Ciudad Autónoma de Buenos Aires, - 2 JUL. 2025

VISTO:

El artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires, la Ley Nº3 y la Ley Nº2095 y sus modificatorias, las Disposiciones N°29/22, N°140/23, N°71/24 y el Expediente N°233/25 de esta Defensoría del Pueblo;

Y CONSIDERANDO QUE:

El artículo 137 de la Constitución de la Ciudad Autónoma de Buenos Aires creó a la Defensoría del Pueblo como órgano unipersonal e independiente, con autonomía funcional y autarquía financiera, dotándola de personería jurídica con legitimación procesal;

La mencionada Ley Nº3 que reglamenta la conformación del organismo, otorga al Defensor del Pueblo, en su artículo 13, incisos n) y o), las atribuciones de dictar el reglamento interno, ejecutar su presupuesto y toda otra acción conducente al mejor ejercicio de sus funciones;

Mediante la Disposición Nº71/24 se aprobó la reglamentación de la Ley N°2095y sus modificatorias para ser aplicado en el ámbito de la Defensoría del Pueblo;

La Coordinación Operativa de Gestión Técnica de esta Defensoría, desempeña el rol de Unidad Operativa de Adquisiciones conforme la Ley N°2095 y sus modificatorias y de acuerdo lo establecido por la Disposición N°140/23;

Mediante la Disposición N° 71/24, fue aprobado el Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios que realice la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, publicado en el BOCBA N°6884 del 30/05/24;

Mediante Memo N°241278/25 la Dirección General de Tecnología solicitó la **"Adquisición de Licencias Solución Ciberseguridad EDR/MAIL Server"**;

En razón de lo expuesto y habiéndose determinado, por parte de la Unidad Operativa de Adquisiciones la modalidad de contratación, corresponde efectuar el llamado a **Licitación Pública**, de acuerdo a lo normado en el artículo 32 de la Ley 2095 y sus modificatorias, y aprobar el Pliego de Condiciones Particulares y Especificaciones Técnicas para la **"Adquisición de Licencias Solución Ciberseguridad EDR/MAIL Server"** para la Defensoría del Pueblo;

La Conducción Ejecutiva de Asuntos Legales, en su carácter de Servicio Jurídico Permanente ha tomado la intervención que le corresponde en orden a sus competencias;

Por todo ello y en uso de las facultades que le confiere el artículo 13, inc. n) y o) de la Ley N°3;

LA DEFENSORA DEL PUEBLO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
RESUELVE:

Artículo 1º: Llamar a **Licitación Pública N° 04/25** para la **"Adquisición de Licencias Solución Ciberseguridad EDR/MAIL Server"** por un monto estimado de pesos: **ciento cincuenta y un millones trescientos sesenta y seis mil doce con 70/100 centavos ($ 151.366.012,70.-)**

Artículo 2º: Aprobar el Pliego de Bases y Condiciones Particulares de la **Licitación Pública** referida en el artículo precedente, que como **Anexo I** integra la presente Resolución.

Artículo 3º: Aprobar el Pliego de Especificaciones Técnicas de la **Licitación Pública** referida en el artículo precedente, que como **Anexo II** integra la presente Resolución.

Artículo 4º: Establecer el día **miércoles 30 de julio de 2025 a las 11:00 horas** como fecha para la apertura pública de ofertas.

Artículo 5º: Designar como integrantes titulares de la Comisión Evaluadora de Ofertas (C.E.O) en el marco de la presente Licitación: al Director Ejecutivo de la Conducción

Ejecutiva Técnica y Administrativa: Sr. Dante Sironi; al Director General de Tecnología Sr. Pablo Maccari y al Director de Operaciones de Tecnología Sr. Leandro Centurión.

Artículo 6º: Designar como integrantes suplentes de la Comisión Evaluadora de Ofertas (C.E.O) en el marco de la presente Licitación: al Subdirector de Conectividad y Redes, Sr. Mariano Talarico y al Director de Planeamiento Informático Sr. Mauro Müller.

Artículo 7°: Los integrantes de la Comisión Evaluadora de Ofertas quedan facultados para ejercer las funciones que se estipulan en los artículos 99, 100 y 101 de la Ley de Compras y Contrataciones Ley N°2.095 y sus modificatorias.

Artículo 8º: Dar intervención a la Coordinación Operativa de Gestión Técnica en su ámbito de competencia.

Artículo 9º: La erogación que demande la presente gestión será imputada en la correspondiente partida presupuestaria.

Artículo 10º: Los pliegos serán gratuitos.

Artículo 11º: Las publicaciones e invitaciones se realizarán de acuerdo a lo normado en los artículos 91 y 92 de la Ley Nº2095 y sus modificatorias.

Artículo 12°: Registrar, publicar en el Boletín Oficial por el término de tres (3) días, y en el sitio web de la Defensoría del Pueblo de la Ciudad de Buenos Aires.

mj/vfm/ETU/COGT
ea/MIR/CEAL

RESOLUCIÓN INTERNA Nº 117/25

María Rosa Muiños
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires

UNIDAD OPERATIVA DE ADQUISICIONES

COORDINACIÓN OPERATIVA DE GESTIÓN TÉCNICA

ANEXO I

RESOLUCIÓN INTERNA N°: 117/25

PLIEGO DE BASES Y CONDICIONES PARTICULARES

LICITACIÓN PÚBLICA N°04/2025

OBJETO DEL LLAMADO: "Adquisición de Licencias Solución Ciberseguridad EDR/MAIL SERVER"

FECHA DE APERTURA: miércoles 30 de julio de 2025 a las 11:00 horas.

1.RÉGIMEN DE CONTRATACIÓN

El presente llamado se sujeta al régimen establecido por el Art. 32 de la Ley 2095 y sus modificatorias, y su Reglamentación para esta Defensoría del Pueblo establecida por la Disposición N°71/24.

El mismo se regirá por la citada normativa, por las disposiciones del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios (Disposición N°71/2024 disponible en la página web del organismo), y las contenidas en el presente Pliego de Bases y Condiciones Particulares.

2.FORMA DE COTIZAR

2.1.PRESENTACIÓN DE OFERTAS

En sobre cerrado. Las ofertas se presentarán en un solo sobre común, perfectamente cerrado, el cual permanecerá en ese estado hasta el día y hora fijados para la apertura.

El sobre y la cotización deberán llevar los siguientes datos: N° de contratación, objeto, fecha y hora de apertura.

Se deberá indicar en la cotización N° de CUIT y N° de Ingresos Brutos correspondientes.

La oferta económica y toda la documentación deberá estar firmada en todas sus hojas por el oferente o su representante legal de puño y letra o mediante firma digital validada por certificadora oficial en los términos de la Ley N°25.506. La firma deberá encontrarse aclarada indicando el carácter del firmante. La oferta económica deberá presentarse por duplicado.

Toda la documentación presentada deberá estar debidamente foliada, en el extremo superior derecho, anverso y reverso con indicación de la cantidad de fojas presentadas (ejemplo: 1 de 10, 2 de 10, etc.).

2.2. MONEDA DE COTIZACIÓN

Pesos Argentinos.

2.3. CONDICIÓN FRENTE AL IVA

El precio contenido en la oferta económica, deberá estar expresado en pesos argentinos, e incluir el monto correspondiente al Impuesto al Valor Agregado (I.V.A).

A los efectos emergentes del Impuesto al Valor Agregado (I.V.A.), este Organismo reviste la condición de Exento; en consecuencia, en las propuestas económicas que el interesado presente junto a las ofertas no se deberá discriminar el importe correspondiente a la incidencia de este impuesto, debiendo incluirse el mismo en el precio cotizado, indicándose el porcentaje de este impuesto incluido. (27%, 21%, 10,5%, según corresponda).

El número de CUIT correspondiente a la Defensoría del Pueblo de la Ciudad de Buenos Aires es: 30-99927523-7.

2.4. DETALLE DE LA COTIZACIÓN

La oferta deberá especificar el precio unitario y cierto en números el que deberá responder estrictamente a la unidad de medida solicitada, el precio total del renglón en números y el total general de la oferta, en base a la alternativa de mayor valor, expresado en letras y números, determinados en la moneda de curso legal.

El importe total de cada renglón cotizado deberá presentarse con 2 (dos) dígitos decimales, en caso de cotizar con más dígitos decimales, se tomarán en cuenta los primeros dos, no realizándose redondeo alguno.

No se aceptarán ofertas que no contengan las condiciones detalladas en el precedente artículo 2.

3.FORMULACIÓN DE LA OFERTA

Las ofertas deberán cotizar la totalidad de los renglones solicitados. No se tendrán en cuenta cotizaciones parciales.

4.CONSULTAS

Las consultas relacionadas con la presente contratación podrán realizarse ante esta Unidad Operativa de Adquisiciones hasta 72 (setenta y dos) horas previas a la fecha establecida para la apertura de las ofertas al siguiente mail: uoa@defensoria.org.ar

5.CIRCULARES Y NOTIFICACIONES

La dirección de correo electrónico consignada por el interesado al momento de la presentación de la oferta, será registrada como la dirección donde se cursarán y serán válidas todas las circulares emitidas y demás comunicaciones que sea necesario remitir a los interesados.

En virtud de ello, la Orden de Compra, entre otras, será remitida al mencionado correo generando esto notificación fehaciente. **Si no existiera respuesta alguna del proveedor dentro de los 3 (tres) días hábiles de remitida la Orden, se considerará tácitamente perfeccionado el contrato.**

6.PRESENTACIÓN DE OFERTAS

Las ofertas deberán presentarse en la Subcoordinación Operativa de Compras y Contrataciones, sita en la sede de la Defensoría del Pueblo, Venezuela 538, primer

piso C.A.B.A., en el siguiente plazo y horario: de lunes a viernes de 11:00 a 16:00 horas, hasta la fecha y horario fijada para el Acto de Apertura.

7.ACTO DE APERTURA

En la Subcoordinación Operativa de Compras y Contrataciones, sita en la sede de la Defensoría del Pueblo, Venezuela 538, primer piso, C.A.B.A.
En la siguiente fecha y horario: **miércoles 30 de julio de 2025 a las 11:00 horas.**

8.DOCUMENTACIÓN COMPLEMENTARIA PARA PRESENTAR CON LA OFERTA

Complementariamente a los instrumentos a presentar con la oferta de acuerdo a lo requerido en el Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios, los oferentes deberán integrar la siguiente documentación:

8.1 GARANTÍA DE OFERTA, de corresponder, según lo estipulado en el Art. 12 del presente Pliego.

8.2 DECLARACIÓN JURADA DE INTERESES PERSONAS HUMANAS – PERSONAS JURÍDICAS: de acuerdo al modelo previsto en el Anexo VII- VIII del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional) conforme personería jurídica del oferente.

8.3 DECLARACIÓN JURADA DE APTITUD PARA CONTRATAR conforme Art. 89 de la Ley N° 2095 y sus modificatorias, de acuerdo al modelo previsto en el Anexo III del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

8.4 CARTA DE PRESENTACIÓN, indicando toda la documentación presentada en la oferta, conforme Anexo IV del Pliego Único de Bases y Condiciones Generales para

la contratación de bienes y servicios. (Descargar desde página web institucional)

8.5 DECLARACIÓN DE LIBRE DEUDA PREVISIONAL, conforme Anexo V del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

8.6 DECLARACIÓN JURADA LEY Nº778, conforme Anexo VI del Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios. (Descargar desde página web institucional)

El Pliego Único de Bases y Condiciones Generales para la contratación de bienes y servicios y los anexos completos que constituyen declaraciones juradas que deben ser parte de la oferta para la presente contratación se encuentran publicados en la página web del organismo para su descarga: https://defensoria.org.ar/compras-y-contrataciones/

8.7 CONSTANCIA DE INSCRIPCIÓN/OPCIÓN EN ARCA, vigente al momento de la presentación de ofertas.

8.8 FORMULARIO DE INSCRIPCIÓN EN EL IMPUESTO A LOS INGRESOS BRUTOS, contribuyentes locales (inscripción en la Dirección General de Rentas – AGIP) O Inscripción en el Régimen de Convenio Multilateral (CM01), según corresponda.

8.9 ACREDITACIÓN DE LA PERSONERÍA O CAPACIDAD DEL FIRMANTE DE LA OFERTA, conforme personería jurídica; Personas Jurídicas: copia del estatuto, acta de designación, etc. según tipo societario. Personas Humanas: copia del DNI.

8.10 PRESENTACIÓN DEL PRESENTE PLIEGO DE BASES Y CONDICIONES

PARTICULARES Y ESPECIFICACIONES TÉCNICAS FIRMADO EN TODAS LAS HOJAS DECLARANDO ACEPTACIÓN DE CONDICIONES.

8.11 PRESENTACIÓN DE COMPROBANTE DE C.B.U (Clave Bancaria Única), expedido por entidad bancaria.

8.12 PRESENTACIÓN DE EXENCIONES IMPOSITIVAS, de corresponder.

9. RIUPP - Registro Informatizado Único y Permanente de Proveedores

La Unidad Operativa de Adquisiciones consulta on-line el estado registral de los proveedores en el Registro.

El oferente deberá haber iniciado el trámite de inscripción previo al momento de la apertura de las ofertas, caso contrario la oferta será desestimada.

Es condición para la preadjudicación y adjudicación que el proveedor se encuentre en estado inscripto en el RIUPP y con la documentación respaldatoria actualizada. Cuando se tratare de licitaciones o concursos de etapa múltiple, el proveedor debe estar inscripto en forma previa a la preselección y adjudicación.

Los proveedores deben mantener la documentación, rubros, y clases ofrecidos actualizados, cumplimentando el trámite de actualización.

En caso de detectar un estado registral desactualizado al momento de la adjudicación esta Defensoría le otorgará al proveedor un plazo de 10 (diez) días hábiles para regularizar tal situación, a los fines de la adjudicación. Este plazo podrá prorrogarse por única vez por un mismo periodo en los casos que estén debidamente fundada las razones que lo ameriten y en los casos en que se tratare de un único oferente.

10.MANTENIMIENTO DE OFERTAS

Los oferentes deberán mantener las ofertas por el término de 30 (treinta) días hábiles contados a partir de la fecha del acto de apertura.

Si el oferente no manifestara en forma fehaciente su voluntad de no renovar la oferta

con una antelación mínima de 10 (diez) días al vencimiento del plazo, aquella se considerará prorrogada automáticamente por un lapso igual al inicial.

11. SUBSANACIÓN DE DEFICIENCIAS

A fin de subsanar omisiones o deficiencias en las ofertas presentadas, esta Unidad Operativa de Adquisiciones se reserva el derecho a requerir con posterioridad a la apertura, toda documentación que no fuera presentada en la oferta y/o aquella que considere necesaria.

Dicha solicitud deberá ser respondida por los oferentes dentro de las 72 (setenta y dos) horas de solicitada. **Bajo apercibimiento de proceder a desestimar la oferta en caso de incumplimiento.**

La misma será solicitada al mail declarado en la DDJJ solicitada en el punto 8.4 del presente pliego.

12. GARANTÍA DE OFERTA Y CUMPLIMIENTO DE CONTRATO

Garantía de impugnación al Pliego de Bases y Condiciones:

La integración de esta garantía deberá realizarse dentro del plazo establecido para realizar las impugnaciones conforme lo establecido en el Art. 9º del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios. La falta de su integración dará lugar a la desestimación sin más trámite. El monto de esta corresponderá al 1% del presupuesto oficial o monto estimado de la compra.

Garantía de Mantenimiento de Oferta: Los oferentes deberán constituir una garantía de mantenimiento de oferta incondicional e irrevocable a favor de la Defensoría del Pueblo de la Ciudad de Buenos Aires, por una suma equivalente al 5 % del valor de la oferta presentada.

Si la oferta fuese con alternativa, el oferente deberá calcularla sobre el mayor valor cotizado. Dicha garantía deberá ser mantenida por los oferentes hasta perfeccionamiento de la Orden de Compra y será constituida a través de póliza de

seguro de caución emitida por una compañía aseguradora local y a satisfacción de la Defensoría del Pueblo de la Ciudad de Buenos Aires.
En el caso de existir impugnación de la pre adjudicación, deberá presentar garantía del 5 % del monto de la oferta del renglón o renglones impugnados.

Garantía de cumplimiento del contrato: El adjudicatario deberá presentar en los términos del Artículo 107 de la Ley 2095 y sus modificatorias, de un 10% sobre el valor total de la adjudicación. La misma deberá constituirse dentro de los 5 (cinco) días del perfeccionamiento de la Orden de Compra de acuerdo a lo establecido en el Artículo 9° del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios. De acuerdo al Artículo 10°: "EXENCIÓN DE PRESENTAR GARANTÍAS" del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios.

Nota: De acuerdo al Artículo 10°: "EXENCIÓN DE PRESENTAR GARANTÍAS" del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios:
"No es necesario constituir la garantía de mantenimiento de oferta ni de cumplimiento del contrato, cuando el monto de la oferta y del contrato, respectivamente, no supere el límite de las 100.000 (cien mil) Unidades de Compra. *El monto de cada unidad de compra para el ejercicio 2025 es de pesos: trescientos setenta con 00/100 centavos ($ 370,00.-). Por lo tanto, las ofertas inferiores a pesos: treinta y siete millones con 00/10 centavos ($ 37.000.000,00.-) quedan eximidas de la presentación de las garantías nombradas precedentemente".*

La excepción a la que hace referencia esta nota, aplica a la Garantía de Mantenimiento de Oferta y a la Garantía de Cumplimiento del Contrato.

13.CRITERIO DE EVALUACIÓN DE OFERTAS

La etapa de evaluación de las ofertas es confidencial, por lo cual durante esta etapa no se concederá la vista del expediente.

De conformidad con el Art. 102° de la Ley N° 2095 y sus modificatorias. Se considerará como la oferta económicamente más conveniente para el organismo aquella que, habiendo cumplido con las cláusulas de los pliegos y los requisitos técnicos, tenga el precio más bajo.

14.VISTA DE EXPEDIENTE

La solicitud deberá ser realizada por el oferente, mediante nota ingresada por Mesa de Entrada dentro del período de 3 (tres) días hábiles administrativos, luego de la publicación en Boletín Oficial y el sitio web de esta Defensoría del Dictamen de la Comisión Evaluadora de Ofertas, de acuerdo a la normativa vigente.

15.CAUSALES DE RECHAZO DE LA OFERTA

Se procederá al rechazo de la oferta en los casos en los cuales corresponda la constitución de garantía y la empresa oferente no la presentara (conforme Art. 9º del Pliego Único de Bases y Condiciones Generales para contratación de bienes y servicios y Art. 98 Ley 2095 y sus modificatorias).

En concordancia con lo establecido precedentemente, se procederá también al rechazo de las ofertas cuando las mismas incurrieren en alguno de los siguientes supuestos:

a). Si el original no estuviera firmado por el oferente o su representante legal.

b). Si estuviera escrita con lápiz.

c). Si contuviera condicionamientos.

d). Si tuvieran raspaduras, enmiendas o interlíneas en el precio, cantidad, plazo de entrega o alguna otra parte que hiciere a la esencia del contrato y no estuvieren debidamente salvadas.

e). Si contuviera cláusulas en contraposición con las normas que rigen la contratación.

f). En los casos de Adjudicación "Por Renglones", se procederá al rechazo del renglón cuyo precio cotizado superase en más de un 20% (veinte por ciento), al precio de referencia estimado por el área técnica. (Valores adjuntos en el Pliego de Especificaciones Técnicas).

g) En los casos de Adjudicación "Global", cuando la oferta superase en más de un 20% (veinte por ciento) el precio de referencia estimado en la Resolución Interna, se procederá al rechazo total de la oferta.

h). Cuando el oferente no realizara la correspondiente "Visita de Obra".

16.ADJUDICACIÓN

La adjudicación se realizará a favor de la oferta más conveniente, de manera global, teniendo en cuenta para ello el precio, la calidad, la idoneidad del oferente, los costos asociados de uso y mantenimiento presentes y futuros y demás condiciones de la oferta, habiendo cumplido con las cláusulas de los pliegos y los requisitos técnicos.

17. VISITA DE OBRA

La empresa oferente deberá efectuar la visita en los edificios de esta Defensoría del Pueblo que indique la Dirección General de Tecnología, la misma reviste el carácter de obligatoria.

La visita podrá efectuarse en día y horario combinado con una antelación no inferior a las 24 (veinticuatro) horas por vía telefónica con: Subcoordinación Operativa de Compras y Contrataciones de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. Tel. de Contacto: 11 3209-0791 u 11 3628-2566.

18. SEGUROS

Los seguros deberán contratarse en Compañías o Entidades Aseguradoras, con domicilio en la Ciudad Autónoma de Buenos Aires, y que resulten aptas para la prestación enunciada a juicio exclusivo de la DPCABA, e incluirá al mismo como cotitular y/o beneficiario, según corresponda.

En cualquier momento la DPCABA podrá requerir la sustitución de la entidad bancaria o de la compañía aseguradora si a su solo juicio las mismas no ofrecen suficiente garantía de solvencia y seriedad.

a) Exigencias de las pólizas sin restricciones

En caso que las primas sean abonadas en cuotas, las respectivas pólizas no deberán tener cláusulas restrictivas alguna, de existir incumplimiento en el pago de las mismas.

b) Accidentes de trabajo

La firma adjudicataria será responsable de su personal por accidentes de trabajo, para lo cual deberá contratar un seguro que cubra la totalidad de las obligaciones fijadas por la Ley sobre Riesgos de trabajo Nº24.557 y sus Decretos Reglamentarios. El seguro deberá cubrir los riesgos y accidentes de trabajo y/o enfermedades profesionales e inculpables, amparando las indemnizaciones por incapacidad permanente, parcial y absoluta, incapacidad temporaria y/o muerte, accidente "in-itinere" y prestación médico-farmacéutica, por el monto máximo que fijare la legislación vigente.

Además, la firma adjudicataria deberá presentar ante la DPCABA "Declaración Jurada", donde conste que todo el personal afectado a la prestación se encuentra cubierto por este seguro, indicando el número de Póliza correspondiente y el nombre de la compañía Aseguradora. Por lo tanto, en cada oportunidad que se produzca alguna modificación en la dotación destacada, deberá comunicarse dentro de las 72 (setenta y dos) horas de producida la misma.

c) Responsabilidad Civil

El adjudicatario deberá contratar un seguro que cubre expresamente la actividad a realizar, POR HECHO Y POR PERSONA, que cubra los riesgos de responsabilidad civil, por los daños que, como consecuencia de la prestación del servicio que se contrata, se ocasionen a personas, cosas y/o bienes de terceros y/o de la DPCABA. - Dicha póliza deberá ser endosada a favor de la DPCABA.

En caso que el monto del mismo no alcanzare a cubrir los daños provocados, la diferencia resultante correrá por parte del adjudicatario.

19. DEPENDENCIA LABORAL

Todo el personal afectado al servicio estará bajo exclusivo cargo de la adjudicataria, no teniendo en consecuencia relación de dependencia alguna con la DPCABA, la que no asume por lo tanto ninguna responsabilidad ante cualquier conflicto o litigio que eventualmente se genere por cuestiones de índole laboral entre la adjudicataria y su personal.

Cada trabajador será notificado de esta situación y suscribirá una declaración jurada, reconociendo que la única relación laboral existente es la que lo vincula con la adjudicataria.

Estas declaraciones juradas deberán ser entregadas a Dirección General de Tecnología junto con las nóminas requeridas para ser incorporadas al expediente respectivo.

Asimismo, la adjudicataria será responsable del cumplimiento de las leyes y normas sanitarias que sean exigibles por la característica de la actividad (Libretas Sanitarias actualizadas, exámenes físicos, etc.).

La adjudicataria deberá cumplir estrictamente con todas las obligaciones que le competen en materia previsional, tributaria o fiscal y de empleo, de acuerdo con las exigencias legales vigentes o las que se dicten en el futuro.

En cualquier momento durante la ejecución del contrato, la DPCABA podrá requerir los comprobantes que acrediten el cumplimiento de dichas obligaciones. La adjudicataria será responsable del cumplimiento de sus obligaciones impositivas.

Todos los impuestos que graven la actividad de la adjudicataria deberán estar incluidos en el precio cotizado.

La adjudicataria queda comprometida a mantener indemne a la DPCABA, de cualquier suma que deba abonar, derivada de las obligaciones laborales y de la seguridad social relacionadas con su personal y/o subcontratista que tenga o pudiera tener a su cargo o que contrate con la modalidad laboral que dispusiera, o prestare servicios en cumplimiento del objeto de la contratación.

Asimismo, La adjudicataria asume en forma exclusiva toda responsabilidad civil derivada de la prestación del servicio comprometiéndose a mantener indemne a la DPCABA respecto de cualquier reclamo originado en hechos ocurridos en ocasión de la prestación del servicio.

La adjudicataria se compromete a notificar de forma inmediata y en un plazo no mayor a los 3 (tres) días hábiles administrativos de haber tomado conocimiento de cualquier reclamación, acción o procedimiento de los que tengan conocimiento y que puedan generar cualquier tipo de responsabilidad respecto de la otra parte.

La adjudicataria se obliga a cumplir acabadamente con todas las normas de Seguridad, Salubridad e Higiene y Protección del Medio Ambiente y con cualquier otra norma aplicable a su actividad y a los Servicios a nivel nacional, provincial y municipal, durante toda la vigencia de la relación contractual. La adjudicataria será la única responsable por los accidentes y/o infracciones que pudieran ocurrir y/o cometerse durante o con motivo de la prestación de los Servicios.

20. CLÁUSULA DE INDEMNIDAD

El adjudicatario se compromete y acuerda en forma irrevocable mantener indemne a la DPCABA por cualquier reclamo, acción judicial, demanda, daño o responsabilidad de cualquier tipo o naturaleza que sea entablada por cualquier persona pública o privada, física o jurídica, o dependientes del adjudicatario, cualquiera fuera la causa del reclamo, responsabilidad que se mantendrá aún terminado el contrato por cualquier causa. La responsabilidad se extenderá a indemnización, gastos y costas, sin que la enunciación sea limitativa. En estos casos la DPCABA queda facultada para afectar cualquier suma que por cualquier concepto la DPCABA adeudara al adjudicatario sin que ello limite la responsabilidad de este último.

21. PENALIDADES

El incumplimiento de las condiciones de tiempo, modo y lugar de cualquiera de las obligaciones asumidas por la contratista en virtud del plexo jurídico aplicable a la

contratación que se celebra, genera la mora automática sin necesidad de interpelación administrativo ni judicial, siendo, asimismo, pasible de ser penalizado y/o sancionado conforme regulación y atribuciones contempladas en la Ley 2095, Artículos 117 y 129 y sus modificatorias, su Reglamentación, y las previsiones de este pliego.

La penalidad o la sanción aplicable lo será sin perjuicio del derecho que le corresponde a la DPCABA por los daños y perjuicios que eventualmente se ocasionen.

A los efectos de la aplicación y graduación de las penalidades previstas en la Ley 2095, sus modificatorias y su reglamentación, el órgano competente debe considerar las circunstancias fácticas del caso, el incumplimiento detectado, su gravedad, el eventual daño causado, así como la aplicación de penalidades y/o sanciones previas.

22.CONTINUIDAD DE LOS SERVICIOS

En caso de producirse una interrupción total o parcial del servicio, la DPCABA podrá efectuarlo directamente por sí o por terceros, a fin de mantener su continuidad, por cuenta y cargo del adjudicatario.

23.PLAZO Y FORMA DE PAGO

- Renglón 1 y 2: Se realizará un pago total al inicio de la entrega de las licencias. La factura deberá emitirse una vez que se haya confirmado la recepción de la Orden de Compra. El área técnica será responsable de verificar la efectiva prestación del servicio o entrega del bien, y de emitir los PRD correspondientes. El pago se efectuará dentro de los 20 días posteriores a la presentación de la factura, el PRD y demás documentación requerida.

- Renglón 3: Se realizarán dos pagos: un primer pago del 50% (cincuenta por ciento) al inicio de la orden de compra, y el saldo del 50% (cincuenta por ciento) al finalizar las capacitaciones, contra la presentación de la factura y el PRD emitido por el área requirente. Los pagos se efectuarán dentro de los 20 días

posteriores a la presentación de la factura, el PRD y demás documentación requerida.

- Renglón 4: Se realizarán 12 (doce) pagos iguales, mensuales y consecutivos, contra la presentación de la factura y el PRD emitido por el área requirente, con la recepción conforme de la prestación del servicio. Los pagos se efectuarán dentro de los 20 (veinte) días posteriores de recibida la factura y el PRD en la Coordinación Operativa de Gestión Económica y Financiera.

Los pagos serán efectuados mediante transferencia bancaria al C.B.U. declarado por el proveedor de acuerdo al artículo 8.11 del presente pliego.

Excepcionalmente, el proveedor podrá solicitar expresamente a través de una nota, el pago mediante la emisión de cheque bancario, detallando los datos que correspondan al efecto.

24. LUGAR Y FORMA DE ENTREGA/ PRESTACIÓN

La prestación/entrega se realizará bajo la coordinación y supervisión de la Dirección General de Tecnología de esta Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

25. PLAZO DE ENTREGA /PRESTACIÓN DE SERVICIO

La entrega/ prestación se realizará bajo la coordinación y supervisión de la Dirección General de Tecnología. Tel. de Contacto: 11-30885326 int.3794, al momento de la emisión de la Orden de Compra, y por el término de 12 (doce) meses.

El proveedor deberá garantizar contar con capacidad técnica y operativa para cumplir con la entrega en el tiempo y la forma en que sean requeridos.

La DPCABA, podrá solicitar una prórroga contractual en las mismas condiciones que las establecidas en el contrato original, por un plazo igual o menor del contrato inicial, no pudiendo el plazo de la prórroga superar el plazo de vigencia original del contrato

26. ORDEN DE COMPRA – CONDICIONES PARA LA EMISIÓN

Previo a la emisión de la Orden de Compra el organismo procederá a solicitar información a la Agencia de Recaudación y Control Aduanero - ARCA a los efectos de verificar la habilidad para contratar de la firma adjudicada quien no deberá contar con incumplimientos tributarios y/o previsionales de acuerdo a la normativa en vigencia (RG 4164/2017 AFIP). Ante la existencia de incumplimiento, esta Defensoría le otorgará al proveedor un plazo de 10 (diez) días hábiles para regularizar tal situación, a los fines de la emisión de la orden de compra. Este plazo podrá prorrogarse por única vez por un mismo periodo en los casos que estén debidamente fundada las razones que lo ameriten y en los casos en que se tratare de un único oferente.

27. RECEPCIÓN DEFINITIVA

La recepción y conformidad definitiva de los bienes entregados y/o la certificación de la prestación de un servicio, será efectuada por Dirección General de Tecnología.

A los efectos de la recepción y conformidad técnica, deberá procederse a la confrontación de la prestación con las especificaciones del pedido que surgen de la Orden de Compra.

En consecuencia, se confeccionará un Parte de Recepción Definitiva el cual será suscripto por el o los responsables de la recepción, dando conformidad a la entrega y/o prestación. Dicha conformidad debe ser acordada dentro de un plazo de 8 (ocho) días corridos de la entrega o finalización de la prestación.

28.CLÁUSULA DE RESCISIÓN

La DPCABA se reserva el derecho a rescindir o disminuir el contrato que origine la presente contratación, por razones presupuestarias, traslados, modificación y /o baja de sedes, etc., sin asistirle derecho alguno al adjudicatario sobre compensaciones, gastos administrativos, constitución de las garantías, lucro cesante e indemnizaciones, etc. Para ejercer este derecho el organismo contratante, efectuará la respectiva comunicación con la anticipación de 30 (treinta) días corridos.

Asimismo, la DPCABA se reserva el derecho de rescindir el contrato que origine la presente contratación para el caso que el futuro adjudicatario no cumpla con las exigencias establecidas en el Pliego de Bases y Condiciones Particulares y Especificaciones Técnicas.

María Rosa Muiños
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

UNIDAD OPERATIVA DE ADQUISICIONES

COORDINACIÓN OPERATIVA DE GESTIÓN TÉCNICA

Anexo II-Resolución Interna N° 117/25

PLIEGO DE ESPECIFICACIONES TÉCNICAS

LICITACIÓN PÚBLICA N°4/2025

OBJETO DEL LLAMADO: "Adquisición de Licencias Solución Ciberseguridad EDR/MAIL Server"

FECHA DE APERTURA: miércoles 30 de julio de 2025 a las 11:00 horas.

Renglón	Descripción	Unidad de medida	Cantidad	Vigencia
1	Licencia de seguridad tipo EDR (Endpoint Detection and Response), del fabricante Kaspersky o equivalente técnicamente, conforme a los requisitos detallados en las especificaciones técnicas.	Licencias	1000	12 meses
2	Licencia de Plataforma de Protección para correo electrónico, (Security for Mail Server), del fabricante Kaspersky o equivalente técnicamente, conforme a los requisitos detallados en las especificaciones técnicas.	Licencias	1000	12 meses
3	Servicio de Implementación y Capacitación	Servicio	1	Única vez
4	Servicio de Soporte Técnico	Servicio	1	12 meses

ESPECIFICACIONES TÉCNICAS

- **Adquisición de licencias de software de Detección y Respuesta para Endpoints (EDR) con capacidades de Protección para Endpoints (EPP) y de Protección para Correos Electrónicos.**

✓ **Renglones: Descripción**

1- Plataforma de EDR con capacidades EPP – 12 meses
2- Plataforma de Protección para Correos Electrónicos – 12 meses
3-- Servicio de Implementación y Capacitación
4- Servicio de Soporte Técnico – 12 meses

Dado que el presente pliego contempla la implementación de una solución integral, esta se llevará a cabo bajo la modalidad de "Llave en mano".
Todos los renglones que componen la presente licitación serán adjudicados a un único oferente y deberán estar respaldados por un mismo fabricante para las soluciones y servicios incluidos en todos los ítems.

✓ **RENGLÓN 1: Plataforma de EDR con capacidades EPP.**

1. Se debe proveer una solución tecnológica que permita la detección, prevención, contención y respuesta ante malware conocido, así como también ataques desconocidos, dirigidos y avanzados.

2. La solución debe incluir los módulos de protección antimalware tradicionales basados en firmas y módulos de protección avanzados basados en comportamiento, que permitan proteger la infraestructura de TI de ciber amenazas complejas.

3. Debe contar con análisis de AV, de reputación de archivos, reputación de URLs y categoría de aplicaciones, así como incluir integración con un Portal de Inteligencia de

Amenazas propio del fabricante en donde se brinde más información acerca del ataque.

4. Debe detectar la amenaza sin necesidad de conocer la firma, es decir, a través del comportamiento de la propia amenaza y proporcionar detección en las comunicaciones desde y hacia los servicios de internet, contra los ataques de malware de día cero, exploits, botnets y ataques dirigidos.

5. Los eventos generados deben ser almacenados en una base de datos por un período de tiempo configurable de acuerdo al tipo de evento y su criticidad.

6. Debe permitir, al menos, las siguientes capacidades de respuesta ante una amenaza:

a. Aislamiento de red del endpoint.
b. Mover archivo a la cuarentena de forma automática y/o manual.
c. Visualizar los archivos que se encuentren en cuarentena.
d. Eliminar el archivo de forma automática y/o manual.
e. Permitir un escaneo sobre las áreas críticas del sistema operativo.
f. Realizar un escaneo de los Indicadores de Compromiso (IOC) asociados al ataque sobre todos los endpoints de la organización.
g. Prevenir la ejecución de dicho archivo o proceso en el resto de los endpoints a partir de su detección.
h. Iniciar y/o terminar algún proceso sobre el endpoint.

7. La solución debe ofrecer la flexibilidad, bajo la misma licencia de producto, de poder desplegar la consola de administración tanto en la nube como en entornos locales (on-premise), para que el organismo tenga la opción de cambiar la modalidad de administración en caso que lo requiera.

8. Independientemente del tipo de despliegue, la consola de administración debe contar con la posibilidad de activar un segundo factor de autentificación (2FA) compatible con Microsoft Authenticator y Google Authenticator.

9. La consola de administración on-premise debe ser accesible vía Web (HTTPS) y/o MMC basado en roles y perfiles de acceso, con capacidades granulares de definición de restricciones y capacidades funcionales.

10. La solución debe de poder desinstalar remotamente cualquier software instalado (propio o de terceros) en las máquinas clientes.

11. La solución propuesta debe contar con la posibilidad de desplegarse utilizando mínimamente los siguientes métodos:
a. De forma local, utilizando el asistente de instalación o por línea de comando.
b. De forma remota, utilizando la Consola de Gestión de la solución propuesta y sin depender de una plataforma de terceros.
c. De forma remota, utilizando el Editor de administración de directivas de grupo de Microsoft Windows (GPO).
d. De forma remota, utilizando Microsoft System Center Configuration Manager.

12. Debe gestionar estaciones de trabajo y servidores tanto Windows, Linux y macOS, así como dispositivos móviles Android y iOS.

13. Debe poder realizar la distribución remota de cualquier software para que sea instalado en las máquinas clientes; y de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones base de la solución.

14. Debe aplicar actualizaciones y parches tanto de Windows como de software de terceras partes (ej. Adobe, Google Chrome, etc.) remotamente en las estaciones de trabajo y servidores.

15. Debe disponer de capacidad de borrado remoto de datos para evitar la pérdida de información en caso del robo o extravío de un dispositivo.

16. El borrado remoto de datos debe permitir establecer criterios selectivos y condiciones para la ejecución de regla de eliminación de datos en equipamiento.

17. Tendrá la capacidad de vuelta atrás automática para poder revertir en tiempo real las acciones maliciosas producidas por una amenaza como, por ejemplo, un ransomware.

18. Al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, debe automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el agente antivirus/EDR instalado. En caso de no tenerlo, debe instalarlo automáticamente.

19. Debe tener la capacidad de importar la estructura de equipos desde el Active Directory para el armado de los grupos jerárquicos.

20. Debe poder realizar el agrupamiento de máquinas por características comunes, entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 7 días, etc.

21. Debe definir políticas de configuraciones diferentes por grupos de estaciones permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos.

22. Debe proporcionar las siguientes informaciones de las computadoras:

a. Si el antivirus está instalado, iniciado y/o actualizado.
b. Minutos/horas desde la última conexión de la máquina con el servidor administrativo y desde la última actualización de firmas.
c. Fecha y horario de la última verificación ejecutada en la máquina.
d. Versión del antivirus instalado en la máquina.
e. Si es necesario reiniciar la computadora para aplicar cambios.
f. Cantidad de virus encontrados (contador) en la máquina.
g. Nombre de la computadora y dominio o grupo de trabajo de la computadora.
h. Sistema operativo con el detalle de Service Pack en el caso de Windows.
i. Cantidad de procesadores y de memoria RAM.
j. Usuario(s) conectados en ese momento.

k. Dirección IP.
l. Aplicativos instalados, inclusive aplicativos de terceros.
m. Actualizaciones de Windows Updates instaladas.
n. Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD. o. Vulnerabilidades de aplicativos instalados en la máquina.

23. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas.

24. Debe reconectar máquinas clientes al servidor administrativo más próximo,basado en reglas de conexión como:
a. Cambio de Gateway.
b. Cambio de subnet DNS.
c. Cambio de dominio.
d. Cambio de servidor DHCP.
e. Cambio de servidor DNS.
f. Cambio de servidor WINS.
g. Aparición de nueva subnet.

25. Debe configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse y gestionarse vía internet.

26. Debe poder realizar la herencia de tareas y políticas en la estructura jerárquica de servidores administrativos.

27. Debe elegir cualquier computadora cliente como repositorio de actualizaciones y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red.

28. Debe hacer de este repositorio de actualizaciones un gateway de conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este dispositivo para recibir y enviar informaciones al servidor administrativo.

29. Debe enviar correos electrónicos para cuentas específicas en caso de algún evento, así como traps SNMP para el monitoreo de eventos.

30. Debe habilitar automáticamente una política en caso de que ocurra un ataque masivo en la red (basado en cantidad de amenazas encontradas en un determinado intervalo de tiempo).

31. Debe realizar actualización incremental de firmas en las computadoras clientes.

32. Debe realizar inventario de hardware y software de todas las máquinas clientes.

33. La solución debe permitir la monitorización y captura de eventos de red relacionados a las actividades en PCs y servidores.

34. El agente EDR de Windows, Linux y macOS debe ser capaz de colectar datos puntuales para un equipo determinado con el fin de obtener las evidencias para un posterior análisis.

35. La solución debe poder tomar entradas para indicadores personalizados de compromiso en formato OpenIOC.

36. La solución debe obtener información exhaustiva y datos forenses en tiempo real sobre los dispositivos.

37. La solución debe proporcionar varios paneles o widgets personalizables para proporcionar información sobre la actividad de los sistemas y resultados analíticos.

38. La solución debe permitir incluir IOCs en lista negra privada de inteligencia bajo formato MD5 / SHA256.

39. La solución debe ser capaz de integrarse con plataformas de SIEM para la administración de logs.

40. La solución debe ser capaz de detectar el ataque localmente, sin depender de un servicio en la nube.

41. La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensión de archivo, archivo MD5 /SHA1 o IOC provisto.

42. Las capacidades de respuesta deben de incluir el aislamiento de los equipos infectados.

43. La solución debe contar con una arquitectura basada en puntos de distribución / actualización para el despliegue de: Actualizaciones, Parches y Paquetes de Software en entornos WAN y así reducir la utilización de ancho de banda.

44. La solución debe de disponer compatibilidad mínimamente con los siguientes sistemas operativos:

a. Windows 7 SP1 y superior
b. Windows 8, Windows 8.1
c. Windows 10, Windows 11
d. MacOS 10.14 o superior.
e. Microsoft Windows Server 2008 SP2 o Superior
f. Microsoft Windows Server 2012 o Superior
g. Microsoft Windows Server 2016 o Superior
h. Microsoft Windows Server 2019 o Superior.
i. Windows Server 2022.
j. CentOS 6.7 y superior.

k. Debian GNU / Linux 9.4 y superior.
l. Debian GNU / Linux 10.1 y superior.
m. Debian GNU / Linux 11.1 y superior.
n. Linux Mint 19 y superior.
o. Red Hat Enterprise Linux 6.7 y superior.
p. CentOS 6.7 y superior.
q. CentOS 7.2 y superior.
r. CentOS 8.0 y superior.
s. openSUSE Leap 15.0 y superior.
t. Red Hat Enterprise Linux 6.7 y superior.

45. La solución EDR con capacidades EPP debe disponer mínimamente los siguientes módulos de protección, control y Harding:
a. Firewall
b. AV de Archivos, Web y Mail.
c. Detección Avanzada ML.
d. Detección reputación Nube.
e. Módulo de prevención de ataques de red (IDS)
f. Prevención de intrusiones en el host (HIPS).
g. Autoprotección (contra ataques a los servicios/procesos del antivirus)
h. Control de dispositivos.
i. Control de acceso a sitios web por categoría.
j. Control de aplicaciones.
k. Protección AMSI
l. Control de vulnerabilidades de Windows y de los aplicativos de terceras partes.
m. Modulo Anti-Ransomware.
n. Modulo Prevención de explotación de vulnerabilidades.
o. Cifrado de disco, carpetas y archivos y unidades removibles.
p. Detección y Respuesta EDR

46. La solución debe contar con modulo antimalware web (módulo para verificación de sitios y downloads antivirus) que incluya la auditoria de tráfico HTTP como Trafico

HTTPS sin necesidad de instalación de plug-in o componente adicional en el navegador.

47. La solución debe contar con un módulo antimalware de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) sin necesidad de instalación de plug-in o componente adicional.

48. El módulo de protección frente a amenazas en el correo debe ser compatible con, al menos, POP3, SMTP e IMAP.

49. La solución debe incluir un componente de protección frente a amenazas en la red que realice un monitoreo del tráfico entrante en busca de actividad característica de los ataques de red.

50. La solución debe tener la capacidad de bloquear el equipo que realiza el ataque de red y restringir el envío de paquetes de tráfico durante un periodo configurable.

51. La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques de red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC.

52. La solución debe contar con un componente de firewall a nivel de host que debe controlar la actividad de la red sobre el protocolo seleccionado, mínimamente: TCP, UDP, ICMP, ICMPv6, IGMP y GRE

53. Las firmas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo)

54. Debe contar con la capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.

55. Debe tener módulo de control que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:

a. Discos de almacenamiento locales y almacenamiento extraíble
b. Impresoras, CD/DVD, Modems
c. Dispositivos de cinta y dispositivos multifuncionales
d. Lectores de smart card
e. Wi-Fi y Adaptadores de red externos
f. Dispositivos MP3, smartphones y Dispositivos Bluetooth

56. Debe contar con capacidad de liberar acceso a un dispositivo determinado y usuarios específicos por un período de tiempo configurable, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.

57. Capacidad de limitar el acceso a sitios de internet por categoría y/o por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y horario.

58. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gestores de descarga, juegos, aplicación de acceso remoto, etc.).

59. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.

60. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.

61. Capacidad de, en caso de que la computadora cliente salga de la red corporativa,

activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

62. La solución debe de poseer módulo de control de aplicaciones que permita la generación de reglas de listas blancas y negras acorde a grupos de categorización dinámica de aplicaciones.

63. La solución debe de poseer módulo de control de aplicaciones que permita la generación de reglas de lista blanca y negra acorde al inventario de aplicaciones detectadas en la organización.

64. La solución debe incluir un componente de protección AMSI diseñado para ser compatible con el módulo de Antimalware Scan Interface de Microsoft

65. La solución debe de poseer módulo prevención de exploits, que permita detectar y contener explotación de vulnerabilidades inclusive aquellas de día 0.

66. La solución debe proporcionar la capacidad de escanear la infraestructura de los puntos finales utilizando Indicadores de Compromiso (al menos en el formato OpenIOC) - se deben soportar tanto las tareas programadas como bajo demanda.

67. La solución debe contar, dentro de su licenciamiento, con integración y acceso con un Portal de Inteligencia contra Amenazas propio del fabricante, que permita consultar información sobre la reputación de hashes, archivos y URLs.

68. La solución debe proveer un diagrama de grafos de la cadena de ataque que proporcione información visual sobre los objetos involucrados, como procesos clave en el dispositivo, conexiones de red, bibliotecas y subárboles de registro.

69. La solución debe ofrecer un proceso de recomendaciones de respuesta a alertas.

70. La solución debe permitir aislar a un equipo de la red, interrumpiendo todas las conexiones TCP/IP activas y bloqueando todas las conexiones de red TCP/IP nuevas en los dispositivos.

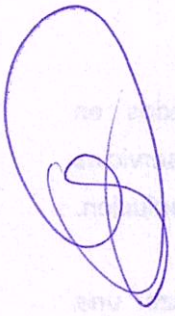
71. La solución debe permitir establecer exclusiones de aislamiento de red. Es decir que las conexiones de red que cumplan las condiciones de la exclusión especificada no se bloquearán en los dispositivos después de que se active el aislamiento de red.

72. La solución debe ofrecer la posibilidad de desbloquear el aislamiento de dispositivos de la red a petición (manualmente) o como una acción automática basada en tiempo, desde la consola de administración central sin intervención del usuario final, o en el dispositivo aislado desde la línea de comando

73. Los archivos en cuarentena se deben almacenar en el dispositivo protegido de forma cifrada de manera que no comprometan la seguridad del dispositivo.

74. La solución debe permitir crear tareas de Análisis de IoC con el fin de encontrar indicadores de compromiso en el dispositivo y realizar acciones de respuesta a la amenaza.

75. La solución debe permitir configurar reglas de prevención de ejecución de archivos utilizando algoritmos hash MD5 y SHA256.



76. La solución debe permitir configurar reglas de prevención de ejecución de archivos utilizando las rutas del archivo.

77. Debe disponer modulo anti ransomware para la detección y contención de ataques del tipo ransomware sobre carpetas compartidas de red.

78. Debe contar con un módulo de cifrado de datos embebido en el agente único de protección, que soporte algoritmos estándar como por ejemplo AES-256 en sistemas operativos Windows de Escritorio.

79. Debe contar con la capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario para sistemas operativos Windows de Escritorio.

80. Debe disponer de la capacidad de cifrar unidades extraíbles o portables.

✓ **RENGLÓN 2: Plataforma de Protección para Correos Electrónicos**

1. Se debe proveer una solución tecnológica que permita la detección y respuesta ante amenazas en correos electrónicos, tanto entrantes como salientes, incluyendo la identificación de malware, phishing, spam y adjuntos infectados.

2. La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.

3. La solución debe ser implementada 100% on-premise y debe disponer de una consola Web de gestión centralizada.

4. Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y securitización por el fabricante de la solución.

5. La solución debe proveer un procedimiento por el cual se pueda realizar una actualización de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes.

6. La solución debe inspeccionar en tiempo real el tráfico de correo (Entrada & Salida) para la remoción de todo tipo de amenazas, virus, worms, troyanos y otros tipos de programas maliciosos incluyendo correos indeseados.

7. La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti-Malware, Anti-Ransomware y de filtrado de contenido.

8. La solución tiene la capacidad de integración con servicios de reputación locales sin la necesidad de enviar datos fuera de la organización.

9. La solución debe disponer de capacidades para el desempaquetado y análisis de archivos compuestos como por ejemplo archivos comprimidos.

10. La solución debe detectar, bloquear y desinfectar mensajes de correos electrónicos infectados, así como sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

11. La solución debe detectar y bloquear mensajes que contengan anexos con macros (Por ejemplo, archivos en formato Microsoft Office con macros), eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

12. La solución debe detectar y bloquear mensajes cifrados, eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

13. La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

14. Los mensajes que se encuentran en el backup deben poder ser guardados y descargados, así como reenviados a su destinatario original u otros destinatarios a ser seleccionados.

15. La solución debe de procesar los mensajes, acorde a las reglas de seguridad estipuladas para los grupos de remitentes y destinatarios.

16. La solución debe poder validar el remitente acorde a la autentificación del remitente utilizando tecnologías SPF, DKIM y DMARC.

17. La solución debe poder firmar correos salientes mediante tecnologías DKIM.

18. La solución debe permitir la inclusión de un mensaje de alerta en el subject del correo en caso que anexos peligrosos o indeseados sean detectados.

19. La solución debe permitir la definición de listas de correo blancas/negras globales y personales.

20. La solución debe contar con tecnologías de validación de imágenes y anexos gráficos para la detección de mensajes de Spam.

21. La solución debe identificar y alertar la presencia de archivos adjuntos maliciosos, sospechosos y aquellos protegidos con contraseña.

22. La solución debe poder eliminar mensajes o sus anexos para archivos maliciosos, sospechosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.

23. La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC).

24. La solución debe disponer de tecnologías para la detección de Spam basado en el reconocimiento de dominios spoofed (look-alike).

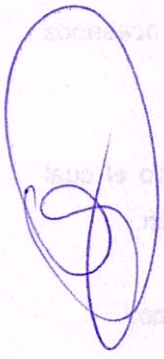
25. La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.

26. La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo ransomware.

27. En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones:

a. Desinfectar
b. Eliminar Anexo
c. Borrar mensaje
d. Rechazar mensaje
e. Ignorar

28. La solución debe permitir la configuración de notificaciones por lo menos a las siguientes direcciones (Administradores, Remitente, Destinatario, adicionales).



29. La solución debe contar con un sistema de alimentación de contenido por parte del fabricante que proporcione información sobre nuevas amenazas, y bases de reputación. Dicha información debe ser actualizada en forma automática y en tiempo real permitiendo enriquecer el motor de análisis de amenazas de la solución.

30. La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna otra información sensible fuera de la institución.

31. La solución debe disponer de soporte para la integración con Microsoft Active Directory y Open LDAP.

32. La solución debe incluir el acceso al Backup personal mediante Single Sign-On (SSO) acorde a integración con directorio LDAP.

33. La solución debe permitir la utilización de expresiones regulares para la composición de reglas de filtrado.

34. La consola de administración Web, debe proporcionar capacidades de acceso basado en roles y perfiles de usuario o Role Based Access Control (RBAC).

35. La solución debe contar con capacidades para en envió de eventos a un sistema (SIEM) utilizando protocolo Syslog.

36. La solución debe permitir la generación de reportes y cuadros de mando acorde al periodo seleccionado (día, semana, mes, año) en formato PDF.

37. La solución debe proporcionar un cuadro de mando web que incluye como mínimo información de: Estado de la Salud del Sistema, Mensajes Procesados (Entrada/Salida) & Amenazas Detectadas.

38. La consola Web debe permitir la personalización del cuadro de mando el cual permite configurar múltiples widgets a criterio del administrador de la solución.

39. La solución debe poder gestionar múltiples dominios de correo electrónico.

40. La solución debe permitir generar reportes en forma manual o programados a intervalos de tiempo determinados.

- ✓ **RENGLÓN 3: Servicio de Implementación y Capacitación**

1. El proyecto deberá incluir la instalación y configuración de todos los componentes de hardware y/o software que formen parte de la oferta, así como la puesta en marcha de los mismos.

2. El servicio de implementación deberá contar con un mínimo de CIENTO VEINTE (120) horas de Servicios Profesionales del fabricante con las siguientes actividades:

a. Presentación de un proyecto y de un cronograma de tareas.

b. Asistencia técnica, respuesta calificada a consultas, aclaración de dudas, sobre los elementos componentes de la presente licitación, para todo el personal que se haya destinado a este proyecto.

c. Apoyo técnico para aprovechar las bondades de los componentes y transferencia de conocimientos a los especialistas designados por el organismo.

d. Análisis, determinación, corrección y documentación de los problemas, si los hubiere.

e. Definición de los recursos entre ambientes y plataformas que sean necesarias contemplar.

f. Definición de la seguridad interna.

g. Implementación, chequeo y revisión de la seguridad interna.

h. Implementación de distintos esquemas de documentación del hardware y del software.

i. Implementación de las metodologías, resguardos y recuperaciones automáticas que provea el sistema.

j. Definición y documentación de los procesos.

k. Pruebas de Integración y Puesta en Producción.

l. Configuración inicial.

m. Reuniones semanales o quincenales para mantenimiento, actualizaciones, consultoría.

3. Una vez notificada la respectiva orden de compra, se deberá presentar ante el organismo el temario de los cursos a dictar y el cronograma de ejecución de los mismos para su aprobación.

4. Se deberá dictar los cursos sobre todos los aspectos técnicos y funcionales relacionados con los equipos ofertados para los agentes que desarrollan tareas de administración y/u operación del organismo, que sean necesarios por cada ítem involucrado.

5. Se indicará en la propuesta la duración estimada de los cursos de capacitación, la cual no podrá ser menor a VEINTE (20) horas, y los medios que utilizará para evaluar el nivel de capacitación adquirido por el personal del organismo.

6. Una vez finalizado el curso, el personal del organismo deberá poseer los conocimientos suficientes para efectuar en tiempo y forma y sin ayuda externa, las siguientes tareas:

a. Instalación de la totalidad del software.

b. Configuración y parametrización del software.

c. Administración y puesta a punto de la totalidad del software.

d. Operación y mantenimiento de la totalidad del software.

7. Las fechas de los cursos serán coordinadas por el organismo.

8. Los cursos deberán incluir un contenido que garantice una completa capacitación del personal del organismo, para la correcta utilización y total aprovechamiento de las prestaciones y características de los equipos adquiridos.

9. Los cursos deberán dictarse de forma remota.

10. Los cursos programados abarcan la capacitación total del personal en cuanto a la utilización de todas las licencias ofertadas, de manera tal que la operación eficiente del sistema quede garantizada.

11. Se suministrarán todos los materiales y equipamiento adicional para la realización de los cursos. Se le entregará un juego completo del material didáctico necesario para los cursos a cada uno de los asistentes.

12. Los cursos deben ser dictados en idioma español, por profesionales certificados por las empresas desarrolladoras de las licencias adquiridas.

13. A fines de confirmar el cumplimiento de la presente exigencia, en su presentación se deberá acompañar la copia de los certificados de los profesionales que destinará a impartir los cursos solicitados y sus correspondientes currículos, quedando a criterio del organismo su aceptación, que, de no ser concedida, generará obligación por parte del proveedor de proponer en forma inmediata a otro profesional, remitiendo asimismo su currículo.

14. Se deberá presentar al organismo, como constancia de cumplimiento de este servicio, un Informe Final de cada curso dictado en el cual consten los datos de los participantes, la asistencia de los mismos, horas de duración, contenido desarrollado, evaluación del curso por parte de los alumnos y en caso de considerarse conveniente, la evaluación de los participantes a través de exámenes.

✓ **RENGLÓN 4: Servicio de Soporte Técnico**

1. Se debe proveer un servicio de Soporte Técnico integral que cubra cualquier tipo de problema relacionado con las licencias incluidas en el presente pliego, abarcando:
a. Nivel 1 - Problemas Críticos: Fallas que interrumpan el funcionamiento de la empresa, provoquen la caída de sistemas o la pérdida de datos.
b. Nivel 2 - Problemas Moderados: Afectaciones en la funcionalidad que no causen corrupción, pérdida de datos ni bloqueo completo del software.
c. Nivel 3 - Problemas No Críticos: Incidentes que impacten parcialmente el producto sin detener procesos esenciales.
d. Nivel 4 - Problemas Menores: Consultas o ajustes que no afecten la funcionalidad del producto.

2. El servicio de Soporte Técnico estará vigente por un período de DOCE (12) meses.

3. El servicio de Soporte Técnico debe garantizar una respuesta oportuna y efectiva según el nivel de criticidad del incidente.

4. El servicio de Soporte Técnico debe garantizar los siguientes tiempos de respuesta, dependiendo de la urgencia de la solicitud y del nivel de soporte contratado:
a. Nivel 1: Máximo tiempo de Respuesta en 2 horas.
b. Nivel 2: Máximo tiempo de Respuesta en 6 horas laborales.
c. Nivel 3: Máximo tiempo de Respuesta en 8 horas laborales.
d. Nivel 4: Máximo tiempo de Respuesta en 10 horas laborales.

5. El servicio de Soporte Técnico debe brindarse a través de una página web, email, sesiones remotas y línea telefónica.

6. Se deberá garantizar que el servicio de Soporte Técnico sea brindado por personal especializado de la empresa fabricante y certificado por la misma, presentando el/los correspondientes CV y/o certificados, o en su defecto, con una carta del fabricante.
7. El servicio de Soporte Técnico debe incluir el soporte y mantenimiento del software que hubiera sido instalado por el fabricante o proveedor del producto y lo amparará ante todo tipo de error propio, del software o del hardware, según corresponda, así como de configuración, instalación, etc., cualquiera sea su origen.

- **Visita Técnica Obligatoria**

Los INTERESADOS deberán, obligatoriamente, visitar los lugares de instalación de la Solución integral, donde se ejecutarán las tareas correspondientes a lo solicitado en el presente llamado a licitación.
En oportunidad de realizar la visita técnica obligatoria, el área técnica extenderá la respectiva constancia, la cual deberá ser presentada juntamente con la oferta.

- **Documentación a Presentar por el Oferente.**

1) Con el fin de acreditar que es una oferta técnicamente admisible y que está calificado para cumplir el contrato si su oferta fuese aceptada, el Licitante deberá presentar la siguiente documentación:

a) Lista de las instalaciones de sistemas y/o productos similares vendidos en los últimos 2 años en el país. Dicho listado debe incluir:

i) Denominación y domicilio de la institución o empresa donde se realizó el trabajo, nombre, apellido y cargo de las personas que puedan ser consultados y fecha de realización.

ii) Características técnicas del equipamiento utilizado

iii) Soporte de servicios electrónicos de asistencia (BBS, FaxBack, diagnóstico remoto, páginas Web, etc.).

b) Enumeración de las instalaciones indicadas en el punto anterior que están aún en proceso de instalación.

c) Documentación que acredite alguna de las siguientes condiciones:

i) Si es fabricante o productor de los bienes ofrecidos con marca debidamente registrada deberá presentar la marca registrada a su nombre.

ii) Si es representante oficial y/o subsidiaria local del fabricante o productor deberá adjuntar la documentación pertinente que acredite el vínculo.

iii) Si es distribuidor autorizado oficialmente por el fabricante o productor deberá presentar la autorización del mismo.

iv) Si quien lo autoriza es la subsidiaria local y/o el representante en Argentina del fabricante o productor, éste deberá acreditar la autorización que posee del fabricante.

- **Documentación Técnica a Presentar por el Oferente**

1. El proveedor local deberá contar experiencia comprobada en el despliegue de soluciones de similar envergadura en el territorio nacional.

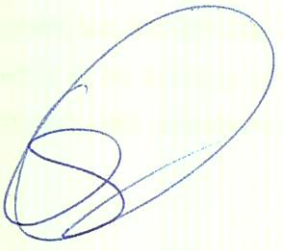
2. El proveedor local deberá contar como mínimo con 3 técnicos certificados en las soluciones ofertadas.

3. El fabricante de las soluciones ofertadas debe contar con, por lo menos, veinticinco (15) años de presencia en el mercado global. Este requerimiento deberá acreditarse mediante un enlace público al sitio web oficial del fabricante o a través de una carta o certificado emitido por el fabricante.

4. El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas en Latinoamérica, dedicados exclusivamente a la investigación y el análisis de amenazas para la región. Este requerimiento deberá acreditarse mediante un enlace público al sitio web oficial del fabricante o a través de una carta o certificado emitido por el fabricante, que incluya los nombres de los analistas en cuestión.

5. El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos cuatro (4) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) en los últimos 36 meses. Este requerimiento deberá acreditarse mediante un enlace público al sitio web oficial del fabricante o su correspondiente sitio asociado a las investigaciones, o bien al sitio web de los proveedores de software en los que se haya publicado la información de las vulnerabilidades identificadas.

6. Certificado de Visita



1. PRECIOS UNITARIOS DE REFERENCIA ESTIMADOS POR EL ÁREA TÉCNICA REQUIRENTE.

RENGLÓN N°	PRECIO UNITARIO ESTIMADO
1	$ 51.824,50
2	$ 34.331,50
3	$ 37.623.932,50
4	$ 27.586.080,20

- ✓ Renglón N°1 precio unitario en pesos por una (1) licencia con vigencia de 12 meses.
- ✓ Renglón N°2 precio unitario en pesos por una (1) licencia con vigencia de 12 meses.
- ✓ Renglón N°3 precio unitario en pesos por servicio de implementación y capacitación.
- ✓ Renglón N°4 precio unitario en pesos por soporte técnico con vigencia de 12 meses.

María Rosa Muiños
Defensora del Pueblo
de la Ciudad Autónoma
de Buenos Aires