C.A.B.A., 18 de agosto de 2026

RES - SAGYP - N° 541 / 2026

VISTO:

La actuación TAE 01-00023453-9/2026 caratulado *"D. G. C. C. S/ RENOVACIÓN DEL PLAN INTEGRAL DE CIBERSEGURIDAD ETAPA I"*; y,

CONSIDERANDO:

Que por la actuación citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, por la la contratación del servicio de renovación tecnológica, actualización, soporte, mantenimiento e incorporación de soluciones especializadas de ciberseguridad, protección de endpoints, gestión de vulnerabilidades, gestión de identidades privilegiadas, monitoreo de seguridad y automatización de respuesta ante incidentes 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. Nota 2F DGIYT 432/26 y Adjuntos 114857/26 y 114858/26).

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 y 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 115604/26).

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 130107/26 y 130108/26, respectivamente, y estableció como presupuesto oficial de la contratación en la suma de dólares estadounidenses cuatro millones

seiscientos mil. (U$S 4.600.000.-). Asimismo, elevó lo actuado a esta Secretaría y recomendó que *"…la adquisición de los Pliegos correspondientes proceda mediante el pago de la suma de* ***Pesos ochocientos mil ($ 800.000.-)****, para participar en la Licitación Pública N° 2-0029*-LPU26." (v. Memo 2110/26).

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 130107/26 y 130108/26, respectivamente, y llamar a Licitación Pública N° 2-0029-LPU26, de etapa única, bajo la modalidad de llave en mano, por la contratación del servicio de renovación tecnológica, actualización, soporte, mantenimiento e incorporación de soluciones especializadas de ciberseguridad, protección de endpoints, gestión de vulnerabilidades, gestión de identidades privilegiadas, monitoreo de seguridad y automatización de respuesta ante incidentes para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cuatro millones seiscientos mil. (U$S 4.600.000.-), para el día 2 de septiembre 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° 2-0029-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 preventiva del gasto y la nota de compromiso para los años que rigen la mentada contratación (v. Adjuntos 121253/26 y 121543/26).

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 15217/2026.

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

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 130107/26 y 130108/26 forman parte de la presente Resolución y regirán para la Licitación Pública N° 2-0029-LPU26, de etapa única, bajo la modalidad de llave en mano, por la contratación del servicio de renovación tecnológica, actualización, soporte, mantenimiento e incorporación de soluciones especializadas de ciberseguridad, protección de endpoints, gestión de vulnerabilidades, gestión de identidades privilegiadas, monitoreo de seguridad y automatización de respuesta ante incidentes para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses cuatro millones seiscientos mil. (U$S 4.600.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0029-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 2 de septiembre 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° 2-0029-LPU26, será por un monto de pesos ochocientos mil ($800.000.-).

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0029-LPU26, al Dr. Matías Vázquez y la Dra. Javiera Graziano como miembros titulares, y a los Dres. Adrián Costantino 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° 2-0029-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 Tecnología 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:
FERRERO, GENOVEVA
SEC DE ADMIN GRAL Y
PRESU DEL P JUD
CMCABA
Fecha: martes, 18 agosto
2026 12:52:13

LICITACION PÚBLICA N° 2-0029-LPU26

RENOVACIÓN DEL PLAN INTEGRAL DE CIBERSEGURIDAD ETAPA I

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 renovación tecnológica, actualización, soporte, mantenimiento e incorporación de soluciones especializadas de ciberseguridad, protección de endpoints, gestión de vulnerabilidades, gestión de identidades privilegiadas, monitoreo de seguridad y automatización de respuesta ante incidentes 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 Cuatro Millones Seiscientos Mil (U$S 4.600.000.-)**, conforme al siguiente detalle:

Renglón 1: Dólares Estadounidenses Un Millón Setecientos Sesenta Mil (U$S 1.760.000.-).

Renglón 2: Dólares Estadounidenses Novecientos Mil (U$S 900.000.-).

Renglón 3: Dólares Estadounidenses Novecientos Veinte Mil (U$S 920.000.-).

Renglón 4: Dólares Estadounidenses Ciento Veinte Mil (U$S 120.000.-).

Renglón 5: Dólares Estadounidenses Novecientos Mil (U$S 900.000.-).

4. RENGLONES A COTIZAR

Renglón 1: Actualización tecnológica del equipamiento existente y licenciamiento correspondiente a los fabricantes Fortinet, Tenable y CyberArk, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Provisión de solución EDR, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 3: Provisión de plataforma de seguridad email en nube, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 4: Provisión de servicio de implementación y migración de las soluciones requeridas en los Renglones 2 y 3, conforme lo indicado en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 5: Provisión de servicios de soporte técnico local y del fabricante, mantenimiento proactivo y resolución de incidentes, 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 una 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 y 4

La adjudicataria deberá proceder a la provisión e implementación de la actualización tecnológica, de la solución y de la plataforma 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 5

El servicio tendrá un plazo de vigencia de treinta y seis (36) meses, contados a partir de la fecha indicada en el Parte de Recepción Definitiva del Renglón 4.

6.4 Prórroga de la Contratación

El contrato aludido en el punto 6.3 podrá ser prorrogado en las mismas condiciones, a exclusivo juicio de este Consejo de la Magistratura, por un período igual o menor del contrato inicial, en los términos del artículo 111° de la Ley N° 2.095 (texto consolidado por Ley N° 6.764).

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 brindar la renovación del equipamiento y licenciamiento 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.

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 y 4:

14.1 Precio Total de cada Renglón, en Dólares Estadounidenses.

Renglón 5:

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. VISITA TÉCNICA

Los interesados deberán realizar una visita a los lugares donde se desarrollarán las tareas objeto de la presente contratación, con el fin de tomar conocimiento de las condiciones operativas del

entorno sobre el cual se ejecutarán las prestaciones, no pudiendo alegar posterior ignorancia y/o imprevisiones.

Las visitas se facilitarán **hasta el día anterior a** la fecha estipulada para la apertura pública de las ofertas, debiendo comunicarse con la Dirección General de Informática y Tecnología, de lunes a viernes de 10.30 a 12.00 horas y de 14.30 a 17.00 horas, al teléfono 11-3694-5762, a los efectos de coordinar el día y hora en que serán efectuadas.

Las sedes objeto de la visita obligatoria son:

Av. Julio A. Rocca 530 de esta Ciudad.

Hipólito Yrigoyen 932 de esta Ciudad.

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

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

17. CONSTITUCIÓN DE GARANTÍAS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. PRESENTACIÓN DE LAS OFERTAS

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

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

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

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

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

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

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

19. APERTURA DE LAS OFERTAS

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

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

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

20. CRITERIO DE EVALUACION Y SELECCION DE LAS OFERTAS

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

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

21. DICTAMEN DE LA COMISION EVALUADORA. ANUNCIO. IMPUGNACION

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

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

Documentación Complementaria:

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

22. ADJUDICACIÓN

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

23. PERFECCIONAMIENTO DEL CONTRATO

Conforme lo establecido por el artículo 24 del PCG.

24. CAUSALES DE EXTINCIÓN DEL CONTRATO

Son causales de extinción del contrato las siguientes:

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

b. Mutuo acuerdo.

c. Quiebra del adjudicatario.

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

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

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

25. PERSONAL DE LA ADJUDICATARIA

25.1 Nómina de Personal

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

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

25.2 Responsabilidad por el Personal

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

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

Estarán a cargo del adjudicatario todas las erogaciones originadas por el empleo de su personal, tales como jornales, aportes y contribuciones, licencias, indemnizaciones, beneficios sociales,

otras erogaciones que surjan de las disposiciones legales, convenios colectivos individuales vigentes o a dictarse, o convenirse en el futuro y seguros.

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

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

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

25.3 Daños a Terceros

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

25.4 Exclusión

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

26. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO

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.

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 y 4:

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

Renglón 5:

El pago de los servicios se efectuará de manera mensual, conforme lo indicado en el Pliego de Bases y Condiciones Generales.

27. 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.

28. 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.

29. COMUNICACIONES

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

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

ANEXO I

DECLARACION JURADA DE APTITUD PARA CONTRATAR

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

FIRMA

…….

ACLARACION

…….

CARÁCTER

……

Ciudad de Buenos Aires, de… …de…….

ANEXO II

DECLARACIÓN JURADA DE PROPUESTA COMPETITIVA

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

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

……

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

ANEXO III

DECLARACIÓN JURADA DE INCOMPATIBILIDAD

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

FIRMA

…….

ACLARACIÓN

…….

CARÁCTER

…….

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

ANEXO IV

CERTIFICADO DE VISITA

Por la presente, se deja constancia de que el/la Sr./Sra. _____ en su carácter de _____ de la empresa _____, ha efectuado la visita obligatoria según cláusula 16 del Pliego de Bases y Condiciones Particulares, a los edificios detallados a continuación:

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

FIRMAS DIGITALES

Firmado digitalmente por:
DIAZ, GASTON FEDERICO
DIRECTOR
CMCABA
Fecha: lunes, 10 agosto 2026
14:36:47

LICITACION PÚBLICA N° 2-0029-LPU26

RENOVACIÓN DEL PLAN INTEGRAL DE CIBERSEGURIDAD ETAPA I

PLIEGO DE ESPECIFICACIONES TÉCNICAS

PLIEGO DE ESPECIFICACIONES TÉCNICAS

1. GENERALIDADES

Las presentes especificaciones indican las prestaciones mínimas que debe brindar la solución ofrecida.

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 licenciamiento 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 las presentes 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 oferente deberá brindar la actualización tecnológica del equipamiento y licenciamiento de los fabricantes Fortinet, Tenable, CyberArk. El equipamiento y licenciamiento involucrado en el presente requerimiento se compone de:

- 1 Hardware FortiSIEM 2200G con su respectivo licenciamiento de EPS.
- 1 Software FortiSOAR suscripción Enterprise – 3 users
- 1 Software Tenable SC – 2000 dispositivos
- 1 Software Tenable.WAS para 30 sitios FQDN
- 1 Software CyberArk 10.000 Workforce Standard Users
- 1 Software CyberArk 50.000 Customer Users

Actualización requerida:

· 1 Hardware FSM-2200G, (FC-10-FSM2G-247-02-36, FC4-10-FSM98-180-02-36 y FC4-10-FSM98-184-02-36)
· 1 Software PN. FC-10-SRVMS-389-02-36 y FC-10-SRVMS-384-02-36
· 1 Software PN TSC-STNDC – 2000 dispositivos
· 1 Software PN TIO-WAS para 30 sitios FQDN
· 1 Software PN WORKFORCE-STANDARD-USER-SAAS 10.000
· 1 Software PN IASSO-B2C-USER-SAAS - 50.000

Garantía del equipamiento y licenciamiento:

La actualización tecnológica del equipamiento y licenciamiento detallado, contará con una garantía contra todo defecto de fabricación y uso por un plazo de treinta y seis (36) meses contados a partir de la fecha indicada en el Parte de Recepción Definitiva de la implementación y puesta en funcionamiento de la actualización tecnológica.

3. ESPECIFICACIONES TÉCNICAS RENGLÓN 2

El oferente deberá proveer el reemplazo por obsolescencia de la tecnología actual que posee el Consejo de la Magistratura de la C.A.B.A. (Fortinet EDR), por una tecnología

que incluya las siguientes funcionalidades, con licenciamiento por un período de treinta y seis (36) meses:

Especificaciones Técnicas

- 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.
- Se requiere de una solución cien por ciento (100%) nube, la cual permita la administración centralizada de estaciones de trabajo y servidores, inclusive si estos se encuentran distribuidos de forma remota. No se aceptan soluciones que involucren hardware o virtualización. La solución no debe generar costos operacionales en las premisas, DC o infraestructura de proveedores cloud que pertenezcan a la compañía. Como también si se requieren módulos o funcionalidades adicionales no se tenga que desplegar una consola o agentes adicionales.
- 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 que serán instalados en estaciones de trabajo y servidores. Las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de orquestarlas entre sí y compartir una

misma base de inteligencia, no se aceptarán soluciones que no se orquesten o con bases de firmas/conocimiento de terceras partes.

- La solución de utilizar un mecanismo de comunicación seguro basado en protocolo SSL vía puerto 443 para facilidad de operación con capacidad de limitar el acceso a la consola poder grupos de direcciones IP.
- La solución debe contar con capacidades de integración con soluciones de correlación de eventos y de igual forma brindar reportes estructurados para dar visibilidad acerca de las características particulares de las amenazas avanzadas, tales como:
    - Reporte que muestre un panel con las principales amenazas detectadas en el tiempo.
    - Reporte sobre los tipos de malwares encontrados y bloqueados.
- Se requiere que se utilice un único agente EDR/AV en el dispositivo, el cual no requiera ser reiniciado en su instalación como desinstalación.
- En caso de requerir activación de funcionalidades adicionales no debe requerir nuevos despliegues de producto.
- El proceso de despliegue del sensor debe ser compatible y tener documentado el uso de plataformas de terceros como (SystemCenter / AWS automatic Deployment / GPO / PowerShell) entre otros.
- El consumo de recursos del agente debe ser en promedio 1% de CPU y no debe tener requerimientos de hardware específicos para su funcionamiento. Solo se garantizará los fos para el funcionamiento de las aplicaciones productivas en los dispositivos.
- Debe ofrecer la posibilidad de instalar, configurar e implementar mejores prácticas, permitiendo remover de forma transparente la solución tradicional existente.
- No debe requerir actualizaciones de patrones y/o firmas para la capa de detección. La solución debe estar basada en AI/ML (Inteligencia Artificial / Machine Learning) y debe tener capacidades de frenar intentos de explotación de

vulnerabilidad basadas en comportamiento sin requerir actualización de firmas para estos efectos.

- La solución debe tener la capacidad de poder instalarse en presencia de otra plataforma de antivirus sin interferir en la operación como también no debe requerir reiniciar el equipo tanto en laptop como en servidores. Como no requerir configurar exclusiones/excepciones en el proceso de despliegue inicial.
- La solución debe tener la capacidad de integración vía API REST. Esta API debe ser Bidireccional.
- La solución debe tener la capacidad de configuración de IOCs para su bloqueo o permiso de ejecución de forma personalizada o automatizada vía API.
- La consola de gestión debe dar visibilidad, detalles y reportes de información de alertas, detecciones, de toda la actividad de los dispositivos hasta 90 días consulta en segundos.
- La solución debe tener la capacidad de dar el detalle de la telemetría de las alertas y detecciones para poder tener un contexto de los ataques mediante análisis retrospectivos y reconstrucción de los eventos y procesos mediante un árbol de procesos de forma gráfica y listado de actividades entre otros.
- La solución debe permitir la creación de tenants adicionales sin costo para la Agencia de Sistemas de la Información, permitiendo una gestión jerárquica (Parent – Child) donde se debe permitir el movimiento entre activos desde la consola de gestión sin necesidad de intervenir localmente los equipos.
- La solución debe permitir la integración nativa y gestionada desde la misma consola de funciones de protección de identidades, sin requerir despliegue de software adicional sobre los activos.
- La solución debe permitir agregar módulos adicionales al ecosistema de protección sin necesidad de realizar despliegues adicionales sobre la infraestructura.
- La solución debe tener un mecanismo para prevenir la modificación o desinstalación del sensor de las maquinas. Este mecanismo debe ser generado

aleatoriamente y no ser una password estática.

- La solución debe dar acceso a una plataforma e-learning que incluya los cursos base de la solución adquirida sin contar con limitación de acceso de usuarios.
- La solución debe poder establecer control u comunicación directa por medio de línea de comandos con los sensores (Windows/Linux/Mac) a fin de poder ejecutar comandos, correr scripts, saber el estado de procesos, conexiones, sacar archivos, o llevar archivos, reiniciar y otros comandos que permitan acelerar un análisis forense con el acceso directo a los equipos sin herramientas de terceros.
- El despliegue de agentes/sensores se debe hacer sobre sistemas operativos:
    - Windows 7 SP1 y superiores
    - Windows 2008 R2 SP1 y superiores
    - Linux en distribuciones soportadas (Amazon 1 y 2, CentOs, Oracle, RHEL, SUSE, openSUSE, Ubuntu, Debian, elrepo, Flatcar, IBM, Alma, rocky)
    - MAC (BigSur, Monterey, Ventura)
- El sensor desplegado sobre los activos de la organización debe consumir en promedio 150MB de memoria RAM para su funcionamiento.
- La solución de protección no debe depender de integraciones con herramientas de Sandbox para incrementar sus capacidades protección.
- La solución debe entregar las mismas capacidades de detección y protección, para sistemas soportados, independiente de la versión del sistemas operativo. Es decir, no se requiere la última versión del sistema operativo para obtener full cobertura de las capacidades de protección de la herramienta.
- La solución requerida debe tener capacidad de remediación (rollback) sobre cambios ejecutados por un proceso malicioso dentro de la máquina.

Gestión de Usuarios

- La solución debe permitir la definición de personalizados para cumplir con los controles de acceso asignados a los administradores, auditores o terceros que

deben ingresar a la consola como permitir el acceso mediante MFA e integración con SSO.

- La solución deber poder delegar roles o permisos sobre grupos o zonas dentro del mismo tenant.
    - La consola debe permitir la gestión de usuarios mediante roles.
    - La consola debe poder tomar los usuarios del Active Directory.
    - Los roles preconfigurados deben tener al menos las siguientes características:
    - Súper Administrador. Cuenta con todos los permisos, puede cambiar los roles asignados a otros usuarios, pero no puede cambiar su propio rol.
    - Permiso de solo Lectura. Cuenta con acceso de sólo lectura. Puede exportar datos.
    - Usuario sin Acceso. Sin acceso a funciones administrativas.

Funcionalidades de la Tecnología

- La solución debe hacer uso de la inteligencia de amenazas basado en la identificación de como los adversarios actúan en sus campañas para poder identificar TTPs atribuibles a grupos de ciberataques.
- La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales.
- Capacidades de detección y prevención de:
- Detección y prevención de virus/malware conocido y desconocido o “día cero”:
    - Detección y prevención de TTPs (mitre) en la explotación de vulnerabilidades.
    - Detección y prevención por indicadores de ataque (File-less attacks).
    - Capacidad de independizar la detección de la prevención por políticas.
    - Identificación y prevención de actividades sospechosas (procesos,

registro, script, comandos, drivers).

  - Identificación y prevención de procesos de borrado de backup, cifrado, borrado de copias de volúmenes usados por los ataques de Ransomware basado en comportamiento.
  - Identificación y prevención de movimientos laterales y Accesos a credenciales.
  - Identificación y prevención de ataques y explotación de vulnerabilidades día cero.

- Capacidades de detección de TTPs en post ejecución como:
  - Capacidad de realizar remediación por indicadores de ataques para evitar persistencia de procesos maliciosos (ASEP).
  - Administración de cuarentena de artefactos para liberar o eliminar de los dispositivos.
- La solución debe contar como mínimo los siguientes elementos de análisis y características:
  - Capacidad de bloqueo de la ejecución de código malicioso, bloqueo exploits de día cero, terminación (Kill) procesos y actividades de comando y control.
  - Capacidad de protección aun cuando los equipos no cuenten con conectividad a la nube.
  - Capacidad de protección de antimalware sin la necesidad de utilizar firmas de Antivirus, ni actualizaciones de IOCs de comportamiento. No se permiten soluciones basadas en firmas o detección de IOC únicamente.
  - Aprendizaje maquina (machine learning en inglés) de forma local en cada punto final con Sistema operativo Microsoft Windows y Mac OS.
  - Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos.
  - Detección y prevención de explotaciones de tipo Force DEP, Heap Spray

preallocation, Force ASLR, SEH Overwrite protection, NULL Page Allocation, Remote library Loading, Untrusted font.

- Detección y prevención de scripts o comandos maliciosos vía powershell o CMD, entre otros incluyendo al menos lo siguiente:
    - Cadenas ejecutadas dinámicamente vía el cmdlet “invoke-expression”
    - Comandos vía –EncodedCommand.
    - Detección y prevención de intentos de borrado de respaldos del sistema (volumen shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware.
    - Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware.
    - Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware.
    - Detección y prevención de movimientos laterales.
    - Detección y prevención de intentos de robo de credenciales.
    - Detección y prevención de intentos de elevación de privilegios.
    - Detección y prevención de intentos de uso de “sticky keys”.
    - Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés).
    - Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe.
- La solución debe tener capacidad de desarrollar actividades forenses como:
    - Contar con un acceso remoto (vía línea de comando) a los equipos que tengan el agente instalado con perfil de administrador validado vía MFA para incorporar un control dual.
    - Permitir la ejecución de comandos ya integrados de forma remota, y a través de una lista muestre el uso de cada uno de ellos.

  - Contar con comandos de colección de datos que permitan dar paso a investigaciones. Los comandos requeridos son:
    - Explorar el sistema de archivos y extraer archivos.
    - Lista de procesos en ejecución.
    - Extraer el registro de eventos de Windows.
    - Consultar registro de Windows.
    - Enumere las conexiones de red actuales y la configuración de la red.
    - Extraer la memoria de un proceso (memory dump).
- Que cuente con comandos de remediación que permitan reacción sobre una acción puntual. Los comandos requeridos son:
  - Eliminar un archivo.
  - Terminar un proceso (Kill process).
  - Eliminar o modificar la clave o el valor del registro de Windows.
  - Enviar scripts programados.
  - Enviar y recibir archivos por demanda.
- La solución deberá contar con la capacidad de aislar una activo (Endpoint/Server) de forma remota, bloqueando así cualquier comunicación externa a la computadora con excepción a la comunicación con la propia consola de gestión de la solución.
- La solución debe hacer un mapeo de alertas basado en el modelo de MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®).
- La solución deber tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo, ubicación, esto basado en el metadato del dispositivo registrado.
- La organización en grupos de forma automática o manual basado en reglas o

filtros de acuerdo a los atributos de los dispositivos.

- La solución debe tener la capacidad de integración con plataforma de inteligencia de terceros de forma nativa como virus total.
- La solución debe contar con un módulo de antivirus de próxima generación con la capacidad de detección y bloqueo de nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercriminales.
- La solución debe incluir un módulo de automatización tipo SOAR nativo que permita desarrollar Playbooks, sin costos adicionales, para la automatización de actividades de respuesta como:
    - Aislamiento automático de dispositivos.
    - Enriquecimiento de inteligencia
    - Auto triage notificaciones personalizadas.
    - Plugin con plataformas de inteligencia, ITSM como ServiceNow, Google Slack, Microsoft Teams, email, Webhooks,
    - Lanzar scripts de forma remota, entre otros.
- Dicha funcionalidad debe ser parte de la misma consola que permite la gestión de políticas visualización de eventos de los elementos de protección en el endpoint.
- La solución debe contar con un "Market Place" para poder realizar las integraciones con terceros mediane API y ver el estado de la integración. También disponer de la posibilidad de realizar la prueba o test de nuevos módulos sin necesidad de nuevos despliegues o autorizaciones de terceros.
- La solución debe poseer la capacidad de generar alertas sobre los usuarios delegados y sobre los grupos de equipos.
- La solución debe contar con un portal de ayuda, webinar y base de conocimiento integrado a la consola para poder ampliar los conocimientos sobre los módulos o webinar para poder aplicar buenas prácticas en el desarrollo de la solución. Como también hacer el escalamiento de casos en caso de requerirse con el fabricante en modalidad 7x24.

- La consola debe incorporar un mecanismo de autodepuración para eliminar los dispositivos sin conectividad contra la consola en un periodo mayor o igual a 45 días calendario, sin embargo, debe permitir configurar políticas de retención personalizadas según sea la necesidad de Agencia de Sistemas de Información.
- El licenciamiento de la solución se debe basar por el promedio de sensores activos en un periodo de un mes y no por el número de sensores desplegados.
- Los procesos de desinstalación de los sensores deben usar un token de autorización aleatorio, no se acepta el uso de passwords o contraseñas para proteger ante la desinstalación de los agentes.
- La solución debe utilizar una estrategia de actualización que permita automatizar el proceso de actualización de la pieza de software sin necesidad de ejecuciones manuales para estos efectos.
- La herramienta de protección debe permitir conectarse remotamente a una máquina para ejecutar tareas de remediación si fuese necesario.
- La ejecución de comandos en los activos gestionados una vez realizada la conexión remota, no debe requerir el despliegue de herramientas de terceros (python u otro similar) para la ejecución de comando. Es decir, debe utilizar comandos nativos del sistema operativo.
- La solución debe tener poseer una capacidad de protección contra Ransomware con un rate de detección y protección del 100% demostrado por algún análisis de terceros reciente.
- La solución debe permitir la comparación de políticas para determinar las diferencias de configuración que puedan existir entre una y otra.
- Tener la capacidad de controlar los dispositivos USB en su ejecución, lectura o escritura como su bloqueo completo para evitar el movimiento de archivos no autorizados, para sistemas Windows y MAC.
- Tener la capacidad de consultar que tipos de objetos son copiados o escritos en los dispositivos de almacenamiento.
- Tener la capacidad de configuración de políticas de auditoria para monitoreo de

toda la actividad de dispositivos externos, esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.

- Tener la capacidad de crear reglas por clase y excepciones por ID de proveedor, ID de producto o número de serie.
- Debe tener la capacidad de informar automáticamente el tipo de dispositivo conectado con información del fabricante, nombre del producto y número de serie.
- Se deben contar con paneles para poder ver la actividad de dispositivos externos como: Audio/video, Imaging, Mass Storge, Mobiles (MTP/PTP), impresoras, Wireless (Bluetooth), Any Class.
- La solución debe permitir generar reglas personalizadas que identifiquen un dispositivo particular independiente la clase del dispositivo.
- Se deben configurar de forma personalizada la notificación que le aparece a los usuarios cuando se realizar alguna restricción en el acceso.
- Capacidad de gestionar las políticas del Firewall, tanto a nivel global como a nivel delegado, de estaciones para sistemas Windows y Mac para la restricción o permisos de puertos, IPs y procesos sin la necesidad de desplegar un nuevo software o servicios adicionales, y sin impacto significativo en el consumo de recursos del sistema.
- Tener la capacidad de configuración de políticas de auditoria para monitoreo de toda la actividad de red esto no debe requerir el despliegue de software adicional sobre los despliegues iniciales.
- Deberá utilizar el control de acceso basado en roles para asegurarse de que únicamente los administradores apropiados vean y administren las reglas del firewall.
- Deberá permitir la creación de un grupo de reglas vacío y construirlo, o comenzar con un grupo de reglas preestablecidas, una colección de reglas básicas que puede editar según sus necesidades.
- Las reglas de Firewall deben poder definir la localización del dispositivo con ello aplicar políticas de forma contextual, para identificar la ubicación se debe hacer

con la definición de:

- Tipo de conexión & SSID, IP Gateway, Servidor DHCP, Prueba de resolución DNS

4. ESPECIFICACIONES TÉCNICAS RENGLÓN 3

Se deberá proveer una plataforma de seguridad email en nube que contemple el siguiente licenciamiento, por un período de 36 meses, a saber:

- 4500 casillas de correo

4.1. Requerimientos Técnicos

- La solución debe ser provista en modalidad nube (SaaS) por el mismo fabricante.
- La solución debe contar con un sistema operativo robustecido e integrado con la solución. MTA propietario, la Administración es vía HTTPS y de manera opcional por SSH y debe contar con al menos certificación SAS70 o superiores para los sites de procesamiento.
- Esquema de alta disponibilidad para sitios SaaS con redundancia geográfica.
- La solución debe ser capaz de integrarse con cualquier plataforma de mensajería; por ejemplo: Microsoft Exchange, Google Workspace, Lotus Notes, Exchange Online en al menos sus 3 últimas versiones.
- Debe contar con la opción de enviar y recibir correo cifrado de dominio a dominio a través de TLS/SSL y permitir agregar los certificados públicos de dominios confiables.

4.2. Requerimientos Funcionales

Administración

- Acceso a la consola vía HTTPS y/o SSH.
- Gestión de administradores por niveles y perfiles de acceso, incluyendo perfiles solo de lectura.

- La solución debe poder integrarse con la herramienta de SSO de la organización para la gestión de la misma.
- Passwords administrativos configurables para cumplir los requerimientos de la empresa.
- Gestión de puertos para control de acceso a los administradores y usuarios.
- Debe contar con un módulo de reportes de utilización del equipo por motor.
- Debe contar con un reporte de que muestre el estado de cada equipo que conforma la solución.
- Debe contar con un sistema de alertas que permita monitorear el estado del equipo.
- La solución debe contar con una herramienta de búsqueda de correos que permita ver el estado de cada correo procesado y que permita ver información a nivel forense, debe estar integrada al costo de la solución.
- La solución debe contar con un API para la conexión con otros sistemas tales como soluciones de SIEM, XDR, o demás basados en los casos de uso y desarrollo de la organización. La organización debe poder generar tantas credenciales de conexión como sean requeridas, manteniendo la trazabilidad del usuario que las generó y la capacidad de deshabilitar/revocar su funcionalidad.
- La solución debe permitir etiquetar correos electrónicos de acuerdo, al menos con los siguientes casos:
    - Correo Externo
    - Remitente Desconocido
    - Remitente Externo
    - Remitente Potencialmente suplantado
    - Dominio recientemente registrado
- Dichas etiquetas deben poder ser personalizadas en formato HTML, tanto en el mensaje desplegado como en los colores utilizados.

Análisis de Emails / Anti-Spam

- La solución debe contar con soporte para análisis de DKIM para el tráfico entrante.
- La solución debe permitir el firmado del correo saliente con llaves generadas en la misma solución. Dichas llaves deben poder ser asignadas por dominio a ser firmado.
- Debe contar con soporte para análisis de SPF para el tráfico entrante.
- Debe soportar con soporte para análisis de DMARC para tráfico entrante.
- Para cada una de las capacidades de autenticación de correo, la organización debe poder generar políticas granulares que se ajusten a los requerimientos de detección y control de la organización.
- La solución debe contar con un sistema de reputación propietario no dependiente del resto de los motores de detección, que opere tanto para los correos salientes como para los correos de entrada.
- La detección de tráfico malicioso debe poder realizarse tanto para tráfico de entrada como de salida, permitiendo el control e identificación de anomalías en cuentas internas.
- La solución deberá permitir identificar amenazas mediante puntajes de los distintos motores a través de la correlación de los mismos, la información debe ser mostrada al administrador a través de la consola para que pueda tomar acciones o tener el detalle de las acciones aplicadas.
- La solución debe permitir la modificación de los umbrales de detección de acuerdo con las necesidades de la empresa, así como la creación de perfiles para distintas rutas, dominios, usuarios o direcciones IP, tanto para correo entrante como para correo saliente.
- Los motores de detección deben actualizarse regularmente y las actualizaciones deben ser descargadas del sitio del fabricante una vez probados para evitar cualquier impacto al tráfico.

- Los motores de detección deben ser configurables de forma independiente para poder ajustarlos a los requerimientos particulares de la empresa, tales como distintas reglas para ip's, dominios, grupos de usuarios, usuarios, etc.
- La solución debe poderse configurar para bloquear correos de marketing o similares (Bulk Mail).
- La solución debe ser capaz de identificar y contener el correo de phishing estándar.
- La solución debe poder configurar listas blancas y negras para los motores de Anti-Spam, tanto a nivel general (a nivel de organización) como individual, de así requerirse.
- Se debe contar con la granularidad que permita que el administrador genere reglas para mensajes específicos tanto permisivos como restrictivos y que hagan override a las reglas estándar definidas por la solución. Ya sea para ip's, dominios, usuarios, etc.
- Las políticas de control de SPAM deben ser modificables; por ejemplo, que permita tener distintas reglas para el tráfico de entrada del tráfico de salida
- Las reglas o políticas de bloqueo deben poder configurarse desde una sola ventana o interfaz.
- Debe contar con una herramienta para gestión de bouncing, y que permita la generación de llaves fijas y dinámicas; estas últimas generadas y rotadas sin necesidad de intervención.
- Debe poseer la funcionalidad de control de Tasa SMTP; volúmenes, recurrencia, hosts, etc; con el fin de controlar ataques tanto entrantes como salientes.
- Poseer integración con directorio activo o bases de datos para verificación de usuarios.
- La herramienta debe contar con reportes a usuario final que permitan tomar acciones como liberar o notificar spam, vía correo electrónico o bien a través de un portal de usuario. Que pueda configurarse desde, para un usuario como para un grupo o bien a toda la empresa.

- Debe contar con la capacidad de utilizar exportar reportes en formato csv y/o pdf y/o html.
- Las opciones de las notificaciones a usuario final deben poder ser configurables por el administrador para restringir o habilitar funcionalidades.
- Debe contar con áreas de cuarentena especificas por motor, y debe permitir la generación de nuevas cuarentenas de acuerdo sea requerido.
- El módulo debe tener la capacidad de configurarse para distintas rutas, direcciones y dominios.
- Debe permitir la utilización de diccionarios específicos que permitan la búsqueda de palabras, frases e incluso expresiones regulares, mismas que serán revisadas en cualquier correo ya en el header, body, attachment y footer.
- La solución debe Soportar configuraciones para limitar los archivos adjuntos que se envían o reciben.
- Debe tener la capacidad de que el usuario pueda auto gestionar su propia cuarentena de mensajes.
- Debe manejar múltiples carpetas o tipos de cuarentena donde puedan recibir acciones predeterminadas como retención y/o liberación manual del mensaje en cuarentena
- Debe tener la capacidad de controlar el tamaño de cuarentena.
- Deberá tener la capacidad de controlar el tiempo de los mensajes en cuarentena.
- La efectividad de la solución para proteger de correo spam debe ser al menos 99%.
- Deberá tener la capacidad de marcar los correos en el subject como SPAM.
- La solución debe permitir imprimir un mensaje personalizado que certifique el análisis del correo en calidad de aviso legal.
- La solución debe poder ser configurado para aceptar correo electrónico de un número limitado de dominios.

Identificación de amenazas

- Deberá realizar el análisis de antivirus tanto conocidos como de día cero, permitiendo la actualización automática del motor y la creación de reglas de análisis de acuerdo con los requerimientos de la organización.
- Deberá contar con un motor de análisis de día cero para poder identificar y contener ataques nuevos para los que no haya firmas.
- El motor de Anti-virus deberá contar con actualizaciones periódicas que se deben descargar del sitio de la solución de correo y no de la empresa Anti-virus, el despliegue de las mismas deberá ser validado para asegurarse de que no existan efectos secundarios que afecten el tráfico.
- Los correos con amenazas deberán ser contenidos en áreas divididas por motor de detección y su gestión por área debe ser independiente.
- Cualquiera de los motores propuestos debe tener la capacidad de detectar y bloquear: virus conocidos a través de firmas, mensajes corruptos sospechosos, mensajes que contengan Riskware/Spyware, Phishing así como permitir bloquear mensajes con archivos cifrados.
- Capacidad de configurar los motores basado en políticas de: rutas, grupos de usuarios, grupos de dominios, usuarios y direcciones IP. Esto en cualquier dirección de tráfico. Adicionalmente, deberá poderse utilizar cualquier encabezado propio del protocolo SMTP para la definición de condiciones en las reglas.
- El administrador de la solución debe poder liberar correos ubicados en las cuarentenas permitiendo su envío directo al destinatario como forzar su reprocesamiento a través de los motores y políticas definidas en la solución.
- Para el motor de protección de ataques de hora cero, se debe permitir que un correo sospechoso sea reprocesado después de recibir actualizaciones a las firmas.
- Cualquiera de los motores debe ser capaz de identificar archivos o códigos maliciosos en el contenido del correo, identificando siempre la extensión original.

Amenazas avanzadas

- La solución debe contar con un módulo para amenazas avanzadas que permita identificar y contener las mismas si estas provienen a través del correo.
- El módulo debe contar con un sandboxing para evaluar tanto archivos como urls para los archivos anexos, estos deben ser analizados a lo más en 5 minutos para el análisis de url's no solo debe ser capaz de ejecutar la mismas a través del sanboxing y poder identificar payloads en el sitio. Si al momento del análisis el sitio no se encuentra activo, el correo, de ser entregado, deberá contar con un mecanismo que proteja al usuario al hacer clic desde cualquier dispositivo que permita la navegación y este deberá hacer el análisis del site sin importar el número de clic's realizados por el receptor.
- Para cada análisis avanzado realizado, la herramienta deberá proveer el detalle del análisis y conclusiones de dicho análisis. Dicho informe debe poder ser descargado, al menos en formato JSON para su análisis posterior. Dicho reporte debe incluir los indicadores de riesgo identificados, así como la evidencia de comportamiento malicioso.
- La solución debe permitir la integración vía API con el tenant de Office 365 de la organización con el objetivo de detectar eventos de fallas de autenticación, aplicaciones riesgosas conectadas y archivos que son compartidos.
- Debe mostrar a través de un dashboard la información relativa a los ataques recibidos, mostrar información forense de cada ataque y permitir ver quien ha sido el más atacado y quienes son los usuarios que regularmente hacen click a los links.
- La solución deberá permitir aislar, de manera automática y sin requerir la instalación de agentes, el acceso a links recibidos por correo electrónico a usuarios que han recibido una mayor tasa de ataques que el resto de usuarios de la organización.
- La solución debe contar con integraciones nativas con soluciones de ciberseguridad de terceros tales como Crowdstrike, Palo Alto, Microsoft Defender, OKTA.

Respuesta ante incidentes

- Esta funcionalidad debe permitir la integración con el ambiente de Exchange, Office 365 y/o G Suite de la organización.
- La integración con el tenant de Office 365 debe realizarse utilizando Graph API.
- La solución debe permitir reaccionar tanto automáticamente como manualmente a eventos de correo electrónico considerado correo electrónico no deseado o riesgoso y que al momento de análisis no haya sido bloqueado por la solución de Antispam.
- Debe contar con la posibilidad de integración con un buzón de abuso en la organización donde se monitorea y analiza mensajes de correo electrónico reportados por los colaboradores de la organización.
- Esta funcionalidad puede ser utilizada como SaaS o implementada On-Premise mediante appliance virtual.
- La solución debe permitir la búsqueda y retiro de correos electrónico no deseados desde los buzones sin límite de concurrencia, es decir, puede retirar el mismo mensaje desde todos los buzones donde se encuentre en una sola acción.
- Debe permitir visualizar el estado de la remediación y si la misma fue exitosa.
- La solución debe permitir la creación de listas basadas en criterios como:
    - Hash del adjunto
    - Nombre del adjunto
    - Cuerpo del mensaje
    - Contenido de encabezados
    - Dirección de correo de destinatario
    - Dirección de correo remitente
    - Asunto del correo
    - URL en el mensaje
- Debe ser posible definir criterios de excepción en las acciones de cuarentena, por ejemplo, buzones donde no se deberá realizar dicha acción.

- El administrador de la solución debe poder restaurar los mensajes retirados de los buzones de los usuarios.
- Debe contar con un API para integración con herramientas de correlación de eventos (SIEM) para poder obtener información sobre los mensajes e incidentes. Adicionalmente, debe permitir la integración son soluciones de SOAR que permitan la creación de incidentes y ejecución de flujos de reacción.
- Debe ser posible la creación de usuarios administradores con diferentes perfiles de acceso.
- El acceso administrativo debe ser mediante HTTPS.
- Debe poder ser posible utilizar autenticación vía SSO como los demás componentes de la solución.
- La solución debe emitir notificaciones vía correo electrónico a los usuarios administradores y grupos de usuarios creados y en base a las políticas definidas en la solución.
- Debe contar con logs de auditoría sobre todas las acciones que realizan los administradores sobre la plataforma.

Reportería

- Debe brindar un botón de reporte integrado en cliente de correo para que los usuarios informen de correos sospechosos con un solo clic, sin necesidad de capturar encabezados o detalles complejos.
- Soporte para reporte desde múltiples clientes de correo (Outlook Desktop/Mac, OWA, Gmail web/móvil).
- Reporte simple por parte del usuario final sin necesidad de conocimientos técnicos.
- Conservación de encabezados, cuerpo y adjuntos del mensaje reportado para análisis Integración con clientes de correo modernos:
    - Microsoft Outlook (Windows, Mac)
    - OWA

  - Gmail (como add-on)
  - Outlook Mobile (iOS/Android)

- Opción de despliegue automático sin intervención manual del usuario.
- Debe ser posible la personalización del botón (texto, ícono, idioma).
- Notificaciones configurables para distintos tipos de reportes (simulados, phishing, training, safelisted).
- Análisis automático de correos reportados para identificar phishing con categorización.

5. ESPECIFICACIONES TÉCNICAS RENGLÓN 4

El adjudicatario deberá realizar la implementación y migración de las soluciones propuestas en modalidad “llave en mano”, por lo que se deberán proveer todos los elementos necesarios, realizar la instalación en sitio, puesta en marcha y configuración de acuerdo con las necesidades establecidas por el Consejo de la Magistratura de la 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.

6. ESPECIFICACIONES TÉCNICAS RENGLÓN 5

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

- Los servicios ofrecidos deben incluir un soporte técnico local en modalidad 7x24x365 para la resolución de incidencias técnicas.
- El soporte técnico local debe ser brindado con personal especializado propio del adjudicatario. Deberá incluir los CVs y certificaciones del personal técnico (al menos 2 ingenieros).
- Se debe contemplar el servicio de soporte técnico del fabricante en modalidad 7x24x365 para el escalamiento de incidencias técnicas.
- El servicio de soporte técnico debe incluir el mantenimiento proactivo de la solución de forma tal de prevenir incidentes, asegurar el cumplimiento de las buenas prácticas del fabricante y optimizar el rendimiento de la tecnología.
- La movilización del personal o cualquier costo asociado que surgiera del servicio de soporte técnico a prestar correrá por exclusiva cuenta del adjudicatario para cada vez que se requiera.
- Los requerimientos de soporte técnico se podrán efectuar telefónicamente, por correo electrónico o vía web.
- Deberán considerarse incluidos dentro del servicio, la aplicación de parches, actualizaciones de software, etc. con el fin de mantener el estado de software de los dispositivos al día con su última actualización disponible por parte del fabricante.
- No deberá existir un límite en el número de casos de soporte que puede solicitar el Consejo de la Magistratura de la Ciudad de Buenos Aires.

- El servicio deberá contemplar el reemplazo parcial o total (RMA) de componentes de la solución que presenten fallas sin incurrir en gastos adicionales por parte del Consejo de la Magistratura de la Ciudad de Buenos Aires.

FIRMAS DIGITALES

Firmado digitalmente por:
DIAZ, GASTON FEDERICO
DIRECTOR
CMCABA
Fecha: lunes, 10 agosto 2026
14:36:48