C.A.B.A., 13 de agosto de 2026

RES - SAGYP - N° 529 / 2026

VISTO:

La actuación TAE 01-00024152-7/2026 caratulado *"D. G. C. C. S/ PLAN INTEGRAL DE CIBERSEGURIDAD ETAPA IV"*; y,

CONSIDERANDO:

Que por la actuación citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, por la adquisición, implementación, mantenimiento y soporte técnico de soluciones especializadas de ciberseguridad, protección de datos, gobierno de la información, privacidad, seguridad cloud y gestión integral de cumplimiento y riesgo tecnológico 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 a los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas (v. Notas 2F DGIYT 433/26 y 694/26 y Adjuntos 114893/26 y 114894/26).

Que en ese marco, la Dirección General de Compras y Contrataciones entendió viable el llamado a Licitación Pública de etapa única, bajo la modalidad de llave en mano, conforme lo dispuesto en los artículos 26, 28, 32, 33, 40, 45 y concordantes de la Ley Nº 2.095 -según texto consolidado por Ley Nº 6.764-, la Resolución CM Nº 276/2020 y la Resolución SAGyP N° 30/2021 (v. Adjunto 118558/26).

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 126802/26 y 126803/26, respectivamente, y estableció como presupuesto oficial de la contratación en la suma dólares estadounidenses nueve millones ciento setenta y un mil (U$S 9.171.000.-). 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 Ochocientos Mil ($ 800.000.-), para participar en la Licitación Pública N° 2-0031-LPU26." (v. MEMO 2063/26).

Que la Ley N° 6.302, al modificar la Ley N° 31, creó la Secretaría de Administración General y Presupuesto y estableció dentro de sus funciones la de ejecutar, bajo el control de la Comisión de Administración, Gestión y Modernización Judicial, el presupuesto anual del Poder Judicial de la Ciudad Autónoma de Buenos Aires (cfr. inc. 4 del art. 27 de la Ley N° 31 -texto consolidado según Ley N° 6.764-) y la de realizar las contrataciones de bienes y servicios (cfr. inc. 6 del art. 27 de la Ley N° 31 -texto consolidado según Ley N° 6.764-).

Que en atención a los antecedentes antes relatados, de acuerdo a lo actuado por la Dirección General de Compras y Contrataciones, a lo solicitado por la Dirección General de Informática y Tecnología, sobre la necesidad de impulsar la contratación de marras para optimizar la administración, trazabilidad, seguimiento y coordinación de tareas, incidencias, proyectos y flujos de trabajo institucionales del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, y en línea con lo dictaminado por la Dirección General de Asuntos Jurídicos, corresponde aprobar los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran vinculados como Adjuntos 126802/26 y 126803/26, respectivamente, y llamar a Licitación Pública N° 2-0031-LPU26, de etapa única, bajo la modalidad de llave en mano, por la adquisición, implementación, mantenimiento y soporte técnico de soluciones especializadas de ciberseguridad, protección de datos, gobierno de la información, privacidad, seguridad cloud y gestión integral de cumplimiento y riesgo tecnológico para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de nueve millones ciento setenta y un mil (U$S 9.171.000.-), para el día 31 de agosto de 2026 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° 2-0031-LPU26, y realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.764), su reglamentación y en la Ley de Procedimientos Administrativos -Decreto 1.510/97- (texto consolidado según Ley N° 6.764).

Que en cumplimiento de la Ley N° 70 (texto consolidado según Ley N° 6.764), la Dirección General de Programación y Administración Contable tomó conocimiento y realizó la afectación correspondiente junto con la nota de compromiso presupuestario para hacer frente la contratación de marras (v. Adjuntos 122011/26 y 121743/26).

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 15205/2026.

Que por la Resolución Presidencia N° 155/2024, ratificada por Resolución CM N° 63/2024, se designó como reemplazo transitorio de la Secretaria de Administración General y Presupuesto del Poder Judicial a la Dra. Clara María Valdez, al amparo de lo dispuesto por el artículo 35 de la Ley N° 31 (texto consolidado según Ley N° 6.764).

Por lo expuesto y en el ejercicio de las atribuciones conferidas por las Leyes Nros. 31 y 2.095 (ambos textos consolidados según Ley N° 6.764), la Resolución CM N° 276/2020, modificada por la Resolución CM N° 248/2024, y la Resolución Presidencia N° 155/2024;

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

Artículo 1º: Apruébanse los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, que como Adjuntos 126802/26 y 126803/26 forman parte de la presente Resolución y regirán para la Licitación Pública N° 2-0031-LPU26, de etapa única, bajo la modalidad de llave en mano, por la adquisición, implementación, mantenimiento y soporte técnico de soluciones especializadas de ciberseguridad, protección de datos, gobierno de la información, privacidad, seguridad cloud y gestión integral de cumplimiento y riesgo tecnológico para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses nueve millones ciento setenta y un mil (U$S 9.171.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0031-LPU26, 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 el día 31 de agosto de 2026 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° 2-0031-LPU26, será por un monto de pesos ochocientos mil ($800.000.-).

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0031-LPU26, a los Dres. Matías Vázquez y Adrián Costantino como miembros titulares, y a los Dres. Hernán Labate y Fabian Leonardi 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° 2-0031-LPU26, y para que realice las publicaciones y notificaciones de este acto conforme lo establecido en la Ley N° 2.095 (texto consolidado según Ley N° 6.764) su reglamentaria Resolución CM N° 276/2020 y modificatoria, y en la Ley de Procedimientos Administrativos - Decreto 1.510/97- (texto consolidado según Ley N° 6.764).

Artículo 6°: Publíquese en la página web del Consejo de la Magistratura y en el Boletín Oficial del Gobierno de la Ciudad Autónoma de Buenos Aires, comuníquese por comunicación oficial mediante SISTAE a la Dirección General de Informática y Tecnóloga y a la Dirección General de Programación y Administración Contable. Pase a la Dirección General de Compras y Contrataciones para sus efectos.

FIRMAS DIGITALES

Firmado digitalmente por:
VALDEZ, CLARA
SEC DE ADMIN GRAL Y
PRESU DEL P JUD
CMCABA
Fecha: jueves, 13 agosto
2026 09:59:29

LICITACION PÚBLICA N° 2-0031-LPU26

PLAN INTEGRAL DE CIBERSEGURIDAD – ETAPA IV

PLIEGO DE BASES Y CONDICIONES PARTICULARES

ANEXO I - DECLARACIÓN JURADA DE APTITUD PARA CONTRATAR

ANEXO II - DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA

ANEXO III - DECLARACIÓN JURADA DE INCOMPATIBILIDAD

ANEXO IV – CERTIFICADO DE VISITA

PLIEGO DE BASES Y CONDICIONES PARTICULARES

1. GENERALIDADES

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

2. OBJETO DE LA CONTRATACIÓN

La presente es una licitación pública de etapa única, bajo la modalidad de llave en mano, que tiene por objeto la adquisición, implementación, mantenimiento y soporte técnico de soluciones especializadas de ciberseguridad, protección de datos, gobierno de la información, privacidad, seguridad cloud y gestión integral de cumplimiento y riesgo tecnológico para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires.

3. PRESUPUESTO OFICIAL

El presupuesto oficial de la presente Licitación Pública asciende a la suma total de **Dólares Estadounidenses Nueve Millones Ciento Setenta y Un Mil (U$S 9.171.000.-)**, conforme al siguiente detalle:

Renglón 1: Dólares Estadounidenses Novecientos Mil (U$S 900.000.-).

Renglón 2: Dólares Estadounidenses Ochocientos Mil (U$S 800.000.-).

Renglón 3: Dólares Estadounidenses Quinientos Cincuenta Mil (U$S 550.000.-).

Renglón 4: Dólares Estadounidenses Un Millón Trescientos Mil (U$S 1.300.000.-).

Renglón 5: Dólares Estadounidenses Un Millón Novecientos Cincuenta Mil (U$S 1.950.000.-).

Renglón 6: Dólares Estadounidenses Cuatrocientos Mil (U$S 400.000.-).

Renglón 7: Dólares Estadounidenses Un Millón Quinientos Cincuenta y Un Mil (U$S 1.551.000.-).

Renglón 8: Dólares Estadounidenses Un Millón Trescientos Cincuenta Mil (U$S 1.350.000.-).

Renglón 9: Dólares Estadounidenses Trescientos Setenta Mil (U$S 370.000.-).

4. RENGLONES A COTIZAR

Renglón 1: Provisión de una solución de identificación, descubrimiento, clasificación y gobierno de la información alojada en la infraestructura tecnológica del Consejo de la Magistratura de la

Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Provisión de una solución para brindar visibilidad, monitoreo y control de seguridad sobre aplicaciones y servicios cloud mediante conexiones directas a las APIs provistas por plataformas SaaS de la suite Microsoft 365 para analizar actividad y contenido ya almacenado en la nube sin interceptar el tráfico en tiempo real, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 3: Provisión de una solución para prevención de fuga de información y control del uso de datos en los distintos entornos tecnológicos del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 4: Provisión de una solución para implementación de controles de prevención de fuga de información en dispositivos endpoint del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 5: Provisión de una solución para brindar visibilidad completa sobre los activos que conforman la superficie tecnológica del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 6: Provisión de una solución para brindar visibilidad, control y protección sobre aplicaciones, servicios digitales avanzados y componentes de procesamiento automatizado de información utilizados por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 7: Servicio de garantía, mantenimiento, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de las soluciones provistas en los renglones 1, 2, 3, 4, 5 y 6, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 8: Implementación de las soluciones provistas en los renglones 1, 2, 3, 4, 5 y 6, incluyendo todos los elementos necesarios, la instalación en sitio, puesta en marcha y configuración de acuerdo con las necesidades establecidas por el Consejo de la Magistratura de la

Ciudad Autónoma de Buenos Aires, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 9: Servicio de capacitación oficial de todas las soluciones a proveer en los Renglones 1, 2, 3, 4, 5 y 6, conforme lo indicado 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 Ochocientos Mil ($ 800.000.-)** y podrá abonarse mediante depósito en efectivo o por transferencia bancaria a la Cuenta Corriente $ N° 000306800050213214, a nombre del Consejo de la Magistratura, en el Banco de la Ciudad de Buenos Aires, Sucursal Nº 52, sita en Av. Presidente Roque Sáenz Peña 541 de esta Ciudad, CBU 0290068100000502132146, CUIT 30-70175369-7.

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

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

6. PLAZOS DE LA CONTRATACIÓN

6.1 Plazo de la Contratación

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

6.2 Plazo de Ejecución Renglones 1, 2, 3, 4, 5, 6 y 8

La adjudicataria deberá proceder a la provisión e implementación de las soluciones requeridas dentro de los 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 7

Los servicios solicitados tendrán un plazo de vigencia de treinta y seis (36) meses, contados a partir de la fecha indicada en el parte de recepción definitiva de la provisión e implementación de las soluciones requeridas.

6.4 Plazo de Ejecución Renglón 9

Las capacitaciones deberán ser efectuadas dentro de los noventa (90) días corridos, contados a partir del perfeccionamiento de la correspondiente Orden de Compra en la Plataforma JUC.

7. MODALIDAD DE LA CONTRATACIÓN

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

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

8. REPRESENTACIÓN OFICIAL. CANAL AUTORIZADO

El oferente deberá contar con expresa autorización de cada uno de los fabricantes, mediante una carta que incluya los datos de la presente licitación, para la presentación de propuestas y la provisión de lo ofertado.

Asimismo, deberá ser un canal de venta y soporte técnico local y autorizado, condición que deberá mantenerse durante todo el plazo de vigencia de la contratación.

Será requisito que las tecnologías a proveer en los renglones 3 y 5 sean de un único fabricante, por lo siguiente:

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

9. CONDICIONES PARA SER OFERENTE

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

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

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

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

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

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

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

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

1. El compromiso de mantener la vigencia de la U.T., por un plazo superior a la duración de la contratación, incluyendo una eventual prórroga contractual.
2. El compromiso de mantener la composición de la U.T. durante el plazo mencionado en el inciso anterior, así como también de no introducir modificaciones en los estatutos de las empresas integrantes que importen una alteración de la responsabilidad, sin la previa aprobación del Consejo.
3. Designación de uno o más representantes legales que acrediten, mediante poder para actuar ante la administración pública, facultades suficientes para obligar a su mandante.
4. De los documentos por los que se confieran los poderes y por los que se constituya la U.T., deberá resultar que los otorgantes o firmantes lo hicieron legalmente, en ejercicio de las atribuciones que les corresponden como autoridades de cada una de las empresas en funciones, en el momento del acto respectivo.
5. Las empresas integrantes de la U.T. serán solidariamente responsables por el cumplimiento del Contrato en caso de adjudicación. Cada una de las Sociedades Comerciales que integren la U.T., deberán presentar acta del órgano social correspondiente de la cual surja la decisión de presentarse a esta licitación pública por contrato asociativo de unión transitoria. A tal efecto, el Consejo intimará a los oferentes para que en el plazo perentorio de dos (2) días a contar desde el día

siguiente al de la recepción de la intimación, se subsane la deficiencia, bajo apercibimiento de desestimarse la oferta.

10. DECLARACIONES JURADAS

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

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

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

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

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

12. CORREO ELECTRONICO Y CONSTITUCIÓN DE DOMICILIO

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

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

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

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

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

13. INFORMACIÓN SOCIETARIA Y HABILIDAD PARA CONTRATAR CON EL ESTADO

Los oferentes deberán cumplir con:

1. Información Societaria

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

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

2. Consulta ARCA

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

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

14. FORMA DE COTIZACION

Las propuestas económicas deberán ser formuladas electrónicamente, a través de la plataforma JUC -juc.jusbaires.gob.ar-, de conformidad con el artículo 12 del PCG, en números y en letras conforme se detalla a continuación:

Renglones 1, 2, 3, 4, 5, 6, 8 y 9:

14.1 Precio Total de cada Renglón, en Dólares Estadounidenses.

Renglón 7:

14.2 Precio Mensual y Precio Total del Renglón, en Dólares Estadounidenses.

Monto Total:

14.3 Monto Total de la Oferta, en Dólares Estadounidenses.

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. CAPACIDAD ECONÓMICO FINANCIERA

A los efectos de acreditar su capacidad económica financiera, cada oferente deberá presentar junto con la propuesta la siguiente documentación:

Estados contables correspondientes a los dos (2) últimos ejercicios anuales firmados por Representante Legal y Contador Público, certificada su firma por el Consejo Profesional de Ciencias Económicas de la jurisdicción correspondiente, así como copia legalizada de las Actas de las Asambleas aprobatorias de los mismos, los cuales deberán tener resultado Positivo. En caso de U.T. la documentación señalada deberá ser presentada por cada uno de los integrantes.

En el caso de Personas Humanas deberá acompañarse el último Estado de Situación Patrimonial y de Resultados correspondientes para fines fiscales, con sus respectivas declaraciones juradas de impuesto a las ganancias con firma autógrafas en todas sus hojas por parte del Oferente o Representante Legal y Dictamen de Contador interviniente, certificada por el Consejo Profesional de Ciencias Económicas de la jurisdicción en donde se encuentre matriculado

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° 6.764-:

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

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

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

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

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

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

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

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

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

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

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

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

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

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 6.764-.

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

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

24. PERSONAL DE LA ADJUDICATARIA

24.1 Nómina de Personal

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

- Nombre y Apellido
- DNI
- Domicilio Actualizado

- Función que desempeña

24.2 Responsabilidad por el Personal

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

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

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

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

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

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

24.3 Daños a Terceros

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

24.4 Exclusión

El Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires se reserva el derecho de

la Exclusión de cualquier personal, recurso, ayudante o coordinador mientras dure la relación contractual.

25. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO

25.1 Certificación de Conformidad

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

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

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

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

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

25.2 Pago

Todos los pagos 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 correspondiente factura.

Renglones 1, 2, 3, 4, 5, 6 y 8:

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

Renglón 7:

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

Renglón 9:

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

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

26. PENALIDADES

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

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

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

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

27. CONSULTAS

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

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

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

28. COMUNICACIONES

Todas las comunicaciones que se realicen entre el Consejo de la Magistratura y los interesados, oferentes y adjudicatarios, que hayan de efectuarse en virtud de las disposiciones de la Ley N° 2.095 (texto consolidado según Ley N° 6.764) y su reglamentación se entienden realizadas a través

del envío de mensajería mediante JUC en forma automática, y a partir del día hábil siguiente al de su notificación.

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

ANEXO I

DECLARACION JURADA DE APTITUD PARA CONTRATAR

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

FIRMA

…….

ACLARACION

…….

CARÁCTER

……

Ciudad de Buenos Aires, de… …de…….

ANEXO II

DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA

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

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

……

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

ANEXO III

DECLARACIÓN JURADA DE INCOMPATIBILIDAD

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

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

…….

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

FIRMAS DIGITALES

Firmado digitalmente por:
DIAZ, GASTON FEDERICO
DIRECTOR
CMCABA
Fecha: lunes, 03 agosto 2026
15:46:46

LICITACION PÚBLICA N° 2-0031-LPU26

PLAN INTEGRAL DE CIBERSEGURIDAD – ETAPA IV

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 prestación y para que ésta responda a sus fines y objetivos, considerándose esos trabajos incluidos en los precios de su oferta.

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

Asimismo, y complementariamente a lo expresado en el párrafo anterior, los errores o las eventuales omisiones que pudieran existir en la presente documentación y especificaciones técnicas no invalidarán la obligación de la empresa de ejecutar las tareas y proveer, instalar y poner en servicio los materiales y equipos en forma completa y correcta, de acuerdo a los fines a los que están destinados.

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

2. ESPECIFICACIONES TÉCNICAS RENGLÓN 1

El adjudicatario deberá proveer tecnologías orientadas a la identificación, descubrimiento,

clasificación y gobierno de la información alojada en la infraestructura tecnológica del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, incluyendo entornos on-premise, virtualizados, servicios en la nube, repositorios estructurados y no estructurados, con el objeto de dotar al organismo de capacidades de visibilidad y gestión sobre los datos sensibles, críticos o regulados.

- Se deberá proveer la solución por un plazo de treinta y seis (36) meses
- La solución deberá estar licenciada para poder cubrir el análisis de 100 TB al inicio del primer año, crecer hasta 150 TB al inicio del segundo y por último llegar a 200 TB al inicio del tercer año.

Requerimientos Generales

- La solución deberá poseer un puntaje igual o mayor a 4.6 en Gartner Insights en Data Security Posture Management y Metadata Management Solutions.

Requerimientos Funcionales

- La herramienta deberá poder ser implementada en ambientes de nube es decir modalidad SaaS (Software as a Service)
- La herramienta deberá poder ser implementada en ambientes en nube del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires y nubes públicas (AWS, Azure, GCP y otras)
- La herramienta deberá poder ser implementada en ambientes On Premise
- La herramienta deberá permitir una arquitectura distribuida incluyendo ambientes on-premise, cloud, híbridos, multi-cloud, y multi-datacenter
- La herramienta deberá permitir una instalación rápida mediante la utilización de Kubernetes a través de frameworks EKS, GKE, AKS, OpenShift etc.
- La herramienta deberá poseer opciones de comunicación segura entre todos sus componentes, con criptografía SSL y certificados homologados por el fabricante
- La herramienta deberá posibilitar la integración abierta con las aplicaciones y sistemas del cliente a través de REST API
- La herramienta deberá contar con tecnología para soportar, repositorio de metadatos con opción de replicación en alta disponibilidad
- La herramienta deberá permitir escalamiento horizontal en los ambientes Kubernetes para atender tareas computacionales intensas (elasticidad)

- La herramienta deberá permitir la instalación remota de los escáneres para realizar el descubrimiento próximo a las fuentes de datos, a fin de minimizar la transferencia de datos y costos de "egress" (en caso aplicable)
- La herramienta deberá permitir una arquitectura abierta con desarrollo customizado, para la ampliación de las funcionalidades nativas, como creación de nuevos módulos y conectores adicionales
- La herramienta deberá posibilitar la integración con proveedores de identidad IDM a través de protocolos SAML o LDAP para autenticación de usuarios en la plataforma
- La herramienta deberá posibilitar la utilización de RBAC (Role Based Access Control), con la posibilidad de customización, para definir diferentes perfiles de acceso a las funcionalidades de la plataforma
- La herramienta deberá posibilitar la utilización de RBAC (con la posibilidad de customización) para definir diferentes perfiles de acceso a los resultados del descubrimiento de datos
- La herramienta deberá permitir la auditoría de los accesos realizados a la plataforma, ya sea a través de la interfaz de usuario o directamente a través de integraciones vía APIs.
- El acceso a la herramienta debe realizarse mediante protocolo web, para el acceso mediante navegadores web mediante un canal HTTPS protegido.
- La herramienta debe permitir la integración nativa con plataformas de gestión como Jira, Service Now, etc.
- La herramienta debe permitir la integración nativa con herramientas de gestión de contraseñas (bóveda de contraseñas) como "Contraseña Segura", CyberArk, etc.
- La herramienta debe permitir la integración nativa con otros catálogos de datos o la importación de información ya catalogada.
- La herramienta debe permitir el descubrimiento automático (incorporación) de todas las fuentes disponibles en las nubes, como GCP, Azure o AWS.

Inventario de Datos

- La herramienta debe integrarse de forma nativa con fuentes de datos estructuradas, semiestructuradas y no estructuradas, como:
    - Bases de datos: Oracle, PostgreSQL, MongoDB y SQL Server
    - Big Data (con Kerberos): HDFS, Hive y Hbase

  - Sistemas de archivos: S3 local, NFS y SMB
  - Aplicaciones: ServiceNow y SAS
  - Office 365: SharePoint, OneDrive, Teams y Outlook
  - IA: Atlas Vector Search, Azure OpenAI, OpenAI, HuggingFace
  - Otros: Elastic Search y Kafka

- La herramienta también debe permitir la integración con Unisys (DMSII), TOTVS ERP y monitoreo de Elastic APM.
- La herramienta debe integrarse de forma nativa con las fuentes de datos a través del protocolo API REST
- La herramienta debería permitir la creación de conectores personalizados con SDK
- La herramienta debe permitir la ejecución separada del escaneo de metadatos y datos.
- La herramienta debe permitir realizar escaneos rápidos para obtener rápidamente "hallazgos" iniciales, antes de realizar el escaneo completo.
- La herramienta debe permitir la clasificación de datos PI (información personal) y PII (información de identificación personal)
- La herramienta debe soportar el uso de expresiones regulares para descubrir datos personales en tecnologías que almacenan datos estructurados y no estructurados.
- La herramienta debe permitir la definición de excepciones para expresiones regulares mediante diccionarios de términos o expresiones regulares personalizadas.
- La herramienta debe tener de forma nativa al menos las siguientes clasificaciones/dominios de datos:
  - Datos de identificación personal: Cédula, RUT, RUN, RUC, tarjeta de registro de elector, tarjeta nacional de salud, pasaporte
  - Datos personales: nombre y apellidos, fecha de nacimiento, etnia, color, nivel educativo, género, identidad y orientación sexual, estado civil, nacionalidad, religión
  - Datos de contacto: correo electrónico, teléfono móvil, teléfono fijo, dirección, código postal
  - Datos financieros: tarjeta de crédito y débito, CVV, IBAN
  - Contraseñas y secretos: Contraseña, Token, Secreto, Clave API, Clave OAuth2,

Clave privada PGP, Clave privada PKCS, Clave de licencia

- Datos electrónicos: IPv4, IPv6, IMEI, MAC

- La herramienta debe ayudar y permitir la generación automática de expresiones regulares a partir de muestras y probar su correcto funcionamiento.
- La herramienta debe permitir la inclusión de nuevas expresiones regulares y soportar la búsqueda de términos cercanos al valor, para reducir los falsos positivos.
- La herramienta debe permitir la verificación de sumas de comprobación de los valores analizados, cuando corresponda, para reducir los falsos positivos; por ejemplo, dígitos de control CPF, algoritmo de Luhn, etc.
- La herramienta debe permitir el escaneo mediante algoritmos de aprendizaje automático en datos no estructurados.
- La herramienta debería permitir el escaneo lateral, utilizando instantáneas de las bases de datos (cuando corresponda), para reducir el impacto en los entornos de producción.
- La herramienta debe soportar el uso de tecnología OCR para clasificar texto en imágenes (BMP, JPG, PNG, PDF, TIFF, etc.) e imágenes contenidas en documentos.
- La herramienta debe permitir la clasificación de objetos según niveles de sensibilidad como datos restringidos, confidenciales, de uso interno y públicos.
- La herramienta debe permitir la personalización y creación de otros niveles de sensibilidad, así como permitir la definición de más de una clasificación de sensibilidad.
- La herramienta debe soportar el entrenamiento de modelos de redes neuronales para clasificar archivos empresariales, como currículums, facturas, boletas, etc.
- La herramienta debe permitir la configuración de ventanas de mantenimiento durante las cuales se puedan analizar los sistemas y, de ser necesario, suspender y reanudar automáticamente el análisis.
- La herramienta debe poder clasificar y buscar datos sin conservar copias de datos personales.
- La herramienta debe tener la capacidad de optimizar el tiempo de escaneo de datos no estructurados utilizando aprendizaje automático, creando modelos predictivos basados en metadatos.
- La herramienta debe ofrecer un catálogo de todo tipo de activos de datos (tablas, archivos, colas, etc.) e IA (vectores, modelos, conjuntos, etc.), actualizado automáticamente, de

forma programada y sin intervención manual.

- La herramienta debe permitir la colaboración del usuario en comentarios y objetos/activos, permitiendo que el usuario se convierta en seguidor del objeto.
- La herramienta debe poder indicar por columna (si corresponde) las respectivas clasificaciones de los datos PI y PII encontrados.
- La herramienta debe poder indicar por columna (si corresponde) a qué tipos de datos, % distintos, % nulos y valores mínimos y máximos, etc.
- La herramienta debe poder indicar todas las clasificaciones de datos PI y PII que se encuentran en el objeto.
- La herramienta debe permitir la revisión de muestras de datos que coincidan con expresiones regulares para eliminar falsos positivos (FP).
- La herramienta debe indicar puntuaciones de riesgo en diferentes niveles de activos, como: columnas, atributos, objetos, entidades, sistemas fuente.
- La herramienta debe tener la capacidad de agregar etiquetas a las propiedades de los objetos (columnas, si corresponde), para que se pueda identificar su clasificación.
- La herramienta debe permitir la personalización de las etiquetas y su aplicación automática según criterios preestablecidos.
- La herramienta debería permitirle realizar una “vista previa” del contenido del objeto (y de la columna, en el caso de las tablas), sin crear copias permanentes de los datos.
- La herramienta debe permitir cargar y exportar el contenido del catálogo de datos a través de la API REST.
- La herramienta debe indicar la correlación entre datos de diferentes objetos y conectarlos gráficamente, con un índice de confianza.
- La herramienta debe indicar si un archivo se puede duplicar, incluso si está en un formato diferente y/o en sistemas diferentes.
- La herramienta debe poder indicar columnas similares, a través del análisis de los datos almacenados.
- La herramienta debe indicar tablas similares encontradas en otros sistemas, según el nivel porcentual de similitud.
- La herramienta debe permitir la agrupación de archivos en grupos lógicos, que contengan las mismas características (Factura, CV, Tarjeta de embarque, etc.)

- La herramienta debe poder indicar nombres descriptivos para las columnas utilizando aprendizaje automático y análisis de los datos almacenados.
- La herramienta debe permitir filtrar los resultados por sistemas, tipos de datos, clasificación, existencia de datos personales, duplicados, violaciones de políticas, formatos, etc.
- La herramienta debe permitir búsquedas y filtros avanzados en forma de "consultas" a través de la interfaz de usuario y la API REST.
- La herramienta debe proporcionar tableros de control para monitorear los principales indicadores del descubrimiento de datos realizado.
- La herramienta deberá permitir visualizar, filtrar y navegar por toda la información contenida en el catálogo de datos.
- La herramienta debe permitir la exportación de sus activos y metadatos a archivos estándar de la industria, al menos CSV.
- La herramienta debería permitir la visualización estilo "mapa de calor" de los sistemas con los datos más clasificados.
- La herramienta debe permitirle crear y guardar consultas/filtros de activos utilizando la información catalogada.
- La herramienta debe permitir el envío de notificaciones sobre nuevas actividades, pendientes o incidencias.
- La herramienta debe permitir la gestión manual de los escaneos, como: iniciar, pausar (sin perder el trabajo realizado) y detener definitivamente.
- La herramienta debe proporcionar la opción de exportar registros del sistema y registros de auditoría, también a través de la API REST
- La herramienta debe proporcionar informes de evaluación de los escaneos realizados (indicadores de catalogación, clasificación, etc.)
- La herramienta debería permitir el aprovisionamiento nativo del contenido del catálogo a los científicos de datos (por ejemplo, en Python).
- La herramienta debe proporcionar indicadores KPI (Key Performance Indicator) a través de dashboards o informes.
- La herramienta debe proporcionar paneles e informes listos para usar o personalizar.
- La herramienta debe proporcionar una capa semántica para informes y paneles

personalizados.

- La herramienta debe permitir la exportación de metadatos a repositorios externos para su posterior análisis con las herramientas de BI del usuario.

Gestión de Datos

Políticas y Gestión de Incidentes y Violaciones de Seguridad

- La herramienta debe proporcionar políticas preconfiguradas sobre las regulaciones de datos sensibles más comunes, como LGPD, PCI DSS, GDPR, etc.
- La herramienta debe permitir la creación de nuevas políticas y la personalización de políticas preexistentes.
- La herramienta debe permitir la configuración de criterios de política (reglas basadas en información catalogada) que se activarán en caso de infracción.
- La herramienta debe permitir la configuración de políticas orientadas a la privacidad de los datos (a nivel de hallazgo individual).
- La herramienta debe permitir la configuración de políticas orientadas a la seguridad de los datos (a nivel de objeto y de tipo/control de acceso).
- La herramienta debe permitir la configuración de políticas orientadas a la gobernanza de datos (a nivel de objeto).
- La herramienta debe permitir la identificación automática de las políticas y que se aplican a qué datos confidenciales y sensibles.
- La herramienta debe permitir la revalidación automática de las políticas actuales con cada escaneo.
- La herramienta debe permitir auditorías y acciones automáticas según reglas de política y notificaciones.
- La herramienta debe tener un mecanismo de integración entre APIs de otros sistemas en caso de violación de una política.
- La herramienta debe permitirle tomar medidas sobre políticas violadas, como: revisar excepciones, delegar o escalar acciones, eliminar falsos positivos, etc.
- La herramienta debe tener la capacidad de crear/integrar un incidente en herramientas de gestión externas, como JIRA, Service Now, etc.
- La herramienta debe permitir la remediación, mediante la orquestación del flujo de trabajo en el concepto de "observabilidad de datos".

- La herramienta debería permitir priorizar las infracciones por nivel de gravedad (por ejemplo, total de infracciones por objeto/activo de datos).
- La herramienta debe permitir que se le asigne al usuario una actividad de remediación específica relacionada con sus datos.
- La herramienta debería permitir a los propietarios de datos delegar actividades de remediación a otras partes interesadas.
- La herramienta debe permitir la automatización de las acciones de remediación mediante la integración de la API REST con herramientas de terceros.
- La herramienta debe permitir la recopilación de información para registros de auditoría de las acciones realizadas, al menos: quién, cuándo, qué tipo de acción.
- La herramienta debe permitir la colaboración entre equipos y la retroalimentación a través de actividades de remediación.
- La herramienta debe tener la capacidad de realizar acciones como eliminar datos confidenciales, poner en cuarentena o revocar privilegios excesivos.
- La herramienta debe poder integrarse con herramientas de terceros para enmascaramiento, anonimización, cifrado, etc.
- La herramienta debe permitir la definición de SLA para acciones de remediación según la gravedad de la política violada.
- La herramienta debe permitir el etiquetado de objetos según su clasificación y nivel de sensibilidad.
- La herramienta debe permitir la integración de sistemas de clasificación y etiquetado como MIP/AIP (Microsoft/Azure Information Protection).
- La herramienta debe tener la capacidad de integrarse directamente a través de API REST con herramientas DLP de terceros.

Ciclo de Vida de la Información

- La herramienta debe permitir definir políticas para la gestión del ciclo de vida de los datos.
- La herramienta debería permitir crear políticas basadas en criterios temporales (filtro de fecha).
- La herramienta debe permitir la creación de políticas específicas para datos de grupos específicos de personas (por ejemplo, personas políticamente expuestas) o productos.
- La herramienta debería permitirle definir políticas de retención legal (por ejemplo,

demandas/justicia, asuntos pendientes u otros motivos).

- La herramienta debería permitirle crear políticas de retención basadas en criterios de metadatos (por ejemplo, fecha de creación del archivo, modificación, formato, etc.).
- La herramienta debe permitir la creación de políticas con criterios de clasificación (contenido, atributos, sensibilidad, etc.)
- La herramienta debe permitir realizar acciones sobre los datos que deben archivarse (por ejemplo, moverlos) o eliminarse.
- La herramienta debe permitir el flujo de trabajo y/o la automatización del proceso de eliminación de datos.

Derechos del Titular y Autogestión

- La herramienta debe permitir la emisión de informes de datos del titular para cumplir con el derecho de acceso y adaptarse a la Ley Nacional de Protección de Datos
- La herramienta debe permitir la personalización de los informes de datos del titular, incluyendo al menos el logotipo y la adaptación de textos/descripciones, en español.
- La herramienta debe permitir una búsqueda completa de datos personales iniciando con el nombre y/o algún dato de identificación personal.
- La herramienta deberá permitir la búsqueda de los datos del titular de forma automática (sin intervención), bajo demanda y utilizando siempre los datos más actualizados disponibles.
- La herramienta debe permitir el seguimiento de los datos del titular de los datos hasta la fuente donde se encontraron (tablas/columnas y archivos).
- La herramienta deberá permitir la solicitud y obtención del reporte de datos personales a través de API REST, permitiendo la integración con herramientas de terceros.
- La herramienta debe permitir la inclusión manual de información/datos adicionales sobre el titular en el informe generado.
- La herramienta debe permitir la emisión de reportes de datos en formatos estándar del mercado, al menos PDF y Excel (XLS o CSV).
- La herramienta debe permitir una solicitud por lotes, si es necesario buscar más de un titular en la misma solicitud.
- La herramienta debe permitir la definición de diferentes perfiles de reporte, según la relación del titular (empleado, cliente, proveedor, etc.)

- La herramienta debe permitir la selección y anonimización de la información que se compartirá en el informe DSAR.
- La herramienta deberá permitir la eliminación automática de datos, a solicitud del titular, o controlar el flujo de trabajo de eliminación.
- La herramienta debe contar con un mecanismo para la revalidación recurrente de los datos que han sido y continúan siendo eliminados.
- La herramienta deberá disponer de un portal de autoservicio para que el titular pueda realizar sus propias solicitudes.
- La herramienta deberá permitir, como mínimo, solicitudes de acceso, rectificación y supresión de datos, además de la gestión de preferencias y consentimientos.
- La herramienta debe permitir controles de seguridad como confirmación positiva por correo electrónico y teléfono para confirmar la identidad y autenticidad del solicitante.
- La herramienta debe permitir la creación y personalización del cuestionario de aplicación en función del perfil, región o normativa local.
- La herramienta debe permitir la personalización de los cuestionarios, al menos el logotipo y el color, y soportar al menos los idiomas portugués (Brasil), inglés y español.
- La herramienta debe permitir la personalización en el modelo "multimarca", siendo las personalizaciones específicas para cada organización/empresa.
- La herramienta deberá permitir adjuntar a la solicitud una fotografía o documento de identidad para acreditar la identidad del solicitante.
- La herramienta debe permitir la gestión y personalización de los flujos de trabajo de cumplimiento de solicitudes (logrando automatizar procesos completos).
- La herramienta debe permitir al solicitante recibir notificaciones sobre el avance del trámite y consultar el estado de su solicitud.
- La herramienta debe proporcionar un panel de control para que el responsable de privacidad pueda tener una visión agrupada de las principales métricas/KPI del DPO.
- La herramienta debe permitir al gerente revisar los datos y la identidad del solicitante antes de aprobar la recolección de datos.
- La herramienta debe permitir al gerente revisar la información antes de enviar el informe al solicitante.
- La herramienta deberá contar con una auditoría de las solicitudes en proceso, ya realizadas,

incluyendo las solicitudes previamente rechazadas.

- La herramienta deberá enviar automáticamente los reportes de datos del titular, una vez aprobados, sin intervención manual.
- La herramienta debe tener la capacidad de buscar registros de consentimiento del titular en diversas fuentes.

Registros de las Actividades de Tratamiento (RAT/RoPA)

- La herramienta debe permitir la gestión y visibilidad de las actividades de tratamiento de datos.
- La herramienta debe señalar los riesgos relacionados con la participación de datos personales, confidenciales y sensibles.
- La herramienta debe permitir la generación y exportación de registros de actividades de procesamiento de datos.
- La herramienta debe cumplir con los requisitos de gestión del cumplimiento normativo, como la Ley Nacional de Protección de Datos.
- La herramienta debe utilizar los resultados del descubrimiento (integración con el catálogo de datos) para completar los registros de la actividad de procesamiento.
- La herramienta debe permitir la creación y personalización de cuestionarios y formularios.
- La herramienta debe permitir la lógica condicional en los formularios (formularios dinámicos, por ejemplo, cambiar la pregunta 3 dependiendo de la respuesta a la pregunta 2)
- La herramienta debe permitir la inclusión de diferentes tipos de campos como texto libre, opciones simples y múltiples, fechas, listas, carga de archivos, etc.
- La herramienta debe permitir el envío de formularios para la colaboración de las áreas de negocio involucradas y el seguimiento.
- La herramienta debe permitir la exportación e importación de formularios para su cumplimentación por terceros (fuera de la organización).
- La herramienta debería permitir la revisión de las evaluaciones realizadas y congelarlas en las versiones aprobadas.
- La herramienta debe proporcionar un informe/visualización de métricas respecto a la documentación de las actividades de procesamiento de datos.
- La herramienta debe permitir el mapeo de procesos de negocio, con flujos y diagramas

explicativos.

Reporte de Impacto a la Protección de Datos (RIPD/DPIA)

- La herramienta debe permitir realizar evaluaciones de procesos desde el punto de vista del riesgo involucrado.
- La herramienta también debería ofrecer diferentes plantillas de evaluaciones estándar como PIA, TIA, AI Readiness, Vendor Assessment, etc.
- La herramienta debe permitir la creación de plantillas personalizadas.
- La herramienta debe permitir la creación y personalización de cuestionarios y formularios.
- La herramienta debe permitir la lógica condicional en los formularios (formularios dinámicos, por ejemplo, cambiar la pregunta 3 dependiendo de la respuesta a la pregunta 2)
- La herramienta debe permitir la inclusión de diferentes tipos de campos como texto libre, opciones simples y múltiples, fechas, listas, carga de archivos, etc.
- La herramienta debe permitir la creación de bibliotecas reutilizables de riesgos y controles relacionados.
- La herramienta debería permitir calcular el nivel de riesgo relacionado mediante una matriz personalizable "probabilidad vs impacto".
- La herramienta debe permitir el envío de formularios para la colaboración de las áreas de negocio involucradas y el seguimiento.
- La herramienta debe permitir la exportación e importación de formularios para su cumplimentación por terceros (fuera de la organización).
- La herramienta debe marcar los riesgos identificados de acuerdo con las respuestas en las evaluaciones realizadas.
- La herramienta debe permitir a los usuarios colaborar en comentarios, delegando preguntas o aclarando dudas.
- La herramienta debería permitir la revisión de las evaluaciones realizadas y congelarlas en las versiones aprobadas.
- La herramienta debe permitir la generación de informes finales de evaluación que puedan ser exportados, compartidos y/o archivados

Consentimiento de Cookies

- La herramienta deberá permitir la visualización de banners de consentimiento geolocalizados, adaptándose automáticamente a la legislación aplicable en función de la ubicación del visitante.
- La herramienta debe garantizar el cumplimiento de múltiples leyes de privacidad: Ley Nacional de Protección de Datos, GDPR, LGPD, Ley 25, CCPA, VCDPA, CPA, PDPL, entre otras.
- La herramienta debe permitir la creación de banners de consentimiento explícito, en los que se bloquea la carga de cookies hasta que el usuario realiza una acción afirmativa, así como banners de consentimiento implícito, en los que las cookies funcionan hasta que el usuario las rechaza, según la configuración y la base legal aplicable.
- La herramienta debe ofrecer banners de cookies multilingües, adaptando automáticamente el idioma en función de las preferencias del navegador del visitante.
- La herramienta deberá permitir banners dinámicos de acuerdo con la normativa de protección de datos aplicable.
- La herramienta debe ser compatible con el modo de consentimiento de Google V2.
- La herramienta debe implementar Control de Privacidad Global (GPC) y OOPS para un control avanzado de las preferencias de privacidad.
- La herramienta debe ser compatible con el marco IAB TCF 2.2 para el cumplimiento de la publicidad y los anuncios digitales basados en el consentimiento.
- La herramienta debe permitir la personalización del banner de cookies con la identidad visual de la empresa, incluyendo:
    - Personaliza el logotipo en el widget
    - Estilo CSS y fuentes personalizadas
    - Edición completa de los textos mostrados en el banner
- La herramienta debe permitir la gestión del consentimiento entre dispositivos (cross-device) y entre dominios (cross-domain).
- La herramienta debe incluir una política de cookies y una descripción de las cookies.
- La herramienta debe realizar escaneos automáticos y periódicos para identificar cookies de terceros y de origen, así como rastreadores no basados en cookies (balizas, scripts, etc.).
- La herramienta debería categorizar automáticamente las cookies y rastreadores identificados.

- La herramienta debe agrupar las cookies y rastreadores por servicio (por ejemplo, Google, Meta, etc.).
- La herramienta debe permitir la integración del banner de consentimiento con los principales gestores de etiquetas del mercado, como Google Tag Manager, Adobe Launch y Tealium.
- La herramienta deberá emitir alertas de privacidad en caso de cambios o inclusión de nuevas cookies y rastreadores
- La herramienta debe mantener registros e historial de consentimiento, listos para auditorías y exportación de evidencia.
- La herramienta debe contar con certificación oficial de Google (compatibilidad con Google Consent Mode) y certificación IAB (TCF 2.2) para garantizar el cumplimiento de los estándares del mercado.
- La herramienta debe proporcionar un panel de control centralizado para la gestión de múltiples dominios y subdominios, permitiendo la configuración, el monitoreo y la aplicación de políticas de consentimiento de manera unificada.
- La herramienta debe proporcionar un panel analítico con gráficos e indicadores, incluida la tasa de consentimiento segmentada por fecha, país, dispositivo o dominio, para facilitar la toma de decisiones y el cumplimiento continuo.

Consentimiento Universal y Preferencias

- La herramienta debe permitir la recopilación centralizada de consentimientos y preferencias de privacidad de múltiples fuentes y canales, consolidando todos los datos en una única fuente confiable.
- La herramienta deberá incluir un Centro de Preferencias personalizable, donde los interesados puedan gestionar sus consentimientos y preferencias de forma autónoma.
- La herramienta debe ofrecer integración a través de una API personalizada, permitiendo la recolección y sincronización de consentimientos de los sistemas internos o externos de la empresa.
- La herramienta deberá permitir la captura del consentimiento en aplicaciones móviles (iOS y Android), en páginas web, plataformas digitales y banners de cookies.
- La herramienta debe permitir la migración de consentimientos históricos desde otras soluciones, manteniendo la trazabilidad e integridad de la información.
- La herramienta debe permitir el registro y la gestión de consentimientos offline, como

formularios físicos o servicios presenciales.

- La herramienta debe permitir la definición de temas de consentimiento amplios (por ejemplo, marketing) o específicos (por ejemplo, notificaciones por correo electrónico sobre nuevos productos).
- La herramienta debe almacenar un historial completo de todas las transacciones de consentimiento, con sus respectivos estados actualizados, permitiendo transparencia y trazabilidad.
- La herramienta debe proporcionar un registro detallado de las actividades de consentimiento, permitiendo auditorías y verificaciones internas o externas.
- La herramienta debe permitir la sincronización automática de las actualizaciones de consentimiento con sistemas internos y de terceros, además de soportar actualizaciones manuales para sistemas no automatizados.
- La herramienta debe ofrecer una vista de todos los usuarios que han dado su consentimiento, con el estado por tema y el historial de cambios por usuario.
- La herramienta debe permitir la recolección de consentimiento utilizando diferentes identificadores, como correo electrónico, número de teléfono, número de cuenta, ID interno, entre otros, permitiendo la correlación de identidades incluso con diferentes puntos de recolección.

3. ESPECIFICACIONES TÉCNICAS RENGLÓN 2

El adjudicatario deberá proveer tecnologías orientadas a brindar visibilidad, monitoreo y control de seguridad sobre aplicaciones y servicios cloud mediante conexiones directas a las APIs provistas por plataformas SaaS de la suite Microsoft 365, para analizar actividad y contenido ya almacenado en la nube sin interceptar el tráfico en tiempo real.

- Se deberá proveer la solución por un plazo de treinta y seis (36) meses para Outlook, OneDrive y Sharepoint para 4.000 usuarios.

Requerimientos generales

- La solución debe ser considerada líder dentro del cuadrante mágico de Gartner para SSE (Security Service Edge).

Arquitectura

- La solución debe ser 100% SaaS. Esto quiere decir que según el modelo de responsabilidad compartida toda tarea de HA y mantenimiento, así como de actualizaciones de la plataforma debe ser responsabilidad del Fabricante.

- La plataforma debe contar con una arquitectura SASE-ready que soporte los servicios de SSE.
- La plataforma debe contar con un plano de control unificado para todas las funcionalidades SSE que soporte.
- El plano de control debe estar separado del plano de datos donde se realizarán los controles del tráfico.
- La comunicación entre los usuarios y la plataforma debe ser encriptada de punto a punto (end-to-end encryption) usando TLS o DTLS.
- Se debe poder configurar en la consola de administración el standard de cifrado a ser utilizado.
- La replicación de políticas debe ser de manera centralizada en los distintos centros de datos donde se brinde control.
- La solución debe funcionar en centros de datos globalmente redundantes, con hardware dedicado e infraestructura de cómputo redundante. Los centros de datos deben estar basados sobre una nube privada. No se aceptan centros de datos hosteados en nube pública.
- La solución debe funcionar en centros de datos interconectados con Internet por más de 4000 conexiones peering.
- La solución debe contar con tecnología para emular direccionamiento de otros países donde no se cuente con un punto de presencia POP físico.
- Cada DC debe tener al menos los siguiente métodos de conexión o despliegue:
- A través de un cliente ligero de redirección de tráfico desde el endpoint
- IPSEC, con ancho de banda disponible por túnel de hasta 1 Gbps
- GRE, con un ancho de banda disponible de hasta 1 Gbps
- Explicit Proxy
- Reverse proxy para control de aplicaciones corporativas
- IOS Profile VPN
- La solución debe contar como mínimo con 75 regiones de centros de datos a nivel mundial
- La plataforma debe contar con puntos de presencia físicos en mínimo 5 países de América del Sur.

- Todos los centros de datos de la plataforma deben contar con capacidad total de cómputo (esto quiere decir que puedan procesar todas las funcionalidades ofertadas que requieran control en línea). No se aceptarán centros de datos virtuales (vPOP) ni centros de datos parciales (que no procesen el 100% de funcionalidades de control en línea).
- La arquitectura de la plataforma debe proporcionar mínimo 99,999 % de disponibilidad y tiempo de actividad (uptime) por año (Calculado con base al percentil 95 mensual) para la funcionalidad NGSWG y debe ser respaldada por un contrato de SLA relevante.
- La plataforma debe poder distribuir los usuarios de manera uniforme a lo largo de múltiples sitios usando GSLB (Global Site Load balancing) para prevenir la sobrecarga y mantener la disponibilidad
- La plataforma debe contar con método de selección automático del punto de presencia disponible más cercano basado en el criterio de menor latencia round.
- Se requiere que el tiempo de procesamiento de tráfico (round-trip processing) no desencriptado no debe ser mayor a 10 ms dentro del centro de datos donde se aplican los diversos controles de seguridad
- Se requiere que el tiempo de procesamiento de tráfico (round-trip processing) desencriptado no debe ser mayor a 50 ms dentro del centro de datos donde se aplican los diversos controles de seguridad

Administración

- La solución debe poder ser gestionada y administrada desde una única consola en Nube. No se aceptarán funciones en consolas diferentes.
- La plataforma debe permitir aprovisionar los usuarios directamente desde directorio activo on premise usando métodos como adaptadores o desde directorio activo en nube vía SCIM.
- La plataforma debe implementar un control de acceso basado en roles (RBAC) para que los administradores administren y restrinjan de manera granular el acceso a los recursos y los datos dentro de la implementación multiusuario.
- La plataforma debe contar con mínimo 10 roles RBAC predefinidos y listos para ser usados.
- Todas las acciones administrativas en el portal de administración deben ser registradas por la plataforma.
- El fabricante de la solución debe contar con un portal público que declare el estado de cada Centro de datos, además de cada servicio (por DC y Global)

- La consola de administración (GUI) debe de forma detalladas sobre el estado y la disponibilidad de los diversos servicios de la plataforma, incluidos los métodos de dirección de tráfico, con vistas granulares de cada centro de datos a nivel mundial.
- La consola de administración (GUI) debe contar con una vista de mapa de túneles GRE e IPsec configurados, con información sobre la distribución global y la cantidad de túneles en uso en cada centro de datos, así como el estado casi en tiempo real del estado del túnel con detalles sobre el rendimiento por túnel.
- La solución deberá proveer una vista centralizada y una consola central de administración para la actividad de los usuarios en SaaS e IaaS.
- La red que soporta la nube privada debe tener presencia significativa dentro de China continental para brindar acceso rápido y confiable a aplicaciones y contenidos tanto nacionales como internacionales.
- Debe contar con características como Zonas de localización en al menos 200 países y territorios en todo el mundo que genere mejor experiencia de usuario.

Reportes y Analítica

- Se requiere una retención de logs de al menos 90 días.
- La solución debe brindar la posibilidad de generar informes en tiempo real que brinden información específica sobre la actividad de la aplicación por usuario, departamento o ubicación.
- Debe tener la capacidad de uso de Analítica para la construcción de Dashboard, la retención de datos para analítica debe ser de debe ser un data lake SaaS (100% interno del vendor)
- Debe generar cuadros de control e informes a demanda que permitan visualizar la información que provee la solución.
- Debe tener una librería con no menos de 25 reportes preconfigurados.
- Debe tener una librería con no menos de 21 widgets pre configurados.
- Se deben poder ver los reportes con diferentes tipos de visualización tales como gráficos cartesianos, gráficos de progresión, mapas, diagramas de Sankey entre otros.
- Los reportes deben poder ser programados para envíos periódicos, permitiendo configurarlos para días específicos de la semana o meses específicos del año.
- Los reportes deberán poderse exportar a formatos txt, csv, excel y pdf.
- Debe poder crear carpetas dentro del módulo de analítica avanzada para poder separar y

organizar los reportes que se hayan creado.

- Se deben poder Ver, clonar, copiar o mover informes: cualquiera de los informes de las carpetas se puede clonar, copiar o mover a carpetas diferentes.
- Se debe contar en la consola de administración con un resumen de actividad durante los últimos siete días, incluidos usuarios, consumo de servicios, volumen de tráfico, sesiones, centros de datos accedidos. Las vistas filtradas por aplicación, centro de datos o período de tiempo están disponibles para profundizar en la latencia del lado del cliente o de la nube a la aplicación, así como datos de tendencia sobre los bytes transferidos.

Integraciones

- La solución debe admitir la transmisión de logs a SIEM onprem y cloud.
- La solución debe contar con una solución SaaS o brindar software que permite la integración con terceros referente a inteligencia de amenazas (threat intelligence), dicha plataforma debe permitir la integración de forma rápida (sin delegar la responsabilidad de crear un módulo al usuario final) con las siguientes soluciones:
    - AWS GuardDuty
    - Carbon Black
    - CrowdStrike
    - Digital Shadow
    - Mandiant
    - ThreatConnect
    - GitHub
    - Microsoft Defender
    - Mimecast
    - MISP
    - Proofpoint Plugin
    - SentinelOne
    - ServiceNow
    - STIX/TAXII
    - Trend Micro Vision One Plugin
    - API Source Plugin

- Por último, debe tener la posibilidad de permitir crear un conector a medida para futuras integraciones que no estén declaradas en el punto anterior.
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para el envío de registros (logs), la solución debe tener conectores para al menos las siguientes soluciones:
    - AWS S3
    - AWS Security Lake
    - Azure Sentinel
    - Azure Storage
    - Chronicle Plugin
    - Microsoft Defender for Cloud Apps
    - Elastic
    - Google Cloud Storage
    - Google Cloud SCC
    - QRadar Plugin
    - Rapid7 Plugin
    - Secureworks
    - Syslog Plugin
    - WebTx Plugin
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para la gestión de ticket con herramientas Ágiles, al menos debe existir un conector para las siguientes tecnologías:
    - ServiceNow
    - Jira Plugin
    - Microsoft Teams
    - Slack Notifier
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para el intercambio de medición de riesgo del usuario interno, así como el riesgo del servicio SaaS utilizado por los usuarios. Además debe contar con un conector listo para usar con las siguientes tecnologías:

- Riesgo de Usuarios
  - Azure AD
  - BeyondCorp
  - Crowdstrike
  - Okta
  - Proofpoint
  - Mimecast
  - Security Advisor
- Riesgo de servicios Cloud:
  - BitSight ThirdPartyTrust
  - ServiceNow

Cloud Access Security Broker (CASB)

Debe contar con capacidades de CASB vía API que:

- Deberá soportar capacidades CASB vía API para aplicaciones SaaS soportadas.
- Deberá contar con el licenciamiento para integrar al menos 3 aplicaciones vía API (Outlook, Sharepoint y OneDrive).
- Deberá permitir obtener información directamente desde aplicaciones SaaS mediante APIs del fabricante de la aplicación.
- Deberá soportar autenticación OAuth 2.0 para integraciones SaaS cuando corresponda.
- Deberá permitir monitoreo, análisis y reporting de actividad cloud.
- Deberá permitir alertar ante actividad sospechosa de usuarios.
- Deberá permitir alertar ante amenazas o violaciones de política de seguridad.
- Deberá permitir revisar actividad pasada y actual en aplicaciones SaaS soportadas.
- Deberá operar fuera de banda para no impactar el tráfico SaaS del usuario.
- Deberá permitir que los administradores tomen acciones de mitigación a partir de los hallazgos.
- Deberá permitir complementar CASB API con controles inline para bloqueo

de accesos en tiempo real.

- Deberá informar en la oferta las aplicaciones SaaS soportadas para integración API.
- Deberá informar qué capacidades están disponibles por cada aplicación SaaS integrada.
- Deberá incluir visualización o monitoreo de aplicaciones, archivos y alertas asociadas al CASB API.
- Deberá permitir reporting de actividad SaaS y eventos de seguridad.
- Deberá permitir seguimiento de cumplimiento de políticas en aplicaciones SaaS soportadas.

4. ESPECIFICACIONES TÉCNICAS RENGLÓN 3

El adjudicatario deberá proveer tecnologías orientadas a la prevención de fuga de información y al control del uso del dato en los distintos entornos tecnológicos del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, permitiendo aplicar políticas de protección sobre navegación web, servicios en la nube, correo electrónico y transferencia de archivos, con criterios basados en clasificación de la información, contexto de negocio y riesgo operativo.

- Se deberá proveer la solución por un plazo de treinta y seis (36) meses para 4.000 usuarios

Requerimientos generales

- La solución debe ser considerada líder dentro del cuadrante mágico de Gartner para SSE (Security Service Edge).

Arquitectura

- La solución debe ser 100% SaaS. Esto quiere decir que según el modelo de responsabilidad compartida toda tarea de HA y mantenimiento, así como de actualizaciones de la plataforma debe ser responsabilidad del Fabricante.
- La plataforma debe contar con una arquitectura SASE-ready que soporte los servicios de SSE.
- La plataforma debe contar con un plano de control unificado para todas las funcionalidades SSE que soporte.
- El plano de control debe estar separado del plano de datos donde se realizarán los controles del tráfico.
- La comunicación entre los usuarios y la plataforma debe ser encriptada de punto a punto

(end-to-end encryption) usando TLS o DTLS.

- Se debe poder configurar en la consola de administración el standard de encripción a ser utilizado.
- La replicación de políticas debe ser de manera centralizada en los distintos centros de datos donde se brinde control
- La solución debe funcionar en centros de datos globalmente redundantes, con hardware dedicado e infraestructura de cómputo redundante. Los centros de datos deben estar basados sobre una nube privada. No se aceptan centros de datos hosteados en nube pública.
- La solución debe funcionar en centros de datos interconectados con Internet por más de 4000 conexiones peering.
- La solución debe contar con tecnología para emular direccionamiento de otros países donde no se cuente con un punto de presencia POP físico.
- Cada DC debe tener al menos los siguientes métodos de conexión o despliegue:
- A través de un cliente ligero de redirección de tráfico desde el endpoint
- IPSEC, con ancho de banda disponible por túnel de hasta 1 Gbps
- GRE, con un ancho de banda disponible de hasta 1 Gbps
- Explicit Proxy
- Reverse proxy para control de aplicaciones corporativas
- IOS Profile VPN
- La solución debe contar como mínimo con 75 regiones de centros de datos a nivel mundial
- La plataforma debe contar con puntos de presencia físicos en mínimo 5 países de América del Sur.
- Todos los centros de datos de la plataforma deben contar con capacidad total de cómputo (esto quiere decir que puedan procesar todas las funcionalidades ofertadas que requieran control en línea). No se aceptarán centros de datos virtuales (vPOP) ni centros de datos parciales (que no procesen el 100% de funcionalidades de control en línea).
- La arquitectura de la plataforma debe proporcionar mínimo 99,999 % de disponibilidad y tiempo de actividad (uptime) por año (Calculado con base al percentil 95 mensual) para la funcionalidad NGSWG y debe ser respaldada por un contrato de SLA relevante.
- La plataforma debe poder distribuir los usuarios de manera uniforme a lo largo de múltiples

sitios usando GSLB (Global Site Load balancing) para prevenir la sobrecarga y mantener la disponibilidad

- La plataforma debe contar con método de selección automático del punto de presencia disponible más cercano basado en el criterio de menor latencia round.
- Se requiere que el tiempo de procesamiento de tráfico (round-trip processing) no desencriptado no debe ser mayor a 10 ms dentro del centro de datos donde se aplican los diversos controles de seguridad
- Se requiere que el tiempo de procesamiento de tráfico (round-trip processing) desencriptado no debe ser mayor a 50 ms dentro del centro de datos donde se aplican los diversos controles de seguridad

Administración

- La solución debe poder ser gestionada y administrada desde una única consola en Nube. No se aceptarán funciones en consolas diferentes.
- La plataforma debe permitir aprovisionar los usuarios directamente desde directorio activo on premise usando métodos como adaptadores o desde directorio activo en nube vía SCIM.
- La plataforma debe implementar un control de acceso basado en roles (RBAC) para que los administradores administren y restrinjan de manera granular el acceso a los recursos y los datos dentro de la implementación multiusuario.
- La plataforma debe contar con mínimo 10 roles RBAC predefinidos y listos para ser usados.
- Todas las acciones administrativas en el portal de administración deben ser registradas por la plataforma.
- El fabricante de la solución debe contar con un portal público que declare el estado de cada Centro de datos, además de cada servicio (por DC y Global)
- La consola de administración (GUI) debe de forma detalladas sobre el estado y la disponibilidad de los diversos servicios de la plataforma, incluidos los métodos de dirección de tráfico, con vistas granulares de cada centro de datos a nivel mundial.
- La consola de administración (GUI) debe contar con una vista de mapa de túneles GRE e IPsec configurados, con información sobre la distribución global y la cantidad de túneles en uso en cada centro de datos, así como el estado casi en tiempo real del estado del túnel con detalles sobre el rendimiento por túnel.
- La solución deberá proveer una vista centralizada y una consola central de administración

para la actividad de los usuarios en SaaS e IaaS.

- La red que soporta la nube privada debe tener presencia significativa dentro de China continental para brindar acceso rápido y confiable a aplicaciones y contenidos tanto nacionales como internacionales.
- Debe contar con características como Zonas de localización en al menos 200 países y territorios en todo el mundo que genere mejor experiencia de usuario.

Reportes y Analítica

- Se requiere una retención de logs de al menos 90 días.
- La solución debe brindar la posibilidad de generar informes en tiempo real que brinden información específica sobre la actividad de la aplicación por usuario, departamento o ubicación.
- Debe tener la capacidad de uso de Analítica para la construcción de Dashboard, la retención de datos para analítica debe ser de debe ser un data lake SaaS (100% interno del vendor)
- Debe generar cuadros de control e informes a demanda que permitan visualizar la información que provee la solución SSE/SWG.
- Debe tener una librería con no menos de 25 reportes preconfigurados.
- Debe tener una librería con no menos de 21 widgets pre configurados.
- Se deben poder ver los reportes con diferentes tipos de visualización tales como gráficos cartesianos, gráficos de progresión, mapas, diagramas de Sankey entre otros.
- Los reportes deben poder ser programados para envíos periódicos, permitiendo configurarlos para días específicos de la semana o meses específicos del año.
- Los reportes deberán poderse exportar a formatos txt, csv, excel y pdf.
- Debe poder crear carpetas dentro del módulo de analítica avanzada para poder separar y organizar los reportes que se hayan creado.
- Se deben poder Ver, clonar, copiar o mover informes: cualquiera de los informes de las carpetas se puede clonar, copiar o mover a carpetas diferentes.
- Se debe contar en la consola de administración con un resumen de actividad durante los últimos siete días, incluidos usuarios, consumo de servicios, volumen de tráfico, sesiones, centros de datos accedidos. Las vistas filtradas por aplicación, centro de datos o período de tiempo están disponibles para profundizar en la latencia del lado del cliente o de la nube a la aplicación, así como datos de tendencia sobre los bytes transferidos.

Integraciones

- La solución debe admitir la transmisión de logs a SIEM onprem y cloud
- La solución debe contar con una solución SaaS o brindar software que permite la integración con terceros referente a inteligencia de amenazas (threat intelligence), dicha plataforma debe permitir la integración de forma rápida (sin delegar la responsabilidad de crear un módulo al usuario final) con las siguientes soluciones:
    - AWS GuardDuty
    - Carbon Black
    - CrowdStrike
    - Digital Shadow
    - Mandiant
    - ThreatConnect
    - GitHub
    - Microsoft Defender
    - Mimecast
    - MISP
    - Proofpoint Plugin
    - SentinelOne
    - ServiceNow
    - STIX/TAXII
    - Trend Micro Vision One Plugin
    - API Source Plugin
- Por último, debe tener la posibilidad de permitir crear un conector a medida para futuras integraciones que no estén declaradas en el punto anterior.
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para el envío de registros (logs), la solución debe tener conectores para al menos las siguientes soluciones:
    - AWS S3
    - AWS Security Lake

  - Azure Sentinel
  - Azure Storage
  - Chronicle Plugin
  - Microsoft Defender for Cloud Apps
  - Elastic
  - Google Cloud Storage
  - Google Cloud SCC
  - QRadar Plugin
  - Rapid7 Plugin
  - Secureworks
  - Syslog Plugin
  - WebTx Plugin
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para la gestión de ticket con herramientas Ágiles, al menos debe existir un conector para las siguientes tecnologías:
  - ServiceNow
  - Jira Plugin
  - Microsoft Teams
  - Slack Notifier
- La solución debe contar con una solución SaaS o brindar software que permita la integración con terceros para el intercambio de medición de riesgo del usuario interno, así como el riesgo del servicio SaaS utilizado por los usuarios. Además debe contar con un conector listo para usar con las siguientes tecnologías:
  - Riesgo de Usuarios
    - Azure AD
    - BeyondCorp
    - Crowdstrike
    - Okta
    - Proofpoint

        - Mimecast
        - Security Advisor
    - Riesgo de servicios Cloud:
        - BitSight ThirdPartyTrust
        - ServiceNow

Agente

- El agente debe tener la capacidad de realizar redirección de tráfico ZTNA, SWG y SDWAN de manera unificada con el propósito de minimizar el tiempo de implementación de diferentes controles SSE a medida se vayan requiriendo y adoptando.
- El agente debe tener la capacidad de incorporar diferentes funcionalidades dependiendo del licenciamiento del plano de control.
- El agente debe poder ser instalado en los siguientes sistemas operativos y plataformas:
    - Microsoft Windows: Windows 10, Windows 11, Windows 365
    - Microsoft Windows Server: 2016, 2019, 2022, 2025
    - Windows Terminal Server 2016, 2019, 2022
    - VDI Citrix Xen Desktop, XenApp 7.13 (Supported OS: Windows 2019, Windows 10 (Single Session), Windows Server (Multi Session)
    - VDI Azure Virtual Desktop (Supported OS: Windows 10 and 11)
    - Apple macOS: 13(Ventura), 14(Sonoma), 15(Sequoia)
    - Apple iOS: 15.1, 16, 17, 18
    - Google Android: 12 (Snow Cone), 13 (Tiramisu), 14 (Upside Down Cake), 15(Vanilla Ice Cream) Android Runtime Version 9, 11
    - Google ChromeOS: ChromeOS 120 and above
    - Linux Ubuntu 20.04, 22.04, 24.04 LTS desktop version
    - Linux Mint Desktop Versions 19, 20, 21 (Cinnamon Edition)
    - Red Hat Enterprise Linux version 9.4 (Plow)
- El agente debe poder ser desplegado por métodos variados de implementación incluyendo:
    - Invitación vía correo electrónico vía an email invite

  - Scripts y políticas Just Another Management Framework (JAMF)
  - System Center Configuration Manager (SCCM)
  - Mobile Device Management (MDM) incluyendo Kandji, MobileIron Cloud o Core, AirWatch, Intune, y XenMobile
  - Microsoft Group Policy Objects (GPO) y Endpoint Manager
  - Identity Provider (IDP) con soporte de SAML 2.0 support, incluyendo Google SAML Auth
  - VMware Workspace ONE
  - VDI Azure Virtual Desktop, Amazon WorkSpaces, Citrix Virtual Apps and Desktop.

- El agente no debe realizar funciones como DLP o TP en el endpoint. Dichas funcionalidades deben ser realizadas en nube.
- "El agente debe admitir actualizaciones automáticas que debe ser de manera centralizada desde la plataforma. Debe permitir las siguientes acciones
- Control de versiones: Indicando si se trabajará con el último reléase, último golden release, o un golden release específico:
- El agente debe permitir desplegar notificaciones personalizadas en tiempo real al usuario
- Debe contar con la posibilidad de definir políticas de hardening por grupos puntuales de usuarios. Dichas políticas permiten la configuración total del agente.
- El agente debe tener la capacidad de detectar si se encuentra en un entorno corporativo o fuera de este. Cambiando incluso de modalidad en caso de funcionamiento dependiendo del lugar donde se encuentre.
- El agente debe tener la capacidad de realizar un control de postura del dispositivo utilizando los siguientes criterios para windows: Estado de cifrado del dispositivo, configuración del registro, procesos en ejecución, presencia de archivos específicos, membresía del dominio y certificados del dispositivo.
- El administrador debe ser capaz de seleccionar la periodicidad con la cual se realiza este chequeo en intervalos de 15, 30, o 60 min.
- La capacidad de realizar un control de postura del dispositivo por parte del agente debe poder permitir habilitar políticas granulares basada en la clasificación del dispositivo.
- El agente debe tener la capacidad de poder realizar tareas de diagnóstico. Como la

obtención de registros de sistema, test de velocidad y/o captura de tráfico.

- El agente tiene que tener la posibilidad de ser visible o no para el usuario, dependiendo de la opción seleccionada por el administrador
- El agente tiene que tener la capacidad de funcionar en modo Fail Open o Fail Close, dependiendo de la opción requerida por el administrador. También debe ser capaz de poder diferenciar por grupos de usuario quienes tendrán una opción o la otra.
- El cliente debe estar diseñado como un agente ligero que permite la operabilidad entre diversos sistemas operativos con un consumo de recursos menor al 5% de un equipo estándar.
- El agente debe realizar un monitoreo constante con GSLB del RTT hacia los POPs más cercanos para conectarse a la mejor opción tras una caída o al siguiente mejor POP tras una caída del principal.

Control de Acceso

- Incluye soporte a filtrado de páginas web a través de múltiples categorías, debe indicar listado de categorías y una descripción de cada una.
- Debe soportar la descarga de los logs transaccionales de las conexiones/transacciones generadas por los usuarios.
- Debe contar con soporte a creación de categorías personalizadas, las cuales pueden basarse desde cero llamando a una lista de URL o modificando una categoría predeterminada.
- Debe incluir soporte para autenticación mediante SAML e integración con un IDP corporativo.
- Debe incluir clasificación dinámica para sitios web no categorizados mediante el uso de Machine Learning.
- Debe incluir la capacidad de generar flujos de trabajo que permitan remediación como por ejemplo: Educar al usuario, enviar a cuarentena, generar una copia legal del objeto que está manipulando (como archivos)
- Debe incluir la funcionalidad de crear reglas basados en tiempo, se solicitan los siguientes casos de uso a cumplir:
    - Tramos de horario
    - Días de la semana
    - Rango de fechas o caducidad

- Debe incluir la capacidad de habilitar en forma automática la función Safe Search sobre los principales motores de búsqueda que existen.
- Debe incluir la funcionalidad de crear reglas cuyo fin busca excepcionar la posibilidad de descifrar tráfico de una conexión basado en los siguientes Criterios:
    - Red de origen
    - Red de destino
    - Categorías
    - Dominios
    - Usuarios/grupos
- Debe incluir soporte a cifrado TLS 1.3 y mantener dicha versión del protocolo.
- Debe incluir inspección TLS mediante una CA entregada por el fabricante de SWG, esta debe ser específica para la organización.
- Debe soportar la posibilidad de utilizar CA de terceros para la creación de certificados a medida de cada requerimiento (necesario para inspección SSL).
- Debe brindar soporte a tecnología Remote Browser Isolation con tecnología propia.
- Debe brindar soporte a agregar control de malware (TP) o control de información (DLP) en la creación de la política de proxy, esto quiere decir que dentro del workflow de creación de regla de navegación se puede llamar a estos microservicios.
- Debe indicar un procedimiento para el uso de CA custom sobre servicios propios de cada sistema operativo protegido a través del control de SWG.
- Debe incluir la posibilidad del control del steering de tráfico desde el plano de control unificado (mismo de creación de reglas de navegación) que permita, por ejemplo; excepción, bypass, bloqueo en base a ciertos criterios como:
    - Aplicación Cloud (iaas/saas)
    - Categoría
    - IP/RED origen
    - IP/RED destino
    - Proceso (en este caso se debe acotar los dominios a los cuales puede excluirse este proceso)
    - Dominios

- Debe permitir manejar excepciones (permitir o denegar acceso) por TLS malformados como:
    - No SNI
    - Malformed SSL
    - Domain Fronting Protection
    - CRL/OCSP Check Failed
    - SSL Handshake Error
    - Self Signed Server Certificate
    - Incomplete Certificate Trust Chain
    - Untrusted Root Certificate
    - Malformed HTTP
    - SSL Host Mismatch
- La solución a ofertar debe poseer las siguientes integraciones con usuarios finales, tales como:
    - Navegador web
    - Sync Clients
    - Aplicaciones móviles
    - Aplicaciones Desktop
    - Aplicaciones no autorizadas y de ecosistemas
    - Instancias personales de servicios en la nube sancionados
    - Dispositivos no administrados que están fuera de la red
- Debe proporcionar control de acceso granular para dispositivos no administrados que se conectan a servicios corporativos en cloud.
- La solución debe permitir la detección y el bloqueo de comunicaciones de malware de Botnet y troyanos salientes de equipos posiblemente infectados dentro y fuera de la organización.
- Debe contar con la posibilidad de clasificar los dispositivos gestionados frente a los no gestionados mediante el uso de diversos criterios, tales como + OPSWAT, registro, proceso, archivo, AD, etc.

- La solución a ofertar debe poseer las siguientes certificaciones, que se alinean a políticas, tales como:
    - SOC-1 Type II / SSAE-16 Type II
    - SOC-2 Type I
    - SOC-2 Type II
    - SOC-3 ISO 50001
    - ISO 14001
    - ISO 9001
    - ISO 27001
    - ISO 27018
    - Miembro de CSA STAR
    - US-EU Safe Harbor
- Debe incluir soporte a creación de políticas basadas en distintos criterios como:
    - Usuarios, Grupos o Unidades Organizacionales
    - IP o País de origen
    - Nivel de confianza del usuario
    - Sistema operativo
    - Navegador
    - Tipo de acceso (IPSEC, Cliente, CEP, etc)
    - Control de postura del dispositivo
    - Cabecera HTTP
- Debe ser una solución basada en tecnología Proxy, no se aceptará control de Firewall.
- Deberá permitir identificar y gestionar el uso de aplicaciones de nube, independientemente que sean gestionadas o no gestionadas.
- Deberá prevenir la exfiltración de datos entre instancias de aplicación de nube personales y corporativas.
- La solución deberá descubrir qué aplicaciones están siendo utilizadas por los usuarios y ponderar el riesgo asociado con su uso. La solución deberá identificar al menos 80,000 aplicaciones de nube.

- La solución deberá eliminar puntos ciegos en cuanto al acceso de Servicios SaaS e IaaS, permitiendo controlar las actividades de los usuarios hacia dichos servicios.
- La solución deberá proveer seguridad a servicios gestionados de nube, como Microsoft 365, G Suite y AWS.
- La solución deberá integrarse de manera transparente al servicio de DLP de la plataforma SASE, permitiendo la protección de contenido sensible que haga match con los perfiles de DLP.
- La solución deberá permitir el enforcement de dispositivos no gestionados que tienen acceso SSO (single sign on) a servicios gestionados de nube, como Box o Microsoft 365. Descubrir crear y aplicar controles de seguridad granular.
- La solución deberá proveer visibilidad automática del tráfico, para descubrir el perfil de riesgo entre miles de aplicaciones usadas dentro del ambiente. A cada aplicación se le deberá un score de riesgo que ayude a determinar el nivel de riesgo general, así como mitigar las amenazas que representan estas aplicaciones en su organización.
- Los niveles de riesgo de las aplicaciones deberán estar basados en atributos definidos por la Cloud Security Alliance (CSA) y deberán incluir factores como la seguridad de la aplicación, el riesgo, la privacidad y los marcos de cumplimiento.
- La solución deberá desplegar notificaciones en tiempo real, así como brindar coaching a los usuarios que estén llevando a cabo actividades riesgosas o intentando mover datos sensibles, mejorando el comportamiento de los mismos.
- Debe incluir soporte a múltiples métodos de despliegue como:
- Cliente propietario de la solución.
    - Forward Proxy - PAC file
    - Forward Proxy - Proxy Chaining
    - Forward Proxy - DNS
    - Forward Proxy - Perfil Agente / Móvil
    - Forward Proxy - GRE
    - Forward Proxy - IPSEC
    - Proxy Reverso - SAML / ActiveSync
    - Proxy Reverso - SAML / ActiveSync
    - Integración con tecnologías SD-WAN

- La solución debe permitir controlar que usuarios o grupos puedan desinstalar o deshabilitar el agente.

Protección de Fuga de la Información

- La solución debe tener un motor DLP en modo microservicio, nativo de la solución que sea 100% Nube. No se permite el uso de DLP externos conectados mediante ICAP. Tampoco se permite la gestión del DLP en una consola separada.
- La solución debe permitir el uso de perfiles predeterminados, en base a industria y al menos 35 perfiles. Dentro de los cuales debe existir:
    - GDPR
    - PCI-DSS
    - HIPAA
- La solución debe soportar más de 1800 tipos de archivos, además debe contar con más de 3000 identificadores predeterminados, esto quiere decir que deben existir identificadores ya creados para búsqueda de datos como email, DNI, nombres, etc. Además, estos identificadores predeterminados deben ser personalizables. Por ejemplo, el identificador predeterminado email debe poder ser modificado para que solo busque emails de dominios corporativos o excluir dominios externos.
- Además de identificadores predeterminados debe permitir la creación de identificadores mediante expresiones regulares (Regex) o diccionarios.
- La creación de reglas de DLP debe llamar a los identificadores predeterminados o a medida (expuesto en los puntos anteriores) y debe tener una lógica booleana para construir expresiones que hagan sentido y transformen estos datos encontrados en información. Por ejemplo, la unión de dos atributos mediante un AND lógico para asegurar la búsqueda de información que contenga un email y un DNI.
- La regla debe permitir definir donde se buscará la información; por ejemplo en las propiedades o cuerpo del archivo. Además debe permitir definir criticidad basado en número de registros encontrados o mediante puntuación.
- Debe tener la capacidad de poder declara por regla, si el nivel de críticidad influirán los registros duplicados o no.
- El motor DLP debe contar con algún clasificador entrenados por ML para la búsqueda de información sensible, ideal contar con más de 25 clasificadores
- El motor DLP debe soportar OCR en tiempo real.

- El motor DLP debe brindar indexación de documentos no estructurados (Fingerprinting).
- El tamaño máximo para la inspección de archivos para Protección del Dato es 128 MB a través de CASB API.
- El tamaño máximo para la inspección de archivos para Threat Protection es 400 MB a través de CASB API.
- El motor DLP debe soportar EDM para control de falsos positivos.
- La solución deberá ofrecer capacidades avanzadas de Data Loss Prevention (DLP) a través del entendimiento de contexto del contenido, mecanismos de Machine Learning para simplificar y acelerar el escaneo de los datos y su clasificación.
- Debe ofrecer la capacidad de detectar cargas y descargas de información sensible hacia y desde internet.
- Debe tener capacidad de gestión y respuesta de incidentes.
- Debe contar con la capacidad de detectar datos en movimiento para servicios de nube y aplicaciones.
- Debe tener la capacidad de detectar el envío de información sensible en tiempo real a páginas y aplicaciones web.
- Debe contar con por lo menos dos clasificadores de documentos estándar AI/ML (currículums, código fuente).
- La solución debe incluir una amplia variedad de perfiles de datos predefinidos que admitan varios casos de uso y requisitos de cumplimiento como mínimo debe contar con GDPR, CCPA, PCI-DSS, HIPAA y GLBA.
- Debe tener la capacidad de asignar los mismos perfiles creados para navegación web o endpoint DLP al correo electrónico.
- Debe tener la capacidad de administrar las políticas de DLP de correo electrónico en la misma consola que se administran las políticas de DLP web y DLP para endpoint.
- La solución DRM debe implementar permisos detallados a nivel de archivo que dicten las acciones del usuario sobre el contenido protegido.
- La integración con etiquetas de sensibilidad debe ser soportada al menos para las siguientes soluciones:
    - Microsoft Purview Information Protection
    - Google

- La capacidad de inspección DLP de la solución SSE debe ser transversal en todos sus módulos, utilizando un motor de inspección unificado que permita la aplicación consistente de identificadores en cualquier componente.
- En la definición de un identificador de datos debe ser posible realizar exclusiones por patrones y expresiones regulares (Regex), agregar validadores y filtros.
- El motor DLP debe soportar la detección de imágenes de stego en CASB Inline.
- La solución debe permitir la configuración de instancias de SharePoint y Google Drive del cliente como destinos forenses, para ubicar archivos detectados por el motor de DLP.
- La solución debe permite el entrenamiento de motores de DLP (Data Loss Prevention) personalizados mediante modelos de Machine Learning, habilitando la detección y clasificación avanzada de patrones específicos dentro de archivos de imagen.
- La solución debe permitir controles granulares de instancias para aplicaciones de Generative AI.

Protección de Amenazas

- Se requiere que la plataforma contenta Motores antimalware, Web IPS y análisis de tipo de archivo verdadero.
- Se requiere que la plataforma incorpore múltiples fuentes de inteligencia de amenazas, además de tener la posibilidad de importar IOC, incluidas URL maliciosas y hash de archivos.
- Se requiere que la plataforma incorpore un análisis y aprendizaje automático de archivos ejecutables portátiles (PE) en línea para la detección y el bloqueo de malware de Paciente Cero.
- Se requiere que la plataforma incorpore un clasificador de machine learning para identificar dominios de phishing en tiempo real bloqueando el acceso a esos sitios.
- Se requiere que la plataforma incorpore Sandboxing estándar para corroborar todas las detecciones de AV/ML.
- La solución deberá ofrecer protección contra malware, amenazas avanzadas, amenazas de nube, sandboxing, análisis ML y más.
- Debe incluir protección de malware desde servicios WEB y Cloud, así como desde IaaS.
- Capacidad de identificación y bloqueo de malware tanto en la carga como la descarga de archivos hacia o desde Internet.

- Debe poder integrarse de forma nativa con soluciones de EDR como Crowdstrike, Carbon Black, entre otras.
- Debe incluir un módulo de protección contra amenazas que incluya los siguientes procesamientos en línea (en un solo pase):
    - Antivirus (AV): Utilizar firmas para detectar malware conocido
    - Web IPS
    - Detección de comando y control (C2 o C&C)
    - Detección basada en aprendizaje automático de archivos ejecutables portátiles en línea (PE), así como sitios y dominios de phishing
- Debe contar con módulos de integración con herramientas externas para para compartir información sobre amenazas, automatizar flujos de trabajo, intercambiar puntuaciones de riesgo y exportar registros.
- La solución Threat Protection debe soportar diferentes tipos de script.
- El IPS debe escanear el tráfico de la red para encontrar y prevenir vulnerability exploits como aplicaciones o servicios maliciosos que intenten afectar en la red.

Análisis de Comportamiento de Usuarios

- Debe incluir control de acceso adaptativo basado en el comportamiento del usuario mediante un motor de UEBA mediante uso de reglas específicas.
- Debe incluir control de acceso adaptativo basado en el comportamiento del usuario mediante un motor de UEBA mediante uso de machine learning.
- La solución debe permitir configuración de reglas de anomalías secuenciales en aplicaciones y servicios en la nube, detectando actividad de datos masivos (carga, descarga, eliminación)
- Detección de actividades adicionales como:
    - Inicios de sesión fallidos.
    - Credenciales compartidas.
    - Países de riesgo.
    - Movimiento de datos sospechoso.
- Debe proveer visibilidad de la instancia de la aplicación para detectar movimiento de datos entre la empresa y las instancias de la aplicación personal.

- Proporcionar un dashboard con los incidentes de comportamiento de usuario que permita visualizar:
    - Listado total del número de Incidentes y los que no han sido investigados.
    - Top Users: Listado de usuarios top con el número de incidentes asociados.
    - Top de Aplicaciones: Listado de aplicaciones con las tasas más altas de incidentes.
    - Top de Aplicaciones: Listado de aplicaciones con las tasas más altas de incidentes.
    - Incidentes: Descripción corta de los incidentes que han sido registrados por una política.

5. ESPECIFICACIONES TÉCNICAS RENGLÓN 4

El adjudicatario deberá proveer tecnologías orientadas a la implementación de controles de prevención de fuga de información en dispositivos endpoint del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, permitiendo proteger datos sensibles frente a accesos no autorizados, transferencias indebidas, cargas hacia destinos no aprobados y otros vectores de exfiltración, integrando dichas capacidades con mecanismos de clasificación, monitoreo en tiempo real y aplicación centralizada de políticas de seguridad.

- Se deberá proveer la solución por un plazo de treinta y seis (36) meses para 4.500 endpoints.

Requerimientos Generales

- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:
    - Deberán trabajar en forma integrada nativamente.
    - El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.

Requerimientos de la Solución

- Dada la criticidad de la solución, y de la importancia para la organización, esta debe de liderar los 5 (cinco) últimos cuadrantes de Gartner para Endpoint Protection Platforms.
- La solución ofertada debe haber sido calificada en su último reporte como líder en los siguientes ámbitos:
    - Lider “Gartner EPP”, Lider “The Forrester Wave – MDR",
    - Lider “The Forrester Wave” – EDR

- Lider - "The Forrester WaveThreat Intelligence”

- La solución deberá poseer un puntaje igual o mayor a 4.7 en Gartner Insights en Endpoint Protection Platforms, Extended Detection and Response y Managed Detection and Response.

Arquitectura General

- Se requiere de una solución cien por ciento (100%) nube, la cual permita la administración centralizada de políticas y la visualización de eventos generados por las capacidades contratadas.
- La solución debe contar con dos componentes generales para su operación y correcto desempeño:
  - Consola única central 100% nube(cloud) para administración y operación de todos los módulos ofrecidos y futuros.
  - Sensores, software o extensiones de browser necesarios para su correcto funcionamiento.
- La solución debe utilizar un mecanismo de comunicación seguro basado en protocolo seguros, tales como, SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.
- La solución no debe requerir infraestructura on-premise para su correcto funcionamiento.
- La solución debe tener un único sensor para todos los propósitos de monitoreo y control.
- La solución debe poseer una única consola de gestión que permita consultar los hallazgos detectados y la construcción de reportes/Dashboard personalizados.
- La solución debe formar parte de un ecosistema XDR el cual permita análisis de contexto con otras soluciones del mismo fabricante y/o análisis de contexto con información recolectada desde fuentes de terceros.
- La solución debe posee capacidades de SOAR nativas en la infraestructura las que deben permitir la creación de mecanismo de automatización si es que fuese requerido.

Funcionalidades DLP de Endpoint

- La solución debe proporcionar un valor rápido y significativo con una configuración mínima (sin definiciones ni regex) para el monitoreo de actividad de usuarios.
- La solución debe ilustrar visualmente los datos en movimiento e incluir destinos de salida específicos o categorizados y detallas potenciales acciones de respuesta.

- La solución debe proporcionar un panel de control que proporciona una visión rápida de la postura de seguridad de datos de la organización.
- La solución debe detectar la salida de datos mediante almacenamiento masivo USB.
- La solución debe detectar la salida de datos a través del navegador web Google Chrome o Microsoft Edge.
- La solución debe mostrar eventos anómalos de salida de datos como detecciones generando una línea base por usuario y la organización.
- La solución debe mostrar eventos de interés de salida de datos según lo definido en las políticas.
- La solución debe detectar la salida de contenido original o derivado de archivos descargados desde ubicaciones web sensibles.
- La solución debe proporcionar definiciones / listas para contenido sensible.
- La solución debe permitir configurar patrones de contenido personalizados mediante regex.
- La solución debe permitir configurar el número de coincidencias para las que se activará un patrón personalizado.
- La solución debe proporciona definiciones out of box para ubicaciones web sensibles.
- La solución debe permitir configurar ubicaciones web sensibles personalizadas.
- La solución debe proporciona granularidad para definir sitios específicos de Microsoft SharePoint.
- La solución debe proporcionar granularidad para definir box específicos de almacenamiento de datos.
- La solución debe distinguir entre el uso de cuentas corporativas y no corporativas para Google.
- La solución debe distinguir entre el uso de cuentas corporativas y no corporativas para Microsoft O365.
- La solución debe distinguir entre el uso de cuentas corporativas y no corporativas para Box.
- La solución debe reconoce las etiquetas de Sensibilidad de Microsoft.
- La solución debe reconocer el tipo de archivo verdadero, incluso si la extensión ha

cambiado

- La solución debe permitir simular una política, que no activará ninguna aplicación por parte de los usuarios finales, pero notificará al administrador de seguridad de datos sobre coincidencias de políticas.
- La solución debe permitir aplicar una política, que desencadena acciones de aplicación contra los usuarios finales.
- La solución debe permitir que las políticas se asignen a usuarios y grupos específicos de Active Directory.
- La solución debe permitir excepciones a las políticas para usuarios y grupos específicos de Active Directory.
- La solución debe permitir bloquear la salida de datos sensibles hacia almacenamiento masivo USB.
- La solución debe permitir bloquear la salida de datos sensibles hacia destinos web a través del navegador.
- La solución debe permitir bloquear o permitir la salida de datos sensibles a destinos web especificados, incluyendo destinos corporativos frente a no corporativos como Google, O365 y Box.
- La solución debe permitir políticas que restringen la salida de datos sensibles a través del portapapeles a destinos web no autorizados.
- La solución debe proporcionar una página de eventos con telemetría de cada evento de salida de datos almacenada durante 30 días.
- Los eventos de salida de datos de interés pueden desencadenar detecciones que se separan del resto de los eventos de salida de datos y se almacenan durante 90 días.
- La telemetría del evento debe incluir detalles de los anfitriones.
- La telemetría de eventos debe incluir los datos de usuario de Active Directory.
- La telemetría de eventos debe incluir detalles de archivos, como nombre, volumen de archivo, tipo de archivo, categoría de archivo, hash de archivo.
- La telemetría de eventos debe incluir la fuente web, si el archivo se ha descargado desde una ubicación web.
- La telemetría del evento debe incluir detalles de destino.
- La telemetría de eventos debe incluir patrones de contenido detectados.

- La solución debe detectar una lista de todos los archivos similares encontrados en el endpoint.
- La telemetría de eventos debe permitir aplicar filtros que faciliten la búsqueda.
- La telemetría de eventos debe permitir exportar a formatos estándar, como csv o json.
- La solución debe explicar por qué ha surgido un evento anómalo de salida de datos.
- La solución debe proporcionar la capacidad para que un usuario con el papel adecuado de RBAC pueda descargar archivos forénsicos para su investigación.
- La solución debe implementa RBAC para restringir a los usuarios a investigar y solicitar acceso para eventos dentro de sus Grupos Anfitriones autorizados, impidiendo el acceso a eventos y la recuperación de pruebas para Grupos Anfitriones no autorizados.
- La solución debe permitir notificaciones configurables y personalizables para los usuarios.
- La solución debe poder automatizar acciones de respuesta basadas en soluciones de protección de datos, incluyendo notificaciones por correo electrónico o Slack, y el aislamiento de red del endpoint.
- La telemetría de eventos debe poder ser integrada por una solución SIEM.
- La solución debe permitir crear políticas compatibles para Microsoft y MAC.
- La solución debe permitir crear y definir aplicaciones locales para la inspección del tráfico generado por dichas apps con el objetivo de identificar potenciales violaciones de políticas de protección de datos.
- La solución debe poseer un dashboard que permita identificar la interacción de los usuarios y aplicaciones con agentes de AI y el potencial riesgo de exfiltración de datos.
- La solución requerida debe permitir obtener visibilidad del uso de IA capturando las interacciones de la IA en navegadores, aplicaciones y plataformas en la nube. La telemetría debe incluir prompts, respuestas y metadatos permitiendo identificar al usuario, información del dispositivo y contexto de la aplicación.
- La solución debe tener capacidad de monitorear la interacción interna de los usuarios de la organización con distintas aplicaciones de AI, ya sea por medio de la actividad en el browser o por aplicaciones locales que se definan.
- La solución debe permitir monitorear, controlar y proteger la actividad en aplicaciones (agentes) que usen modelos de AI.
- La solución debe permitir identificar intentos de inyección de prompts maliciosos

permitiendo bloquear su ejecución con el objetivo de proteger la infraestructura.

- La solución debe permitir integración flexible con Agentes de AI utilizados y/o desarrollados internamente ya sea por medio de aplicación (SDK,API), Agentic, Gateway u colectores OpenTelemetry.
- La solución debe estar diseñada para identificar intentos de manipulación de la AI los cuales intentan eludir los controles de seguridad.
- La solución debe tener la capacidad de detectar y prevenir prompts con información considerada critica para la organización.
- La solución debe permitir crear reglas de acceso para evitar la interacción de usuarios con aplicaciones AI no permitidas.
- La solución debe tener la capacidad de detectar y prevenir el uso de contenido no apropiado, violento y que busquen generar daño en la interacción con la AI.
- La solución debe permitir interactuar con diferentes Browsers para colectar información y/o datos de interacción de los usuarios con distintos proveedores de AI públicos tales como ChatGPT, Gemini, Claude, entre otros.
- La Solución debe proporcionar mecanismos que permitan la integración via SDK y/o API con soluciones internas (Agentes AI) de tal forma que permita el monitoreo y control de controles de seguridad en línea.
- La solución debe permitir crear guard rails para transformar los datos enviados a traves del prompt, reemplazando, enmascarando y/o eliminando los datos.
- La solución debe registrar las ofensas a las políticas en la plataforma XDR permitiendo crear reglas de correlación acorde a las necesidades del negocio.
- La solución debe permitir crear contenido personalizado para monitorear en el proceso de interacción de los usuarios con las aplicaciones de AI
- La solución debe permitir crear políticas en modo reporte para evaluar su efectividad previo a pasar el modo bloqueo.
- La solución debe permitir crear alias de información que faciliten la identificación de usuarios u otro en la infraestructura.
- La solución tener mecanismos estandarizados para la recolección de telemetría respecto al uso y monitoreo de la interacción de agentes de AI.
- La solución debe tener la capacidad de integración a nivel de network proxy para la

inspección de todo el tráfico utilizando mecanismos de API Gateway (Kong, LiteLLM, Portkey, y otros).

6. ESPECIFICACIONES TÉCNICAS RENGLÓN 5

El adjudicatario deberá proveer tecnologías orientadas a brindar visibilidad completa sobre los activos que conforman la superficie tecnológica del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, permitiendo identificar, inventariar y contextualizar en forma continua los distintos dispositivos, sistemas y entornos conectados, con el objeto de fortalecer la gestión del riesgo, la priorización operativa y la toma de decisiones en materia de ciberseguridad.

- Se deberá proveer el licenciamiento para hasta 10.000 activos por el período de 36 meses.

Requerimientos Generales

- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:
  - Deberán trabajar en forma integrada nativamente.
  - El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.
- La solución debe ser considerada líder dentro del cuadrante mágico de Gartner para plataformas de protección CPS para la gestión de activos del año 2026.
- La solución deberá poseer un puntaje igual o mayor a 4.6 en Gartner Insights en CPS Protection Platforms, IoT Security y Vulnerability Assessment.

Requerimientos funcionales de la plataforma

- La solución propuesta debe ser una plataforma basada en la nube (SaaS), complementada con equipos locales de propósito específico (hardware y software) incluidos como parte del servicio.
- La solución deberá incluir la actualización del licenciamiento de software y/o Firmware por la vigencia del contrato.
- La solución debe incluir el licenciamiento de todas las funcionalidades requeridas.
- La solución debe cumplir al menos con las siguientes certificaciones:
  - SOC 2 Type 2
  - ISO/IEC 27001
  - ISO/IEC 27017

  - Criminal Justice Information Services (CJIS)
  - CSA STAR Level 1
  - VPAT

- La solución deberá proporcionar un inventario automático de activos y visibilidad de forma pasiva de toda la superficie de ataque en la infraestructura de la red con al menos los siguientes atributos:
  - Nombre del Dispositivo.
  - Marca.
  - Modelo.
  - Clasificación automática basada en el tipo de dispositivos. (PC, servidores, teléfonos, HVACs, IP cámaras, celulares, imágenes de Docker, repositorios de código y nombres de dominio, etc.)
  - Clasificación automática basada en la categoría del dispositivo. (Cómputo, Comunicaciones, Nube, Seguridad, Manufactura, Automatización, Multimedia, etc.)
  - Localización.
  - Sistema Operativo y/o firmware.
  - Número de serie.
  - Dirección IP.
  - Dirección MAC.
  - Factores de riesgo y clasificación.
  - Lista de riesgos de seguridad asociados.
  - Aplicaciones instaladas.
  - Mapa de conexiones hacia otros dispositivos.
  - Actividad observada por cada dispositivo.
- La solución debe agrupar los activos en al menos 20 categorías.
- La solución debe contar con una consola de administración en la nube.
- La solución debe proporcionar un Tablero de la Exposición de la Superficie de Ataque para obtener una comprensión integral y de alto nivel de los riesgos.

- La solución debe cumplir con lo siguiente:
    - Debe recolectar y analizar los datos de las actividades de TI/OT/IoT, BMS tanto en redes alámbricas como inalámbricas.
- La solución SAAS propuesta debe recolectar los datos a través de dos métodos:
    - Por medio de CAASM (Gestión de la Superficie de Ataque de Activos Cibernéticos) vía APIs nativas.
    - Equipos virtuales locales de propósito específico (sensores o colectores) que recolectarán la telemetría de la red mediante la conexión a puertos tipo espejo (SPAN o Mirror) y forman parte de la arquitectura de la solución.
- La solución deberá recolectar los datos basados de la siguiente manera:
    - Vía CAASM:
        - EPP/EDR
        - Vulnerability Management
        - Cloud Provider
        - Firewall
        - Router
        - Switches
        - Microsoft Active Directory
        - Microsoft System Center (SCCM)
        - Virtualization: (VMWare, Hyper V)
    - Vía la telemetría de la red (Equipos Colectores):
        - Comunidad SNMPv2/3
        - Wireless LAN Controller
        - Puerto SPAN/Espejo a través de la conectividad al switch core/distribución
- Los colectores deben ofrecer opciones de despliegue en formato virtual, como aplicación y en Kubernetes. Esto permitirá a la entidad recopilar información de diversas maneras, según su estrategia y necesidades futuras, sin costo adicional durante la vigencia del contrato, cumpliendo con los requisitos de implementación de los colectores.
- El despliegue de la solución no debe requerir agentes, ni ejecutar ningún tipo de escaneo,

debe ser de modo pasivo y supervisar los dispositivos y brindar un monitoreo continuo de toda la red.

- Debe tener la capacidad para realizar una segmentación lógica (boundaries) de la red, por medio de rangos de direcciones IP, VLAN, por marca, modelo, tipo, sistemas operativos, entre otros.
- Debe contar con opciones de conectividad en redes donde se permita la opción de un puerto tipo SPAN, TAP, RSPAN y ESPAN, en cuyo caso deberá considerarse la obtención de tráfico en forma distribuida.
- Debe identificar la comunicación de cualquier dispositivo (TI, OT, IoT, BMS) que presente alguna actividad hacia dominios extranjeros (ejemplo, chinos, rusos, iraníes, etc.) no deseados.
- Debe identificar el tráfico o actividades de cualquier dispositivo (TI, OT, IoT, BMS) hacia las redes sociales, mensajería instantánea, multimedia, video bajo demanda, blog y microblogging, entre otros.
- Debe identificar las actividades de cualquier dispositivo (TI, OT, IoT, BMS) que realice transferencia de archivos hacia nubes públicas (ejemplo: Dropbox, Wetransfer, Google Drive, Amazon, Azure, entre otros).
- Debe tener la capacidad para mostrar el inventario, conexiones de red de manera gráfica, alertas, actividades, factores de riesgo, acción (enforce), aplicaciones de cualquier dispositivo (TI, OT, IoT, BMS) que se encuentren conectados.
- Debe descubrir dispositivos OT y BMS tales como sistemas HVAC, sistemas de luces, sensores de temperatura, aires acondicionados, UPS, controles de acceso, entre otros que se encuentran en el centro de datos y distribuidos en las instalaciones de las oficinas.
- Debe soportar los protocolos industriales más comunes, tales como: CIP, DNP3, EtherNet/IP, PCCC, S7Comm, S7Comm-Plus, Modbus, Tristation, GE Fanuc, GE Mark VIe, DeltaV, FTE, VNET, MMS, RNRP, CNCP, HSMS, OPC-DA, OPC-

  HDA, OPC-AE, OPC-UA, BACnet, KNX, Fox, entre otros.
- Debe permitir el etiquetado personalizado de los activos identificando dispositivos específicos.
- Debe generar un mapa de activos interactivo que muestra gráficamente el dispositivo y la topología de red asociada al mismo.
- Debe mostrar los patrones de comunicación, los protocolos utilizados y las

comunicaciones lógicas. Además, debe permitir agrupación por diferentes criterios, tales como tipo de activo, nivel de riesgo y filtrar por múltiples criterios como fabricante, tipo, marca y fecha de descubrimiento.

- Debe permitir exportar los reportes en al menos los siguientes tres formatos de archivos: Tipo Excel (.xlsx), Archivos Separados por Comas (.csv), JavaScript Object Notation (JSON), reportes gráficos en PDF.
- Debe permitir la programación automática de generación de reportes.
- Debe enviar notificaciones de manera automática sobre incidentes encontrados mediante correo electrónico e integración a la plataforma de correlación de eventos (SIEM).
- Debe generar alertas en tiempo real de cualquier actividad anómala conforme a las políticas de riesgos de seguridad preestablecidas y permitir la generación de reportes para las siguientes categorías, entre otras:
    - Actividad.
    - Alertas.
    - Aplicaciones.
    - Conexiones.
    - Dispositivos.
    - Aplicar una acción (Enforcement)
    - Hosts
    - Integraciones
    - Sistemas Operativos
    - Políticas
    - Factores de riesgo
    - Servicio
    - Tráfico
    - Usuarios
    - Vulnerabilidades.
- Debe proporcionar un control de acceso basado en roles (RBAC) o múltiples roles de usuario para facilitar la separación de funciones.

- Debe tener acceso a la interfaz de Administración por autenticación incorporada a la solución o Autenticación SAML (SSO).
- Debe detectar amenazas y anomalías mediante el monitoreo continuo de comunicaciones y protocolos del dispositivo (tanto externos como internos), sin necesidad de programar o realizar algún tipo de escaneo.
- Debe detectar lo siguiente:
    - Protocolos Industriales
    - Uso de protocolos inseguros
    - Uso de protocolos de gestión (Telnet, SSH, FTP)
    - Uso de protocolos sin encriptación
    - Comunicaciones internas y externas
    - Tráfico de red
    - Nuevos dispositivos descubiertos
- Debe proporcionar un set de políticas de seguridad alineadas al cumplimiento de ISO 27001, PCI DSS, MITRE ATT&CK ICS, CIS Controls, NIST CSF, entre

  otros.
- Debe proporcionar una amplia cobertura de protocolos de plano de datos OT y TI.
- Debe monitorear continuamente las conexiones alámbricas y redes inalámbricas tipo WiFi y Bluetooth, alertando si alguna de estas conexiones viola la política de seguridad preestablecida, tales como:
    - Conexiones a dominios maliciosos conocidos
    - Conexiones a dominios extranjeros no permitidas
    - Conexiones de redes internas y externas
    - Cantidades de datos anormales que se transmiten
    - Reporte de activos no detectados en los últimos 7 días.
- Debe configurar consultas estándar (Query) o árboles de decisión de una manera simple y sencilla, con la finalidad de poder identificar dispositivos específicos, su estado, brechas de seguridad, reportes, políticas e información de riesgo.
- Debe proveer, en caso de ser necesario, la consulta activa, a través de la comunicación en su idioma nativo, para interactuar y recopilar información específica directamente de los

dispositivos.

- Debe monitorear y alertar, por ejemplo, si alguna de las siguientes condiciones se presenta:
    - Dispositivos utilizando credenciales sin cifrado
    - Utilización de certificados inválidos
    - Transmisión de credenciales administrativas sin cifrar
    - Utilización de protocolos no cifrados
- Debe tener la capacidad de integrarse de forma nativa, por conectores APIs con las siguientes categorías de soluciones con la finalidad de enriquecer los datos, ejecutar una acción o alertar:
    - Infraestructura de red (switches, routers, WLC)
    - Herramientas de riesgos de seguridad. (Sistemas de gestión de vulnerabilidades).
    - Herramientas de gestión de identidades y acceso (IAM)
    - Herramientas de protección de dispositivos finales ((EPP, EDR)
    - Bases de datos de inventarios de activos o CMDB
    - Ambientes virtuales (Vmware, Hyper-V)
    - Entornos de nubes públicas (AWS, GCP, MS Azure)
    - Infraestructura de seguridad (firewall, NAC)
    - SIEM
    - DHCP/DNS
    - Gestión de dispositivos móviles (MDM)
    - Cloud Protection
- Debe contar con la interfaz de programación de aplicaciones API REST con la finalidad de habilitar integraciones (DevOps) y facilitar los requerimientos de automatización.
- Debe realizar un monitoreo continuo, un análisis de seguridad centralizado y automatizado que permita detectar y alertar inmediatamente sobre la comunicación que utiliza puertos y servicios no autorizados, escaneos de puertos, entre otros.
- Debe permitir agregar, eliminar o modificar las funciones (Dashlets) según la operación de los usuarios y administradores.
- Debe identificar los riesgos asociados a la deuda técnica, es decir, se deberá indicar cuáles

son las versiones del sistema operativo en fin de vida (EoL), sin actualizar, o con anuncio de fin de soporte (EoS), entre otros.

- Debe soportar una arquitectura distribuida con una administración centralizada.
- Debe proporcionar la siguiente información, sin utilizar ningún tipo de agente o escaneo:
    - Versión del sistema operativo.
    - Información sobre el firmware.
    - Los riesgos de seguridad asociados a ese activo y estos deberán ser listados en una página con el resumen y la prioridad dentro de la interfaz de administración del usuario.
    - Integración mediante APIs.
- Debe tener la capacidad para exportar Listas de Control de Acceso (ACL) en formato Cisco, Aruba y CSV para algún dispositivo específico.
- Debe detectar dispositivos que sean susceptibles a riesgos de seguridad como Log4j, WannaCry, PwnedPiper, ModiPwn, URGENT/11 y BLEEDINGBIT, entre otros.
- Debe contar con un índice de riesgo que muestre en forma gráfica los activos más vulnerables a los eventos detectados.
- Debe proveer la calificación del riesgo identificado (CVSS Score) para realizar un mapeo de la criticidad de los activos y ayudar a definir la correcta priorización de los activos para su remediación.
- Debe de proveer una breve descripción de cada riesgo identificado por activo.
- Debe agrupar activos que sean afectados por un mismo riesgo de seguridad de forma automática.
- Debe poder indicar el estatus del riesgo por activo (Abierto, Resuelto, En proceso).
- Debe contar con un módulo de reporteo sobre riesgos de seguridad completamente adaptable para los diferentes usuarios y administradores de la plataforma.
- Debe identificar actividad maliciosa a través de un monitoreo continuo, generando alertas en tiempo real sobre comportamientos anormales, actividades sospechosas y amenazas detectadas en los dispositivos.
- Debe proporcionar un resumen de auditoría de las actividades de cualquier dispositivo (IT, IoT, OT, IoMT) conectado a la red.

- Debe tener la capacidad de crear capturas de tráfico en formato PCAP, para exportarlas, con la finalidad de ser analizadas por otras herramientas.
- Debe almacenar los eventos de seguridad, al menos 90 días en un ambiente de nube, sin costo adicional y disponibles para su análisis e investigación.
- Debe realizar la detección de riesgos y alertas en tiempo real para identificar, analizar e iniciar una respuesta a un incidente, a través de las integraciones existentes con sus sistemas actuales de seguridad de red.
- Debe permitir la creación de tableros de control (dashboards) personalizados de acuerdo a las necesidades de administración que requiera "El Cliente".
- Debe proporcionar el conjunto de políticas del marco de seguridad MITRE ATT&CK ICS para la rápida detección de actividades sospechosas.
- Debe tener la capacidad de integrarse mediante APIs a la herramienta de tickets, por ejemplo, Jira, Service Now, entre otras.
- Debe ser capaz de identificar los riesgos de seguridad conocidos para todos los dispositivos, obteniéndose sin la necesidad de ejecutar escaneos.
- Debe contar con un índice de riesgo de los activos con mayor exposición con base en sus riesgos de seguridad de los eventos detectados.
- Debe incluir un motor de políticas estableciendo condiciones basadas en las actividades de comportamiento, perfil y conexiones IP de los dispositivos.
- La consola de administración debe proporcionar un enlace al sitio web de VirusTotal, con la finalidad de obtener información adicional sobre el tipo de amenaza.
- El motor de políticas de la solución debe ser capaz de asignar un nivel de severidad utilizando la clasificación baja, media o alta.
    - El motor de políticas de la solución debe soportar la construcción y definición de políticas personalizadas a través de la interfaz gráfica de usuario (GUI) en la consola.
- El motor de políticas de la solución debe permitir la ejecución de las siguientes acciones cuando una política se activa:
    - Alertar.
    - Etiquetar/Desetiquetar.
    - Aplicar una acción (Enforce) en el dispositivo infractor, tales como bloquearlo,

activar un escaneo de riesgos de seguridad, etc.

7. ESPECIFICACIONES TÉCNICAS RENGLÓN 6

El adjudicatario deberá proveer tecnologías orientadas a brindar visibilidad, control y protección sobre aplicaciones, servicios digitales avanzados y componentes de procesamiento automatizado de información utilizados por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, permitiendo identificar, monitorear, contextualizar y gobernar en forma continua las interacciones, integraciones y flujos de datos asociados, con el objeto de fortalecer la gestión del riesgo, la trazabilidad operativa, el cumplimiento normativo y la toma de decisiones en materia de ciberseguridad.

- Se deberá proveer la solución por un plazo de treinta y seis (36) meses, contemplando una capacidad de hasta 10.000.000 (diez millones) de consultas mensuales sobre procesos automatizados, así como la generación de hasta doce (12) reportes mensuales vinculados a la infraestructura objeto de análisis.

Requerimientos Generales

- La solución deberá contemplar capacidades de integración fluida, flexible y agnóstica con distintos modelos, servicios de inferencia y plataformas de procesamiento automatizado de información, ya sean de carácter público, privado o implementados en entornos propios del organismo.
- La solución deberá permitir la integración vía API con aplicaciones y servicios digitales avanzados, facilitando la ejecución de casos de uso y la validación de compatibilidad, estabilidad y rendimiento operativo.
- La solución deberá admitir la integración con plataformas de intermediación y orquestación de modelos, mediante conectores de protección o mecanismos equivalentes, que permitan aplicar controles sobre el consumo, exposición y gobierno de dichos servicios.
- La solución debe permitir la implementación en la infraestructura de CMCABA en una nube pública, compatible al menos con AWS AKS, GCP GKE y Azure AKS, y en una nube privada basada en Kubernetes u OpenShift.
- La solución deberá soportar integración nativa con múltiples plataformas, APIs estándar y servicios digitales avanzados del mercado, garantizando interoperabilidad con distintos proveedores, motores de procesamiento y entornos de operación.
- La solución debe poseer redundancia y alta disponibilidad.
- La solución debe soportar la compatibilidad con aplicaciones, chatbots, MCP y agentes.

- La solución debe soportar al menos estos 2 modos de despliegue:
    - 1- In-line: dentro de la infraestructura de Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires y en medio del flujo.
    - 2- out band: Como un servicio SaaS en infraestructura del fabricante

Administración/Control de Acceso

- La solución debe permitir asociar usuarios con roles específicos a cada proyecto.
- La solución deberá permitir la gestión centralizada de conexiones con múltiples proveedores de servicios de procesamiento, inferencia y generación de información.
- RBAC: La solución debe permitir definir roles de usuario:
    - básico (solo acceso a la aplicación),
    - administrador de la organización (permisos totales)
    - roles personalizados con permisos granulares.
- Proporcionar una API RESTful completa y documentada para la integración.
- Admitir la autenticación mediante inicio de sesión único con proveedores externos.
- Admitir OAuth 2.0 para la autenticación.
- Admitir SAML para la autenticación federada.
- Implementar un control de acceso basado en roles granular.
- Permitir la creación de roles personalizados con permisos específicos.
- Permitir la integración con Active Directory para la gestión de usuarios y grupos.
- Compatibilidad con la autenticación mediante API Key para integraciones.

Gestión de Políticas y Seguridad

- La solución deberá permitir el análisis integral de las interacciones, contemplando tanto los requerimientos ingresados como los resultados generados por los servicios de procesamiento, inferencia y generación de información, a fin de aplicar políticas de protección, control, trazabilidad y auditoría.
- La solución deberá contar con paquetes predefinidos de cumplimiento normativo europeo, que permitan identificar contenidos, interacciones o comportamientos potencialmente contrarios a regulaciones vigentes de la Unión Europea, habilitando la ejecución de acciones configurables de alerta, bloqueo, registro, auditoría y trazabilidad.

- Paquete de Temas Restringidos: La solución debe detectar y bloquear intentos de generar asesoría médica, financiera o legal no autorizada.
- La solución deberá contemplar capacidades preconfiguradas para la identificación, clasificación y prevención de exposición de datos personales e información sensible, permitiendo detectar y bloquear dichos contenidos antes de que sean transmitidos, procesados o utilizados por servicios digitales avanzados, plataformas externas o componentes de procesamiento automatizado de información.
- La solución deberá contemplar capacidades preconfiguradas para identificar y bloquear intentos de manipulación, evasión de controles, abuso de instrucciones u ofuscación de contenido, permitiendo registrar los eventos detectados y generar evidencia auditable sobre las acciones realizadas.
- La solución deberá contemplar la definición y configuración de criterios personalizados de detección, incluyendo palabras clave, expresiones regulares, reglas declarativas, análisis contextual y lenguaje natural o mecanismos equivalentes, permitiendo ejecutar acciones específicas de identificación, registro, alerta y bloqueo frente a interacciones potencialmente maliciosas, dañinas o contrarias a los objetivos y políticas de seguridad del organismo.
- Control de Versiones del Escáner: La solución debe tener la capacidad de rastrear, actualizar y revertir cambios en los escáneres mediante flujos de trabajo basados en código y API.
- Habilitar y deshabilitar reglas individualmente y en proyectos
- Control de versiones de las políticas aplicadas, que permite rastrear qué conjunto de reglas estaba activo en una fecha específica;
- La solución debe ser capaz de implementar barreras de protección personalizadas
- La solución deberá permitir la definición de políticas de protección mediante lenguaje natural o mecanismos equivalentes, con capacidad de evaluar intención, contexto y semántica de las interacciones, a fin de identificar intentos de evasión, manipulación o uso indebido que no puedan ser detectados únicamente mediante reglas estáticas.
- La solución debe tener la Capacidad de crear barreras de protección definiendo listas de palabras clave prohibidas (denial lists) para prevenir la exfiltración de términos corporativos sensibles o el uso de lenguaje inapropiado.
- La solución debe poder crear barreras de protección personalizadas configurando expresiones regulares (Regular Expressions) para la identificación y bloqueo o

enmascaramiento preciso de patrones de datos sensibles, tales como números de tarjetas de crédito (PCI), documentos de identidad, llaves de API o tokens de seguridad.

- La solución debe permitir editar respuestas en caso de bloqueo.
- La solución debe contar con un registro de las solicitudes originales, las solicitudes filtradas, las respuestas generadas y el motivo específico de cualquier bloqueo.
- La solución deberá contemplar capacidades para definir inspecciones, controles y criterios de detección mediante lenguaje natural, interfaces declarativas o mecanismos equivalentes, permitiendo identificar contenido no autorizado, sensible, riesgoso o contrario a las políticas definidas por el organismo.
- La solución debe proporcionar compatibilidad con inspecciones basadas en expresiones regulares para la detección de patrones específicos (correos electrónicos, URL, números de tarjeta).
- La solución debe poder permitir la construcción de políticas centralizadas mediante conjuntos agrupados de modelos y reglas de inspección, con al menos las siguientes características:
- El mismo modelo puede utilizarse en distintas políticas con diferentes reglas de inspección.
- La misma regla de inspección puede utilizarse en distintas políticas.
- La solución deberá proporcionar una interfaz conversacional para la interacción directa con servicios y componentes de procesamiento automatizado de información, bajo mecanismos de protección, control, trazabilidad y aplicación de políticas de seguridad.
- La solución debe poder hacer pruebas según diferentes criterios de seguridad que marcan el contenido instantáneamente.
- La solución debe poder crear criterios de seguridad personalizados para satisfacer necesidades específicas del negocio y no solo para ataques estandarizados como OWASP u algún otro.
- La solución debe poder editar y publicar criterios de seguridad, ya sea ajustando los existentes o creando nuevas versiones.
- La solución debe brindar un entorno de pruebas de las medidas de seguridad configuradas.
- El entorno de pruebas también debe permitir combinar medidas de seguridad para lograr una protección por capas, visualizar su comportamiento y agruparlas en paquetes para una gestión más sencilla.

- La solución deberá contemplar capacidades para transformar automáticamente los hallazgos priorizados derivados de campañas de validación, pruebas adversariales y evaluación de exposición en conjuntos personalizados de controles preventivos, detectivos y correctivos, habilitando su aplicación automática en tiempo de ejecución para reducir los riesgos específicos identificados.
- La solución debe contar con al menos los siguientes Modos por reglas o proyecto:
    - Modo Bloqueo (prevenir entrega),
    - Modo Auditoría (marcar sin bloquear)
    - Modo Redacción (enmascarar datos; solo para keywords y regex).
- La solución debe poder definir configuraciones de escáner específicas por escenario, aplicación o geolocalización.

Rendimiento

- La Solución debe poder generar y verificar alta precisión (F1 Score), capacidad de procesamiento (QPS - Consultas por segundo) y baja latencia de extremo a extremo.
- La solución debe poder evaluar la eficacia de los escáneres comparando resultados "esperados" (etiquetado humano) contra los resultados "reales" del sistema.

Seguridad y Configuración

- La solución deberá permitir la evaluación de la superficie de ataque de aplicaciones, servicios digitales avanzados y componentes de procesamiento, inferencia y generación automatizada de información, contemplando como mínimo la ejecución del conjunto integral de técnicas, vectores de ataque y escenarios adversariales detallados a continuación:
    - Topic steering
    - Developer role attack
    - Sugar-coated poison
    - Invasive context engineering
    - Persona bullying
    - Adversarial metaphor
    - Fallacy failure
    - Word game

  - Style injection
  - Scenario nesting
  - Refusal suppression
  - Math prompt
  - Flip
  - Payload splitting
  - Persuasive adversarial prompts
  - Single-turn crescendo
  - Conditional context change
  - Fictional context change
  - DAN (do anything now)

- La solución debe ser capaz de enviar esta categoría de prompt maliciosos manipuladas con al menos las siguientes técnicas de codificación y ofuscación:
  - Base 64 converter
  - Leetspeak converter
  - Unicode confusable converter
  - Caesar converter
  - Repeat token converter
  - Single character converter
- La solución deberá contemplar capacidades para ejecutar evaluaciones adversariales avanzadas de manera autónoma, progresiva e iterativa, permitiendo ajustar dinámicamente las técnicas, secuencias e interacciones de prueba en función de los resultados obtenidos y de las respuestas generadas por los controles de defensa, a fin de identificar posibles mecanismos de evasión, manipulación o degradación de la postura de seguridad. Esta funcionalidad deberá contemplar, como mínimo, los siguientes métodos de ataque avanzado:
  - Método Crescendo
  - Método FRAME
  - Método Trolley

- La solución debe poder validar que el sistema soporte pruebas a nivel de API, incluyendo verificaciones TLS y fuzzing de API. Asimismo, los resultados deben registrarse con detalle suficiente para identificar vulnerabilidades de protocolo, configuración o endpoints.
- La solución deberá contemplar capacidades para crear y ejecutar escenarios adversariales personalizados, orientados a sondear contextos, fuentes de información, repositorios, bases de conocimiento y componentes asociados a aplicaciones o servicios de procesamiento automatizado de información. Asimismo, deberá permitir validar la adaptación progresiva de las estrategias de prueba ante rechazos, restricciones o respuestas defensivas, asegurando que las exposiciones, filtraciones o accesos indebidos a información sean capturados, registrados, contextualizados y atribuidos al escenario adversarial inicial.
- La solución deberá contemplar la generación de informes ejecutivos y técnicos que presenten hallazgos accionables, severidad, impacto, evidencia, trazabilidad y recomendaciones de remediación. Asimismo, deberá proveer indicadores cuantitativos y cualitativos orientados a medir la postura de seguridad, la resistencia ante intentos de evasión o manipulación, el nivel de exposición y la resiliencia general del entorno evaluado.
- La solución debe tener la capacidad de programar las campañas de ataque con un control granular (ataques específicos, objetivos y tiempos) y que se ejecuten de forma fiable.
- La solución debe registrar y poder explorarse al menos lo siguiente de cada campaña de ataque:
    - tipo de ataque
    - técnicas de conversión
    - intención
    - prompts generados y respuestas del sistema
- La solución debe disponer un dashboard mostrando el resultado de cada uno de los tipos de atacket/Test ejecutados con al menos la siguiente información:
    - Resultados de resistencia a agentes
    - Resultados de ataques de agentes
    - Resultados de ataques de firma, dentro de este detalle Vulnerabilidades por categoría de intención:
        - acoso
        - actos ilegales

  - desinformación
  - contenido sexualmente explícito
  - toxicidad / odio
  - violencia / daño
  - Resultados de ataques operacionales

- La solución debe poder exportar un reporte en formato .csv con el resultado del test.
- Guía de Remediación: Los informes de la solucion deben incluir recomendaciones de remediación adaptadas a las vulnerabilidades observadas, con pasos accionables para desarrolladores y equipos de seguridad.
- La solución deberá contemplar capacidades para generar hallazgos estructurados, priorizados y accionables a partir de ejercicios de validación adversarial, pruebas de exposición y análisis de seguridad. Estos hallazgos deberán poder integrarse de forma nativa con componentes de protección, inspección y control de la misma plataforma, permitiendo su conversión automática en políticas, criterios de inspección y reglas específicas aplicables en tiempo de ejecución.
- La solución deberá contemplar la generación de una matriz comparativa de clasificación para los modelos, servicios o componentes evaluados, detallando indicadores cuantitativos y cualitativos asociados a su postura de seguridad, evolución temporal y desempeño general frente a los escenarios adversariales ejecutados. La matriz deberá incluir, como mínimo, las siguientes variables:
  - Indicador de postura o resiliencia
  - Tendencia del indicador
  - Desempeño promedio
- La solución deberá contemplar capacidades para capturar, registrar y representar las secuencias de ejecución utilizadas durante las evaluaciones adversariales avanzadas, incluyendo ramificaciones, reintentos, pivotes, cambios de estrategia y decisiones tomadas en función de los resultados obtenidos. Dichas secuencias deberán poder visualizarse mediante grafos, árboles o mecanismos equivalentes, permitiendo su auditoría, trazabilidad y revisión posterior.
- La solución debe tener la capacidad de configurar el número máximo de peticiones por segundo hacia un endpoint de API y que se cumpla de forma consistente.

- La solución debe permitir que la concurrencia sea configurable para ejecución secuencial. Por ej. al fijarla en 1, no se emita una nueva petición hasta que la anterior haya finalizado y se haya registrado.

Observabilidad/Monitoreo/Auditoría

- La solución debe brindar Visualización instantánea de los registros para monitorear el comportamiento del sistema.
- La solución deberá brindar capacidades de registro, trazabilidad y auditoría sobre las interacciones procesadas, incluyendo solicitudes ingresadas, resultados generados, eventos de seguridad, acciones aplicadas y evidencia asociada para análisis posterior.
- La solución debe soportar extracción y reenvío de logs hacia almacenamiento externo o herramientas SIEM.
- La solución debe Monitorear resultados de decisiones y resaltar fragmentos de texto específicos que activaron el escáner para dar transparencia al bloqueo.
- La solución debe otorgar visualización en tiempo real del volumen de infracciones de políticas y tipos de riesgos detectados.
- La solución deberá contemplar mecanismos de monitoreo, análisis e interceptación en tiempo real sobre los flujos de información entrantes y salientes de aplicaciones y servicios de procesamiento, inferencia y generación automatizada de información, a fin de aplicar controles de seguridad, prevención de exposición de datos, trazabilidad y cumplimiento normativo.
- La solución debe otorgar visibilidad de los detalles de la barrera de seguridad que bloqueó la solicitud, incluyendo el nombre de la barrera, el tipo, la acción de la política (bloqueada/aprobada/oculta) y otros detalles como:
    - Resultado
    - Tipo (solicitud/respuesta)
    - Usuario
    - Modelo
    - Interacción
    - Marca de tiempo
    - Resultados por barrera
    - Análisis de solicitud y respuesta por barrera

- La solución debe proporcionar un Panel de control que incluya al menos lo siguiente:
    - Número de solicitudes y bloqueos escalares y temporales
    - Estadísticas de uso del modelo, incluyendo los más y menos utilizados
    - Reglas de inspección más y menos activas
    - Métricas de latencia por modelo
    - Tasa a lo largo del tiempo de uso
    - Permitir el filtrado por período, proyecto, usuario y modelo.

8. ESPECIFICACIONES TÉCNICAS RENGLÓN 7

El oferente deberá brindar, por el plazo de treinta y seis (36) meses, contados a partir de la fecha indicada en el Parte de Recepción Definitiva de la provisión e implementación de cada solución requerida, 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, 2, 3, 4, 5 y 6.

Soporte técnico reactivo/proactivo

- El 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.
- El Oferente en su propuesta deberá tener presente que a lo largo de la vigencia del plazo de soporte técnico y garantía solicitado deberá incluir 4 recursos full time con nivel SemiSenior, dedicado a la gestión de la solución provista, pudiendo trabajar en forma remota sobre la plataforma de CMCABA.
- Esta 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.

Grados de severidad de la solicitud: Las solicitudes se clasificarán en grados de severidad en función del impacto de las mismas sobre el funcionamiento del sistema.

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

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

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

SLA	**SEVERIDAD 1**	**SEVERIDAD 2**	**SEVERIDAD 3**	**SEVERIDAD 4**
Tiempo de respuesta	15 minutos	30 Minutos	60 minutos	60 minutos
Tiempo Solución Temporal	12 horas	24 horas	72 horas	--
Tiempo Solución	40 horas	80 horas	1 mes	A convenir

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.

9. ESPECIFICACIONES TÉCNICAS RENGLÓN 8

El adjudicatario deberá realizar la implementación de las soluciones propuestas bajo la modalidad de 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.

10. ESPECIFICACIONES TÉCNICAS RENGLÓN 9

El adjudicatario deberá brindar el servicio de capacitación oficial de todas las nuevas soluciones a proveer en los Renglones 1, 2, 3, 4, 5 y 6, las que deberán contar al menos con las siguientes características:

Cada una de las capacitaciones deberá ser brindada por el fabricante de la solución, en un esquema de horario laboral de 9 a 18 horas, de lunes a viernes, coordinando la ejecución de las mismas con el Consejo de la Magistratura de la C.A.B.A.

La duración de las capacitaciones para cada una de las soluciones deberá contar con un mínimo de doce (12) horas.

El Consejo de la Magistratura de la C.A.B.A. requerirá la participación de al menos cuatro (4) agentes de la Dirección General de Informática y Tecnología en dichas capacitaciones, las cuales deberán contar con partes teóricas y prácticas con el objetivo de conocer en forma pormenorizada la solución a gestionar.

Si bien las capacitaciones pueden ser brindadas en forma virtual (mediante soluciones de colaboración tales como Zoom, Microsoft Teams, Google Meets, etc.), en caso de ser presenciales, las mismas deberán ser dictadas en la Ciudad Autónoma de Buenos Aires. El oferente brindará un certificado de asistencia a las capacitaciones a cada uno de los agentes que participen en las mismas.

El adjudicatario deberá brindar los elementos necesarios para el aprendizaje (manuales, acceso a plataformas web) a cada uno de los agentes participantes del Consejo de la Magistratura de la C.A.B.A.

11. CRITERIOS TRANSVERSALES

Estos requisitos deberían aplicar a toda solución ofertada, más allá de la tecnología:

Integración Nativa con Plataformas Existentes

El oferente deberá acreditar que la solución propuesta puede integrarse con las plataformas actualmente gestionadas por el organismo, mediante mecanismos estándar o nativos, incluyendo como mínimo: API REST, syslog, webhooks, exportación/importación de IOC/indicadores, y esquemas de autenticación segura basados en tokens u otros métodos equivalentes.

Normalización y Envío de Eventos

La solución deberá poder generar, exportar y remitir eventos de seguridad hacia la plataforma SIEM institucional, preferentemente en formatos estándar o ampliamente soportados por la industria, tales como syslog, JSON estructurado o equivalentes.

Consumo por Automatización/Orquestación

La solución deberá permitir que los eventos, alertas, artefactos, observables, IOC, incidentes o hallazgos puedan ser consumidos por una plataforma SOAR para ejecución de playbooks, enriquecimiento, ticketing, contención y respuesta.

Autenticación Segura y Segregación de Accesos

Toda integración deberá contemplar cuentas técnicas dedicadas, perfiles RBAC, trazabilidad de acciones administrativas y autenticación segura sobre APIs o conectores.

Trazabilidad y Retención

La solución deberá conservar trazabilidad de eventos, acciones automáticas, cambios de configuración y actividades administrativas, habilitando su correlación con el SIEM y su explotación por el SOAR.

FIRMAS DIGITALES

Firmado digitalmente por:
DIAZ, GASTON FEDERICO
DIRECTOR
CMCABA
Fecha: lunes, 03 agosto 2026
15:46:47