación, incluyendo una eventual prórroga contractual.
2. El compromiso de mantener la composición de la U.T. durante el plazo mencionado en el inciso anterior, así como también de no introducir modificaciones en los estatutos de las empresas integrantes que importen una alteración de la responsabilidad, sin la previa aprobación del Consejo.
3. Designación de uno o más representantes legales que acrediten, mediante

poder para actuar ante la administración pública, facultades suficientes para obligar a su mandante.

4. De los documentos por los que se confieran los poderes y por los que se

   constituya la U.T., deberá resultar que los otorgantes o firmantes lo hicieron legalmente, en ejercicio de las atribuciones que les corresponden como autoridades de cada una de las empresas en funciones, en el momento del acto respectivo.

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

10. DECLARACIONES JURADAS

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

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

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

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

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

12. CORREO ELECTRONICO Y CONSTITUCIÓN DE DOMICILIO

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

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

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

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

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

13. INFORMACIÓN SOCIETARIA Y HABILIDAD PARA CONTRATAR CON EL ESTADO

Los oferentes deberán cumplir con:

1. Información Societaria

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

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

2. Consulta 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.

14. FORMA DE COTIZACION

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

Renglones 1, 3, 5, 7, 9 y 10:

14.1 Precio Total de cada Renglón, en Dólares estadounidenses.

Renglones 2, 4, 6 y 8:

14.2 Precio Mensual de cada Renglón.

14.3 Precio Total de cada Renglón, en Dólares Estadounidenses.

Monto Total:

14.4 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.

15. VISITA TÉCNICA

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

Las visitas se facilitarán **hasta un (1) día antes** de la fecha estipulada para la apertura pública de las ofertas, debiendo comunicarse con la Dirección General de Informática y Tecnología, de lunes a viernes de 10.30 a 12.00 horas y de 14.30 a 17.00 horas, al teléfono 15-4159-9006, a los efectos de coordinar el día y hora en que serán efectuadas.

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

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

16. CONSTITUCIÓN DE GARANTÍAS

Para afianzar el cumplimiento de todas las obligaciones, los oferentes y adjudicatarios deben constituir las siguientes garantías de corresponder y sin límite de validez, conforme el artículo 93° de la Ley N° 2.095 -según texto consolidado por Ley N° 6.588-:

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

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

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

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

   En caso de tratarse de una póliza de caución que NO contenga firma

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

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

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

c) De impugnación a la preadjudicación de las ofertas: será de cinco por ciento (5%) del monto de la oferta del renglón o los renglones impugnados. Si el dictamen de evaluación para el renglón o los renglones que se impugnen no aconsejare la adjudicación a ninguna oferta, el importe de la garantía de impugnación se calculará sobre la base del monto de la oferta del renglón o renglones del impugnante. Esta garantía deberá integrarse en el momento de presentar la impugnación.

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

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

electrónico correspondiente del sistema JUC, dentro del plazo legal establecido.

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

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

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

17. PRESENTACIÓN DE LAS OFERTAS

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

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

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

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

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

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

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

18. APERTURA DE LAS OFERTAS

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

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

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

19. CRITERIO DE EVALUACION Y SELECCION DE LAS OFERTAS

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

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

20. DICTAMEN DE LA COMISION EVALUADORA. ANUNCIO. IMPUGNACION

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

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

Documentación Complementaria:

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

21. ADJUDICACIÓN

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

22. PERFECCIONAMIENTO DEL CONTRATO

Conforme lo establecido por el artículo 24 del PCG.

23. CAUSALES DE EXTINCIÓN DEL CONTRATO

Son causales de extinción del contrato las siguientes:

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

b) Mutuo acuerdo.

c) Quiebra del adjudicatario.

d) Rescisión, conforme lo establecido en los artículos 122 al 127 de la Ley Nº 2.095 -según texto consolidado por Ley Nº 6.588-.

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

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

24. PERSONAL DE LA ADJUDICATARIA

24.1 Nómina de Personal

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

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

24.2 Responsabilidad por el Personal

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

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

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

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

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

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

24.3 Daños a Terceros

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

24.4 Exclusión

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

25. 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.

26. SEGUROS

Coberturas de seguros a requerir

Generalidades:

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

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

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

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

De las compañías aseguradoras:

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

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

De las coberturas de seguro en particular:

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

1) Seguros Laborales.

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

3) Seguro de Responsabilidad Civil Comprensiva.

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

1) Seguros Laborales

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

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

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

"Por la presente, la A.R.T, renuncia en forma expresa a reclamar o iniciar toda acción de repetición, de subrogación o de regreso contra el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, sus funcionarios y/o empleados, sea con fundamento en el Art. N°39 ap. 5 de la Ley N°24.557, o en cualquier otra norma jurídica, con motivo de las

prestaciones en especie o dinerarias que se vea obligada a abonar, contratar u otorgar al personal dependiente o ex dependiente del adjudicatario, amparados por la cobertura del contrato de afiliación N° XXXX, por acciones del trabajo o enfermedades profesionales, ocurridos o contraídas por el hecho o en ocasión de trabajo."

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

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

Alcance de la Cobertura: Se deberá amparar a la totalidad del personal afectado durante la jornada laboral incluyendo cobertura *in-itinere.*

Sumas mínimas a Asegurar:

Muerte: pesos diez millones ($ 10.000.000,00.-).

Invalidez Total y/o parcial permanente por accidente: pesos cuatro millones ($ 4.000.000,00.-).

Asistencia Médico Farmacéutica (AMF): pesos dos millones ($ 2.000.000,00.-).

La citada póliza deberá incluir el siguiente texto:

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

3) Seguro de Responsabilidad Civil Comprensiva.

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

Suma Asegurada Mínima:

La misma será por un monto mínimo de pesos diez millones ($ 10.000.000.-). 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."*

27. 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.

28. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO

28.1 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.

28.2 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.

Anticipo Financiero:

Se abonará el cuarenta por ciento (40%) del monto total adjudicado en concepto de anticipo financiero.

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

El importe adelantado se descontará al liquidarse los montos facturados.

El monto restante se abonará conforme se indica a continuación:

Renglones 1, 3, 5, 7 y 9:

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

Renglones 2, 4, 6, 8 y 10:

El pago del saldo se efectuará por anticipado, luego de la emisión del Parte de Recepción Definitiva correspondiente al Renglón 9, 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 en garantía del pago anticipado; seguro que tendrá vigencia hasta la conformidad definitiva.

29. PENALIDADES

29.1 Generalidades

El incumplimiento en término y/o satisfactorio de las obligaciones contractuales coloca al adjudicatario en estado de mora y, por lo tanto, sujeto a la aplicación, previo informe de las áreas técnicas, de las penalidades establecidas en el Capítulo XII del Título VI de Ley N° 2.095 -según texto consolidado por Ley N° 6.588- 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.

29.2 Particularidades

El primer incumplimiento de lo dispuesto en el apartado Niveles de Servicio del Pliego de Especificaciones Técnicas, dará lugar a la aplicación de una multa equivalente a 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.

30. 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.

31. COMUNICACIONES

Todas las comunicaciones que se realicen entre el Consejo de la Magistratura y los interesados, oferentes y adjudicatarios, que hayan de efectuarse en virtud de las disposiciones de la Ley N° 2.095 (texto consolidado según Ley N° 6.588) y su reglamentación se entienden realizadas a través del envío de mensajería mediante JUC en forma automática, y a partir del día hábil siguiente al de su notificación.

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

ANEXO I

DECLARACION JURADA DE APTITUD PARA CONTRATAR

El que suscribe (nombre y apellido, representante legal o apoderado)……..con poder suficiente para este acta DECLARA BAJO JURAMENTO, que (nombre y apellido o razón social)……CUIT N°…..... está habilitado/o para contratar con el PODER JUDICIAL DE LA CIUDAD AUTONOMA DE BUENOS AIRES, en razón de cumplir con los requisitos del artículo 89 de la Ley N° 2095 (según texto consolidado por Ley N° 6.588) y que no está incurso en ninguna de las causales de inhabilidad establecidas en los incisos a) a j) del artículo 90 del citado plexo normativo y del PCP.

FIRMA

…….

ACLARACION

…….

CARÁCTER

……

Ciudad de Buenos Aires, de… …de…….

ANEXO II
DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA

El que suscribe, (nombre y apellido, representante legal o apoderado)……..con poder suficiente para este acta, DECLARA BAJO JURAMENTO que la oferta realizada por la firma (nombre y apellido o razón social)……CUIT N°…… no ha sido concertada con potenciales competidores, de conformidad con lo establecido por el artículo 16 de la Ley N° 2.095 (texto consolidado según Ley N° 6.588) y modificatorias.

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

……

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

ANEXO III
DECLARACIÓN JURADA DE INCOMPATIBILIDAD

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

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

…….

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

ANEXO IV

CERTIFICADO DE VISITA

LICITACIÓN PÚBLICA N° 2-0036-LPU24

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

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

LICITACION PÚBLICA N° 2-0036-LPU24

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA SEGUNDA ETAPA

PLIEGO DE ESPECIFICACIONES TÉCNICAS

ÍNDICE:

PLIEGO DE ESPECIFICACIONES TÉCNICAS.

1. GENERALIDADES.

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

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.

2. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 1.

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

- Antimalware Avanzado (Ampliación FortiEDR).
- Threat Intelligence.
- Sandboxing.
- NGN Firewall.

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:

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

2.1 Especificaciones técnicas antimalware avanzado.

Características Generales.

- Se deberán proveer un mil quinientas (1.500) licencias del antimalware FortiEDR Discover, Protect and Respond, con el objetivo de ampliar las licencias existentes.
- 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 deberá ser 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.

2.2 Especificaciones técnicas Threat Intelligence

El Consejo de la Magistratura de la Ciudad de Buenos Aires requiere una solución de ciberinteligencia de amenazas que ayude a dar un mejor manejo y visibilidad del riesgo digital en la misma.

- La solución debe estar licenciada para el monitoreo y gestión de riesgo de 1.000 activos de la entidad, por un período de 36 meses.
- La solución debe recopilar inteligencia de varias fuentes, como dark web, Open Source e investigación técnica.
- La inteligencia debe tener una calificación de confianza basada en el estándar de la industria, como (Admiralty System) para todos los informes publicados.
- Todos los informes de inteligencia deben calificarse según los criterios de relevancia específicos para el panorama de amenazas del cliente.
- La inteligencia de amenazas presentada debe cubrir amenazas relevantes para el sector de la industria y los ataques mas relevantes a organizaciones pares del cliente.
- La solución debe supervisar e informar sobre amenazas en nuevas vulnerabilidades y exploits que se discuten activamente en la dark web y fuentes abiertas.
- La inteligencia de amenazas debe estar asignada al marco MITRE ATT&CK.
- La inteligencia debe proporcionarse y actualizarse en tiempo real a medida que se recopila nueva información o contexto de diversas fuentes.
- La solución debe proporcionar inteligencia sobre fugas de credenciales a través de infracciones de terceros en una vista de línea de tiempo limpia.

- La solución debe tener una fuerte presencia en los sitios de darknet examinados y solo por invitación, como foros y mercados.
- La solución debe hacer monitoreo extensivo de dark web para inteligencia específica de la organización mediante el monitoreo de salas de chat ocultas, sitios web privados, redes punto a punto, plataforma de redes sociales, sitios del mercado negro y botnets.
- La solución debe hacer descubrimiento de datos filtrados en la dark web, incluidos archivos confidenciales, datos financieros/de tarjetas de crédito, PII, etc.
- La solución deber poder demostrar la capacidad de interactuar con actores en dark web y recopilar inteligencia a través de HUMINT.
- La solución debe tener la habilidad de pivotar hacia la inteligencia en términos de varios filtros tales como:
    - Nombre del adversario.
    - Motivación adversaria.
    - Industria de destino.
    - Geografía objetivo.
    - Tipos de informes.
    - Calificaciones de relevancia.
- La solución debe tener capacidad para producir informes de alerta temprana basados en ataques iniciales y futuros y nuevos TTP.
- La solución debe tener capacidad para informar exclusivamente sobre ataques de Ransomware y TTP relacionados.
- La solución debe tener capacidad para realizar una investigación inicial dentro del sistema utilizando enriquecimientos en tiempo real para buscar IOC.
- La solución debe tener la capacidad de seguimiento y monitoreo de marca como:
    - Detectar credenciales violadas, es decir, correos electrónicos. (En caso de clientes Bancarios también se pueden incluir los datos de la Tarjeta).
    - Monitorear posibles infecciones de Stearler Infection.
    - Identifique las credenciales filtradas que están disponibles en la dark web.
    - Detectar información filtrada y datos confidenciales.
    - Capacidad de monitorear al Cliente como marca para cualquier ataque de phishing inminente.

- Hacer detección de sitios de phishing mediante el uso de marcas de agua digitales.
- Identificar la dirección IP y los correos electrónicos de los usuarios phishing a través de campañas de phishing.
- Capacidad de identificar dominios similares basados en el uso del logo de la marca.
- Capacidad para identificar nombres de dominio de apariencia similar que coincidan estrechamente con el Cliente.
- Identificar informacion alojada en Buckets de internet tales como AWS S3, Azure, Digital Ocean, entre otros.
- Identificar codigo fuente con informacion sensible en repositorios de codigo tales como GitHub.
- Realizar monitoreo de VIP, donde se evalúen menciones tales como: menciones en Telegram, en darknet, en stealer infections y dox sites.
- Evaluacion de riesgos de Proveedores, donde se deberá evaluar, nivel de riesgo del proveedor, superficie de ataques del proveedor, menciones en la darknet del proveedor, brechas de seguridad del proveedor, incidentes de ransomware del proveedor, distribucion geografica de activos del proveedor, etc.
- Servicio de eliminación: eliminación de contenido sospechoso (sitios/perfil/etc.).

- La solución debe hacer exposición y escaneo de Shadow IT: escaneos de puertos, dispositivos mal configurados, escaneos de certificados SSL, etc.
- La solución debe tener soporte para categorizar los hallazgos de inteligencia de amenazas a través de MITRE ATT&CK Framework, etc.
- La solución debe mostrar vulnerabilidades o configuraciones incorrectas del servidor (nube/en premisas).
- La solución debe contar con informes de activos vulnerables y activos de shadow IT.
- La solución deberá tener integración con proveedores de nube pública para la identificación de activos.
- La solución debe tener la capacidad para escanear y monitorear la infraestructura de Internet del Cliente para:

  - Identificación de Activos.
  - Identificar el cambio en los activos frente a Internet.
  - Identificación de Cambios en Puertos abiertos.
  - Identificar cualquier certificado SSL caducado o a punto de caducar.
- Deberá tener funciones para analizar e investigar los IOC a pedido, como búsquedas de reputación de IP/Dominio/Hash/CVE para varios parámetros, tales como:
  - Información básica.
  - Búsqueda de listas negras.
  - Ubicación geográfica.
  - Información de la red.
  - Informes de inteligencia previos.
- La plataforma debe tener características para integrarse con plataformas de colaboración como Microsoft Teams o Slack para el envío de notificaciones.
- La plataforma debe tener funciones para proporcionar acceso basado en roles, alertas personalizadas, alertas de flash, etc.
- Deberá tener la capacidad de proporcionar analista y reportes por demanda para cualquier requerimiento de aclaración e investigación personalizada.
- La solución debe poder ser administrada vía portal Web y vía API Rest.
- La solución deberá disponibilizar toda la información vía API REST con la intención de que la empresa pueda tener capacidades de SecOps incluyendo la superficie de ataque externa, Inteligencia de amenzas centradas en el advesario y protección de marca.
- La solución deberá ser 100% SaaS, por lo que no se debe requerir la implementación de Hardware para su puesta en producción.

2.3 Especificaciones técnicas Sandboxing.

Se deberán proveer dos (2) appliances virtuales, cumpliendo con las siguientes especificaciones:

Características del equipamiento

- Throughput mínimo en modo sniffer de 1 Gbps.
- Capacidad de procesar al menos 160 archivos por hora en modo dinámico.

- Capacidad de procesar archivos utilizando prefiltros de sandbox de al menos 10000 archivos por hora.
- Capacidad de procesar al menos 75.000 emails por horas mediante FortiMail.
- La solución debe permitir al menos 8 VMs simultáneas para sandboxing.
- Incluir la licencia necesaria para utilizar al menos 8 VMs.
- Incluir al menos ocho (8) licencias de Microsoft Windows y ocho (8) licencias de Microsoft Office.
- La solución debe de ser del tipo appliance virtual.

Requerimientos Mínimos de Funcionalidad.

- La solución debe proporcionar la funcionalidad de inspeccionar el tráfico entrante en busca de malware desconocido (APT - Advanced Persistent Threat y Zero-Day Threats), ransomware con filtrado avanzado de amenazas y análisis de ejecución en tiempo real, e inspección del tráfico saliente. devoluciones de llamada.
- Poseer la capacidad de prevenir amenazas desconocidas.
- Debido a que el malware es muy dinámico y un Antivirus reactivo común no es capaz de detectarlos con la misma velocidad con la que se crean sus variaciones, la solución ofrecida debe contar con funciones de prevención de malware desconocido incluidas en la propia herramienta (zero-day).
- El dispositivo de protección debe poder analizar archivos automáticamente localmente, donde el archivo se ejecutará y simulará en un entorno controlado.
- Deberá admitir el monitoreo de archivos traficados en Internet (HTTPs, FTP, HTTP, SMTP), así como archivos traficados internamente entre servidores de archivos usando SMB en todos los modos de implementación: sniffer, transparente y L3.
- La solución debe poder inspeccionar el tráfico cifrado SSL.
- La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
- Seleccionar a través de la política qué tipos de archivos se someterán a este análisis.
- Implementar e identificar la existencia de malware en archivos adjuntos de correo electrónico y URL conocidas.

- Implementar la detección y el bloqueo inmediatos de malware que utiliza mecanismos de escaneo en archivos PDF.
- La solución debe soportar los siguientes sistemas operativos dentro de su entorno controlado: Windows 7, Windows 8.1, Windows 10, Windows 11, MacOS, Android, Linux.
- Admite el análisis de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en el entorno de sandbox.
- Deberá soportar como mínimo los siguientes tipos de Archivos: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm,.dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf,.pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx,.swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx,.xz, .z, .zip.
- Los entornos controlados que posee la solución deben tener al menos las siguientes aplicaciones instalados: Internet Explorer, Adobe Flash Player, Adobe Reader, Microsoft .NET Framework, Microsoft Office, Java Runtime y MSVC Runtime.
- Deberá incluir un módulo de web filtering para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan.
- Al finalizar un análisis, debe poder informar sobre las actividades realizadas durante su ejecución. La mínima información con la que debe contar es: procesos iniciados, archivos creados/modificados/eliminados, cambios realizados en el registro y comportamiento de red.
- Deberá ser posible descargar un archivo PCAP para revisar el comportamiento del archivo analizado.
- Deberá permitir hacer un análisis de los archivos con intervención interactiva del operador sobre la máquina virtual.
- Deberá permitir realizar una grabación de video del comportamiento del malware.
- Deberá contener mecanismos de cache para evitar múltiples análisis del mismo archivo.

- La solución debe incluir la totalidad del licenciamiento requerido para la ejecución de los ambientes controlados.
- Para el análisis de correo electrónico, debe extraer la URL contenida en el cuerpo o adjunto del mensaje y acceder a la URL, descargar el archivo correspondiente y ejecutarlo en un ambiente controlado.
- La solución debe tener una nube de inteligencia propietaria del fabricante que se encargue de actualizar toda la base de seguridad a través de firmas.
- La solución debe admitir topologías de implementación en modo sniffer.
- La solución debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP, BCC o relay SMTP.
- La solución debe admitir topologías de implementación mediante el intercambio de archivos (SMB, NFS).
- La solución debe admitir topologías de implementación bajo demanda, es decir, mediante envío manual a través de la consola gráfica.
- La solución debe admitir topologías de implementación a través de la API JSON.
- La solución debe tener la posibilidad de permitir la carga de máquinas virtuales personalizadas.
- Todo análisis y bloqueo de malware y/o código malicioso debe ocurrir en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y/o códigos maliciosos.
- La solución debe ser compatible con las reglas YARA como estándar para crear reglas para la detección de malware.
- Deberá permitir que el administrador de la solución descargue el archivo original, analizado por la solución sandbox.
- En caso de un veredicto positivo, debe presentar una descripción detallada del comportamiento de la máquina comprometida, que contenga al menos información sobre el tipo de archivo para fines de auditoría.
- En el caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre IP Malware Origin con fines de auditoría.

- En el caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos información sobre la IP de destino (cliente que descargó el malware) para fines de auditoría.
- En caso de un veredicto positivo, debe proporcionar detalles del comportamiento de la máquina comprometida, que contenga al menos un resumen del comportamiento del malware con fines de auditoría.
- En el caso de archivos identificados como sospechosos, deben poder diferenciarse en al menos tres niveles de riesgo: alto, medio o bajo.

2.4 Especificaciones Técnicas NGN Firewall.

Se deberán proveer seis (6) appliances, con las siguientes características:

- FW Throughput (64 bytes) [Gbps]: 140.
- Sesiones concurrentes (TCP): 12.000.000 ampliable a 40.000.000.
- New Sessions/Second (TCP): 750.000 ampliable a 2.000.000.
- IPsec VPN Throughput (512 byte) [Gbps]: 55.
- Gateway-to-Gateway IPsec VPN Tunnels: 20.000.
- Client-to-Gateway IPsec VPN Tunnels: 100.000.
- SSL-VPN Throughput [Gbps]: 11.
- Concurrent SSL-VPN Users: 10.000.
- IPS Throughput (Enterprise Mix) [Gbps]: 22.
- SSL Inspection Throughput (IPS, avg. HTTPS) [Gbps]: 12.
- Application Control Throughput (HTTP 64K) [Gbps]: 34.
- NGFW Throughput [Gbps]: 17.
- Threat Protection Throughput [Gbps]: 15.
- Cantidad máxima de FortiSwitches Soportados: 196.
- Cantidad máxima de FortiAPs (Total): 4096.
- Cantidad máxima de FortiAPs (Tunnel Mode): 2048.

- Cantidad por default de dominios virtuales: 10.
- Cantidad máxima de dominios virtuales: 250.
- Dieciséis (16) interfaces de aceleración de hardware 1 GE RJ45
- Ocho (8) interfaces de aceleración de hardware 1 GE SFP.
- Doce (12) interfaces de aceleración de hardware 25 GE SFP28.
- Cuatro (4) slots 100 GE QSFP28 / 50 GE QSFP+.

Características Generales.

- La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- Las funcionalidades de protección de red que conforman la plataforma de seguridad, deberán poder ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación.
- La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q.
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding.
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM).
- Los dispositivos de protección de red deben soportar DHCP Relay.

- Los dispositivos de protección de red deben soportar DHCP Server.
- Los dispositivos de protección de red deben soportar sFlow.
- Los dispositivos de protección de red deben soportar Jumbo Frames.
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá soportar NAT estática (1-a-1).
- Deberá admitir NAT estática (muchos-a-muchos).
- Deberá ser compatible con NAT estático bidireccional 1-a-1.
- Deberá ser compatible con la traducción de puertos (PAT).
- Deberá ser compatible con NAT Origen.
- Deberá ser compatible con NAT de destino.
- Deberá soportar NAT de origen y NAT de destino de forma simultánea.
- Deberá soportar NAT de origen y NAT de destino en la misma política.
- Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico.
- Deberá ser compatible con NAT64 y NAT46.
- Deberá implementar el protocolo ECMP.
- Deberá soportar SD-WAN de forna nativa.
- Deberá soportar el balanceo de enlace hash por IP de origen.
- Deberá soportar el balanceo de enlace por hash de IP de origen y destino.
- Deberá soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Deberá ser compatible con el balanceo en al menos tres enlaces.
- Deberá implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales.
- Deberá permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Enviar logs a sistemas de gestión externos simultáneamente.

- Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Deberá soporta protección contra la suplantación de identidad (anti-spoofing).
- Implementar la optimización del tráfico entre dos dispositivos.
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3).
- Soportar OSPF graceful restart.
- Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red.
- Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico.
- Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente.
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3.
- Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster.
- La configuración de alta disponibilidad debe sincronizar: Sesiones.
- La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red.
- La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN.
- La configuración de alta disponibilidad debe sincronizar: Tablas FIB.
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace.
- Deberá soportar la creación de sistemas virtuales en el mismo equipo.

- Para una alta disponibilidad, el uso de clústers virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos.
- Deberá permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.
- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red.
- El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.
- Deberá existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi.
- La consola de administración debe soportar como mínimo, inglés y español.
- La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.
- La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

Características Firewall.

- Deberá soportar controles de zona de seguridad.
- Deberá contar con políticas de control por puerto y protocolo.
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Contar con control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad.

- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall.
- Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos especficos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).
- Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución debe permitir la implementación sin asistencia de SD-WAN.
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN.
- La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall.

Características Control de Aplicaciones

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Capacidad de detección de miles de aplicaciones en al menos dieciocho (18) categorías, entre las que se deberá incluir: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- Capacidad de reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.

- Capacidad de identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Capacidad de identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Actualización de la base de firmas de la aplicación de forma automática.
- Capacidad de limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Capacidad de permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
- El fabricante deberá permitir solicitar la inclusión de aplicaciones en su base de datos.
- Capacidad de permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Capacidad de permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Capacidad de permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo: permitir a Hangouts el chat pero impedir la llamada de video.
- Capacidad de permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Capacidad de crear de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).

- Posibilidad de crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Posibilidad de crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como Categoría de Aplicación.
- Posibilidad de configurar Application Override seleccionando las aplicaciones individualmente.

Características Threat Prevention.

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
- Deberá incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware).
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
- Deberá sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad.
- Deberá soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.
- Deberá r permitir el bloqueo de vulnerabilidades y exploits conocidos.
- Deberá incluir la protección contra ataques de denegación de servicio.
- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo.
- Deberá tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo.
- Deberá tener los siguientes mecanismos de inspección IPS: Desfragmentación IP.
- Deberá tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP.
- Deberá tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets).

- Deberá ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Detectar y bloquear los escaneos de puertos de origen.
- Bloquear ataques realizados por gusanos (worms) conocidos.
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
- Deberá poder crear firmas personalizadas en la interfaz gráfica del producto.
- Identificar y bloquear la comunicación con redes de bots.
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.
- Los eventos deben identificar el país que origino la amenaza.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Deberá permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad.
- En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles.

- Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).

Características URL Filter.

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
- Tener por lo menos 75 categorías de URL.
- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Permitir página de bloqueo personalizada.
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, soportar proxy web transparente.

Características User Identity.

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios.

- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.
- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.
- Deberá permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo).
- Deberá soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Deberá de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Deberá incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores.

Características QoS & Shaping.

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.

- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado.
- En QoS debe permitir la definición de tráfico con máximo ancho de banda.
- En QoS debe permitir la definición de colas de prioridad.
- Soportar marcación de paquetes DiffServ, incluso por aplicación.
- Soportar la modificación de los valores de DSCP para Diffserv.
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Deberá soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

Características DLP.

- Permite la creación de filtros para archivos y datos predefinidos.
- Los archivos deben ser identificados por tamaño y tipo.
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones.
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.

Características Geolocalización.

- Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países.

- Deberá permitir la visualización de los países de origen y destino en los registros de acceso.
- Deberá permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

Características VPN.

- Soporte VPN de sitio-a-sitio y cliente-a-sitio.
- Soportar VPN IPSec.
- Soportar VPN SSL.
- La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Deberá tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting.
- Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
- Deberá permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
- Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.

- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.

3. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 3.

El adjudicatario deberá proveer una tecnología que posea las características especificadas a continuación para la detección y gestión de vulnerabilidades de Infraestructura y en ambientes de Directorio Activo.

Requerimientos generales.

Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:

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

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.

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.
- Ampliar el licenciamiento de 2.000 a 2.500 activos a escanear con la solución Tenable.SC existentes en CMCABA.
- Contar con la capacidad de realizar la detección y gestión de vulnerabilidades en ambiente de Directorio Activo para 6.000 identidades.

3.1 Características generales módulo de Gestión de Vulnerabilidades (Tenable.SC).

- La entidad requiere una solución de ciberinteligencia de amenazas que ayude a dar un mejor manejo y visibilidad del riesgo digital en la misma.

- 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.

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.

3.2 Análisis de Seguridad Continua de Directorio Activo.

Requerimientos Generales.

- Se requiere una solución que permita ejecutar un análisis de Seguridad continuo y en tiempo real del entorno Microsoft Active Directory.
- Deberá ser implementada en modalidad OnPrem y deberá contar con un método seguro de conexión al Active Directory.

- La solución no deberá requerir de agentes instalados en los controladores de dominio.
- La solución debe identificar debilidades en las configuraciones del Directorio Activo incluyendo objetos, protocolos, relaciones de confianza, atributos y otros parámetros relacionados.
- La solución debe identificar ataques específicos dirigidos a la estructura de Active Directory.
- La solución debe tener la capacidad de analizar en detalle cada configuración incorrecta que cause riesgos de seguridad – con un lenguaje sencillo, contextualizando dicho riesgo para los equipos involucrados.
- La solución debe tener recomendaciones de corrección para cada configuración incorrecta en Active Directory.
- La solución debe evaluar las relaciones de confianza peligrosas entre bosques y dominios.
- La solución debe capturar los cambios que ocurren en AD y presentarlos en la consola de administración.
- La solución debe contar con un tablero con los principales ataques y vulnerabilidades por dominio.
- La solución debe permitir la correlación de los cambios de Active Directory y las omisiones de seguridad.
- La solución debe analizar un ataque en detalle explotando las descripciones a través del marco MITRE ATT&CK.
- La solución debe proporcionar una interfaz web para administrar todas las funcionalidades.
- La solución debe tener una capacidad nativa para crear paneles personalizados.
- La solución debe admitir un modelo flexible de control de acceso basado en roles (RBAC).
- La solución no deberá realizar cambios en Active Directory, sus objetos y atributos.
- La solución no debe almacenar ni sincronizar ninguna credencial de los objetos de Active Directory.
- La solución debe admitir entornos con varios bosques (forest) y dominios.

- La solución debe soportar el monitoreo continuo de entornos de Directorio Activo con nivel funcional de bosque (forest) y dominio desde Windows 2003 en adelante.
- La solución debe admitir la retención de eventos recopilados durante un mínimo de un año.
- La solución debe descubrir y mapear la superficie de ataque de Active Directory y sus dominios monitoreados con los siguientes patrones:
    - No depender de agentes o sensores para recopilar información de AD.
    - La solución debe seguir las mejores prácticas de privilegios mínimos, la cuenta de servicio utilizada para conectarse a Active Directory, con el nivel de acceso más bajo esperado para la cuenta de servicio como parte del grupo de usuarios de dominio.
    - Interfaz web que consolida y presenta los dominios monitoreados y las posibles relaciones de confianza establecidas entre ellos de forma unificada.
- La solución debe analizar continuamente la postura de seguridad de AD, evaluando mínimamente:
    - Validación de GPO desvinculados, deshabilitados o huérfanos.
    - Validación de cuentas deshabilitadas en grupos privilegiados.
    - Dominio que usa una configuración peligrosa de compatibilidad con versiones anteriores a través de cambios en los atributos de dSHeuristics.
    - Validación de atributos relacionados con el roaming de credenciales vulnerables (ms-PKI-DPAPIMasterKeys) administradas por un usuario sin privilegios.
    - Validación de dominios sin GPO de protección de información, deshabilitando antiguos protocolos vulnerables como NTLMv1.
    - Validación de cuentas con contraseñas que nunca caducan.
    - Validación de contraseñas reversibles en GPOs.
    - Validación de uso de contraseñas reversibles en cuentas de usuario.
    - Validación del uso de protocolo criptográfico débil (por ejemplo, DES) en cuentas de usuario.
    - Validación del uso de LAPS (Solución de contraseña de administrador local) para administrar contraseñas para cuentas locales privilegiadas.

- Validación si el dominio tiene un nivel funcional desactualizado.
- Validación de cuentas de usuario con contraseña antigua.
- Validación si el atributo AdminCount se establece en usuarios estándar.
- Validación del uso reciente de la cuenta de administrador predeterminada.
- Validación de usuarios con permiso para unir equipos al dominio.
- Validación de cuentas inactivas.
- Validación de equipos que ejecutan un sistema operativo obsoleto.
- Validación de restricciones de inicio de sesión para usuarios privilegiados en un entorno con múltiples niveles (1, 2 y 3) de segregación de activos.
- Validación de derechos peligrosos configurados en AD Schema.
- Validación de relaciones de confianza peligrosas con otros Bosques (Forests) y Dominios.
- Validación de cuentas que tienen un atributo de Historial SID peligroso.
- Validación de cuentas mediante control de acceso compatible con Windows 2000.
- Validación del último cambio de contraseña de KDC.
- Validación del último cambio de la contraseña de la cuenta de Azure AD SSO.
- Validación de cuentas que pueden tener una contraseña en blanco/vacía.
- Validación de uso del grupo nativo de Usuarios Protegidos.
- Validación de privilegios sensibles peligrosos (por ejemplo: Depurar un programa, Reemplazar un token de nivel de proceso, etc.) asignados a los usuarios.
- Validación de una posible contraseña de texto claro.

4. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 5.

El adjudicatario deberá proveer una tecnología que posea las características especificadas a continuación para un ambiente de testing / laboratorio de 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.

- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:

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

Requerimientos de la solución.

Características de licenciamiento

- Se requiere licenciamiento en modalidad suscripción de la solución de Testing / Laboratorio para el módulo CyberArk Identity y ampliar en 20.000 licencias el módulo CyberArk Identity para usuarios externos (IASSO-B2C-USER-SAAS), por el período de treinta y seis (36) meses.
- Se requiere licenciamiento en modalidad suscripción por el período de treinta y seis (36) meses de una solución de Gestión de Accesos Privilegiados para 50 usuarios, los cuales deberán contar con licencia para grabar sesiones de auditoría en al menos 20 de ellos.

4.1 Características Generales Gestión de Ciclo de Vida de la Identidad.

- Deberá 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 debe 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 debe 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 debe 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 debe 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 debe 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 debe 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 debe proporcionar un portal WEB para el usuario final 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.
    - 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.
- Deberá 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 debe tener la capacidad de ampliar su esquema configurando atributos personalizados para satisfacer requisitos empresariales complejos.
- El servicio de directorio de soluciones debe ser autoescalable para admitir millones de identidades y miles de atenciones simultáneas.
- Deberá 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 debe admitir la integración con los servicios de directorio en la nube y on-premises, lo que debe admitir mínimamente:
  - Microsoft Active Directory.
  - Microsoft Azure AD.
  - Directorio de Google.
  - Directorios LDAP.
- Las integraciones con un directorio de terceros no deben sincronizarse con estas bases de datos, es decir, cargar todo el directorio configurado en la nube, la solución debe actuar como intermediario entre los servicios de directorio de terceros y la solución.
- La solución debe 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 debe tener la capacidad de configurar LOS PROVEEDORES DE IDENTIDAD (IDP) de los terceros afines al Consejo de la Magistratura de la Ciudad de Buenos Aires 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.

4.2 Características generales Gestión de Accesos Privilegiados.

- La solución propuesta deberá ofrecerse como servicio (SaaS) y al menos tener las certificaciones SOC 2 Type 2, ISO27001 e ISO 27018 (PII).

- La comunicación a internet necesaria por la solución debe ser solo de salida (outbound) y no depender de canales de conexion IPSec o Direct Connect.
- La solución propuesta deberá tener la capacidad de cifrar, en reposo y en tránsito todos los datos que utilice, incluyendo contraseñas, reportes almacenados, grabaciones y registros de usuarios. Lo anterior utilizando algoritmos que cumplan con los estándares en FIPS 140-2, como AES-256 y RSA-2048.
- La solución debe ayudar a la organización a administrar y monitorear los accesos privilegiados y el uso de las credenciales privilegiadas, utilizadas por identidades humanas y no humanas, asociadas a infraestructura en ambientes híbridos; incluyendo servidores, bases de datos, dispositivos de comunicaciones, soluciones de seguridad y aplicaciones en un centro de datos, así como en ambientes de nube pública.
- Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.
- La solución ofertada debe incluir un componente para gestionar la identidad de la fuerza de trabajo (IAM), esto como parte de la visión de Consejo de la Magistratura de la Ciudad de Buenos Aires de tener una plataforma centralizada donde pueda gestionar cualquier tipo de identidad.
- La solución de Seguridad de Cuentas Privilegiadas deberá tener la capacidad de administrar la plataforma de forma centralizada a través de un portal web y capacidad para restringir accesos a través de zonas de red confiables.
- Dada la criticidad de la solución, y de la importancia para la organización, esta debe de liderar los 3 últimos cuadrantes de Gartner, Privilege Access Access Management (PAM).
- Dada la criticidad de la solución, y de la importancia para la organización, esta debe de liderar últimos cuadrantes de Forrester, Workforce Idenity Platforms.
- La solución ofertada debe proporcionarse en un esquema SaaS con un SLA del servicio que debe ser mínimo de 99.9%, considerando que la responsabilidad del servicio debe quedar de lado del fabricante del PAM y no depender de terceros.
- Deberá tener la capacidad de ejecutar operaciones de forma masiva (bulk operations) sobre las cuentas privilegiadas, como altas y modificaciones.

- La solución debe tener la capacidad de soportar el uso de aplicaciones y servicios que se ejecuten en un sistema hibrido, esto quiere decir en entornos nube y en la premisa.
- La solución ofertada no debe estar limitada en la cantidad de dispositivos, aplicaciones o activos a proteger, o a la cantidad de sesiones.
- El fabricante de la solución ofertada debe tener una libreria de aplicaciones o Martketplace el cual debe contar con diferentes plug-ins de integración nativos para plataformas terceras.
- La solución ofertada debe tener la capacidad de gestionar el ciclo de vida de la identidad privilegiada, esto quiere decir ayudar en los procesos de aprovisionamiento, desaprovisionamiento de accesos y control privilegiado.
- La solución debe tener la capacidad de automatizar procesos propios de su gestión, de tal manera que pueda agilizar procesos de aprovisionamiento/desaprovisionamiento, aprobación, entre otros.
- La solución propuesta deberá ser en formato SaaS, pero que incluya a lo menos los componentes de Proxy (Jump Server) y procesos de cambio de contraseña, en ambientes on premise, cercano a los usuarios y aplicaciones, con el fin de optimizar el tráfico, y seguridad junto con interrupciones de microcorte que no afecte las sesiones locales.
- La solución de Seguridad de Cuentas Privilegiadas debe ser una solución basada en software y debe estar disponible como SaaS o en modelo de suscripción para implementación en ambientes de Nube (AWS, Azure y Google Cloud) y/o instalable sobre entorno físico o virtualizado con infraestructura (servidores / software en entorno virtualizado, S.O., capa de balanceo de tráfico / redirección, etc.).
- La solución debe ser modular y escalable para adaptarse a crecimientos de utilización o expansión de funcionalidades e incluso esquemas de Alta Disponibilidad de roles y/o componentes. Es decir, debe poder crecer por cada rol de forma independiente según sea requerido, sin incurrir en licenciamiento adicional.
- Análisis de comportamiento y mitigación de riesgo para acceso en aplicaciones de negocio para colaboradores y terceros (UBA).

- La solución se debe basar en algoritmos de aprendizaje de máquina (machine learning) no supervisados. Es decir, los modelos estadísticos con los casos de uso ya deben estar listos y calibrados.
- La solución debe medir el riesgo de la autenticación verificando el comportamiento histórico de la identidad a través del conjunto de los siguientes atributos:
  - GeoVelocidad.
  - Geolocalización.
  - Dia de la semana.
  - Horario de acceso.
  - Sistema operativo.
  - Fallas de login consecutivas.
- La solución debe permitirles a los administradores personalizar los rangos de puntuación (0 a 100) para las categorías:
  - Sin riesgo.
  - Riesgo bajo.
  - Riesgo medio.
  - Riesgo alto.
- El riesgo calculado durante la autenticación por el motor de análisis del comportamiento de los usuarios debe compartirse con los módulos (SSO y MFA) que realizan el login, para los casos de uso citados en este documento, y utilizarlo como contexto para:
  - Solicitar autenticación de múltiples factores de forma dinámica.
  - Permitir el login sin el uso de múltiples factores.
  - Negar la autenticación.
- Deberá brindarles a los administradores de la solución la capacidad de explorar los datos históricos a través de dashboards, filtros y gráficos configurables, verificar las alertas y los factores que los influenciaron y explorar los eventos capturados y sus atributos.
- Deberá proveer gráficos de línea de tiempo, donuts, mapas con la geolocalización de los eventos, gráficos de barras, tablas analíticas y mapas de relación. Sus dimensiones y categorías deben ser personalizables.

- "La solución debe 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.
  - 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 debe permitir confirmación de código por correo electrónico.
- La solución debe soportar clientes tipo Oath OTP (por ejemplo, Google Authenticator).
- La solución debe permitir preguntas y respuestas previamente configuradas.
- La solución debe permitir que los usuarios realicen el restablecimiento de contraseña y el desbloqueo del usuario, autoservicio mediante los múltiples métodos de factor de autenticación citados para la verificación positiva a través del portal de soluciones, Windows y la pantalla de inicio de sesión del sistema operativo MacOS, y a través de las API de REST que ofrece la solución.
- La solución debe permitir la autenticación dinámica basada en el contexto de riesgo y seguridad aprendido por la solución, permitiendo la creación de un perfil para cada usuario, aprovechando los atributos históricos y situacionales específicos del mismo, como la ubicación, el dispositivo, la red, el horario y el índice de riesgo de comportamiento.
- La solución debe permitir a los usuarios agregar y modificar factores de autenticación directamente en un portal con una definición de período de omisión de autenticación multifactor.

- La solución debe proporcionar un catálogo de aplicaciones web con modelos de configuración de inicio de sesión único (SSO) que contengan al menos un catálogo de más de 1000 tipos de las aplicaciones más conocidas del mercado, con el fin de facilitar la configuración de estas integraciones.
- La solución debe permitir la configuración de las aplicaciones web mínimamente a través de los siguientes protocolos y métodos:
  - SAML 2.0.
  - Modo cliente Oauth 2.0.
  - WS-Federation.
  - Conexión OpenID.
  - Ntlm.
  - Modo de servidor Oauth 2.0.
  - 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 debe almacenarse de forma segura en la solución para la finalización automática en futuros inicios de sesión en estas aplicaciones.
  - Contraseñas y MFA de Active Directory.
  - Código QR propio.
  - Código OTP vía SMS enviado por la propia solución.
  - Código OTP vía E-mail enviado por la propia solución.
  - Notificaciones push a dispositivos móviles enviado por la propia solución.
  - OTP de terceros que soporten OATH.
  - Tokens de terceros en cumplimiento con FIDO2.
  - Autenticación biométrica de dispositivos como Windows Hello y Apple Touch ID.
- La solución propuesta deberá contar con la capacidad de integrarse con sistemas tipo SIEM, tales como Splunk, RSA, Qradar.
- La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, equipos de comunicaciones, Bases de Datos, Aplicaciones Web. Detallar cuales son los requerimientos para realizar esta capacidad.

- La solución propuesta deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video. Detallar los requerimientos para realizar esta operación.
- La solución propuesta deberá poder restringir la ejecución de comandos / Aplicaciones que se estén ejecutando con las cuentas privilegiadas gestionadas por la solución, sin la necesidad de tener que realizar configuraciones en los sistemas target. Detallar los requerimientos para realizar esta operación, y que plataformas son soportadas.
- La solución de Seguridad de Cuentas Privilegiadas deberá tener la capacidad de administrar diferentes orígenes o plataformas que estén certificadas y soportadas tanto por la solución propuesta como por la marca de la integración, entre las cuales deberán encontrarse por lo menos las plataformas:
  - Sistemas Operativos: Windows, *NIX, IBM iSeries, Z/OS, HPE Nonstop, MAC OS, ESXi, Infoblox NIOS, Linux RedHat, Oracle Linux, Solaris.
  - Aplicaciones de Windows: Cuentas de servicio, tareas programadas, grupo de aplicaciones IIS, COM+, acceso anónimo de IIS.
  - Bases de datos: Oracle, MSSQL, DB2, SAP Hana, MongoDB, MySQL, Informix.
  - Dispositivos de Seguridad: FireEye, Imperva SecureSphere, Juniper, CheckPoint GAiA, CISCO Pix.
  - Manejador de vulnerabilidades: Rapid7, Tenable.
  - Dispositivos de red: Cisco, Juniper, CheckPoint, BlueCoat, Fortinet, F5, Palo Alto, Radware.
  - Aplicaciones: SAP, SalesForce, Google, VMWare vSphere, Office 365, OneDrive, Chef.
  - Servicios de nube: Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), CloudSigma.
  - RPAs: Blue Prism, UiPath, WorkFusion.
  - Directorios: Microsoft, ORACLE, Novell, Ping Identity.
  - Interfaces genéricas: SSH/Telnet, Web, PuTTY, RDP.
  - ODBC – Contraseñas almacenadas en tablas de base de datos.

- La solución propuesta deberá tener la capacidad de contar con un método para detectar llaves SSH pares, llaves huérfanas y relaciones de confianza en la organización.
- La solución propuesta deberá tener la capacidad de almacenar de forma segura y controla el acceso a las llaves privadas SSH.
- La solución propuesta deberá tener la capacidad de permitir la automatización de rotación de llaves.
- La solución debe tener la capacidad de entregar un acceso remoto seguro (externo a la red corporativa) a los usuarios sin necesidad de instalación de clientes VPN en los dispositivos de usuarios remotos y garantizando un acceso seguro con MFA sin necesidad de modificar los recursos de autenticación corporativos como el AD.
- Deberá proveer un motor de UBA, que además de supervisar y adaptase según el comportamiento, debe también tener la capacidad de detectar acciones en sesiones privilegiadas, con al menos soporte para SSH, Windows, SQL, Entradas de Teclado y SCP.
- La Solución debe entregar sesiones administrativas a las que se acceda y monitoree en tiempo real, con el uso compartido de pantalla y el control de periféricos, como el teclado y el ratón (asistencia remota), y mediante la grabación de comandos y vídeos de los mismos, en formato estándar de ejecución no propietaria de la solución, permitiendo que los comandos y vídeos generados se puedan indexar para futuras búsquedas, permitiendo el filtro de comandos y acciones realizadas a lo largo de la sesión grabada, lo que le permite buscar acciones específicas en la sesión grabada.
- La solución debe ser capaz de detectar comportamientos que tipifican abusos, comportamientos anormales y fuera de los estándares aprendidos/asignados, aplicando acciones atenuantes automáticas como la reautenticación, suspensión y terminación de sesiones y rotación de credenciales privilegiadas en caso de actividad sospechosa de alto riesgo, detectando al menos los siguientes casos:
    - Durante horarios irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios, en un momento irregular, según su perfil de comportamiento).

- Durante días irregulares (cuando un usuario recupera una contraseña de cuenta con privilegios en un día irregular de acuerdo con su perfil de comportamiento).
- A través de IP irregular y desconocida (cuando un usuario accede a cuentas con privilegios de una dirección IP o subred inusual, de acuerdo con su perfil de comportamiento), o cuando se realiza una conexión a un equipo con una cuenta con privilegios que no se administra en la solución.

- La solución ofertada deberá tener la capacidad de ofrecer un acceso offline o fuera de línea, de tal manera que pueda brindar la resiliencia necesaria en casos de falla de red o de los componentes de la solución.
- La solución propuesta deberá tener la capacidad de intervenir y/o terminar remotamente una sesión en tiempo real cuando se ejecuta una actividad sospechosa o es requerido por el administrador o auditor.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de los siguientes Sistemas Operativos: Windows, Unix, Linux, IBM iSeries, Z/OS, HP Tandem, MAC OS, ESX/ESXi, XenServers, Linux RedHat, etc. Detallar todos los Sistemas Operativos que son soportados por la solución.
- La solución propuesta debe permitir que los administradores de la solución no tengan acceso a las contraseñas almacenadas si así se define por el negocio.
- La solución propuesta deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar las contraseñas que son controladas por otros departamentos de la compañía, como por ejemplo que los administradores de Windows Server no puedan visualizar las contraseñas ni accesos a instancias de bases de datos SQL Server. Esto es para garantizar la separación de roles lo más posible para evitar el uso indebido de las cuentas privilegiadas protegidas por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de las siguientes Bases de datos: Oracle, MSSQL, DB2, Postgresql, mongoDB, Teradata, etc. Detallar todos los motores de base de datos SQL y NOSQL que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas basadas en los siguientes servicios de directorio: Microsoft AD, Azure AD,

Google. Detallar todos los servicios de directorio que son soportado por la solución.

- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de dispositivos de red (Firewalls, Routers, Switches, APs, etc). Detallar un listado completo con todos los diferentes dispositivos de Red que son soportados por la solución.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Aplicaciones Cloud como Facebook, Google G Suite, Google Gmail, GitHub, Docker, Puppet, Cloudflare, Aqua, IBM Cloud, LinkedIn, instagram, Twitter, Amazon, Azure, VMware, Office 365, Paloalto, RedHat Ansible/OpenShift, salesforce.
- En el caso que la cuenta privilegiada de una plataforma SaaS (ejemplo consola Cloud) posea un doble factor de autenticación en el inicio de sesión, en este escenario la solución debe poder permitir que el usuario agregue el factor necesario a lo menos en cuentas AWS y Azure. Detallar.
- La solución propuesta deberá ser capaz de soportar cualquier repositorio de datos mediante conexión ODBC.
- La solución propuesta deberá ser capaz de soportar Conexiones de tipo Ad Hoc.
- La solución propuesta deberá permitir búsquedas dentro de los videos de auditoría.
- La solución propuesta deberá ser capaz de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows (Windows Services), Scheduled Tasks, IIS Service Accounts, etc. para su administración en la solución. Detallar como se realiza este proceso.
- La solución ofertada debe incluir un MFA nativo y también permitir la integración con soluciones 2FA.
- Integración con soluciones de análisis de vulnerabilidades.
- La solución debe disponer de un servicio REST API (Application Programming Interface) vía WebServices para administrar y aprovisionamiento de la solución, que permita entre otras cosas automatizar procesos.

- Deberá supervisar las sesiones privilegiadas, grabar, detectar, correlacionar y mitigar comportamientos anormales, en todas las sesiones soportadas por PAM, entre ellos servidores Linux/Unix, Windows, controladores de dominio de Microsoft Active Directory, estaciones de trabajo Windows, diversos activos de red y de Seguridad, así como aplicaciones Cliente servidor/Web y servicios en Nube ya sean IaaS, SaaS o PaaS.
- Deberá proveer un motor de UBA, que además de supervisar y adaptase según el comportamiento, debe también tener la capacidad de detectar acciones en sesiones privilegiadas, con al menos soporte para SSH, Windows, SQL, Entradas de Teclado y SCP, sin la necesidad de incurrir a la instalación de agentes.
- La solución propuesta deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.
- La solución propuesta deberá tener la capacidad de soportar controles duales, la solución debe soportar diferentes configuraciones de aprobaciones cuando por ejemplo un usuario solicite una contraseña. Esto debe incluir notificaciones automáticas vía email.
- La solución propuesta deberá tener la capacidad de que un usuario pueda solicitar el uso de una cuenta privilegiada para una fecha u hora futura.
- La solución propuesta deberá tener la capacidad de soportar procesos flexibles de workflows para designar múltiples aprobadores. Por ejemplo: se requieren dos o más aprobaciones antes de que el acceso sea autorizado.
- La solución propuesta deberá tener la capacidad de generar logs de los procesos de workflow y/o la habilidad de generar reportes o auditarlos.
- La solución propuesta deberá tener la capacidad de cambiar contraseñas cada X días, meses, años.
- La solución propuesta deberá tener la capacidad de cambiar múltiples contraseñas en una sola vez para un solo sistema o sistemas agrupados bajo un solo criterio.
- La solución propuesta deberá tener la capacidad de cambiar una contraseña o un grupo de contraseñas:
  - De acuerdo con una política (cada x días u 'on-demand').

  - Cambios manuales efectuados por un usuario.
  - Automáticamente, cuando una contraseña no haya sido sincronizada (falla en verificación).

- La solución propuesta deberá tener la capacidad de asignar contraseña a un valor aleatorio.
- La solución propuesta deberá tener la capacidad de cambiar manualmente una contraseña por un administrador en cualquier momento.
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el valor de una contraseña después de un tiempo especificado de un "check out" de la contraseña.
- La solución propuesta deberá tener la capacidad de cambiar automáticamente la contraseña de una cuenta que acaba de ser definida en el sistema.
- Soporte a verificación de contraseña.
- La solución propuesta deberá tener la capacidad de verificación automática del valor de una contraseña en el sistema correspondiente.
- Soporte a Reconciliación de Contraseña.
- La solución propuesta deberá tener la capacidad de automáticamente reconciliar contraseña que se hayan detectado como "out of sync" o que se hayan perdido, sin utilizar herramientas externas de restauración.
- La solución propuesta deberá tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de súper-usuarios de todos los sistemas.
- La solución propuesta deberá tener la capacidad de mantener el historial de contraseñas, ej. Las últimas tres contraseñas o por periodo de tiempo y proveer fácil acceso a ellas a través de la interfaz web del producto.
- La solución propuesta deberá tener la capacidad de administrar cuentas de súper-usuario que han sido renombradas de su nombre por default.
- La solución propuesta deberá tener la capacidad de soportar conexiones transparentes a un dispositivo target, sin la necesidad de ver o teclear la contraseña como parte de la conexión. Detallar los requerimientos para realizar esta funcionalidad.

- La solución propuesta deberá tener la capacidad de soportar conexión directa a dispositivos UNIX/LINUX de administración (SSH) pudiendo grabar la sesión.
- La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, equipos de comunicaciones, Bases de Datos, Aplicaciones Web. Detallar cuales son los requerimientos para realizar esta capacidad.
- La solución propuesta deberá tener la capacidad de hacer búsquedas de comandos privilegiados dentro de las grabaciones de video. Detallar los requerimientos para realizar esta operación.
- La solución propuesta deberá poder restringir la ejecución de comandos / Aplicaciones que se estén ejecutando con las cuentas privilegiadas gestionadas por la solución, sin la necesidad de tener que realizar configuraciones en los sistemas target. Detallar los requerimientos para realizar esta operación, y que plataformas son soportadas.
- La solución propuesta deberá tener la capacidad de intervenir y/o terminar remotamente una sesión en tiempo real cuando se ejecuta una actividad sospechosa o es requerido por el administrador o auditor.
- La solución propuesta debe incluir un llavero de credenciales de usuario final, sin incurrir a un costo de licenciamiento adicional.
- La solución propuesta debe proporcionar un control centralizado y estar integrado a la misma plataforma de seguridad.
- La solución propuesta debe ser colaborativa, de tal manera que pueda brindar agilidad en los procesos de interacción con otros usuarios.
- La solución propuesta debe tener la capacidad de sincronizar las credenciales o secretos almacenados a la misma bóveda de seguridad del PAM.
- La solución propuesta debe tener un portal web en esquema SaaS tanto para la gestión como para el acceso de los secretos.
- La solución debe proporcionar un catálogo de aplicaciones web con modelos de configuración de inicio de sesión único (SSO)que contengan al menos un catálogo de más de 1000 tipos de las aplicaciones más conocidas del mercado, con el fin de facilitar la configuración de estas integraciones.

- La solución debe proporcionar el poder crear notas de secretos donde pueda personalizar o agregar nuevos campos.
- La solución debe proporcionar la capacidad de poder adjuntar archivos que se deseen subir a la plataforma para utilizarlo como un repositorio seguro de archivos.
- La solución debe proporcionar la capacidad de manejar diferentes tipos de roles de tal manera que pueda crear grupos o pequeñas células de trabajo.
- La solución debe proporcionar la capacidad de proporcionar un plugin de acceso rápido a las aplicaciones ya integradas y ser compatible con Edge, Firefox y Chrome.
- La solución propuesta debe tener capacidades de proporciona seguridad, privacidad y productividad mejorada, así como ofrecer una experiencia de usuario familiar.
- La solución deberá tener la capacidad de elimina el riesgo de acceso no autorizado y uso malicioso de identidades comprometidos, credenciales, cookies y endpoints.
- La solución deberá proteger el acceso a datos confidenciales desde dispositivos administrados y no administrados.
- La plataforma deberá proporcionar una plataforma de lanzamiento o "launchpad" segura para cada recurso y aplicación, asegurando las credenciales y habilitando una verdadera experiencia sin contraseña (passwordless).
- La plataforma de seguridad deberá estar integrada en cada capa de seguridad dentro de su infraestructura o plataforma de identidad.
- La solución propuesta deberá prevenir posibles intentos de acceso no autorizado mediante la manipulación de cookies.
- La solución propuesta deberá ofrecer controles sobre el acceso al portapapeles "Clipboard", la descarga de archivos y de impresión para garantizar que los datos corporativos confidenciales permanezcan protegidos.
- La plataforma deberá estar diseñada para priorizar la privacidad del usuario. Evita el seguimiento no deseado, lo que garantiza que las actividades del usuario permanezcan privadas y que el historial de navegación no se comparta con terceros.

- La plataforma de seguridad deberá proveer facilidad en la navegación, deberá proporcionar una barra lateral que brinda acceso rápido a aplicaciones, herramientas y recursos de uso frecuente.
- La solución propuesta debe tener la capacidad de proteger identidades no humanas (cuentas de servicio, robots, escáneres de vulnerabilidades, entre otros.).
- La solución debe contar con una librería de integraciones de tal manera que pueda acelerar el proceso de integración nativo con las aplicaciones que utilicen identidades no humanas o de servicio.
- La solución ofertada deberá tener capacidad de brindar resiliencia en caso de que existan inconvenientes de comunicación entre las plataformas integradas.
- La plataforma deberá tener la capacidad de proteger aplicaciones que se encuentre en ambiente on premise así como aplicaciones que se encuentren ejecutando en nube.
- La solución debe tener la capacidad de tener métodos de autenticación más robustos para las aplicaciones.
- La plataforma de seguridad debe soporte el uso de peticiones REST y SOAP para entregar los secretos de manera segura.
- La solución ofertada debe ofrecer esquemas de autenticación de secretos basado en credenciales y basado en atributos para las diferentes aplicaciones de Consejo de la Magistratura de la Ciudad de Buenos Aires.
- La solución ofertada debe soportar diferentes métodos de autenticación para las aplicaciones del Consejo de la Magistratura de la Ciudad de Buenos Aires, entre las principales están (contraseña, ID, API Key, JWT, biométrico, OS User, path, MD5 Hash, IP/Hostname).
- La solución debe de estar de manera integrada y no requeririr del uso de software terceros como parte de sus tareas operacionales.
- La solución debe soportar de manera nativa la integración con Service Now (MID Server) y con Tenable.
- La solución ofertada debe proporcionar un de acceso basado en el privilegio mínimo.
- La solución ofertada deberá soportar diferentes principios de acceso privilegiado de tal manera que pueda robustecer los accesos en ambientes

estáticos y dinámicos, así como disminuir el riesgo e impacto en el acceso otorgado.

- La solución ofertada debe proporcionar un esquema de acceso privilegiado "standing", en cual se tienen capacidades como almacenamiento de cuentas en bóveda digital, rotación, aislamiento, monitoreo y grabación de sesión.
- La solución ofertada debe proporcionar un esquema de acceso privilegiado "JIT (Just-In-Time)", en el cual el acceso privilegiado puede ser dado al momento, pero a intervalos limitados de tiempo con procesos de elevación o aprobación de acceso.
- La solución ofertada debe proporcionar un acceso privilegiado "Zero Standing", en el cual se remueven los privilegios en el acceso de manera permanente y se los proporciona de manera temporal, dentro de un intervalo de tiempo específico y bajo un proceso de aprobación.
- La solución ofertada deberá proporcionar estas capacidades de manera integrada a la misma plataforma, sin limitarse a la cantidad de dispositivos a proteger.
- La solución ofertada deberá proporcionar integración nativa con aplicaciones IaaS y PaaS.
- La solución ofertada deberá proporcionar un portal para la creación de políticas consistentes tanto para ambientes on premise, así como para ambientes en nube y multinube.
- La solución ofertada deberá proporcionar una experiencia nativa de conexión al usuario final de tal manera que pueda ayudar a acelerar la adopción de la plataforma.
- La solución ofertada deberá proporcionar integración nativa con aplicaciones IaaS y PaaS.
- La solución de ofertada debe de proporcionar un esquema de conexión VPN-less esto quiere decir que pueda permitir conectarse de manera remota a recursos que puedan estar en premisa o en nube.
- La plataforma deberá soportar el aprovisionamiento temporal de roles y grupos para el acceso privilegiado para servidores Windows, Linux, Bases de datos (Oracle, SQL Server, MySQL, DB2, PostgresSQL) y Kubernetes.

- La solución deberá proporcionar un esquema de acceso MFA nativo como parte del proceso de autenticación y autorización del acceso.
- La plataforma ofertada deberá tener la granularidad para definir políticas de acceso basados en atributos o características propias de la nube, tales como VPC, Subnets, Segmentos y tags.
- La plataforma ofertada deberá otorgar capacidades para automatizar los procesos de aprobación de acceso, mediante un aplicativo móvil y también utilizando herramientas colaborativas empresariales tales como Slack o Teams.
- La plataforma de seguridad deberá de tener la capacidad de rotar, aislar, monitorear y grabar la sesión para el esquema de acceso "Standing".
- La plataforma de seguridad deberá tener la capacidad de revocar los privilegios una vez que haya terminado la sesión privilegiada.
- El fabricante de la solución debe ser miembro de C3 Alliance, el cual es una red formada por mas de 200 proveedores de software empresarial y soluciones de seguridad, de tal manera que pueda llegar a proteger estas plataformas de manera nativa.
- La solución, debe contar con una herramienta propia para generar plugins personalizados para plataformas que sean propias del cliente.
- La solución debe tener la capacidad de instalar complementos de terceros, proporcionado por los proveedores oficiales (por ejemplo: Microsoft, Oracle), disponibles en el Marketplace (librería de aplicaciones) de la herramienta.
- La solución debe soportar otras integraciones de manera nativa o debe tener una base de datos de integración con terceros de manera, que contenga un mínimo de 850 plugins o conectores para la integración a terceros.
- La solución debe tener un portal de autenticación biométrico utilizado para los proveedores o terceros.
- La plataforma debe de contar con un MFA nativo para el acceso de terceros, esta debe tener un factor biométrico y passwordless.
- La plataforma propuesta debe contar con un servicio de directorio de terceros desde donde se pueda enrollar y asignar diferentes privilegios para el acceso de proveedores.

- La plataforma debe de proporcionar un esquema de acceso VPN-less a los proveedores, de tal manera que no sea necesario el uso de agentes para las conexiones remotas.
- La plataforma debe proporcionar un aislamiento, monitoreo y grabación de todas las sesiones que realicen los proveedores.
- La plataforma debe proporcionar un aplicativo móvil para que pueda ser utilizado como parte del segundo factor de autenticación, sin costo adicional.
- La plataforma debe ofrecer la escalabilidad y elasticidad necesaria para que puedan soportar las diferentes sesiones concurrentes, sin incurrir en un costo de licenciamiento adicional.
- La solución ofertada debe soportar conexiones remotas sin el uso de agentes VPN o de conexiones Ipsec.
- La solución ofertada de estar en la capacidad del monitoreo de sesiones remotas sin incurrir o alterar las acciones realizadas por el usuario privilegiado, de esta manera se podrá asegurar el no-repudio en el acceso.
- La solución ofertada debe estar en la capacidad de soportar múltiples sesiones remotas, a un mismo activo, respetando los principios del no-repudio.
- La solución deberá tener la capacidad de monitorear en tiempo real las sesiones privilegiadas establecidas.
- La solución deberá tener la capacidad de suspender la sesión privilegiada establecida.
- La solución deberá tener la capacidad de terminar la sesión privilegiada establecida.
- La solución no deberá permitir la interacción de dos usuarios sobre la misma sesión, dado que esto eliminaría el cumplimiento de registro de auditoría.
- La solución deberá tener la capacidad de evitar la manipulación de sesiones establecidas.
- La solución deberá tener la capacidad de descubrir cuentas privilegiadas humanas y no humanas.
- La solución deberá tener la capacidad de descubrir cuentas de servicio que tengan dependencias con aplicaciones o servicios ejecutados en la organización.

- La solución deberá tener la capacidad de descubrir usuarios y llaves SSH sobre sistemas Unix y Linux.
- La solución ofertada deberá tener la capacidad de descubrir credenciales en ambientes de nube pública.
- La solución ofertada deberá tener la capacidad de clasificar y proteger las cuentas privilegiadas que se hayan descubierto.
- La solución ofertada deberá proporcionar capacidades de escaneos de una sola vez o de manera recurrente para el proceso de descubrimiento.
- La solución ofertada deberá tener la capacidad de programar los escaneos.
- El fabricante de la solución deberá otorgar una metodología basado en las mejores prácticas para apoyar en el proceso de adopción de las plataformas, así como el manejo del descubrimiento y on-boarding de las cuentas privilegiadas.
- La solución ofertada deberá tener la capacidad de crear políticas para que las cuentas que se descubran sean protegidas en un esquema automatizado.
- La solución ofertada deberá tener la capacidad de descubrir credenciales de servicio o cuentas no humanas que puedan estar en archivos de configuración (xml, web.config, entre otros).
- La solución debe detectar incidentes de seguridad en cuentas privilegiadas no autorizadas y determinar la puntuación de riesgo general en función de todos los eventos de seguridad.
- La solución debe tener la capacidad de crear líneas de base matemáticas para que los usuarios regulares determinen el uso normal de sus cuentas privilegiadas.
- La solución debe tener la capacidad de notificar a los administradores de seguridad sobre eventos de alto riesgo utilizando los mecanismos de notificación adecuados, como informes, correo electrónico, mensajes de texto o sistemas externos, como dispositivos de gestión de eventos e información de seguridad (SIEM) o ITSM, cuando el riesgo supera un umbral especificado.
- La solución debe aprovechar el aprendizaje automático para crear un modelo de comportamiento para cada usuario privilegiado que pueda adaptarse automáticamente a medida que el trabajo del usuario y el acceso cambien con el tiempo.

- La solución debería tomar la corrección automática de una cuenta privilegiada detectada que ha sido comprometida.
- La solución debería detener la sesión del usuario privilegiado, requiriendo que el usuario se vuelva a autenticar cuando el riesgo exceda un umbral específico.
- "La solución debe permitirle a los administradores personalizar los rangos de puntuación (0 a 100) para las categorías:
  - Sin riesgo.
  - Riesgo bajo.
  - Riesgo medio.
  - Riesgo alto.
- La solución deberá tener la capacidad de ejecutar acciones de prevención ante un riesgo que pueda afectar la CIA de un activo.
- La solución deberá tener un motor de orquestación para desde ahí poder tomar acciones hacia plataformas terceras, via REST API.
- La solución deberá tener diferentes mecanismos de integración hacia plataformas de SIEM, tales como vía Web Hook, API, Syslog.
- La solución propuesta deberá tener la capacidad de orquestar y automatizar el ciclo de vida de la identidad.
- La solución propuesta deberá tener la capacidad de automatizar acciones sobre plataformas terceras.
- La solución propuesta deberá tener una librería de aplicaciones o plantillas para integrarse con aplicaciones terceras.
- La plataforma deberá tener una interfaz amigable y que no requiera ningún tipo de desarrollo de código para las integraciones con terceros.
- La solución propuesta deberá estar integrada como parte de la plataforma de PAM.
- La solución propuesta deberá soportar OpenID, Oauth 1.0, Oauth 2.0 y Client Credentials para autorizarse sobre aplicativos terceros.
- La plataforma deberá otorgar la capacidad de integrarse con sistemas en nube y en premisa.
- La plataforma deberá otorgar la capacidad de crear flujos dinámicos de acciones, enfocados con la identidad.

- La plataforma ofertada debe soportar el uso de API Rest para la integración con plataformas terceras.
- La plataforma ofertada no solo debe automatizar el ciclo de vida de la identidad sino también a automatizar los propios procesos de la plataforma de seguridad, así como prevenir o mitigar riesgos detectados como parte del monitoreo continuo del PAM en plataformas terceras.

5. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 7.

El adjudicatario deberá proveer una tecnología que posea las características especificadas a continuación para una solución de resguardo de configuraciones de dispositivos de seguridad y comunicaciones multimarca.

Requerimientos generales.

- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:
  - Deberá trabajar en forma integrada nativamente.
  - El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.
- Se requiere una suscripción a la solución de Resguardo de Configuraciones para 100 dispositivos de Seguridad.
- 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.

5.1 Especificaciones Técnicas.

- La Solución a proveer contará deberá ser brindada en modalidad virtual appliance, permitiendo mediante la misma el resguardo y la centralización y administración de archivos de configuración de 100 dispositivos de seguridad que forman parte de la infraestructura de CMCABA.
- Deberá contar con mecanismos de cifrado para el resguardo de los archivos correspondientes a los dispositivos administrados.
- La solución deberá analizar el archivo resguardado de configuración antes y después de su transferencia, de manera tal de asegurar la integridad del mismo.

- La comunicación entre los usuarios de la consola y la Consola de administración debe establecerse a través de un protocolo seguro.
- El acceso a la Solución por parte de los usuarios, deberá integrarse con esquemas de autenticación basados en LDAP / Microsoft AD.
- La Solución deberá soportar de forma nativa, los siguientes dispositivos de seguridad:
    - Linux (RHEL, CentOS, OpenSUSE) con opción de resguardo para:
        - Apache.
        - BIND.
        - SNMP.
        - OpenLDAP.
        - OpenSSH.
        - DHCP.
        - Squid.
        - Splunk.
        - FreeRADIUS.
        - OpenVPN.
        - Log files.
    - 3COM SuperStack 4400.
    - 3COM SuperStack 5500.
    - A10 Thunder SeriesA.
    - A10 Galaxy Management System.
    - Aruba Airwave.
    - ArubaOS-CX.
    - Barracuda NG Firewall.
    - Barracuda Web Application Firewall.
    - Barracuda Load Balancer.
    - Barracuda SPAM Firewall.
    - Barracuda Web Filter.
    - Carbon Black Response.
    - Check Point GAIA.
    - Check Point Scalable Platform.
    - Check Point SecurePlatform based devices.

- Check Point IP Series - IPSO (Nokia).
- Check Point SmartCenter.
- Check Point Provider-1.
- Check Point Smart-1.
- Check Point VSX.
- Check Point UTM Edge X.
- Check Point Connectra.
- Check Point SG80/1100 Series.
- Cisco ACE.
- Cisco ACS.
- Cisco ASA and FWSM (including contexts).
- Cisco FirePower Gateway & Management.
- Cisco IOS / IOS-XE / IOS-XR based devices.
- Cisco ISE.
- Cisco Ironport.
- Cisco ISE - Identity Service Engine.
- Cisco WLC - Wireless LAN Controllers.
- Citrix NetScaler (ADC) VPX, VDX.
- Citrix XenServer.
- F5 BigIP Series.
- F5 F5OS.
- FireEye EX Series.
- FireEye FX Series.
- FireEye HX Series.
- FireEye AX Series.
- FireEye CM Series.
- Fortinet FortiAnalyzer.
- Fortinet FortiAuthenticator.
- Fortinet FortiADC.
- Fortinet FortiGate.
- Fortinet FortiMail.
- Fortinet FortiManager.
- Fortinet FortiProxy.

- Fortinet FortiSandbox.
- Fortinet FortiSwitch.
- Fortinet FortiWeb.
- Imperva SecureSphere.
- Juniper JUNOS.
- McAfee Firewall Enterprise.
- McAfee Web Gateway.
- Mikrotik RouterOS.
- Palo Alto Firewall Platforms.
- Palo Alto Panorama Management.
- Trend Micro InterScan Web Security Virtual Appliance (ISWSVA).
- Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA).
- Integrarse con otras soluciones que usando copia de archivos mediante SCP y SFTP.

- Adicionalmente deberá soportar otros dispositivos, tales como:
  - APC Network Management Card (NMC).
  - AVI Networks Vantage.
  - Accedian VCX.
  - Accedian LTS.
  - Accedian GX.
  - Alcatel-Lucent Omnistack.
  - Alcatel-Lucent Omniswitch.
  - Allied Telesis Switches.
  - Arbor TMS.
  - Arbor SP.
  - Arbor APS.
  - Arbor AED.
  - Arista Switches EOS.
  - Arista.
  - Array Networks SPX.
  - Aruba Controllers.
  - Aruba Virtual Controllers (IAP).
  - Astaro Security Gateway.

- Audiocodes Mediant.
- Avocent Advanced Console Server (ACS).
- BalaBit SCB - Shell Control Box.
- BalaBit SSB - Syslog-ng .
- BalaBit STORE BOX.
- Big Switch Big Monitoring Fabric (BMF).
- Bloxx Web Filter.
- Blue Coat Content Analysis System (CAS).
- ProxySG/ASG.
- ProxyAV.
- Management Server.
- Director.
- PacketShaper.
- Bomgar.
- Brocade EdgeIron.
- Brocade FastIron.
- Brocade Fabric Switches.
- Brocade VDX Vyatta.
- Brocade NOS.
- Cisco ADE.
- Cisco APIC.
- Cisco CatOS (Catalyst) based switches.
- Cisco CBS - Cisco Business Switches.
- Cisco CSR/ASR.
- Cisco CSS.
- Cisco DNA Center (DNAC).
- Cisco ESA.
- Cisco ENCS - Enterprise Network Compute System.
- Cisco FireSIGHT IPS & Management Center (NGIPS).
- Cisco FXOS.
- Cisco IMC.
- Cisco Meraki GS.
- Cisco MDS storage switches.

- Cisco NX-OS Nexus switches.
- Cisco PIX.
- Cisco SG/SF.
- Cisco UCS - Cisco Unified Computing System.
- Cisco Unity Express.
- Cisco Viptela vManage.
- Cisco WAAS.
- Cisco WSA.
- Cisco Enterprise License Manager.
- Cisco Unified Presence.
- Cisco Emergency Responder.
- Cisco Unified Contact Center Express.
- Cisco Unity Connection.
- Cisco Meraki MS.
- Cisco Meraki MX.
- Cisco Meraki MR.
- Cisco Meraki Networks.
- Claroty Continuous Threat Detection (CTD).
- Claroty Clarity SRA.
- Consentry LANShield.
- Crossbeam C-Series.
- Crossbeam X-Series.
- Nvidia Cumulus Switches.
- D-Link DGS 3100.
- D-Link Dell Networking N-Series.
- D-Link Dell OS10.
- Dell N-Series.
- Dell S-Series.
- Dell SonicWall NSA.
- Dell Dell Networking OS10.
- Digi PortServer TS.
- Digi ConnectPort LTS.
- Digi CM.

- Efficient IP SOLIDServer.
- Enterasys Switches.
- ExtremeWare Switches.
- Extreme XOS Devices.
- Extreme BOSS.
- Extreme VOSS.
- Extreme WING.
- FarSite FarLinx Gateways.
- Forcepoint Web Security (previously WebSense).
- Forcepoint Mail Security (previously Websense Email Security Gateway).
- Fujitsu Fabric Eternus.
- GenieNetworks GenieATM .
- Genua genucenter.
- Gigamon GigaVUE.
- HP A-Series Switches.
- HP Blade System.
- HP Comware Switch.
- HP G-Series Switches.
- HP GbE2c .
- HP OfficeConnect.
- HP Procurve Switches.
- HP Synergy Switch Module.
- HP Virtual Connect Manager.
- Hillstone NG Firewall (StoneOs).
- Hirschmann RS.
- Hirschmann RSR.
- Hirschmann MS.
- Hirschmann OCTOPUS.
- Hirschmann PowerMICE.
- Hirschmann MACH.
- Huawei Switches (VRP).
- Huawei Routers (VRP).

- IBM SAN Volume Controller.
- IBM DataPower.
- IBM Integrated Management Module (IMM).
- IBM QRadar.
- Indeni Virtual Appliance.
- Infoblox NetMRI.
- Infoblox Network Appliance.
- Infoblox WAPI.
- Juniper JUNOS SPACE.
- Juniper SRX.
- Juniper J-series.
- Juniper M-series.
- Juniper MAG.
- Juniper Network Security Manager (NSM).
- Juniper ScreenOS-based devices (SSG, ISG, Netscreen Firewall, etc).
- Juniper Secure Access Series (Binary & XML).
- Juniper SA IVS.
- Juniper WLC (Trapeze).
- Juniper WXOS.
- Progress Kemp LoadMaster.
- Keysight Vision ONE.
- Keysight IXIA Vision One.
- Lantronix SLC Console Manager.
- Lenovo Flex System Fabric Scalable Switch.
- MRV LambdaDriver Management Module.
- MRV OptiDriver.
- Macmon appliances.
- Onyx Mellanox Onyx Advanced Ethernet Operating System.
- Microsens Switch.
- Mirapoint Message Server.
- Mirapoint RazorGate.
- Moxa Industrial Ethernet Switches.
- NetAPP FAS.

- NetApp ONTAP.
- NetScout PFOS.
- Netgate pfSense Firewall.
- Nokia IP Series (IPSO).
- Nokia SAR.
- Nomadix Access Gateway.
- Nortel 4500 Series.
- Nortel 5600 Series.
- Nortel 8300 / 8600 Series.
- Nortel Baystack.
- Nortel Ethernet Routing Switches (ERS).
- Nozomi N2OS devices.
- OPNsense Firewall.
- Opengear IM4200.
- Opengear IM7200.
- Oracle PDG.
- Oracle Session Router.
- Oracle SBC.
- Oracle SLB.
- Oracle SMX.
- Phoenix Contact mGuard.
- Pine-App Mail-SeCure.
- Proofpoint Enterprise Protection.
- Pulse Connect Secure.
- Qiata File Transfer Appliances.
- RSA Authentication Manager.
- Siemens RUGGEDCOM Routers and Switches (ROS & ROX).
- Radware Alteon.
- Radware AppDirector.
- Radware LinkProof.
- Radware vADC.
- Raisecom RAX devices.
- Riverbed SteelHead.

- Riverbed SteelFusion Core.
- Ruckus ZoneDirector.
- Ruckus SmartZone.
- SEPPMail Appliances.
- SafeNet DataSecure.
- SafeNet Network HSM.
- SentinelOne Hologram (previously Attivo BOTsink).
- Silver Peak NX Appliances.
- Silver Peak VX Appliances.
- Smoothwall Secure Web Gateway.
- Sonus Tenor DX VOIP Switch.
- Stonesoft StoneGate SMC.
- Stormshield UTM Firewall.
- Symantec Encryption Management Server.
- Symantec Messaging Gateway (Brightmail).
- DSM.
- TP-Link Smart Switch.
- Tenable Nessus vulnerability assessment.
- TippingPoint SMS.
- Tufin T Series Appliances.
- Tufin Virtual Appliance.
- Tufin Aurora.
- Ubiquiti AirOS devices.
- VMWare ESX Hypervisor.
- Vectra Networks X-Series.
- Viptela vManage.
- Wallix Bastion.
- WatchGuard Firebox X.
- WatchGuard XTM.
- ZPE NodeGrid.
- Zertificon SecureMail.
- Zertificon Z1.
- Zhone CPE.

  - Zhone MALC.
  - Zhone Raptor XP.
  - Varmour Application Controller.
- Deberá contar con un inventario actualizado de dispositivos gestionados, contando como mínimo, con la siguiente información de los mismos:
  - Adjuntar Número de IP.
  - Número de Serie.
  - Datos de Marca.
  - Modelo.
  - Registro Tipo (de acuerdo a los administrados nativamente por la solución).
  - Grupo del cual va a formar parte.
  - Identificación - Nombre del Dispositivo (resolviéndolo automáticamente por consulta al DNS).
  - Prefijo para los archivos generados.
  - Adjuntar Responsable.
  - Ubicación.
  - Nomenclatura de Mail para envío de notificaciones.
  - Contrato de soporte.
  - Fecha de compra.
  - Fecha de expiración de mantenimiento.
  - Configuración de credenciales para la operatoria sobre el dispositivo.
  - Política definiendo las tareas y su ejecución en el tiempo (Schedule).
- Deberá permitir la creación de campos adicionales, a los definidos precedentemente, para la inclusión de información adicional sobre un dispositivo.
- Deberá contar con la posibilidad de configurar alertas, sobre el campo que contemple la fecha de renovación de soporte de los dispositivos administrados.
- La solución deberá permitir el agregado de dispositivos:
  - Manualmente.
  - Importándolos desde un archivo CSV.
- La solución deberá emitir alertas en el caso de que sean descubiertos nuevos dispositivos de red.

- Se deberá poder definir grupos de dispositivos administrados, a los cuales se le podrá determinar el uso de una política determinada.
- Se deberá poder definir políticas, contemplando la configuración del mantenimiento en el tiempo de las versiones a resguardar de las configuraciones, tareas a ejecutar sobre los dispositivos y frecuencia de ejecución, las cuales podrán ser aplicadas a un dispositivo o grupo de dispositivos, de manera diferenciada.
- Deberá permitir la ejecución de comandos en los dispositivos administrados, pudiendo visualizarse, desde la consola de administración la salida de la ejecución.
- Deberá permitir la instalación de agents que ayuden a gestionar dispositivos remotos que no son directamente accesibles por la tecnología.
- Deberá permitir la configuración de dominios de administración para organizar los dispositivos y separar / delegar su gestión en grupos diferentes.
- Desde la consola de administración, se deberá poder visualizar el estado general de la solución contemplando como mínimo:
    - Eventos críticos.
    - Dispositivos con cambios en su configuración.
    - Actividad de los usuarios de la solución.
    - Dispositivos administrados.
    - Operaciones en curso.
- Deberá permitir la ejecución de monitoreo sobre los puertos definidos para la conexión tcp, definida para un dispositivo o grupo de dispositivos, debiendo generar alertas vía e-mail en caso de detectarse alguna falla.
- Deberá contar con la funcionalidad de comparar configuraciones. Permitiendo definir una configuración de base, con el objetivo de poder detectar los cambios con relación a configuraciones posteriores, informando de las mismas mediante, como mínimo, e-mail y syslog.
- Deberá contar con la posibilidad de ejecutar templates de cambios a los dispositivos, como mínimo para cambiar las siguientes variables:
    - Radius Server.
    - VLAN Ip Address.
    - VLAN Netmask.
    - Default gateway.

- Deberá contar con la posibilidad de cargar e instalar imágenes a nivel firmware en los dispositivos.
- Deberá contar con la posibilidad de clonar la configuración de un dispositivo en otro para duplicarlo.
- Deberá permitir la ejecución de tareas, sobre los dispositivos administrados, en forma manual, por fuera de la política de ejecución definida.
- Deberá permitir la visualización de los archivos de configuración resguardados.
- La Consola de Administración deberá resumir la actividad efectuada sobre un dispositivo en particular o grupo de dispositivos, tanto en tiempo real como en períodos de tiempo a definir por el usuario.
- La solución deberá permitir la asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y consulta.
- Deberá contar con un esquema de roles que permita separar la administración de un dispositivo o grupo de dispositivos, para un usuario en particular.
- Deberá contar con reportes preconfigurados y la opción de reportes configurables, contemplando como mínimo:
    - Operaciones efectuadas satisfactoriamente.
    - Operaciones fallidas.
    - Cambios de configuración.
    - Actividad de usuario.
    - Programación de ejecución de reportes.
- Los reportes deberán contemplar periodos de tiempo, definidos por el usuario.
- Deberá permitir exportar los reportes, como mínimo a los siguientes formatos: HTML, PDF, XML, CSV, o ser exportados a un formato de texto estándar, para poder utilizar herramientas de análisis de terceros.
- Deberá permitir la generación de alarmas, ante eventos a definir desde la consola de administración.
- Deberá contar con un módulo de auditoría que resguarde toda la actividad de los usuarios y los procesos automáticos que componen la solución.
- La solución deberá permitir la generación de un archivo, definiendo los comandos a ejecutarse sobre un dispositivo no administrado nativamente por la solución, para efectuar el backup o posterior recuperación del mismo, sobre el dispositivo.

- Deberá brindar la posibilidad de actualizar la tecnología en línea o en modo fuera de línea.
- Deberá contar con políticas de cumplimiento por dispositivos, las cuales:
    - Alerten por cantidad de violaciones de Alto, Bajo y medio nivel.
    - Chequee líneas de configuración bajo formato Regex.
    - Brinde capacidad de remediar configuraciones erróneas.
    - Brinde capacidad de definir nuevas reglas mediante formato LUA.
    - Chequee configuración de políticas de password.
- Deberá contar con un dashboard de status de actividad donde se informe como mínimo:
    - % Backups realizados en las últimas 24 horas.
    - Dispositivos en cumplimiento.
    - Dispositivos en línea.
    - Storage utilizado.
    - Memoria utilizada.
    - Status de Virtual Appliance.
    - Últimas actividades de usuario.
    - Últimos cambios de configuración.
    - Últimos eventos críticos.
- Deberá contar con logs de Eventos y un sistema del tipo syslog.
- Deberá contar con una completa gestión de usuarios administrativos, con las siguientes funciones:
    - Usuario y password.
    - Password de cifrado.
    - Link de activación de cuenta si npassword por email.
    - Expiración de password.
    - Uso de radius.
    - Uso de ldap.
    - Uso de TOTP como ser Google Authenticator, Authy y KeeOtp.
- Capacidad de añadir nuevos roles basado en permisos sobre los dispositivos, backups, templates, firmware y compliance.

6. ESPECIFICACIONES TÉCNICAS RENGLONES 2, 4, 6 y 8.

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, 5 y 7 por el plazo de treinta y seis (36) meses, contados a partir desde la fecha indicada en el parte de recepción definitiva de 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.
- Deberá incluir 3 recursos full time con nivel SemiSenior, dedicado a la gestión de las soluciones ofertadas por el lapso del contrato, pudiendo trabajar en forma remota sobre la plataforma de CMCABA.
- 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.

- Contrato de nivel de servicio:

(*) Se entiende por "funcionalidades críticas" aquellas que interfieren con los procesos de aseguramiento (atención de reclamos), provisión, relacionados en forma directa con el servicio comprometido con el cliente (SLA).

- **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.

- **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 reléase)

- **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.

7. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 9

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.

8. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 10.

El adjudicatario deberá brindar el servicio de capacitación oficial de todas las nuevas soluciones a proveer, en los Renglones 1, 3, 5 y 7, el que deberá contar al menos con las siguientes características:

Cada una de las capacitaciones deberá ser brindada 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.