RESO SAGYP N° 470/25

Buenos Aires, 14 de agosto del 2025

VISTO:

El TAE A-01-00020434-6/2025 caratulado *"D. G. C. C. S/ Plan integral de seguridad informática tercera etapa"; y*

CONSIDERANDO:

Que por la actuación citada en el Visto, tramita la solicitud efectuada por la Dirección General de Informática y Tecnología, por la contratación de la tercera etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, soporte técnico local y del fabricante, servicio de mantenimiento y garantía para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires. En tal sentido, la mentada Dirección General propuso cláusulas para incorporar en los proyectos de Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas (v. Nota DGIYT 308/25 y Adjuntos 61840/25 y 61841/25)

Que en ese marco, la Dirección General de Compras y Contrataciones entendió viable el llamado a Licitación Pública de etapa única, bajo la modalidad de llave en mano, conforme lo dispuesto en los artículos 26, 28, 32, 33, 40, 45 y concordantes de la Ley Nº 2.095 (según texto consolidado por Ley Nº 6.764), la Resolución CM Nº 276/2020, modificada por la Resolución CM N° 248/2024, y la Resolución SAGyP N° 30/2021 (v. Adjunto 108657/25).

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 124316/25 y 124318/25 y estableció como presupuesto oficial la suma de dólares estadounidenses seis millones trescientos mil (USD 6.300.000.-). 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 seiscientos mil ($ 600.000.-), para participar en la Licitación Pública N° 2-0015-LPU25*." (v. Memo DGCC 1699/25).

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 garantizar el normal funcionamiento del Poder Judicial de la Ciudad Autónoma de Buenos Aires, y en línea con lo dictaminado por la Dirección General de Asuntos Jurídicos, corresponde aprobar los Pliegos de Bases y Condiciones Particulares y de Especificaciones Técnicas, los cuales obran vinculados como 124316/25 y 124318/25, y llamar a Licitación Pública N° 2-0015-LPU25 por la contratación de la tercera etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses seis millones trescientos mil (USD 6.300.000.-), para el día 2 de septiembre de 2025 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° 2-0015-LPU25, 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 presupuestaria correspondiente para hacer frente la contratación de marras (v. Adjunto 114000/25).

Que la Dirección General de Asuntos Jurídicos tomó la intervención que le compete y emitió el Dictamen DGAJ N° 14114/2025.

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 124316/25 y 124318/25 forman parte de la presente Resolución y regirán para la Licitación Pública N° 2-0015-LPU25, por la contratación de la tercera etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires, con un presupuesto oficial de dólares estadounidenses seis millones trescientos mil (USD 6.300.000.-).

Artículo 2°: Llámase a Licitación Pública N° 2-0015-LPU25, de etapa única, bajo la modalidad de llave en mano, fijándose como fecha límite para la presentación de ofertas y la apertura pública de ofertas para el día 2 de septiembre de 2025 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° 2-0015-LPU25, será por un monto de pesos seiscientos mil ($ 600.000-).

Artículo 4°: Desígnase, en el marco de la Licitación Pública N° 2-0015-LPU25, a la Dra. Javiera Graziano y al Dr. Matías Vázquez como miembros titulares, y a los Dres. Hernán Labate y Fabián 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° 2-0015-LPU25, 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 correo electrónico oficial 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.

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

FIRMAS DIGITALES

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

LICITACION PÚBLICA N° 2-0015-LPU25

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA TERCERA ETAPA

PLIEGO DE BASES Y CONDICIONES PARTICULARES

31. COMUNICACIONES

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 contratación de la tercera etapa del Plan Integral de Seguridad Informática, consistente en la provisión e implementación de soluciones, soporte técnico local y del fabricante, servicio de mantenimiento y garantía, para el Poder Judicial (áreas administrativa y jurisdiccional) de la Ciudad Autónoma de Buenos Aires.

3. PRESUPUESTO OFICIAL

El presupuesto oficial para la presente contratación asciende a la suma total de **Dólares Estadounidenses Seis Millones Trescientos Mil (U$S 6.300.000.-)**, el cual se compone de la siguiente manera:

Renglón 1: Dólares Estadounidenses Ochocientos Ochenta y Cinco Mil (U$S 885.000.-).

Renglón 2: Dólares Estadounidenses Un Millón Setecientos Mil (U$S 1.700.000.-).

Renglón 3: Dólares Estadounidenses Seiscientos Treinta y Cinco Mil (U$S 635.000.-).

Renglón 4: Dólares Estadounidenses Setecientos Noventa Mil (U$S 790.000.-).

Renglón 5: Dólares Estadounidenses Quinientos Veinticinco Mil (U$S 525.000.-).

Renglón 6: Dólares Estadounidenses Seiscientos Cincuenta Mil (U$S 650.000.-).

Renglón 7: Dólares Estadounidenses Trescientos Setenta y Cinco Mil (U$S 375.000.-).

Renglón 8: Dólares Estadounidenses Quinientos Veinte Mil (U$S 520.000.-).

Renglón 9: Dólares Estadounidenses Doscientos Veinte Mil (U$S 220.000.-).

4. RENGLONES A COTIZAR

Renglón 1: Provisión, implementación y puesta en funcionamiento de una solución de alta disponibilidad (HA) para la solución de seguridad FORTINET SIEM, actualmente utilizada por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, incluyendo licenciamiento por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 2: Provisión suscripción de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de las soluciones provistas en el Renglón 1, por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 3: Provisión, implementación y puesta en funcionamiento de una solución de microsegmentación a nivel datacenter, licenciada por un plazo de treinta y seis (36) meses, para doscientos cincuenta (250) dispositivos, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 4: Provisión de suscripción de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de las soluciones provistas en el Renglón 3, por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 5: Provisión, implementación y puesta en funcionamiento de una solución de gestión de parches que se integre de forma nativa con la plataforma de gestión de vulnerabilidades Tenable.SC, que actualmente posee el Consejo de la Magistratura de la C.A.B.A., licenciada por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 6: Provisión de suscripción de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de las soluciones provistas en el Renglón 5, por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 7: Provisión, implementación y puesta en funcionamiento de solución de capacitación y concienciación de usuarios propios y para envío de newsletters a usuarios externos, licenciada por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

Renglón 8: Provisión de suscripción de servicio de garantía, soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de las soluciones provistas en el Renglón 7, por un plazo de treinta y seis (36) meses, conforme las características indicadas en el presente Pliego de Bases y Condiciones Particulares y en el Pliego de Especificaciones Técnicas.

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

5. PLIEGOS

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

El valor de los Pliegos asciende a la suma de **Pesos Seiscientos Mil ($ 600.000.-)** y podrá abonarse mediante depósito en efectivo o por transferencia bancaria a la Cuenta Corriente $ N° 000306800050213214, a nombre del Consejo de la Magistratura, en el Banco de la Ciudad de Buenos Aires, Sucursal Nº 52, sita en Av. Presidente Roque Sáenz Peña 541 de esta Ciudad, CBU 0290068100000502132146, CUIT 30-70175369-7.

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

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

6. PLAZOS DE LA CONTRATACIÓN

6.1 Plazo de la Contratación

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

6.2 Plazo de Ejecución Renglones 1, 3, 5 y 7

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

6.3 Plazo de Vigencia Renglones 1, 3, 5 y 7

Las Soluciones solicitadas tendrán un plazo de vigencia de treinta y seis (36) meses, contados a partir de la fecha indicada en el parte de recepción definitiva de la entrega e implementación de las soluciones requeridas.

6.4 Plazo de Ejecución Renglones 2, 4, 6, 8 y 9:

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

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. GARANTÍA TÉCNICA, SOPORTE Y CANAL CERTIFICADO

Los oferentes deberán acreditar su condición de Canal Certificado para la comercialización y soporte post venta de los productos ofertados mediante nota del fabricante.

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

Las soluciones requeridas deberán contar con treinta y seis (36) meses de garantía, contados a partir de la fecha indicada en el Parte de Recepción Definitiva de su entrega e implementación.

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

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

9. CONDICIONES PARA SER OFERENTE

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

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

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 y lo detallado a continuación:

Renglones 1 al 9:

14.1 Precio Total de cada Renglón, en Dólares Estadounidenses.

Monto Total:

14.2 Monto Total de la Oferta, en Dólares Estadounidenses.

Asimismo, en la oferta deberá consignarse expresamente y en detalle el equipamiento y servicios ofertados a fin de permitir su correcta evaluación.

No se admitirán cotizaciones en otras monedas a la indicada en las bases y condiciones establecidas para la presente contratación en la plataforma JUC. No se admitirán cotizaciones parciales, resultando obligatoria la presentación de propuestas por la totalidad de lo requerido.

En el precio el oferente debe considerar incluidos todos los impuestos vigentes, derechos o comisiones, movimientos dentro de los edificios, seguros, reparación de eventuales daños por culpa del adjudicatario, responsabilidad civil, beneficios, sueldos y jornales, cargas sociales, gastos de mano de obra auxiliar, gastos y costos indirectos, gastos y costos generales, costos de entrega, fletes, armado, medios de descarga y acarreo y todo otro gasto o impuesto que pueda incidir en el valor final de la prestación.

En caso de discrepancia entre la propuesta económica expresada en números y letras, prevalecerá esta última.

SE DEJA CONSTANCIA QUE EN CASO DE DIFERIR EL VALOR CONSIGNADO ENTRE LA PROPUESTA ECONOMICA CARGADA COMO DOCUMENTACIÓN ANEXA Y LA CARGADA EN JUC, SE ESTARÁ AL VALOR INGRESADO EN LA GRILLA DE JUC.

15. VISITA TÉCNICA

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

Las visitas se facilitarán **hasta dos (2) días antes** de la fecha estipulada para la apertura pública de las ofertas, debiendo comunicarse con la Dirección General de Informática y Tecnología, de lunes a viernes de 10.30 a 12.00 horas y de 14.30 a 17.00 horas, al teléfono 15-4159-9006, a los efectos de coordinar el día y hora en que serán efectuadas.

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

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

16. CONSTITUCIÓN DE GARANTÍAS

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

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

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

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

b) De Mantenimiento de Oferta: será del cinco por ciento (5%) sobre el valor total de la oferta. En

caso de resultar adjudicatario esta garantía se prolongará hasta la constitución de la garantía de cumplimiento del contrato. Al momento de presentar sus propuestas, los oferentes deberán IDENTIFICAR e INDIVIDUALIZAR la garantía de mantenimiento de la oferta completando el formulario electrónico correspondiente del sistema JUC.

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

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

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

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

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

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

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

Vencido el mismo, se lo intimará a su cumplimiento por igual plazo.

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

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

17. PRESENTACIÓN DE LAS OFERTAS

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

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

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

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

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

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

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

18. APERTURA DE LAS OFERTAS

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

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

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

19. CRITERIO DE EVALUACION Y SELECCION DE LAS OFERTAS

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

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

20. DICTAMEN DE LA COMISION EVALUADORA. ANUNCIO. IMPUGNACION

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

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

Documentación Complementaria:

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

21. ADJUDICACIÓN

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

22. PERFECCIONAMIENTO DEL CONTRATO

Conforme lo establecido por el artículo 24 del PCG.

23. CAUSALES DE EXTINCIÓN DEL CONTRATO

Son causales de extinción del contrato las siguientes:

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

b. Mutuo acuerdo.

c. Quiebra del adjudicatario.

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

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

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

24. PERSONAL DE LA ADJUDICATARIA

24.1 Nómina de Personal

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

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

24.2 Responsabilidad por el Personal

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

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

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

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

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

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

24.3 Daños a Terceros

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

24.4 Exclusión

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

25. SEGURIDAD E HIGIENE

En los casos en que corresponda, la adjudicataria deberá dar cumplimiento a la normativa vigente en materia de “Seguridad e Higiene en el Trabajo” (Ley 19587 – Decreto 351/79 y otros vigentes).

La documentación a presentar ante la Dirección de Seguridad del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires antes del inicio de los trabajos será la siguiente:

1 - Presentación del responsable de Seguridad e Higiene de la empresa (es el responsable del

cumplimiento de las normas de Seguridad e Higiene de la empresa por las tareas que ésta realice en el Consejo de la Magistratura).

2 - Certificado de cobertura de ART con cláusula de no repetición que accione a favor del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

3 - Plan de contingencias de la empresa por las tareas que son objeto de la presente contratación, conforme a las normativas vigentes en la materia, presentado y aprobado en la ART de la empresa que realice los trabajos.

4 - Constancias de capacitación al personal que realice los trabajos en los edificios en materia de Seguridad e Higiene en el Trabajo según normas vigentes en la materia.

5 - Constancias de entrega de elementos de protección personal a los trabajadores que realicen las tareas en los edificios que son objeto de la presente contratación, según normas vigentes en la materia.

Por otra parte, deberá presentar constancia de capacitación y/o matrícula habilitante del personal en las tareas que desarrollará.

6 - Formulario 931 AFIP de la totalidad de los meses del año en curso.

26. SEGUROS

Coberturas de seguros a requerir

Generalidades:

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

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

La contratación de los seguros que aquí se requieren es independiente de aquellos otros que deba poseer el adjudicatario a fin de cubrir los posibles daños o pérdidas que afecten a sus bienes o los

de sus empleados, sean los mismos o no de carácter obligatorio.

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

De las compañías aseguradoras:

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

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

De las coberturas de seguro en particular:

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

1) Seguros Laborales.

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

3) Seguro de Responsabilidad Civil Comprensiva.

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

1) Seguros Laborales

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

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

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

"Por la presente, la A.R.T, renuncia en forma expresa a reclamar o iniciar toda acción de repetición, de subrogación o de regreso contra el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires, sus funcionarios y/o empleados, sea con fundamento en el Art. N°39 ap. 5 de la Ley N°24.557, o en cualquier otra norma jurídica, con motivo de las prestaciones en especie o dinerarias que se vea obligada a abonar, contratar u otorgar al personal dependiente o ex dependiente del adjudicatario, amparados por la cobertura del contrato de afiliación N° XXXX, por acciones del trabajo o enfermedades profesionales, ocurridos o contraídas por el hecho o en ocasión de trabajo."

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

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

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

Sumas mínimas a Asegurar:

Muerte: pesos veinte millones ($ 20.000.000,00.-).

Invalidez Total y/o parcial permanente por accidente: pesos ocho millones ($ 8.000.000,00.-).

Asistencia Médico Farmacéutica (AMF): pesos cuatro millones ($ 4.000.000,00.-).

La citada póliza deberá incluir el siguiente texto:

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

3) Seguro de Responsabilidad Civil Comprensiva.

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

de la Ciudad Autónoma de Buenos Aires o de terceros.

Suma Asegurada Mínima:

La misma será por un monto mínimo de pesos veinte millones ($ 20.000.000.-). Se detallan de manera enunciativa y no taxativa las coberturas adicionales a incluirse de corresponder en cada caso:

A) Responsabilidad Civil emergente de escapes de gas, incendio, rayo y/o explosión, descargas eléctricas.

B) Daños por caída de objetos, carteles y/o letreros

C) Daños por hechos maliciosos, tumulto popular.

D) Grúas, Guinches, auto elevador (de corresponder).

E) Bienes bajo cuidado, custodia y control.

F) Carga y descarga de bienes fuera del local del asegurado.

El contrato deberá contener un endoso en carácter de co-asegurado sin restricción de ninguna especie o naturaleza a favor del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires. Los empleados del Consejo de la Magistratura y del Ministerio Público de la Ciudad Autónoma de Buenos Aires deberán ser considerados terceros en póliza.

La citada póliza deberá incluir el siguiente texto:

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

27. PLAZO DE ENTREGA DE PÓLIZAS DE SEGUROS

Las pólizas de seguro mencionadas en el Punto precedente, deberán ser presentadas en la Mesa de Entradas de este Consejo, sita en Av. Julio A. Roca 530, en un plazo de cinco (5) días desde la recepción de la Orden de Compra.

En este marco, será responsabilidad del adjudicatario asegurar la vigencia de las coberturas durante el plazo contractual.

28. CERTIFICACIÓN DE CONFORMIDAD Y FORMA DE PAGO

28.1 Certificación de Conformidad

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

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

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

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

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

28.2 Pago

Todos los pagos 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, 3, 5 y 7:
Se abonará el cuarenta por ciento (40%) del monto total de los Renglones 1, 3, 5 y 7 en concepto de anticipo financiero.

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

El pago de lo restante se efectuará en una única vez, conforme lo indicado en el Pliego de Bases y Condiciones Generales, una vez emitido el Parte de Recepción Definitiva de la provisión, implementación y puesta en funcionamiento de las soluciones requeridas.

Renglones 2, 4, 6, 8 y 9:
El pago se efectuará por anticipado, conforme lo indicado en el Pliego de Bases y Condiciones Generales.

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

29. PENALIDADES

29.1 Generalidades

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

29.2 Particularidades

El primer incumplimiento de lo dispuesto en el apartado Niveles de Servicio del Pliego de Especificaciones Técnicas, dará lugar a la aplicación de una multa equivalente a veinte mil ciento cincuenta (20.150) unidades de compra.

El segundo incumplimiento de lo dispuesto en aquel apartado, dará lugar a la aplicación de una multa equivalente a cincuenta mil trescientos cincuenta (50.350) unidades de compra.

A partir del tercer incumplimiento, estos darán lugar a la aplicación de una multa equivalente a ciento cincuenta y un mil cien (151.100) unidades de compra en cada ocasión.

El Consejo de la Magistratura podrá rescindir el contrato de pleno derecho, cuando la suma de las penalidades aplicadas alcanzare en su monto el cinco por ciento (5%) del importe total del contrato.

30. CONSULTAS

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

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

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

31. COMUNICACIONES

Todas las comunicaciones que se realicen entre el Consejo de la Magistratura y los interesados, oferentes y adjudicatarios, que hayan de efectuarse en virtud de las disposiciones de la Ley N° 2.095 (texto consolidado según Ley N° 6.764) 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 Punto 15 del PCP, a los edificios detallados a continuación:

SEDE	FECHA	FIRMA Y ACLARACIÓN AGENTE CERTIFICADOR
Avda. Julio A. Roca 530		
Hipólito Yrigoyen 932		
Suipacha 150		

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

FIRMAS DIGITALES

DIAZ Gaston Federico
DIRECTOR
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES

LICITACION PÚBLICA N° 2-0015-LPU25

PLAN INTEGRAL DE SEGURIDAD INFORMÁTICA - TERCERA ETAPA

PLIEGO DE ESPECIFICACIONES TÉCNICAS

ÍNDICE:

PLIEGO DE ESPECIFICACIONES TÉCNICAS

1. GENERALIDADES

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

El adjudicatario deberá realizar cualquier tipo de trabajo que, aunque no esté debidamente aclarado en los Pliegos, sea necesario ejecutar para la correcta y completa terminación de la encomienda y para que ésta responda a sus fines y objetivos, considerándose esos trabajos incluidos en los precios de su oferta.

Cuando las tareas a realizar debieran ser unidas o pudieran afectar en cualquier forma obras existentes, los trabajos necesarios al efecto estarán a cargo de la adjudicataria y se considerarán comprendidos sin excepción en la propuesta.

El adjudicatario proveerá todo lo necesario, ya sean elementos de infraestructura, hardware o software, para la instalación y puesta en marcha del equipamiento, aun cuando no fueran especificados en el presente Pliego.

En el caso que un oferente crea conveniente ofertar una solución de prestaciones superiores, la misma deberá cumplir en un todo con estas Especificaciones Técnicas.

El oferente deberá detallar ampliamente el sistema y equipamiento ofertado para realizar las funciones requeridas en el presente Pliego.

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

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

2. ESPECIFICACIONES TÉCNICAS RENGLÓN 1.

El adjudicatario deberá proveer tecnologías (con los respectivos equipamientos de corresponder) con la finalidad de implementar un esquema de alta disponibilidad (HA)

para la solución de seguridad FORTINET SIEM actualmente utilizada por el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

Requerimientos generales

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

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

Los oferentes deberán contar con expresa autorización del fabricante para distribuir el equipamiento ofertado y ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato, mediante una presentación de carta de autorización.

Solución FORTINET SIEM

Características del equipamiento

- La solución para armar el esquema de alta disponibilidad HA, deberá estar implementada mediante al menos dos appliances de hardware, adicionales a los existentes, para conformar el esquema.
- La solución debe tener al menos 128 GB de memoria.
- La solución debe tener al menos 36TB de disco distribuido en no menos de 12 discos para HA y a su vez 7,68 TB en discos SSD.
- La solución debe poseer como mínimo 4 interfaces con puertos GE RJ45.
- La solución debe poseer la capacidad de desplegar nodos virtuales de recolección de eventos sin la necesidad de licenciamiento adicional. Permitiendo la virtualización en los siguientes hipervisores: VMware ESX, Microsoft Hyper-V, KVM.

Características Generales

- Debe tener una interfaz gráfica basada en WEB.
- Debe tener un control de acceso basado en roles enriquecidos para restringir el acceso a la GUI y datos en varios niveles.
- Debe tener toda la comunicación entre módulos protegida por HTTPS.
- Debe realizar un seguimiento completo de auditoría de la actividad del usuario.
- Debe tener autenticación de usuario flexible: local, externa a través de Microsoft AD y OpenLDAP, Cloud SSO SAML.

- Escaneo de red activo y pasivo.
- Inventario de activos.
- Inventario de servicios.

Funcionalidades mínimas Requeridas

Gestión de vulnerabilidades:

- Monitoreo continuo de vulnerabilidades.
- Escaneo activo autenticado / no autenticado.
- Verificación de remediación.

Detección de Intrusiones:

- Gestión de registros
- Visualización y análisis de las actividades de red NetFlow.
- Supervisión de la disponibilidad del servicio.
- Análisis de protocolo de red / captura de paquetes.

Gestión de eventos e incidentes:

- Visualización de las actividades de registro.
- Correlación de eventos.
- Visualización de los incidentes.
- Identificación de patrones de eventos que indiquen una posible amenaza o vulnerabilidad.
- Determinar la magnitud del riesgo de los ataques o compromisos potencialmente dañinos.
- Creación de informes con configuraciones del usuario

Panel de control:

- Creación de dashboard con configuraciones del usuario.
- La plataforma debe colectar los eventos de seguridad de múltiples marcas para lo cual se debe incluir el licenciamiento necesario para esto.
- Debe tener una arquitectura que permita escalar la recolección de datos mediante la implementación de múltiples colectores.
- Los colectores deben poder almacenar eventos en el búfer cuando el Supervisor no está disponible.

- Debe permitir el almacenamiento de logs en una base de datos de NoSQL o Elasticsearch con el fin de soportar grandes volúmenes de datos sin afectar la estabilidad de la solución.
- Debe permitir el descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad. Esta información debe alimentar una base de datos de administración deconfiguraciones, la cual se debe mantener actualizada por medio de redescubrimientos programados.
- La plataforma debe tener la capacidad de comportarse como una herramienta del tipo CMDB.
- Debe contar con un visor personalizado de log de tráfico.
- Debe ser capaz de aprovechar una variedad de fuentes públicas y privadas de datos para enriquecer los datos fuente.
- Debe ser capaz de clasificar claramente los diferentes tipos de datos que recoge para ayudar en la analítica o consultas ad hoc por los analistas SOC. También debe ser capaz de clasificar tales datos basados en su sensibilidad o protección requerida de seguridad / privacidad donde sea apropiado y también debe ser capaz de agrupar datos similares.
- Debe proporcionar una capacidad nativa para recibir fuentes de inteligencia de amenazas de fuentes abiertas y comerciales.
- Debe ser capaz de realizar análisis en tiempo real basado en datos históricos dentro de la plataforma, y debe proporcionar la capacidad de permitir el desarrollo de análisis personalizados y realizar análisis sin comprometer la velocidad o la estabilidad de la solución global.
- Debe ser capaz de generar alertas basadas en condiciones programadas de una variedad de análisis de seguridad, disponibilidad y rendimiento. También debe soportar varias maneras de comunicar estas alertas y proporcionar un flujo de trabajo para su investigación y confirmación.
- Debe proporcionar capacidades nativas para producir dashboards y análisis visuales predeterminados y personalizados para los consumidores típicos de SOC, así como proporcionar la capacidad de integrarse con soluciones de terceros que pueden proporcionar funciones similares a través de múltiples plataformas SOC.
- Debe proporcionar acciones correctivas manuales, secuenciadas y/o automatizadas sobre los controles de seguridad gestionados a través de la solución SIEM. Esto puede proporcionarse directamente a través del propio SIEM o a través de la integración con sistemas de gestión externos.

- Debe tener su propia herramienta de gestión de tickets y permitir la integración con herramientas de terceros ConnectWise, ServiceNow, SalesForce y Remedy.
- Debe ser capaz de almacenar y administrar datos internos y de gestión de configuración dentro de las Bases de Datos de Gestión de Configuración (CMDB). Esto necesitará incluir una capacidad nativa pero también debe soportar la integración con plataformas CMDB de terceros.
- Debe incluir un análisis de anomalías en base a estadísticas y técnicas de aprendizaje automático.
- Debe poderse implementar de forma distribuida, de tal forma que los colectores sean independientes del motor de correlación, permitiendo que ante una caída del enlace que comunica al motor de correlación, los eventos se puedan almacenar por un tiempo determinado.
- Debe tener la capacidad de correlacionar los eventos recibidos en memoria antes de escribir en disco, logrando así la capacidad de correlación en tiempo real.
- Debe contar con capacidad de monitoreo activo de disponibilidad de performance mediante el monitoreo contante de SNMP, servicios TCP, entre otros, de tal forma que permita generar estadificas de uso de recursos como CPU, memoria, Trafico de red, entre otros.

Funcionalidades de monitoreo:

- Debe tener la capacidad colectar archivos de configuración de red de los dispositivos monitoreados, almacenada en un repositorio de versiones.
- Debe tener la capacidad de colectar las versiones del software instalado en los dispositivos monitoreados, almacenado en un repositorio de versiones.
- Debe contar con la característica de detección automática de cambios en el software instalado en las plataformas monitoreadas.
- Debe tener la capacidad de definir métricas customizadas.
- Debe tener la capacidad de detectar desviaciones de una línea base de la infraestructura monitoreada.
- Debe monitorear las caídas e inicios de los sistemas vía Ping, SNMP, WMI, así como análisis del inicio o caída de interfaces críticas, procesos y servicios críticos, cambios en BGP/OSPF/EIGRP o caídas de puertos del tipo Storage.
- Debe hacer modelamiento de disponibilidad basado en transacciones sintéticas vía Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route y puertos TCP/UDP genéricos.

- Debe proporcionar la capacidad de soportar solicitudes de información ad-hoc o programadas de la solución para satisfacer las necesidades de auditoría o cumplimiento.
- Debe proteger la integridad y confidencialidad de la información almacenada con algoritmos de hashing fuertes mínimo SHA 256.
- Debe proporcionar reportes de auditoría y cumplimiento con plantillas de PCI, COBIT, SOX, ISO, ISO 27001, HIPPA, GLBA, FISMA, NERC, GPG13, SANS Critical Controls
- Debe proporcionar una arquitectura altamente escalable donde la capacidad de procesamiento, memoria y almacenamiento se puede aumentar o disminuir de acuerdo con la carga real en la producción.
- Debe soportar plataformas de desarrollo y lenguajes de programación para el desarrollo personalizado dentro de la solución y sus componentes tipo XML
- Debe admitir el descubrimiento y la supervisión de estos servidores de aplicaciones: Apache, Tomcat, IBM WebSphere, Microsoft ASP.NET, Oracle GlassFish Server, Oracle WebLogic, RedHat JBOSS.
- Debe admitir la autenticación de los siguientes servidores para descubrimiento y monitoreo: Cisco, Access Control Server (ACS), Cisco Identity Solution Engine, (ISE), CyberArk Password Vault, CyberArk,
- Debe admitir la configuración para enviar syslog en un formato específico para Fortinet FortiAuthenticator, Juniper Networks SteelBelted RADIUS, Microsoft Internet Authentication Server (IAS), OneIdentity Safeguard, Vasco DigiPass.
- Debe soportar las siguientes bases de datos para descubrimiento y monitoreo: IBM DB2 Server, Microsoft SQL Server, MySQL Server, Oracle Database Server.
- Debe soportar los siguientes servidores de DHCP y DNS para descubrimiento y monitoreo: Infoblox DNS/DHCP, ISC BIND DNS, Linux DHCP, Microsoft DHCP (2003-2008), Microsoft DNS (2003-2008).
- Debe soportar el siguiente servidor de directorio para descubrimiento y monitoreo: Microsoft Active Directory.
- Debe soportar el siguiente servidor de gestión de documentos para descubrimiento y monitoreo: Microsoft SharePoint.
- Debe soportar los siguientes servidores web de gestión para descubrimiento y monitoreo: Cisco Application Centric Infrastructure (ACI), Fortinet FortiManager.

- Debe soportar la siguiente aplicación de escritorio remoto para descubrimiento y monitoreo: Citrix Receiver (ICA).
- Debe soportar las siguientes herramientas de control de código fuente para la recopilación de registros a través de API: GitHub y GitLab.
- Debe soportar mínimamente los siguientes servidores VoIP para descubrimiento y monitoreo: Avaya, Cisco, Fortinet.
- Debe soportar los siguientes Servidores Web para descubrimiento y monitoreo: Apache Web Server, Microsoft IIS for Windows 2000 o 2003, Microsoft IIS for Windows 2008, Nginx Web Server.
- Debe soportar los siguientes servidores Blade para descubrimiento y monitoreo: Cisco UCS Server, HP BladeSystem.
- Debe soportar las siguientes aplicaciones Cloud para monitoreo: AWS Access Key IAM, Permissions and IAM Policies AWS CloudTrail API, AWS EC2, CloudWatch API, AWS RDS, Box.com, Cisco FireAMP Cloud, Google Apps Audit, Microsoft Azure Audit, Microsoft Office 365 Audit, Microsoft Cloud App Security, Microsoft Azure Advanced Threat Protection (ATP), Microsoft Windows Defender, Advanced Threat Protection (ATP), Okta, Salesforce CRM Audit.
- Debe soportar la siguiente consola de acceso de dispositivos para descubrimiento y monitoreo: Lantronix SLC Console Manager.
- Debe soportar las siguientes aplicaciones de antivirus y seguridad de host (HIPS) para descubrimiento y monitoreo: Cisco Security Agent (CSA), CloudPassage Halo, Crowdstrike, Digital Guardian, ESET NOD32 Anti- Virus, FortiClient, MalwareBytes, McAfee ePolicy Orchestrator (ePO), Sophos, Symantec, Trend Micro.
- Debe soportar los siguientes dispositivos para monitoreo: APC Netbotz Environmental Monitor, APC UPS, Generic UPS, Liebert FPC, Liebert HVAC, Liebert UPS.
- Debe soportar los siguientes Firewalls para descubrimiento y monitoreo: Cisco Adaptive Security Appliance (ASA), Dell SonicWALL Firewall, Fortinet FortiGate Firewall, Juniper Networks SSG Firewall, McAfee Firewall Enterprise (Sidewinder), Sophos UTM.
- Debe soportar los siguientes balanceadores de carga y firewalls de aplicaciones para descubrimiento y monitoreo: Citrix Netscaler Application Delivery Controller (ADC), F5 Networks Application Security Manager, F5 Networks

Local Traffic Manager, F5 Networks Web Accelerator, Qualys Web Application Firewall.

- Debe ser compatible con las siguientes aplicaciones de monitoreo de gestión de cumplimiento de red: Cisco Network Compliance Manager, PacketFence Network Access Control (NAC).
- Debe soportar los siguientes sistemas de protección de intrusos IPS para descubrimiento y monitoreo: AirTight Networks SpectraGuard, Cisco FireSIGHT, Cisco Intrusion Protection System, Cisco Stealthwatch, Cylance Protect Endpoint Protection, Cyphort Cortex Endpoint Protection, FireEye Malware, Protection System (MPS), FortiDDoS, Fortinet FortiSandbox, IBM Internet Security Series Proventia, Juniper DDoS Secure, Juniper Networks IDP Series, McAfee IntruShield, McAfee Stonesoft IPS, Motorola AirDefense, Radware DefensePro, Snort Intrusion Protection System, Sourcefire 3D and Defense Center, TippingPoint Intrusion Protection System.
- Debe soportar los siguientes Security Gateways para descubrimiento y monitoreo: Barracuda Networks Spam Firewall, Blue Coat Web Proxy, Cisco IronPort Mail Gateway, Cisco IronPort Web Gateway, Fortinet FortiMail, Fortinet FortiWeb, McAfee Vormetric Data Security Manager, McAfee Web Gateway, Microsoft ISA Server, Squid Web Proxy, SSH Comm Security CryptoAuditor, Websense Web Filter.
- Debe soportar los siguientes servidores para descubrimiento y monitoreo: HP UX Server, IBM AIX Server, IBM OS400 Server, Linux Server, Microsoft Windows Server, Sun Solaris Server.
- Debe soportar los siguientes dispositivos de almacenamiento para descubrimiento y monitoreo: Brocade SAN Switch, Dell Compellant Storage, Dell EqualLogic Storage, EMC Clarion Storage, EMC Isilon Storage, EMC VNX Storage Configuration, NetApp Filer Storage, Nimble Storage, Nutanix Storage.
- Debe soportar detección de amenazas en ThreatConnect. Las siguientes fuentes de inteligencia de amenazas externas son soportadas: Emerging Threat, FortiGuard, FortiSandbox, Malware Domain, SANS, ThreatStream, ThreatConnect, TruSTAR, Zeus. En general cualquier fuente que provea un archivo CSV o que soporte STIC/TAXII standard.
- Debe soportar los siguientes servidores de virtualización para descubrimiento y monitoreo: HyperV, Hytrust CloudControl, VMware ESX.

- Debe soportar los siguientes VPN Gateway para descubrimiento y monitoreo: Cisco VPN 3000 Gateway, Cyxtera AppGate Software Defined Perimeter (SDP), Juniper Networks SSL VPN Gateway, Microsoft PPTP VPN Gateway, PulseSecure.
- Debe soportar los siguientes scanners de vulnerabilidades para descubrimiento y monitoreo: AlertLogic Intrusion Detection and Prevention Systems (IPS), McAfee Foundstone Vulnerability Scanner, Nessus Vulnerability Scanner, Qualys Vulnerability Scanner, Rapid7 NeXpose Vulnerability Scanner, Rapid7 InsightVM Integration, Tenable.io.
- Debe soportar los siguientes aceleradores de red WAN para descubrimiento y monitoreo: Cisco Wide Area Application Server, Riverbed SteelHead WAN Accelerator.
- Debe soportar los siguientes dispositivos de Wireless LAN para descubrimiento y monitoreo: Aruba Networks Wireless LAN, Cisco Wireless LAN, FortiAP, FortiWLC, Motorola WiNG WLAN AP

Servicio de implementación

El adjudicatario deberá realizar la implementación de las soluciones requeridas, debiendo 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.

3. ESPECIFICACIONES TÉCNICAS DEL RENGLÓN 3

El adjudicatario deberá proveer la tecnología de microsegmentación a nivel datacenter con la finalidad de realizar una estrategia de microsegmentación de seguridad para la infraestructura que posee el Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires:

Requerimientos generales

- Los oferentes deberán ser un canal debidamente aprobado por el fabricante, por lo que se requiere la presentación de una carta de autorización a presentar oferta.
- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:
    - Deberán trabajar en forma integrada nativamente.
    - El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.
- Los oferentes deberán contar con expresa autorización del fabricante para distribuir el equipamiento ofertado y ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato.

Requerimientos funcionales

- Se requiere una solución de seguridad ZTS, cuyo objetivo principal es la contención de la proliferación de brechas y ataques de ransomware sobre una superficie de ataque de entornos híbridos (On-Prem y Cloud) mediante la visualización continua de los patrones de comunicación entre las cargas de trabajo y dispositivos (Ej. OT/IoT), y que permita la creación de políticas de seguridad granulares que solo permitan el tráfico requerido y necesario, y que permita el aislamiento automático de brechas al restringir el movimiento lateral tanto de forma proactiva o durante un ataque activo.
- La implementación de la solución de microsegmentación/ZTS no deberá requerir hacer absolutamente ningún cambio en los flujos existentes, ruteo, VLANs o redirección del tráfico en la red física/lógica o virtual existente en la organización, es decir deberá ser un control lógico, en lugar de un control físico de segmentación.
- La protección de la solución ZTS deberá ser implementada directamente a nivel de carga de trabajo a proteger, y no a través de controles de tráfico perimetrales, ya sean Firewalls Internos o Externos.

- Deberá permitir proteger aplicativos críticos a través del enfoque de "Application Ring-fence", siendo una solución totalmente agnóstica a la red o topología de red física, es decir será una plataforma "Application Centric" y no "Network Centric".
- Deberá permitir a las organizaciones llevar a cabo migraciones a ambientes de nube al ofrecer visibilidad de flujos y comunicaciones en entornos híbridos que destaquen las dependencias y flujos entre aplicaciones.
- Deberá ofrecer visibilidad de los activos y flujos de comunicación que permitan cuantificar el riesgo y reducir puntos ciegos.
- Deberá permitir crear fronteras lógicas entre ambientes IT y OT
- Ayudar en el proceso de respuesta a incidentes para defender y responder ante ataques de ransomware.
- Deberá ser una solución reconocida por:
    - Gartner: Market Guide for Microsegmentation, 12 de Junio, 2023
    - Forrester: Microsegmentation Solutions Landscape Q2, 2024
- Deberá ser una solución basada en únicamente 2 capas:
    - Capa de Protección de carga de trabajo: a través de un agente liviano que colecte metadatos, flujos y telemetría de la carga de trabajo e instrumente el control de tráfico nativo.
    - Capa Central de Cómputo y Procesamiento de Políticas de seguridad: a través de una consola SaaS que centralice, procese y analice los flujos y telemetría del entorno distribuído de protección, consola gráfica para el análisis de flujos, metadatos, definición y programación de políticas de seguridad y aplicación y envío de las mismas.
- Para evitar puntos únicos de falla, no se aceptarán soluciones que utilicen capas intermedias conocidas como "agregadores" o "colectores", que limiten la escalabilidad de la arquitectura ZTS.

Arquitectura e implementación

- La solución deberá basarse en un modelo SaaS, donde la consola central sea hospedada en la nube y cuyo servicio sea administrado, soportado y operado por el fabricante de la solución, por lo que no deberá tener ningún componente de agregación o gestión a ser instalado en infraestructura, salvo el componente que protegerá directamente las cargas de trabajo.

- La plataforma SaaS deberá contar con certificación SOC 2 Tipo 2, emitida por un auditor independiente.
- Los agentes dedicados a la protección de la carga de trabajo deberán comunicarse directamente con la plataforma SaaS usando el protocolo de comunicación segura TLS1.2.
- La administración de la solución ZTS deberá ser realizada utilizando protocolos seguros de transporte basado en el protocolo TLS1.2.
- La arquitectura de la solución deberá ser de 2 capas, es decir el agente a instalar en el dispositivo a proteger se comunicará directamente a la consola SaaS, para evitar puntos únicos de falla, no se aceptarán soluciones basadas en 3 capas que incluya un agregador o intermediario.
- El agente de protección de la carga de trabajo deberá específicamente instrumentar el control de tráfico nativo del sistema operativo donde se instala, es decir el agente NO deberá estar en-línea en el flujo de comunicación del activo protegido.
- De forma opcional y en caso de requerirse, el agente podrá utilizar un proxy de conexión a internet ajeno a la solución, en caso de que no sea factible otorgar conectividad directa a Internet a la consola central. No se darán por válido un agregador que funcione como proxy de la misma marca del fabricante de la solución ZTS.
- La solución ZTS deberá ser totalmente agnóstica a la red y topología actualmente desplegada, y no deberá tener dependencia alguna de ningún componente de la red ni de la infraestructura para que pueda operar de manera correcta.
- Para facilitar el despliegue masivo de los agentes de protección de las cargas de trabajo, deberá permitir su implementación utilizando herramientas de automatización y entrega de software de uso general, tales como SCCM, Chef, Ansible, Puppet o cualquier otra herramienta que permita la ejecución de scripts de instalación o bien Powershell.
- Deberá permitir la instalación del agente de protección de forma manual, utilizando archivos ejecutables o scripts definidos por el fabricante de la solución.
    - La instalación y desinstalación del agente de protección deberá ser llevada a cabo sin la necesidad de reiniciar el sistema operativo en ninguna circunstancia.

- La solución permitirá la actualización del software de protección de manera remota y sin intervención directa del equipo donde se encuentre el agente.

Capa de Protección de la carga de trabajo

- El componente de protección de carga de trabajo podrá ser desplegado en los siguientes ambientes:
  - Usuarios Finales: Equipos terminales como Laptops, Workstations, Escritorios Virtualizados (VDI) con Sistemas Operativos Windows/MacOS con soporte de interfaces de red sin cable (WiFi), capaz de identificar si está conectada a una red corporativa o fuera de la red corporativa.
  - Datacenter o Nube privada/pública IaaS
  - Nube Pública (agentless)
  - Entornos Kubernetes
  - Infraestructura legacy IBM: zOS, AS/400, AIX.
- El componente de la capa de protección de la carga de trabajo (llamado agente) deberá ser instalado mediante un software que deberá contar con las siguientes características mínimas:
  - No ser intrusivo en el sistema operativo, ni deberá comprometer la integridad del Sistema Operativo con la modificación o alteración del Kernel.
  - No requiere reinicio para su instalación y ejecución
  - Contar con mecanismos de protección ante ataques o manipulación (anti-tampering)
- Debe soportar microsegmentación tanto en cargas de trabajo físicas/bare-metal así como cargas de trabajo virtualizadas, agnóstica a la plataforma de virtualización utilizada.
- Debe permitir la creación de barreras o perímetros lógicos a nivel aplicativo, donde los activos tengan su comunicación restringida sólo a lo que ha sido previamente identificado y permitido de manera explícita, especialmente en el contexto de aplicaciones que deben permitir su comunicación sólo en el contexto estrictamente necesario y establecido, conocido como ring-fencing.

- Debe permitir seleccionar el nivel de protección de la carga de trabajo, con lo cual se facilite el proceso de transición desde visibilidad hasta protección completa y minimizar impactos o disrupciones:
    - Inactivo: Visibilidad básica, sin tomar control del firewall local del OS.
    - Visibilidad: Permite todo el tráfico, brindando mayor nivel de visibilidad
    - Selectivo: Permite definir reglas intermedias para bloquear tráfico y crear excepciones.
    - Completo: Negará todo el tráfico de forma implícita y solo permite lo explícitamente definido mediante una política de seguridad.
- El software que será instalado en la carga de trabajo a proteger debe cumplir con los siguientes requerimientos:
    - Deberá colectar telemetría de los flujos de comunicación desde y hacia la carga de trabajo protegida, colectando información de protocolo IP, protocolo de Transporte (TCP/UDP), Número de Puerto, Información de procesos locales del Sistema Operativo, Usuario dueño del proceso.
    - EL agente o software NO deberá ser un agente en línea, es decir, NO se permite que el agente intervenga o modique el stack o pila de comunicación nativo del sistema operativo.
    - El agente o software NO deberá ser intrusivo, es decir que no modifique o altere en ninguna forma el Kernel del sistema operativo.
    - El agente o software NO deberá solicitar reinicio de la carga de trabajo a proteger.
    - El agente o software deberá instrumentar y programar el componente nativo del sistema operativo responsable del filtrado del tráfico a nivel kernel, es decir será el medio para programar las reglas, mas no el control de tráfico en sí, es decir, en función de la plataforma, deberá instrumentar los siguientes componentes:
        - Linux: iptables/nftables.
        - Windows: Windows Filtering Platform (WFP)
        - Unix: ipfilter
    - El agente o software deberá tener mecanismos internos de protección ante ataques (Anti-tampering), con la capacidad de detectar, corregir y registrar eventos de:

  - Manipulación de políticas de control de tráfico
  - Manipulación y/o fallas de procesos y servicios propios del agente
  - Protección mediante token de autenticación para realizar tareas de mantenimiento o desisntalación.
  - Registro de eventos Anti-tampering para poder ser monitoreados y analizados por una plataforma o SIEM externo.

- El agente o software deberá ser capaz de co-existir en entornos desplegados que ya contengan políticas de seguridad y tráfico pre-existentes en el sistema operativo, escenarios comunes:
  - Hosts orquestados por Kubernetes
  - Soluciones que hagan uso del Firewall de Host, ej. EDR.
- El agente o software podrá hacer uso de proxy corporativo para la conexión a la consola central, con los siguientes requisitos:
  - Túnel de cifrado del tráfico utilizando protocolo TLS 1.2 end-to-end.
  - Protocolo de transporte hacia el proxy: HTTP
  - No deberá requerir autenticación del proxy.
- El software/agente deberá soportar su instalación como mínimo en los siguientes sistemas operativos/plataformas:
  - IBM AIX 7.1 TL4 o posterior
  - Amazon Linux 2016 o posterior
  - Red Hat Enterprise Linux (RHEL) 5.0, 6.2, 7, 8, 9 o posterior
  - CentOS 6.2, 7, 8
  - CentOS Stream 8, 9
  - Rocky Linux 8, 9
  - Alma Linux 8, 9
  - Oracle Linux 6.2, 7, 8, 9 o posterior con Kernel RedHat
  - Oracle Linux 5.8, 6.2, 7, 8, 9 o posterior con Kernel Unbreakable (UEK)
  - Debian 7 o posterior
  - Solaris 10 U8, 11.1 o posterior (Arquitectura x86 y SPARC 64 bit)

- SUSE Linux (SLES) 11 SP3, 12, 15 o posterior
- Ubuntu LTS 12.04 o posterior
- Ubuntu Non-LTS 20.10 o posterior
- Windows Server 2003 SP1, SP2
- Windows 2008 SP1, SP2
- Windows 2008 R2 SP1 o posteriores
- Windows 7 o posteriores
- MacOS 11 o posteriores

- El software/agente deberá ser compatible para ser instalado en entornos de aplicaciones basadas en microservicios, soportando los siguientes elementos, bajo una matriz de compatibilidad definida por el fabricante:
  - Plataformas de orquestación
    - AWS Elastic Kubernetes Service (EKS)
    - Azure Kubernetes Service (AKS)
    - IBM Cloud Kubernetes Service (IKS)
    - K3s:
    - Kubernetes
    - Openshift
    - Rancher Kubernetes Engine (RKE)
  - Container Runtime
    - Contarinerd
    - CRI-O
  - Network Plugins (CNI)
    - AWS VPN CNI
    - Azure CNI
    - Calico
    - Kubenet
    - Flannel

- Openshift SDN (OVS)
- OVN-Kubernetes
- Canal
- Antrea

- El agente deberá ser capaz de identificar reglas de seguridad pre-existentes, en el caso de servidores Linux o Unix, existencia de reglas en iptables o ipfilter, en el caso de Windows, existencia de reglas en plataforma de Filtrado o a nivel de GPO (Group Policy Object Firewall Rules), y en caso de requerirse, el agente podrá ser configurado en un modo especial de co-existencia, bajo 3 escenarios:
    - Firewall Exclusivo: La solución ZTS será el único gestor de reglas, se descartarán todas las reglas pre-existentes.
    - La solución ZTS tomará el control y precedencia sobre las reglas de seguridad pre-existentes, es decir, primero serán evaluadas las reglas definidas por ZTS y posteriormente reglas pre-existentes
    - La solución ZTS programará las reglas de seguridad, después de las reglas pre-existentes.
    - Se podrán utilizar las etiquetas asociadas a las cargas de trabajo para acotar los criterios de co-existencia.
- Mecanismos para despliegue de agentes
    - Perfiles para despliegue y personalización de atributos
    - Script automatizado
    - Utilizar herramientas para distribución de software
- La operación del agente no debe ser interrumpida en caso de cortarse la comunicación con la consola central, en caso de ocurrir una desconexión, el agente deberá ser capaz de retener de manera temporal los flujos y telemetría en un caché de tamaño fijo temporal que sea sobre-escrito, sin que sature el sistema de archivos local, tras reanudar la comunicación, los flujos y telemetría serán vaciados de manera automática.
- El software/agente podrá ser administrado de manera remota a través de la consola de administración para realizar las siguientes tareas:
    - Visualización del estado del agente

  - Información del sistema operativo huésped
  - Cambio de modo de protección (Activo, Visibilidad, Selectivo, Completo)
  - Actualización de versión del agente
  - Suspensión provisional del agente
  - Obtención remota de paquete de diagnóstico
  - Desvincular agente y desinstalar del sistema operativo huésped

- En el caso de la desinstalación del agente de protección, se deberán remover las reglas creadas con la plataforma ZTS, y dar al usuario la opción de mantener el host protegido bajo los siguientes estados:
  - Abierto: Se permitirá la comunicación a cualquier puerto abierto, una vez desinstalado
  - Guardado: Se regresará al estado anterior del set de reglas guardado previo a la instalación.
  - Recomendado: Permitirá únicamente protocolo SSH hasta el reboot del host Linux/Unix.

Consola de Administración central

Generales

- La consola de administración gráfica deberá ser en un entorno Web con uso de protocolos seguros TLS 1.2 como mínimo, así como también la comunicación entre la consola y los agentes desplegados en las cargas de trabajo protegidas.
- Deberá proporcionar una interface de programación (API) tipo REST que permita la interacción directa a través de lenguajes de programación o kits de desarrollo (SDK’s).
- Deberá contar con control de acceso basado en Roles (RBAC), con lo cual se podrá asociar de manera granular el nivel de acceso a los usuarios (utilizando el modelo de etiquetas) a los roles definidos en la solución ZTS.
- Deberá soportar autenticación local así como externa de usuarios, soportando autenticación externa con Azure AD, ADFS, Okta, OneLogin, Ping Identity a través de los protocolos SAML y LDAP.

- La consola debe almacenar hasta un máximo de 90 días equivalentes de flujos, donde la capacidad de retención estará en función del volumen de flujos generados, a mayor cantidad de flujos, menor será la capacidad de retención.
- La consola de administración podrá ofrecer la capacidad, mediante licenciamiento adicional, de poder integrar informes de vulnerabilidades de herramientas soportadas y correlacionarlos con los activos protegidos y poder desplegar un mapa de vulnerabilidades y calificación del riesgo en las comunicaciones con base en la exposición de la vulnerabilidad del activo y flujos reportados.
- La consola deberá generar en todo momento registros de auditoría y trazabilidad de los eventos operativos, administrativos, así como los generados por los agentes instalados en las cargas de trabajo.
- Deberá contar con paneles gráficos o Dashboards que permitan saber la situación y estado de la plataforma ZTS con respecto a:
    - Estado y modo de protección de las cargas de trabajo protegidas, versiones del agente, sistemas operativos, cantidad de políticas definidas
    - Estado situacional y superficie de exposición al ransomware sobre puertos y protocolos inseguros, aplicaciones y servicios inseguros.
- Deberá permitir la creación de reportes calendarizados bajo las siguientes categorías:
    - Sumario Ejecutivo
    - Reporte detallado por aplicativo deseado
    - Reporte de hits de reglas
    - Exportación de tráfico
    - Reporte de exposición al ransomware.

Modelado de Activos

- La solución ZTS deberá permitir asignar etiquetas personalizadas a los activos protegidos con base en las siguientes categorías como mínimo:
    - Rol o función del Activo (ej. Web, Proc, Db, K8s, Middleware)
    - Aplicativo: (ej. Nomina, Finanzas, ERP, Pagos)

  - Entorno: (ej. Desarrollo, Pruebas, Producción, Stage, PCI, DMZ).
  - Localización: (ej. DC1, DC2, Azure, AWS, GCP, DRP).

- Cada carga de trabajo protegida deberá contener al menos estas 4 dimensiones o categorías definidas, de forma tal que permitan una fácil agrupación, identificación, mapeo, visualización y sobre todo creación de políticas y reglas de seguridad asociadas.
- En adición a las 4 categorías o dimensiones definidas, se podrán definir categorías personalizadas, siendo 20 categorías el máximo soportado. Estas categorías personalizadas pueden ser por ejemplo: Unidad de Negocio (BU), Sistema Operativo (OS), Cumplimiento, Plataforma, etc.
- Las etiquetas podrán ser agrupadas mediante grupos de etiquetas.
- La plataforma ZTS deberá realizar el descubrimiento automático de los aplicativos tomando como base las etiquetas de Aplicativo, Entorno y Localización, este descubrimiento automático facilitará el proceso para visualización de flujos, modelado asistido de reglas de seguridad, exposición de ransomware del aplicativo, miembros asociados al aplicativo.
- Deberá contar con la implementación de algoritmos de IA y Machine Learning a través de los cuales se puedan identificar los activos relacionados a servicios centrales o comunes como:
  - Active Directory
  - Bases de Datos
  - Centralizadores de eventos de seguridad
  - DNS, entre otros.
- Para entornos de nube nativa, la solución deberá ingestar las etiquetas nativas de nube y asociarlas al modelo multidimensional de etiquetas de la solución ZTS.
- La solución permitirá crear activos no administrados, es decir que no tienen el agente de protección, sin embargo representan flujos de interés que pueden ser modelados con el esquema de etiquetas, y por consiguiente ser utilizados en la definición de reglas de seguridad.
- La solución deberá permitir crear contenedores lógicos de listados de IP’s, que permitan de una forma genérica de asociar flujos de comunicaciones y puedan

ser utilizados por la plataforma ZTS para visibilidad o reglas de seguridad (ej. Internet, VPN, DMZ), con las siguientes características:

- Listas de IP's por FQDN: permitirán definir un dominio o comodín (wildcard) para resolver las IP's asociadas
- IP's individuales
- Bloque CIDR
- Rangos de direcciones IP
- Emplear criterios de exclusión

- La solución ZTS deberá contar con un listado predefinido de servicios de comunicación, siendo así mismo posible la creación de servicios personalizados, con las siguientes opciones:
  - Servicios agnósticos al Sistema Operativo:
    - Basados en Puertos y Protocolos (Ej. 8443/TCP)
  - Servicios específicos de entrada o salida de Microsoft Windows
    - Puerto Protocolo (Ej. 135/TCP)
    - Ruta lógica del proceso (C:\Windows\System32\lsass.exe)
    - Nombre del Servicio (LSASS)
    - Se podrá usar cualquier combinación de estos atributos para definir un servicio basado en Windows.
  - Estos servicios podrán ser utilizados en la construcción de reglas de seguridad.
- Deberá permitir la creación lógica de Grupos de Usuarios de entornos Active Directory a través de la definición de:
  - Nombre del Grupo (Ingeniería)
  - Identificador de Seguridad o SID (ej. S-1-5-21-1004336348-1177238915-682003330-512)
  - Estos grupos de Usuarios podrán ser utilizados en reglas de seguridad Adaptativas o basadas en identidad.

Visibilidad de Flujos y Telemetría

- Deberá contar con mecanismos para la visibilidad y el filtrado lógico de los flujos de comunicación, que permitan identificar y profundizar en los flujos de interés, útiles en el proceso de visibilidad y definición de reglas de segmentación.
    - Origen y Destino| Origen ó Destino
    - Servicio
    - Criterios específicos de exclusión
    - Ventana de tiempo a evaluar: última hora, 24 horas, semana, mes, indefinido, personalizado.
- Capacidad de guardar los criterios de búsqueda y filtrados definidos para su reutilización posterior.
- Aplicar filtros globales para visualizar o descartar flujos:
    - Permitidos
    - Bloqueados
    - Potencialmente bloqueados
    - Agrupaciones de IP’s
    - Direcciones privadas
    - Direcciones Públicas
    - Tráfico unicast, broadcast, multicast.
- Clasificación de los flujos por colores, para identificación de flujos bloqueados, permitidos o potencialmente bloqueados (por ausencia de regla).
- Deberá tener la capacidad de creación de un mapa gráfico de dependencias e intercomunicación entre aplicativos a través de la colección de flujos y telemetría de las cargas de trabajo protegidas y la información del contexto y etiquetas asociadas.
- En adición, deberá permitir la creación de un diagrama relacional o de malla de los flujos end-to-end, que permita:
    - Definir de criterios de agrupación de flujos por etiquetas, que permitan un análisis top-down
    - Agrupar atributos de los flujos por los siguientes elementos

- Origen: Proceso, Aplicación, Lista de IP’s, Direcciones Públicas/Privadas, Cargas de trabajo.
- Destino: Proceso, Aplicación, Puerto, Lista de IP’s, Direcciones Públicas/Privadas, Cargas de trabajo

- Este tipo de diagrama permitirá identificar de manera inmediata patrones de comunicación anómalos, como escaneos de puertos.
- Deberá permitir identificar de manera detallada y en modo tabular los detalles más relevantes de los flujos de comunicación, incluyendo como mínimo la siguiente información:
    - Decisión de la política de seguridad sobre el flujo observado (permitido, bloqueado, potencialmente bloqueado)
    - Origen y destino de la comunicación asociado a los activos
    - Mapeo del activo a las etiquetas identificadas
    - Puerto de comunicación
    - Protocolo
    - Proceso asociado al flujo
    - Usuario
    - Cantidad de Flujos observados
    - Cantidad de Bytes transitados
    - Marca de tiempo del primer flujo observado
    - Marca de tiempo del último flujo observado
    - Resolución de FQDN’s a IP’s públicas
    - Capacidad de exportar los resultados observados en la consola a formato .csv
- Deberá permitir la creación de reglas de seguridad sobre demanda que permitan la comunicación específica de flujos seleccionados con un solo click.
- Deberá contar con la opción de visualizar flujos en modo borrador, con esta funcionalidad se permitirá:
    - Crear reglas de seguridad a modo de borrador (draft)

  - Evaluar el impacto potencial de las reglas creadas contra los flujos inspeccionados previo a su aplicación y aprovisionamiento en las cargas de trabajo
  - Modelar las políticas de seguridad deseadas y simular el resultado con los flujos reales existentes reportados por las cargas de trabajo para minimizar riesgos o disrupciones
  - Identificar flujos de comunicación dentro de la aplicación (intra-scope) así como flujos provenientes de otras aplicaciones (extra-scope).

- A su vez deberá permitir con la opción de visualizar los flujos de forma precisa a como han sido reportados por la carga de trabajo respecto a la política de seguridad, para identificar de manera específica flujos que han sido permitidos o bloqueados.
- Mapeo en colores de los flujos contra las reglas definidas
- Deberá permitir la exportación de resultados de búsquedas de flujos en modo tabular en formato .csv con los detalles de las comunicaciones

Creación de Reglas de Segmentación

- Deberá aprovechar las etiquetas modeladas en las cargas de trabajo (Rol, Aplicación, Entorno, Localización) que permita definir bajo el contexto de la organización el enfoque de las cargas de trabajo asociadas a una regla, ya sea como proveedora o consumidora del servicio.
- Deberá permitir crear conjuntos de regla utilizando un alcance (scope) común, es decir, seleccionar previamente algún aplicativo bajo un entorno específico y/o ubicación utilizando las etiquetas, de forma tal que las reglas creadas bajo ese conjunto sean aplicadas bajo dicho alcance. Con esto se logrará reducir la creación de reglas genéricas o sin algún alcance definido y facilitar la administración operativa de los conjuntos de reglas existentes.
- Los conjuntos de reglas deberán permitir definir la lógica de acceso bajo 3 modalidades:
  - Reglas intra-aplicativo: Es decir, definirán la lógica de comunicación entre los distintos roles de un mismo aplicativo (Ej. Reglas de Acceso Web a Procesamiento y Base de Datos de un mismo aplicativo)

  - Reglas inter-aplicativo: Es decir, definir la lógica de acceso de un aplicativo que consume servicios de la aplicación a proteger (proveedora).
  - Reglas asociadas a listas de direcciones IP's: Definen la lógica de acceso provenientes de direcciones IP's asociadas a listas previamente definidas (Ej. Lista IP Red LAN).

- La solución ZTS deberá permitir definir políticas de seguridad utilizando los siguientes niveles de granularidad en la definición del acceso:
  - A nivel aplicativo: Permitirá la comunicación entre todas las cargas de trabajo de una aplicación sin importar el servicio.
  - A nivel de Rol: Permitirá la comunicación de manera específica entre los roles definidos del aplicativo, sin importar el servicio.
  - A nivel de Rol por servicios específicos: Permitirá únicamente la comunicación entre los roles definidos del aplicativo y específicamente por los puertos y servicios definidos, lo que permitirá el nivel máximo de segmentación posible en una aplicación.
- Deberá permitir la incorporación y combinación de los atributos disponibles de los activos modelados, servicios, puertos y procesos, grupos de usuarios disponibles en la plataforma:
  - Etiquetas de activos: Rol, Aplicativo, Entorno, Localización
  - Servicios por Puerto y Protocolo
  - Servicios de Sistema Operativo Windows: Basados en Ruta del proceso/ejecutable
  - Listas de IP, incluyendo FQDN's.
  - Grupos de Usuarios Windows (SID)
- Deberá crear por defecto reglas basadas en estado (conocidas como reglas stateful), sin embargo y bajo demanda, deberá permitir crear reglas sin estado (stateless).
- En el caso de sistemas operativos Windows, deberá permitir la creación de reglas granulares basadas en el proceso, y que incluso puedan utilizar puertos dinámicos, al permitir definir combinaciones de servicios Windows tal como:

- Puerto, Protocolo, Proceso, Servicio (ej. 443/TCP; c:\windows\myprocess.exe; myservice)
- Puerto, Protocolo, Proceso (ej. 443/TCP; c:\windows\myprocess.exe)
- Puerto, Protocolo, Servicio (ej. 443/TCP; myservice)
- Puerto, Protocolo (ej. 443/TCP)
- Proceso (ej. c:\windows\myprocess.exe)
- Servicio (myservice)

- Deberá permitir duplicar conjuntos de reglas definidos, lo que permitirá definir nuevos conjuntos de reglas aprovechando reglas existentes.
- Deberá contar con un modelo de plantillas de reglas previamente definidas, que se podrán importar a la solución ZTS para acelerar el proceso de creación de reglas de soluciones comerciales, ej. Active Directory, Exchange, Sharepoint, SQL, Windows Update Service, entre otros.
- Deberá permitir importer y exporter los conjuntos de reglas desde la consola administrativa.
- En el caso de sistemas operativos Linux, la solución deberá permitir crear reglas específicas de IPtables en el conjunto de reglas.
- La solución deberá permitir evaluar el impacto de la aplicación de las reglas, previo a su implementación o programación en las cargas de trabajo, a través de la evaluación de los flujos previamente colectados por la solución ZTS y las reglas previamente definidas, de manera tal que permita identificar el resultado potencial de dicha regla a través de códigos de colores, identificando:
  - Flujos permitidos por la regla, previo a su despliegue
  - Flujos bloqueados por la regla, previo a su despliegue
  - Flujos potencialmente bloqueados, por no contar con una regla, previo a su despliegue.
- El proceso de análisis de flujos y visibilidad, deberá permitir en todo momento rastrear el conjunto de reglas que corresponda con el tráfico observado, lo que permitirá eficientar el proceso operativo de administración de reglas.
- La solución deberá permitir la creación de reglas observando la direccionalidad del tráfico, es decir, se podrán definir reglas por:

  - Ingreso de comunicación
  - Egreso de comunicación

- Para escenarios de automatización de la seguridad, por ejemplo, mediante herramientas SOAR, deberá permitir la creación de reglas de "aislamiento" de activos previamente definidas, y mediante la asignación dinámica de etiquetas (Ej. Cuarentena) a un activo, de forma automática sea aislado el elemento de la red.
- Deberá permitir el uso de recursos nativos del sistema operativo para crear túneles cifrados de tráfico punto a punto, como acción de una regla de seguridad, esto mediante el uso del protocolo IPSec existente en el sistema operativo.
- Utilizando los objetos no administrados, que se pueden definir en la consola, se podrán crear conjuntos de reglas que tengan efecto en estos entornos (Ej. OT, iOT), donde aunque no exista un agente instalado, se podrán aplicar políticas de control desde la perspectiva de los activos que cuenten con el agente, para controlar el tráfico proveniente de este tipo de objetos.
- Deberá permitir el aprovisionamiento granular de los cambios y reglas definidas, permitiendo seleccionar cuáles son los elementos que requieren aprovisionamiento de manera puntual.
- Deberá contar con la capacidad de manejar un histórico de políticas de seguridad, lo cual permitirá dar marcha atrás (roll back) en caso de requerirse, pudiendo almacenar hasta 1,000 versiones históricas, dando visibilidad de los objetos modificados, desde un simple servicio, reglas, ajustes de seguridad, así como el usuario responsable de dicho cambio.
- Deberá contar con un componente que permita la generación recomendada de reglas de seguridad a partir de los flujos previamente observados bajo un alcance definido (Ej. Aplicativo), el cual podrá sugerir las reglas necesarias para micro-segmentar o nano-segmentar dicho aplicativo, pudiendo incluso refinar las reglas de seguridad con base en nuevos flujos previamente no observados.
- Deberá permitir crear reglas "temporales" previo a configurar el modo Full Enforcement, que permitan de manera explícita negar de manera selectiva el tráfico requerido (Ej. Bloqueo de Desarrollo a Producción), y crear excepciones específicas, esta capacidad permitirá una transición gradual de un modelo de

únicamente visibilidad a un modelo totalmente de confianza cero (Zero Trust), pasando por una etapa intermedia o selectiva.

Integración con soluciones de terceros

- La solución ZTS deberá soportar la integración de informes de vulnerabilidades de las siguientes marcas:
    - Qualys
    - Tenable
    - Rapid7
- La solución ZTS deberá contar con una interfaz de programación aplicativa (API) abierta y documentada, con los siguientes requisitos:
    - Basada en arquitectura REST
    - Utilizar codificación JSON sobre protocolo HTTPS
    - Utilizar mecanismos de autenticación y autorización usando el mismo modelo RBAC de la plataforma.
    - Utilizar llaves de sesión como autenticación temporal
    - Utilizar llaves API para autenticación persistente.
    - Contar con métodos para realizar las tareas operativas de la plataforma:
        - Cargas de trabajo
        - Objetos de políticas de seguridad
        - Reglas y conjuntos de reglas
        - Aprovisionamiento
        - Visualización
        - Administración de la plataforma, como mínimo.
- La solución ZTS deberá tener la capacidad técnica de integrarse con dispositivos de red y procesamiento de paquetes para poder extender las capacidades de protección en entornos donde no se puede instalar un agente de protección, si no a nivel de listas de control de acceso o políticas a nivel de balanceo debiendo soportar al menos, esta funcionalidad es deseable, y si tiene costo adicional, será necesario especificarlo:

- Balanceador de carga F5 Networks Big-IP (LTM y AFM)
- VMware AVI Load Balancer (antes AVI Vantage)
- Citrix ADC (Netscaler)
- Cisco Nexus 9200 y 9300 series
- Arista 7000 series

Servicio de implementación

El adjudicatario deberá realizar la implementación de las soluciones requeridas, debiendo 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.

4. ESPECIFICACIONES TÉCNICAS RENGLÓN 5

El adjudicatario deberá proveer una solución de gestión de parches que se integre de forma nativa con la plataforma de Gestión de vulnerabilidades Tenable.SC que actualmente posee el Consejo de la Magistratura de la C.A.B.A., a los efectos de implementar todos los paquetes de resolución para dichas vulnerabilidades.

Requerimientos generales

- Será requisito que las tecnologías a proveer en el presente renglón sean de un único fabricante, por lo siguiente:
  - Deberán trabajar en forma integrada nativamente.

    - El soporte técnico posterior deberá ser brindado en un único canal de comunicación y resolución.

- Los oferentes deberán contar con expresa autorización del fabricante para distribuir el equipamiento ofertado y ser un canal de venta y soporte técnico local y autorizado durante el plazo que dure el contrato.

Requerimientos de la solución

Características de licenciamiento

- Se requiere una plataforma de gestión de parches, en modalidad suscripción por el período de treinta y seis (36) meses para un total de 3.000 activos del parque que CMCABA posee al día de hoy.
- La solución debe ser capaz de integrarse con la solución actual de Gestión de Vulnerabilidades Tenable SC de manera de obtener información sobre los riesgos más críticos y aquellas vulnerabilidades que requieren ser mitigadas con prioridad. El sistema deberá ser capaz de adquirir información de los activos vulnerables, las vulnerabilidades existentes, el score de VPR (Vulnerability Priority Rating) para luego disponibilizar los parches que las resuelvan.
- La solución debe estar basada en una consola on-premise y agentes distribuidos.
- Se requiere el soporte para 3000 activos Windows, incluyendo sistema operativo, drivers y BIOS y contar además con un catálogo de aplicaciones de terceros que incluya al menos 1900 productos soportados.
- La solución deberá soportar además entornos Mac y Linux.
- Deberá permitir la definición de cadenas de aprobación, las mismas deberán permitir configurar a que productos alcanzan, los responsables que deben aprobar y el orden de los mismos y también permitir la aprobación automática.
- Deberá permitir ejecutar implementaciones por fases, incluyendo una primera fase de prueba definiendo un pequeño grupo específico de dispositivos antes de pasar a grupos de distribución cada vez más grandes para cubrir su entorno de producción.
- El sistema de gestión de parches deberá poder definir qué grupos deben recibir implementaciones de parches, en qué orden y qué debe suceder durante la transición de los retrasos de tiempo, el nivel de cumplimiento o el proceso de aprobación.

- La solución deberá utilizar un sistema de distribución de contenido que permita optimizar el uso de recursos, como por ejemplo arquitectura peer to peer y de esa manera permitir que los endpoints participen en la entrega de parches y el manejo de cache.
- Deberá tener la capacidad de crear políticas de aplicación de parches definiendo grupos de dispositivos, implementaciones por fases, personalizaciones de instalación, programaciones y colas, ventanas de mantenimiento estáticas o dinámicas, etc.
- Deberá contar con dashboards que brinden visibilidad sobre el progreso de la aplicación de parches, el estado de riesgo y cumplimiento.
- Deberá incluir la capacidad de monitorear los procesos de implementación en tiempo real y, si es necesario, brindar la capacidad de pausar una implementación específica o global.
- Deberá incluir la capacidad de crear pausas para grupos de dispositivos específicos o productos o parches específicos. Todas estas pausas se pueden reanudar justo donde se dejaron una vez que el administrador esté listo.
- Deberá incluir la capacidad de identificar si un parche tiene un impacto negativo en los dispositivos, el administrador podrá crear una política de reversión para que los dispositivos que instalaron el parche lo eliminen y reinstalen inmediatamente la versión desinstalada anteriormente o una versión definida por el administrador.
- El sistema de gestión de parches deberá incluir con al menos dos tipos de controles:
    - Una lista de bloqueo, es un control global que impedirá la instalación de cualquier parche que se agregue a esta lista. El sistema de gestión agrega parches que se encuentren con problemas durante las pruebas a esta lista para todos los clientes, y los administradores pueden agregar sus propios parches a esta lista.
    - Excepciones que permitan a los administradores definir exclusiones específicas de parches para grupos de dispositivos específicos. Las excepciones también permitirán la restricción de las actualizaciones de productos a una versión específica, lo que le permite evitar que las actualizaciones interrumpan otras aplicaciones que dependen de una versión determinada.
- El sistema de gestión de parches deberá incluir reportes detallados para:

- Estado de aplicación de parches por dispositivo: revisar el cumplimiento de la aplicación de parches, la actividad de implementación y la categorización de la estrategia de parches para dispositivos individuales
- Panel de control por producto: revisar la tasa general de cumplimiento de parches para un producto individual en su entorno y qué flujos de trabajo de automatización se incluyen en el producto.
- Por producto, por dispositivo: Revisar el estado de los parches del producto en un dispositivo individual
- Estado de parche individual: Revisar el estado de un parche en particular, incluida una lista de CVE corregidos por el parche y la puntuación CVSS asociada con el CVE.

- El sistema de gestión de parches deberá identificar parches en función de criterios definidos, como la calificación de prioridad de vulnerabilidad (VPR) o las calificaciones de CVE, así como la definición de programas de parches en función de la gravedad clasificada.
- El sistema de gestión de parches deberá incluir la creación de unidades de negocio para agrupar activos y se actualizarán automáticamente de acuerdo con el riesgo según el tipo de activo, para dirigirse rápidamente a los dispositivos con un alto riesgo de exposición.

Servicio de implementación

El adjudicatario deberá realizar la implementación de las soluciones requeridas, debiendo 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.

5. ESPECIFICACIONES TÉCNICAS RENGLÓN 7

El adjudicatario deberá proveer una la solución de capacitación y concienciación de usuarios segregada en dos instancias, una para usuarios propios del Consejo de la Magistratura de la C.A.B.A. y otra para enviar newsletters a usuarios externos.

Requerimientos Generales

- La solución debe permitir gestionar el programa de concientización, con métricas de correlación y registros de auditoría que permitan conocer en forma objetiva el grado de efectividad de las acciones realizadas.
- Dar cumplimiento a diversos estándares de seguridad y calidad, como ser ISO 27001, PCI DSS, GDPR y protección de datos personales entre otras.
- La solución debe contar:
  - Tablero de Control.
  - Programador de eventos de capacitación.
  - Visor de eventos planificados.
  - Esto de eventos en tiempo real.
  - Reportes gerenciales en tiempo real.
  - Reportes automáticos por email.
  - Registros de auditoria en tiempo real.
- La plataforma debe poseer contenidos de concientización y evaluación predefinidos actualizados, los cuales deben ser personalizables en su totalidad con la posibilidad de incorporarlos en múltiples idiomas.
- El idioma de la plataforma no debe ser modificado por ningún proceso de importación si el usuario final selecciona un idioma específico desde su perfil, o bien si un usuario administrativo asignó un idioma específico.
- La plataforma debe permitir la sincronización y autenticación de usuarios de la manera más conveniente para el Consejo de la Magistratura de la C.A.B.A. y debe permitir su estructuración de acuerdo a grupos que reflejen el orden interno.

- La plataforma debe permitir asignar diferentes roles a los usuarios con el fin de lograr una adecuada segregación de funciones.
- La plataforma debe poseer interfaces simples y responsivas para los diferentes roles de usuarios.
- La plataforma debe permitir la creación de instancias dependientes entre sí de manera jerárquica (Plataforma de gestión de múltiples organizaciones, Multitenant).
- El modelo de implementación de la plataforma debe estar basado en SaaS (Software as a Service).
- La totalidad del software ofertado deberá contar con las últimas versiones liberadas por el fabricante.
- La plataforma debe contener un Dashboard que permita visualizar rápidamente indicadores de utilidad sobre los últimos sucesos en la plataforma y así, agilizar la toma de decisiones:
    - Totalizadores
    - Usuarios contratados, activos e inactivos.
    - Última campaña ejecutada.
    - Último contenido personalizado creado.
    - Lista de administradores con la última fecha de inicio de sesión.
    - Línea de tiempo con inicios de sesión administrativos.
    - Configuraciones personalizadas y por defecto de la plataforma.
- La plataforma de concientización debe permitir el uso de sus herramientas de educación y refuerzo y de evaluación a través de campañas programables.
- La plataforma debe poseer una herramienta de programación de campañas.
- Las campañas deben poseer una fecha de inicio y de expiración determinadas y poder ser asignadas tanto a grupos de usuarios, áreas funcionales y niveles jerárquicos como a usuarios individuales.
- Las campañas deben brindar la posibilidad de enviarse en días y horarios aleatorios dentro de su rango de fechas de inicio y expiración, en horario laboral.
- Las campañas programadas deben tener la posibilidad de editarse.

- Las campañas deben permitir volver a asignarse de manera automática a aquellos usuarios que no hayan completado la campaña en el tiempo estipulado hasta que la finalicen.
- Las campañas deben permitir la selección de un contenido predefinido o personalizado para ser asignado a los usuarios elegidos.
- Las campañas deben permitir la inclusión de un nombre y descripción que permitan al usuario administrador una mejor gestión de las mismas.
- Las campañas deben permitir el envío muestral, seleccionando un porcentaje de usuarios que formará parte de la muestra. La campaña será enviada sólo al porcentaje de usuarios establecido, elegidos aleatoriamente sobre el total de usuarios destinatarios de la campaña.
- Las campañas deben brindar la posibilidad de ser previsualizadas en la plataforma antes de ser calendarizadas.
- Las campañas deben tener la posibilidad de agruparse mediante campañas relacionadas y aparecer como una única entidad en el calendario.
- Debe ser posible descargar todas las interacciones de la agrupación.
- Las campañas deben permitir el envío de pruebas a la casilla de correo electrónico del propio administrador, siendo estas pruebas fieles a la configuración realizada, de manera de observar el resultado final de la campaña de igual modo en que lo haría un usuario final en su correo electrónico.
- Las campañas deben permitir la opción de constituir campañas de prueba que no afecten los reportes, ni creen registros dentro de auditoría de usuarios ni de campañas.
- Debe permitir filtrar las campañas por tipo: campañas reales o campañas de prueba.
- Las campañas deben brindar la posibilidad de configurar detalles avanzados que dependen de la herramienta que se esté utilizando.
- La ejecución de las campañas debe ser realizada automáticamente por la herramienta.
- Al ejecutarse una campaña, si el contenido correspondiente a la misma está disponible en diferentes idiomas, la plataforma debe asignar de manera automática a cada usuario el contenido en el lenguaje que le corresponda.
- Las campañas deben permitir ser detenidas, suspendiendo el envío de todos los correos relacionados con la campaña y cesando la recolección de sus estadísticas.

- La plataforma debe poder enviar una notificación de campañas pendientes que lleguen a los usuarios que tengan una o más campañas asignadas que aún no hayan finalizado.
- Las campañas que requieren que el usuario final ingrese a la plataforma de concientización deben:
    - Permitir personalizar el tipo de notificación que el usuario final recibirá, posibilitando elegir como mínimo entre las siguientes opciones:
        - Correo de notificación propio de la plataforma
        - Correo de notificación con URL personalizada de ingreso
        - No enviar correo de notificación
- El contenido de las notificaciones que recibirá el usuario final debe ser 100% personalizables. Esta funcionalidad debe:
    - Permitir la creación de un contenido 100% personalizado para cada notificación en cada uno de los idiomas disponibles en la plataforma.
    - Permitir el uso de variables en el asunto y contenido del correo de notificación personalizado.
    - Permitir la previsualización del correo de notificación personalizado.
    - Permitir el envío de pruebas del correo de notificación personalizado al correo electrónico del usuario administrador en cada uno de los idiomas disponibles en la plataforma.
    - Enviar de manera automática un correo de bienvenida a la plataforma a cada uno de los usuarios que nunca hayan recibido el mensaje con anterioridad.
- El contenido del correo de bienvenida debe ser 100% personalizable. Esta funcionalidad debe:
    - Permitir la creación de un contenido 100% personalizado para cada uno de los idiomas disponibles en la plataforma.
    - Permitir el uso de variables en el asunto y contenido del correo de bienvenida personalizado.
    - Permitir la previsualización del correo de bienvenida personalizado.
    - Permitir el envío de pruebas del correo de bienvenida personalizado al correo electrónico del usuario administrador en cada uno de los idiomas disponibles en la plataforma.

    - Enviar un mensaje que se visualice al solicitar la recuperación de la contraseña desde la pantalla de inicio de sesión.
- La plataforma debe contener subsecciones relativas al calendario y una lista de campañas.
- El listado de campañas debe presentar las campañas pasadas y futuras en una tabla con distintas opciones de filtrado.
- Las campañas deben acompañarse de una opción para ver toda la información presente en cada una de ellas.
- La plataforma de concientización debe permitir la visualización de las campañas programadas correspondientes a las herramientas de educación y refuerzo y de evaluación.
- La plataforma debe poseer una vista de calendario que permita ver mes a mes cada una de las campañas calendarizadas, incluyendo campañas pasadas y futuras.
- La vista de calendario debe mostrar una visión simplificada de cada campaña calendarizada que conste del nombre, su estado y las posibles acciones a realizar.
- Aquellas campañas que aún no han comenzado, deben poder ser editadas o eliminadas.
- Aquellas campañas que se encuentran en curso, es decir, ya han iniciado pero aún no han expirado, deben:
    - Mostrar una barra de progreso que refleje el número de correos que han sido enviados en dicha campaña.
    - Permitir acceder a datos estadísticos que muestren en tiempo real las interacciones de los usuarios dentro de cada campaña, haciendo uso de:
        - Recursos gráficos para datos agregados.
        - Tablas con opciones de paginación, ordenamiento y búsqueda para registros específicos de auditoría.
        - Filtros por grupos para una vista discriminada del detalle estadístico.
- Aquellas campañas que han expirado deben permitir acceder al detalle estadístico mencionado en el punto anterior.
- Debe permitir filtrar las campañas por tipo: campañas reales o campañas de prueba.

- La vista de calendario debe brindar la posibilidad de ver cada uno de los detalles específicos de cada campaña calendarizada, configurados durante su creación, incluyendo su descripción.
- Si una campaña presenta fallas en el envío de uno o más correos a sus destinatarios, el sistema deberá ejecutar un proceso de reenvío de correos de manera automática por única vez. Si el reenvío automático vuelve a experimentar fallas, el sistema deberá presentar un mensaje al usuario con rol administrativo en el estado de la campaña, en el detalle de la campaña y a través de los reportes administrativos.
- El sistema deberá presentar un botón para Reintentar envío manualmente.
- La plataforma de concientización deberá brindar herramientas de reportes que muestren los datos estadísticos recolectados por las campañas realizadas, tanto individualmente como en conjunto en determinado período de tiempo. Las herramientas de reportes deben:
    - Mostrar reportes gerenciales con datos agregados de campañas realizadas entre determinados períodos de tiempo.
    - Interactivos y con ayudas visuales para una visualización cómoda.
    - Actualizados en tiempo real.
    - Diferenciados por tipos de campañas según la herramienta de evaluación o de educación y refuerzo utilizada.
    - Con información agregada para niveles gerenciales.
    - Mostrar reportes detallados por campaña individual.
    - Interactivos y con ayudas visuales para una visualización cómoda.
    - Con información agregada e información detallada de cada usuario según los datos estadísticos del tipo de campaña.
    - Permitir correlacionar datos de las distintas acciones realizadas con las campañas, demostrando el cambio real de comportamiento de los usuarios y el grado de efectividad de las campañas realizadas.
    - Enviar reportes automáticamente por email a determinados usuarios administradores de la plataforma.
    - Los reportes a enviar y el momento de su envío deben ser configurables.
    - Permitir realizar filtros sobre los reportes generados. Los filtros deben ser:

  - Por rango de fechas.
  - Por tópico o escenario.
  - Por grupo, área funcional o nivel jerárquico de usuarios involucrados.
- Los reportes deben hacer uso de recursos gráficos, en específico de los siguientes gráficos:
  - Gráficos sobre campañas:
  - Gráfico evolutivo.
  - Gráfico de embudo.
  - Gráfico de correlación entre diferentes actividades de concientización.
  - Gráficos sobre usuarios. Ranking de usuarios de riesgo.
- Permitir la impresión y exportación de cada recurso gráfico generado en los siguientes formatos:
  - JPG
  - PNG
  - SVG
  - PDF
  - CSV
  - JSON
  - XSLX
- Permitir la realización de anotaciones sobre los recursos gráficos generados, tanto en forma de texto como imágenes, permitiendo además la exportación e impresión.
- Permitir la obtención de datos suficientes para derivar los siguientes indicadores de riesgo:
  - Ejecución de software malicioso:
    - Exposición de la organización.
  - Costo tecnológico:
    - Limpieza de equipos.
    - Restauración de backup.

        - Restauración de información no respaldada.
    - Costo de negocio:
    - Costo de improductividad.
    - Costo de oportunidad.
    - Impacto en la imagen.
    - Fuga de información:
        - Exposición de la organización.
    - Costo tecnológico:
    - Costo de tareas reactivas a la fuga de información.
    - Costo de negocio:
    - Valor de la información comprometida.
    - Grado de conocimiento de los usuarios sobre las políticas de seguridad de la organización.
    - Imagen que los usuarios poseen sobre el área de seguridad.
    - Comparativa: Inversión vs. Riesgo económico mensurable
- Permitir la exportación de datos en formato XLS y CSV.

- Debe registrar todas las actividades que ocurren en la plataforma, tanto aquellas realizadas por usuarios finales y administradores como así también aquellas realizadas por la misma plataforma.
- Los registros de auditoría no pueden ser alterados por ningún usuario de la plataforma ni por la plataforma misma.
- Los registros de auditoría, en caso de que correspondan a una acción de modificación de datos, deben destacar las diferencias con los registros anteriores que correspondan.
- Debe permitir demostrar el cumplimiento de políticas y atender a las exigencias de auditoría interna y externa.
- Los registros de auditoría correspondientes a las campañas de la plataforma deben mostrar, como mínimo, la siguiente información:
    - Recuento de eventos pasados, futuros y eliminados por cada una de las herramientas de educación y refuerzo y evaluación de la plataforma.

- Lista de eventos pasados, futuros y eliminados por cada una de las herramientas de educación y refuerzo y evaluación de la plataforma que detalle:
    - Tipo de campaña.
    - Fecha de inicio y de expiración.
    - Contenido utilizado.
    - Grupos y usuarios destinatarios.
    - Vista general de eventos pasados que muestre, por cada una de las herramientas de educación y refuerzo y evaluación de la plataforma:
    - Cantidad de campañas enviadas.
    - Número de interacciones de los usuarios en cada una de ellas, contemplando todos los tipos de acciones posibles en cada tipo de campaña.
    - Posibilidad de conocer los usuarios de riesgo de la organización y los usuarios modelo.
    - Detalle de acciones realizadas por cada uno de los usuarios en cada una de las campañas enviadas.
    - Detalle de cada campaña realizada que incluya:
        - Datos generales de la campaña.
        - Configuraciones específicas de la campaña según el tipo de herramienta utilizada.
        - Estado de la campaña.
    - Datos estadísticos agregados, presentados tanto en forma de texto como de gráficos.
    - Datos específicos discriminados por usuario asignado a la campaña que detallen su interacción con la misma, incluyendo:
    - Dirección IP del usuario que realizó la acción.
    - User Agent del usuario que realizó la acción.
    - Historial de cada campaña realizada que incluya:
    - Acciones realizadas por usuarios administradores:
        - Creación de la campaña.

- Modificación de la campaña.
- Eliminación de la campaña.
- Acciones realizadas por la plataforma:
- Envío de la campaña

- Cada acción del historial de campaña debe detallar:
  - Fecha de la acción realizada.
  - Tipo de acción.
  - Usuario.
  - Acción realizada.
  - Detalle de la configuración de la campaña en cada momento, indicando de manera clara posibles cambios en los valores entre una acción y la siguiente.

- Los registros de auditoría correspondientes a los usuarios finales de la plataforma deben mostrar, como mínimo, la siguiente información:
  - Lista de usuarios de la plataforma, detallando la siguiente información:
    - Nombre de usuario.
    - Nombre, apellido y correo electrónico del usuario.
    - Grupos, áreas funcionales y niveles jerárquicos a los cuales pertenece cada usuario.
    - Cantidad de campañas que impactaron al usuario, categorizadas según el tipo de herramienta empleada, ya sea para educación y refuerzo o para evaluación.
    - Vista general por usuario que contenga:
      - Nombre de usuario.
      - Nombre, apellido y correo electrónico del usuario.
      - Grupos a los cuales pertenece cada usuario.
      - Datos estadísticos mostrados en forma de gráficos que detallen, de manera agregada, las interacciones del usuario con cada tipo de herramienta de educación y refuerzo y evaluación de la plataforma.

- Vista por cada componente de la plataforma que contenga:
    - Nombre de usuario.
    - Cantidad total de acciones en las que el usuario fue involucrado o que ejecutó, desglosado por el tipo de herramienta utilizada, ya sea de educación y refuerzo o de evaluación

- Posibilidad de descargar un detalle de todas las campañas del componente en cuestión realizadas por cada uno de los usuarios de la plataforma.
- Historial de cada usuario que contenga:
    - Lista de acciones que el usuario realizó dentro de la plataforma.
    - Lista de acciones que la plataforma realizó e involucraron al usuario.
- Por cada acción, debe registrarse:
    - Fecha de la acción realizada.
    - Tipo de acción.
    - Acción realizada.
    - Campaña correspondiente a la acción registrada.
    - Contenido correspondiente a la campaña registrada.
    - Dirección IP del usuario que realizó la acción.
    - User Agent del usuario que realizó la acción.
    - Lista de campañas del usuario, que contenga:
        - Lista de campañas en las que el usuario fue alcanzado.
        - Fecha de inicio y expiración de cada campaña.
        - Contenido correspondiente a la campaña registrada.
        - Detalle de campañas del usuario, que contenga, por cada campaña:
        - Lista de acciones que el usuario realizó dentro de la campaña.
        - Lista de acciones que la plataforma realizó e involucraron al usuario en la campaña.
    - Dirección IP del usuario que realizó la acción.

    - User Agent del usuario que realizó la acción.

- Todos los registros de auditoría deben estar enlazados entre sí para favorecer una navegación simple e intuitiva desde un detalle general a un detalle granular.
- Todas las tablas de auditoría deben:
    - Ser exportables en los siguientes formatos: CSV y XLS
    - Poseer herramientas de ordenación, paginación y búsqueda.
    - Permitir la impresión y exportación de cada recurso gráfico generado en los siguientes formatos: JPG, PNG, SVG, PDF, CSV, JSON, XSLX
- Deben contar con contenido diseñados desde cero por un equipo de profesionales técnicos y pedagógicos.
- Deben poseer soporte multi-idioma en el core de la plataforma.
- Deben actualizarse regularmente para reflejar tanto los cambios en el entorno de seguridad como los avances en el conocimiento de la disciplina.
- Deben poseer lenguaje sencillo, sin terminología técnica excluyente y permitir su comprensión 100%, por personas sin conocimientos profesionales sobre informática.
- Deben estar diseñados para favorecer el desarrollo de hábitos seguros y el cambio de comportamiento de las personas por sobre la simple asimilación de conocimientos teóricos.
- Deben ser aplicables a la vida personal y privada de los usuarios finales, y no sólo a su vida laboral.
- Deben permitir la generación de contenido personalizado específico para cada una de las herramientas de educación y refuerzo y evaluación:
    - Tomando como plantilla un contenido predefinido.
    - Creando un contenido nuevo.
- La plataforma debe proveer un editor de contenidos preparado específicamente para la creación simple e intuitiva de cada uno de los tipos de contenidos personalizables.
- Dichos editores deben estar embebidos en la plataforma y no requerir el uso de software de terceros.
- Deben permitir el uso de variables.
- Deben permitir la posibilidad de añadir y poder utilizar nuevas variables a pedido.

- Deben permitir la optimización automática de imágenes.
- Debe permitir la carga individual de usuarios, grupos, áreas funcionales y niveles jerárquicos.
- Debe permitir la carga masiva de usuarios, grupos, áreas funcionales y niveles jerárquicos.
    - A través de un archivo CSV.
    - Desde Microsoft Entra ID.
    - Desde Google Workspace.
- Las opciones de carga en masa de usuarios y grupos deben poder ser configuradas para ser ejecutadas en forma diaria, de manera de mantener la plataforma siempre sincronizada con los usuarios y grupos pertinentes.
- Debe permitir la edición en masa de usuarios, grupos, áreas funcionales y niveles jerárquicos.
- Debe permitir la autenticación de usuarios a través de diferentes métodos:
    - Propio de la plataforma con credenciales o sin ellas.
    - A través de Microsoft Entra ID.
    - A través de Auth0.
    - A través de Google Workspace.
- Debe permitir la posibilidad de configurar el segundo factor de autenticación para usuarios en las instancias que tengan configurada la autenticación con credenciales de la plataforma.
- Debe permitir configurar un doble factor de autenticación para usuarios administrativos.
- Debe permitir la generación de códigos de respaldo dentro del proceso de activación del doble factor de autenticación en usuarios administrativos.
- Debe permitir definir una estructura organizacional bajo la cual agrupar a los diferentes usuarios de la organización. Para esto, debe permitir:
    - Crear, editar y eliminar grupos.
    - Editar los usuarios pertenecientes a un grupo.
    - Crear, editar y eliminar áreas funcionales.

    - Editar los usuarios pertenecientes a un área funcional.
    - Crear, editar y eliminar niveles jerárquicos.
    - Editar los usuarios pertenecientes a un nivel jerárquico.
- Debe permitir restablecer y modificar contraseña de un usuario.
- Debe permitir realizar acciones individuales y en masa sobre los usuarios:
    - Eliminar.
    - Activar o desactivar.
    - Cambiar el rol.
    - Asignar grupos, pudiendo elegir entre mantener o sobrescribir grupos actuales del usuario.
    - Asignar lenguaje.
    - Anonimizar.
- Debe permitir realizar acciones individuales y en masa sobre los grupos, áreas funcionales y niveles jerárquicos:
    - Eliminar.
    - Activar o desactivar.
    - Depurar: eliminar todos aquellos grupos, áreas funcionales o niveles jerárquicos que hayan sido creados pero no registren actividad dentro de la plataforma ni posean usuarios asignados.
- Debe permitir anonimizar usuarios, permitiendo que sus datos estadísticos se conserven en la plataforma pero imposibilitando realizar el trazado hacia atrás para conocer a qué usuario específico pertenecen.
- Debe mostrar los usuarios, grupos, áreas funcionales y niveles jerárquicos de la plataforma en tablas independientes, las cuales deben:
    - Poseer herramientas de búsqueda.
    - Poseer herramientas de ordenamiento.
    - Poseer herramientas de paginación.
    - Poseer herramientas de exportación en los siguientes formatos: CSV y XLS
- Debe permitir guardar, por cada usuario, los siguientes datos:

  - Usuario.
  - Nombre.
  - Apellido.
  - Correo electrónico.
  - Lenguaje.
  - Grupos.
  - Teléfono.
  - Foto de Perfil.
  - Estado.
  - Rol.
- Debe permitir guardar, por cada grupo, área funcional y nivel jerárquico, los siguientes datos:
  - Nombre.
  - Estado.
  - Origen: Si el grupo, área funcional o nivel jerárquico ha sido creado manualmente por un usuario administrador o automáticamente mediante un proceso de sincronización.
- Debe permitir que los grupos, áreas funcionales y niveles jerárquicos de un usuario creados automáticamente sean sobrescritos en posteriores procesos de sincronización, mientras se mantienen aquellos creados manualmente por un usuario administrador.
- Debe permitir ver los siguientes datos de los usuarios:
  - Fecha de creación.
  - Fecha de edición.
- Debe tener filtros en la tabla de usuarios del detalle de cada campaña, que permitan visualizar en la tabla sólo las agrupaciones que fueron destinatarias de la campaña.
- Debe permitir crear grupos que contengan a aquellos usuarios que realizaron o no interacciones específicas con cada campaña. Dichos usuarios se deben asignar automáticamente al grupo, área funcional o nivel jerárquico al momento de su creación.

- Debe permitir crear grupos inversos que contengan a aquellos usuarios excluidos de un grupo.
- Las interfaces de la plataforma deben utilizar tecnologías modernas como HTML5 y CSS3.
- Debe brindar la posibilidad de mostrar la imagen institucional del Consejo de la Magistratura de la C.A.B.A.
- Debe presentar indicadores generales acerca del uso de la plataforma que se actualicen en tiempo real:
    - Totalizadores.
    - Componentes y catálogos contratados.
    - Usuarios contratados, activos e inactivos.
    - Última campaña ejecutada.
    - Último contenido personalizado creado.
    - Lista de administradores con la fecha de su último inicio de sesión.
    - Línea de tiempo con inicios de sesión administrativos.
- El Dashboard de Implementación debe mostrar todas las posibles configuraciones de la plataforma y los valores actuales, indicando con colores las opciones de configuración personalizadas o por defecto:
    - Debe brindar la posibilidad de añadir dominios e IPs de la plataforma a las listas blancas de la organización.
    - Debe brindar la posibilidad de lanzar campañas de prueba y verificar su ejecución con éxito a un grupo reducido de usuarios colaboradores, cargados manualmente.
    - Debe brindar la posibilidad de importar o sincronizar los usuarios y grupos de la organización y gestión de grupos, áreas funcionales y niveles jerárquicos.
    - Debe brindar la posibilidad de configurar un método de autenticación de los usuarios.
    - Debe brindar la posibilidad de configurar un servidor propio de correo electrónico.
    - Debe brindar la posibilidad de configurar las diferentes formas de notificación.

- Debe brindar la posibilidad de definir qué notificaciones reciben los usuarios y personalizar el contenido.
- Debe brindar la posibilidad de configurar el envío de un certificado al usuario.
- Debe brindar la posibilidad de configurar un logotipo propio, datos de la organización y título de la pantalla de inicio de sesión.
- Debe brindar la posibilidad de personalizar el feedback que recibe el usuario.
- Debe brindar la posibilidad de definir los contenidos a utilizar, que pueden ser contenidos provistos por la plataforma o bien crear contenidos personalizados.
- Debe brindar la posibilidad de configurar la forma de asignar los contenidos y los certificados.
- Debe brindar la opción de configurar la edición o no de los campos en el perfil del usuario.
- Debe brindar la posibilidad de definir los campos que cada usuario puede editar en su perfil.
- Debe brindar la posibilidad de editar nombres de hosts personalizados.
- Debe brindar la posibilidad de controlar el acceso por dirección IP.
- Debe brindar la posibilidad de configurar los datos para el funcionamiento del botón de reporte de Phishing.
- Debe brindar la posibilidad de configurar reportes administrativos que se envían por correo a usuarios administrativos
- Debe brindar la posibilidad de buscar por nombre del contenido en la galería de contenidos.
- Debe brindar la posibilidad de personalizar los colores que el usuario final visualiza en la plataforma.

- Interfaz de Usuario Final:
  - Debe permitir la navegación del usuario en su interfaz accediendo a la plataforma con credenciales o sin ellas.
  - Debe poseer la opción de reemplazar el título de la plataforma, que se muestra en la pantalla de inicio de sesión.
  - Debe mostrar al usuario final un tablero o dashboard que resuma de manera sencilla y atractiva:

    - Las campañas que posee asignadas.
    - El grado de avance de las campañas asignadas.
    - El contenido sin asignar disponible para su visualización, según las configuraciones realizadas por el administrador de la plataforma.
    - Las campañas que ha finalizado.
    - Descripción de las insignias de gamificación obtenidas.
    - Posición del usuario en el ranking de puntos de experiencia.
    - El nivel del usuario en base a sus puntos de experiencia.
    - Información sobre la cantidad de puntos de experiencia que otorgan los distintos contenidos asignados, disponibles y finalizados.
  - Debe brindar una vista específica para cada herramienta de educación y refuerzo y evaluación que correspondan.
  - Debe permitir al usuario final la edición de su perfil y de su contraseña.
- Debe permitir configurar un servidor propio de correo para todos aquellos correos que son enviados desde la plataforma a sus usuarios.
- Debe permitir configurar mediante OAuth 2.0 para Microsoft Exchange Online.
- Debe permitir establecer un número máximo de correos a enviar por minuto a través del servidor.
- El servidor de correo propio no debe ser utilizado para la herramienta de simulación de Phishing y Ransomware ya que podría afectar su reputación. Tal herramienta debe utilizar siempre el servidor de correo de la plataforma.
- Debe permitir establecer una dirección de correo que reciba las respuestas de los usuarios finales a los distintos correos de notificación enviados por la plataforma.
- Debe permitir configurar el campo From de los correos.
- Debe permitir personalizar al 100% el correo electrónico enviado para:
  - Correo de bienvenida.
  - Recordatorios.
  - Campañas pendientes.
  - Reseteo de contraseña.

    - Aviso de asignación de campañas.
- Debe permitir configurar qué usuarios van a recibir el correo de bienvenida.
- Debe permitir configurar la frecuencia de los recordatorios.
- Debe permitir configurar el título de la plataforma.
- Debe permitir configurar los datos de cuenta del Consejo de la Magistratura de C.A.B.A., detallando como mínimo el nombre, el logotipo o isologotipo y cualquier otra información pertinente.
- Debe permitir crear, editar y eliminar nombres de hosts personalizados que serán utilizados en la URL de las campañas de simulación de Phishing y Ransomware.
- Debe permitir personalizar el Dashboard del usuario final.
- Debe permitir personalizar las páginas de error 404.
- Debe permitir personalizar los colores que el usuario final visualiza en la plataforma.
- Debe permitir configurar la vista del usuario final para:
    - Módulos interactivos
    - Videos
    - Videojuegos
    - Newsletters
- Debe permitir configurar la asignación al usuario final para:
    - Módulos interactivos
    - Videos
    - Exámenes
- Debe permitir configurar un pool de URLs, un conjunto de URLs utilizado en videojuegos.
- Debe permitir configurar las URLs a utilizar en los videojuegos:
    - URLs predefinidas.
    - URLs personalizadas.
- Debe permitir personalizar las Insignias que recibirán los usuarios finales por su desempeño.

- Debe permitir visualizar los Puntos de experiencia que recibirán los usuarios finales por las actividades realizadas.
- Debe permitir seleccionar y personalizar el feedback brindado al usuario al responder la pregunta de validación de los newsletters, los momentos educativos y los exámenes, tanto para respuestas correctas como incorrectas:
    - Utilizar exclamación y mensaje predefinido.
    - Utilizar exclamación y mensaje personalizado.
- Debe permitir configurar los remitentes de los correos electrónicos de simulación:
    - Valor definido en el escenario.
    - Valor fijo que no provoque una suplantación de identidad.
- Debe permitir configurar la cabecera Reply-to presente en los correos de simulación.
- Debe permitir configurar los datos para el funcionamiento del botón de reporte de Phishing:
- Debe permitir definir los destinatarios de los correos reportados como Phishing.
- Debe permitir la descarga del instalador del botón de reporte de Phishing.
- Debe permitir configurar el medio por el cual serán enviados los correos electrónicos relacionados con simulaciones.
    - Servidor de correos predefinido.
    - Direct Message Injection a través de Google.
    - Direct Message Injection a través de Microsoft.
- Debe proveer un encabezado de correo electrónico único que permita identificar los correos de Phishing y Ransomware de la plataforma de manera unívoca y segura.
- Debe permitir controlar el acceso por dirección IP a la plataforma:
    - Debe permitir definir uno o más rangos de direcciones IP autorizadas a acceder a la plataforma.
    - Debe permitir definir uno o más rangos de direcciones IP restringidas a acceder a la plataforma.
- Debe permitir configurar qué campos de su perfil puede editar cada usuario, posibilitando una configuración granular en la cual se pueda decidir de manera flexible la combinación de campos que será de sólo lectura en el perfil del usuario.

- Debe permitir la gestión de instancias dependientes entre sí mediante una relación de padre/hijo.
- Las instancias intermedias en la estructura deben permitir las siguientes funciones:
    - Visualizar como mínimo la siguiente información sobre sus instancias hijas:
    - Totalizadores.
    - Componentes y catálogos contratados.
    - Usuarios contratados, activos e inactivos.
    - Última campaña ejecutada.
    - Último contenido personalizado creado.
    - Fecha de último inicio de sesión administrativo.
    - Línea de tiempo con inicios de sesión administrativos.
    - Configuraciones personalizadas y por defecto de la plataforma.
    - Campañas creadas.
    - Instancias padres e hijas.
    - Acceder como administradores, en caso que se permita, a sus instancias hijas.
    - Permitir o no el acceso desde su instancia padre.
    - Crear contenidos personalizados y compartirlos con sus instancias hijas.
    - Crear, editar y eliminar campañas de prueba dentro de la misma instancia multitenant.
    - Crear, editar y eliminar campañas de cualquier tipo que alcancen a grupos de usuarios de cualquiera de sus instancias hijas.
- La plataforma deberá contar con APIs REST que permitan obtener:
    - Listado completo de campañas de simulación de Phishing realizadas junto con el detalle de cada campaña.
    - Listado de las campañas externas a la plataforma realizadas por los usuarios junto con el detalle de cada campaña.
    - Debe tener parámetros opcionales que varían según el tipo de campaña. Si no se especifica ningún filtro, la API mantendrá el comportamiento por defecto.
    - Listado sobre todas las campañas en las que participó un usuario.

    - La API debe permitir su integración con otros sistemas.
- Los servidores donde se encuentre desplegada la plataforma deben poseer un nivel de seguridad que cumple con los siguientes estándares de seguridad:
    - ISO 27001
    - SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
    - PCI Level 1
    - FISMA Moderate
    - Sarbanes-Oxley (SOX)
- La plataforma debe requerir alguno de los siguientes sistemas operativos en versiones que actualmente tengan soporte oficial:
    - Microsoft Windows
    - Apple Mac OS
    - GNU/Linux
- La plataforma debe requerir alguno de los siguientes navegadores web en versiones que actualmente tengan soporte oficial para los sistemas operativos mencionados anteriormente.
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
    - Apple Safari
- La aplicación debe encontrarse desplegada en una plataforma certificada y extendida como Heroku. Los archivos utilizados por la misma, a su vez, deben encontrarse almacenados en infraestructuras certificadas y ampliamente difundidas como Amazon S3.
- Contar con seguridad física de grado militar, Tests de Penetración y Evaluación de Vulnerabilidades contínuos, Gestión de Seguridad de Datos y Sistemas, Políticas de Backup, Planes de Recuperación ante Desastres, Políticas de Privacidad, y Buenas Prácticas.
- Brindar una disponibilidad del 99,99% de la información almacenada en su SLA.

- Las bases de datos utilizadas por la plataforma se deben encontrar encriptadas utilizando el esquema de cifrado por bloques AES-256
- La plataforma debe poseer copias de seguridad separadas por clientes.
- La plataforma debe realizar un backup diario de la información de cada cliente.
- La plataforma debe poseer un esquema de base de datos independiente por cada cliente.
- La plataforma debe contar con una Política de Privacidad.
- La plataforma no debe almacenar en sus bases de datos información sensible ingresada por los usuarios durante las simulaciones de Phishing.
- Debe existir una separación de ambientes en la plataforma que permitan que las tareas de desarrollo y testing transcurran en ambientes independientes entre sí, con su propio entorno y bases de datos. Dichos ambientes deben ser independientes a su vez de la aplicación que está en producción, la cual tiene también su propio entorno y base de datos. Nunca se debe utilizar la base de datos de producción en otro ambiente que no sea el de producción.
- Todos los servidores de correo que utilice la plataforma deben contar con sus correspondientes registros SPF, DKIM y DMARC.
- El desarrollo de la plataforma debe realizarse siguiendo como guía diferentes estándares, como la Guía de desarrollo seguro de OWASP.
- La plataforma debe realizar anualmente un análisis de vulnerabilidades. El mismo se debe realizar por terceros externos a la empresa.
- La plataforma debe poseer un programa de bug bounty privado donde analistas de seguridad buscan vulnerabilidades y conducen penetration tests en la plataforma.
- La plataforma debe estar registrada en el programa CSA STAR (CSA Security, Trust & Assurance Registry).
- La plataforma no debe requerir la instalación de plugins adicionales como Java, Flash y Silverlight.

Instancia de Usuarios Internos

- La plataforma debe contar con el licenciamiento progresivo, de forma tal de permitir integrar 3.000 usuarios internos del Consejo de la Magistratura de la C.A.B.A. en el primer año, 5.000 en el segundo y 7.000 en el tercero

- La plataforma debe permitir al usuario sin credenciales recibir un correo de bienvenida y tener un enlace de acceso a la plataforma.
- La plataforma debe contar con herramientas de educación y refuerzo de concientización que deben cumplir con los siguientes requerimientos:
    - Módulos interactivos de concientización
        - Deben permitir su asignación a usuarios finales por medio de campañas.
        - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
            - Módulo interactivo enviado.
            - Módulo interactivo comenzado.
            - Módulo interactivo finalizado.
            - Interacciones del usuario.
        - Debe permitir la configuración de envío de recordatorios automáticos.
        - Debe permitir editar la fecha de los recordatorios.
        - Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña pero aún no la han finalizado.
        - Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
        - Debe permitir la configuración de envío de recordatorios manuales.
        - Los recordatorios deben mostrar el detalle de cada envío realizado, su estado actual y la cantidad de correos enviados correctamente.
        - Debe permitir especificar la frecuencia en días con la cual serán enviados los recordatorios de cada campaña.
        - Debe brindar la flexibilidad de configurar la estrategia de concientización de acuerdo a los siguientes puntos:
        - Configurar qué módulos interactivos puede ver el usuario final, de manera de poder decidir:
        - Si los usuarios finales puedan acceder y completar módulos de manera proactiva (sin estar asignados en una campaña)

- Si los usuarios finales sólo podrán ver módulos interactivos que les han sido asignados dentro de una campaña
- Configurar cuántas veces es posible asignar un módulo interactivo determinado a un mismo usuario, de manera de poder decidir:
- Si el programa de concientización estará basado en el refuerzo de contenidos.
- Si el programa de concientización brindará sólo contenidos únicos a cada usuario.
- Los módulos interactivos deben mostrarse en la interfaz del usuario final según los criterios configurados y divididos entre:
- Módulos asignados al usuario final dentro de una campaña.
- Módulos completados por el usuario final proactivamente.
- Módulos disponibles para el usuario final.
- Módulos pendientes del usuario final.
- Debe permitir el uso de contenidos que cumplan con las siguientes características:
- Presencia de actividades interactivas desarrolladas específicamente para facilitar el aprendizaje y asimilación de contenidos:
- Preguntas de múltiple opción con orden aleatorio de respuestas y feedback tanto en respuestas correctas como incorrectas.
- Actividad de arrastrar conceptos y soltarlos donde corresponda.
- Actividad de selección múltiple.
- Actividad de viñetas interactivas.
- Actividad interactiva para detectar correos electrónicos de Phishing.
- Actividad interactiva para detectar URLs peligrosas.
- Actividad interactiva para detectar sitios web maliciosos.
- Actividad interactiva para detectar archivos adjuntos maliciosos.
- Actividad interactiva para detectar engaños de ingeniería social.
- Actividad interactiva para desarrollar una contraseña segura siguiendo indicadores puntuales.

- Presencia de contenido multimedia:
- Imágenes.
- Videos.
- Embebidos desde sitios como Youtube o Vimeo.
- Cargados directamente desde archivo hacia la plataforma.
- El contenido predefinido debe estar desarrollado para ser visualizado en su completitud por el usuario final en un tiempo de entre diez y doce minutos.
- Presencia de todas las características detalladas en el punto 2.2.6.
- Debe permitir configurar si los usuarios que no sean notificados sobre el módulo interactivo ya finalizado previamente, puedan ser o no asignados a un examen derivado.
- Debe permitir su visualización en un reproductor de módulos interactivos diseñado especialmente para la correcta visualización de todos los tipos de actividades interactivas, contenido multimedia y texto.
- El reproductor de módulos interactivos debe permitir al usuario final continuar con un módulo interactivo previamente comenzado desde el mismo lugar en donde lo abandonó por última vez.
- El reproductor de módulos interactivos debe cumplir con los requerimientos de interfaz detallados en el punto 2.2.8.
- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.
- Debe ser posible descargar el certificado correspondiente a cada usuario en particular en formato PDF.

- Newsletters de concientización:
  - Debe permitir su asignación a usuarios finales por medio de campañas.
  - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
    - Newsletter enviado.
    - Newsletter abierto.

        - Respuesta correcta o incorrecta en pregunta de validación.
    - Debe permitir la configuración de envío de recordatorios automáticos.
    - Debe permitir editar la fecha de los recordatorios.
    - Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña, pero aún no la han finalizado.
    - Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
    - Debe permitir el uso de contenidos que cumplan con las siguientes características:
        - El contenido predefinido debe estar desarrollado para ser visualizado en su completitud por el usuario final en un tiempo no superior a dos minutos.
        - Debe permitir añadir preguntas al final de cada newsletter para validar la lectura y comprensión de los contenidos.
        - El contenido debe seguir patrones de diseño responsivos válidos para cualquier cliente de correo electrónico de uso extendido.
    - Debe proveer al usuario final un visor de newsletters diseñado especialmente para su correcta visualización dentro de la plataforma.
    - Debe permitir configurar si un usuario final puede ver, dentro de su interfaz de usuario:
        - los newsletters que posee asignados dentro de una campaña.
        - los newsletters que le han sido enviados previamente.
        - los newsletters disponibles en la plataforma.
    - Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.
- Videos de concientización:
    - Deben permitir su asignación a usuarios finales por medio de campañas.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:

- Video enviado.
- Video comenzado.
- Video finalizado.
- Respuesta correcta o incorrecta en pregunta de validación.

- Debe permitir la configuración de envío de recordatorios automáticos.
- Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña pero aún no la han finalizado.
- Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
- Debe brindar la flexibilidad de configurar la estrategia de concientización de acuerdo con los siguientes puntos:
    - Configurar qué videos puede ver el usuario final, de manera de poder decidir:
        - Si los usuarios finales realizarán videos de manera proactiva (sin que estén asignados en una campaña).
        - Si los usuarios finales sólo podrán ver videos que les han sido asignados dentro de una campaña.
    - Configurar cuántas veces es posible asignar un video determinado a un mismo usuario, de manera de poder decidir:
        - Si el programa de concientización estará basado en el refuerzo de contenidos.
        - Si el programa de concientización brindará sólo contenidos únicos a cada usuario.
- Los videos deben mostrarse en la interfaz del usuario final según los criterios configurados y divididos entre:
    - Videos asignados al usuario final dentro de una campaña.
    - Videos completados por el usuario final.
    - Videos disponibles para el usuario final.

- Debe permitir el uso de contenidos que cumplan con las siguientes características:
    - Debe permitir añadir preguntas al final de cada video para validar la visualización y comprensión de los mismos.
    - El contenido predefinido debe estar desarrollado de manera de ser visualizado en su completitud por el usuario final en un tiempo de tres minutos.
- Debe permitir su reproducción en un reproductor de videos diseñado especialmente para la correcta visualización del video y sus actividades.
- Debe permitir al usuario responder preguntas de validación tras finalizar el video.
- El reproductor de videos no debe permitir al usuario final avanzar al siguiente paso sin haber reproducido el video en su totalidad.
- El reproductor de videos no debe permitir al usuario final adelantar el video.
- Debe permitir la posibilidad de añadir un examen relacionado.
- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.

- Videojuegos de concientización
    - Debe permitir utilizar URLs personalizadas en los videojuegos.
    - Deben permitir su asignación a usuarios finales por medio de campañas.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Videojuego enviado.
        - Videojuego comenzado.
        - Videojuego finalizado.
        - Interacciones del usuario.
        - Puntaje del usuario.
        - Posición en el ranking.
    - Debe permitir la configuración de envío de recordatorios automáticos.

- Debe permitir editar la fecha de los recordatorios.
- Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña pero aún no la han finalizado.
- Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
- Debe permitir la configuración de envío de recordatorios manuales.
- Los recordatorios deben mostrar el detalle de cada envío realizado, su estado actual y la cantidad de correos enviados correctamente.
- Debe permitir especificar la frecuencia en días con la cual serán enviados los recordatorios de cada campaña.
- Debe brindar la flexibilidad de configurar la estrategia de concientización de acuerdo con los siguientes puntos:
    - Configurar qué videojuegos puede ver el usuario final, de manera de poder decidir:
        - Si los usuarios finales puedan acceder y completar videojuegos de manera proactiva (sin estar asignados en una campaña)
        - Si los usuarios finales sólo podrán ver los videojuegos que les han sido asignados dentro de una campaña
    - Configurar cuántas veces es posible asignar un videojuego determinado a un mismo usuario, de manera de poder decidir:
        - Si el programa de concientización estará basado en el refuerzo de contenidos.
        - Si el programa de concientización brindará sólo contenidos únicos a cada usuario.
- Los videojuegos deben mostrarse en la interfaz del usuario final según los criterios configurados y divididos entre:
    - Videojuegos asignados al usuario final dentro de una campaña.

        - Videojuegos completados por el usuario final proactivamente.
        - Videojuegos disponibles para el usuario final.
        - Videojuegos pendientes del usuario final.
    - Debe permitir el uso de contenidos que cumplan con las siguientes características:
        - Presencia de actividades interactivas desarrolladas específicamente para facilitar el aprendizaje y asimilación de contenidos.
        - Combinación de desafíos intelectuales y de habilidad.
    - Los videojuegos predefinidos deben estar desarrollados para ser jugados en su completitud por el usuario final en un tiempo variable según la dificultad, temática y tipo de videojuego.
    - Debe permitir su visualización en un reproductor diseñado especialmente para la correcta visualización de todos los tipos de Videojuegos.
    - Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.
- Simulación de ataques de Phishing
    - Debe permitir su asignación a usuarios finales por medio de campañas.
    - Debe permitir configurar Direct Message Injection (DMI) para poder inyectar de manera directa los correos electrónicos correspondientes con simulaciones de Phishing en la bandeja de entrada de los usuarios destinatarios de la campaña.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Correo de simulación de Phishing enviado.
        - Correo de simulación de Phishing abierto.
        - Click sobre el enlace dentro del correo de simulación de Phishing.
        - Datos ingresados en el formulario de la página de destino de la simulación de Phishing.

- Correo de Phishing reportado.

- Las campañas deben permitir configurar si los usuarios finales que reciban la simulación de Phishing podrán ingresar o no su contraseña en el formulario de Phishing de la página de destino de la simulación.
- En caso de que se decida impedir el ingreso de la contraseña, el campo correspondiente debe encontrarse deshabilitado. La plataforma deberá considerar que un usuario ingresó sus datos en el formulario de Phishing con sólo haber tipeado un carácter en cualquier otro campo diferente al de contraseña.
- Las campañas deben permitir personalizar la URL de los enlaces de simulación de Phishing, brindando las siguientes opciones:
    - Dominio:
        - Posibilidad de seleccionar un dominio de una lista de dominios predefinidos brindados por la plataforma.
        - Posibilidad de añadir dominios personalizados propios o solicitados de manera específica al proveedor.
        - Posibilidad de añadir un certificado SSL a cada uno de los dominios personalizados.
        - Posibilidad de seleccionar un dominio de manera aleatoria entre los dominios disponibles.
    - Subdominios:
        - Posibilidad de crear, editar y eliminar diferentes subdominios.
        - Posibilidad de seleccionar un subdominio a utilizar en la simulación de Phishing y combinarlo con los dominios disponibles.
- Las campañas deben permitir una previsualización de la URL que recibirán los usuarios asignados a la simulación.
- Todas las campañas de simulación deben poseer enlaces que lleven a sitios seguros con certificados SSL válidos.

- La comunicación entre el usuario y la plataforma se realizará siempre por medio del protocolo criptográfico TLS, cifrada mediante un certificado emitido por COMODO RSA Domain Validation Secure Server CA o Let's Encrypt, con uso de una clave RSA de 2048 bits y un algoritmo de firma SHA256withRSA.
- Las campañas deben permitir el anexo de momentos educativos, configurando:
    - La acción que activará el momento educativo.
    - Cuando se mostrará el momento educativo (instantáneamente o posteriormente mediante correo electrónico).
- Debe permitir el uso de contenidos que cumplan con las siguientes características:
    - El contenido debe estar desarrollado en correspondencia con trampas de Phishing reales tanto de tópicos internos a las organizaciones como externos a ellas.
    - El contenido debe seguir patrones de diseño responsivos válidos para cualquier cliente de correo electrónico de uso extendido.
- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.
- Debe permitir insertar un código QR en las simulaciones.

- Simulación de ataques de Ransomware
    - Debe permitir su asignación a usuarios finales por medio de campañas.
    - Debe permitir configurar Direct Message Injection (DMI) para poder inyectar de manera directa los correos electrónicos correspondientes con simulaciones de Ransomware en la bandeja de entrada de los usuarios destinatarios de la campaña.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Correo de simulación de Ransomware enviado.
        - Correo de simulación de Ransomware abierto.

- Click sobre el enlace dentro del correo de simulación de Ransomware.
- Apertura del archivo de Ransomware descargado por medio de un enlace.
- Archivo de Ransomware descargado por medio de un archivo adjunto.
- Apertura del archivo de Ransomware descargado por medio de un archivo adjunto.
- Encriptación posible en carpeta del usuario.
- Correo de Ransomware reportado.

o Las campañas deben permitir personalizar la URL de los enlaces de simulación de Ransomware, brindando las siguientes opciones:

- Dominio:
  - Posibilidad de seleccionar un dominio de una lista de dominios predefinidos brindados por la plataforma.
  - Posibilidad de añadir dominios personalizados propios o solicitados de manera específica al proveedor.
  - Posibilidad de añadir un certificado SSL a cada uno de los dominios personalizados.
  - Posibilidad de seleccionar un dominio de manera aleatoria entre los dominios disponibles.
- Subdominios:
  - Posibilidad de crear, editar y eliminar diferentes subdominios.
  - Posibilidad de seleccionar un subdominio a utilizar en la simulación de Ransomware y combinarlo con los dominios disponibles.

o Las campañas deben permitir una previsualización de la URL que recibirán los usuarios asignados a la simulación.

- Todas las campañas de simulación deben poseer enlaces que lleven a sitios seguros con certificados SSL válidos.
- La comunicación entre el usuario y la plataforma se realizará siempre por medio del protocolo criptográfico TLS, cifrada mediante un certificado emitido por COMODO RSA Domain Validation Secure Server CA o Let's Encrypt, el cual hace uso de una clave RSA de 2048 bits y un algoritmo de firma SHA256withRSA..
- Las campañas deben permitir el anexo de momentos educativos, configurando:
    - La acción que activará el momento educativo.
    - Cuando se mostrará el momento educativo (instantáneamente o posteriormente mediante correo electrónico).
    - Debe permitir el uso de contenidos que cumplan con las siguientes características:
        - El contenido debe estar desarrollado en correspondencia con trampas reales tanto de tópicos internos a las organizaciones como externos a ella.
        - El contenido debe seguir patrones de diseño responsivos válidos para cualquier cliente de correo electrónico de uso extendido.

- El archivo de Ransomware simulado debe:
    - Poseer un nombre personalizable y traducible.
    - Poseer un tipo personalizable, pudiendo elegirse entre:
        - Archivo HTML.
        - Archivo HTML comprimido dentro de un ZIP.
        - Archivo ejecutable (para Windows o Mac).
- La plataforma debe permitir la posibilidad de utilizar las fuentes Hanken Grotesk y Montecatini Pro en el editor HTML.

- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.

- Simulación de ataques de Smishing
    - Las campañas deben permitir acortar la URL de los enlaces de simulación de Smishing.
    - Debe permitir su asignación a usuarios finales por medio de campaña.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Enviados: Se envió el SMS al usuario.
        - Entregados: Se entregó el SMS al usuario.
        - Click sobre el enlace: El usuario hizo click en un enlace dentro del SMS de simulación de Smishing.
        - Datos ingresados: El usuario ingresó datos en el formulario de la página de destino de la simulación de Smishing.
        - Momentos educativos enviados por email: El usuario realizó una acción que activó el envío del Momento Educativo por email.
        - Momentos educativos abiertos: El usuario visualizó el Momento Educativo en su correo electrónico o de manera instantánea en su navegador.
        - Momentos educativos contestados correctamente: El usuario contestó correctamente la pregunta del Momento Educativo utilizada para validar la lectura del mismo.
        - Momentos educativos contestados incorrectamente: El usuario contestó incorrectamente la pregunta del Momento Educativo utilizada para validar la lectura del mismo.
    - Las campañas de Smishing deben ofrecer diversas posibilidades de configuración:
        - Posibilidad de personalizar tanto el texto del SMS como el de la landing page.

- Los usuarios que reciben el SMS y acceden al enlace pueden ingresar su contraseña en el formulario de la landing page.
- Posibilidad de personalizar la URL de los enlaces de la simulación de Smishing, seleccionando Dominio y Subdominio.
- Posibilidad de activar Momentos Educativos, indicando la acción que los desencadena y cuándo se presentan al usuario, ya sea de forma instantánea o posteriormente mediante correo electrónico.
- Posibilidad de elegir el tipo de envío de los SMS a los usuarios asignados: de manera secuencial a todos los usuarios o de manera aleatoria en un determinado período de tiempo.
- Posibilidad de realizar un envío muestral de la campaña a un porcentaje de los usuarios.

- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.

- Simulación de ataques de USB Drop
  - Debe permitir su asignación a usuarios finales por medio de campañas.
  - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
    - Archivo abierto:
      - Fecha de apertura
      - Fingerprint asociado
      - Macros activadas:
      - Fecha de activación
      - Fingerprint asociado
  - Las campañas deben permitir medir el comportamiento de los usuarios cuando encuentran una memoria USB que no les pertenece.
  - Las campañas deben permitir conocer la fecha en la cual la campaña comienza a recolectar estadísticas acerca de la interacción de los usuarios.

- Las campañas deben permitir conocer la fecha de finalización de la recolección de estadísticas acerca de la interacción de los usuarios.
- Las campañas de simulación deben permitir asignar un nombre para identificar la campaña de manera sencilla.
- Las campañas deben permitir asignar una descripción a la campaña que podrá ser visualizada en el calendario.
- Las campañas de prueba no deben afectar a los reportes, ni crear registros dentro de auditoría de usuarios ni de campañas.
- Los archivos que pueden descargar y utilizar en las campañas de simulación de ataques USB Drop deben ser los siguientes:
    - Word
    - Word con macros
    - Excel
    - Excel con macros
    - PDF
- Las campañas deben poseer un campo opcional que permite especificar dónde van a ubicarse las memorias USB de la simulación.
- Cada vez que un usuario abra un archivo - entre las fechas de inicio y expiración seleccionadas - debe generar un registro de auditoría dentro de la campaña.
- El dispositivo desde el cual el usuario abra el archivo debe estar en condiciones de alcanzar los servidores de la plataforma.

- Exámenes
    - Debe permitir su asignación a usuarios finales por medio de campañas.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Examen enviado.
        - Examen comenzado.
        - Examen aprobado o desaprobado.
        - Respuestas realizadas en cada pregunta.

- Debe permitir la configuración del tiempo disponible para completar el examen en cada campaña.
- Debe permitir determinar la cantidad de preguntas que cada usuario recibirá por campaña, sobre el total de preguntas disponibles para cada examen, seleccionándolas de manera aleatoria.
- Debe permitir determinar, por cada campaña, si los usuarios finales verán las preguntas de manera aleatoria o siguiendo un orden predeterminado.
- Debe permitir la configuración del porcentaje necesario de respuestas correctas para considerar el examen como aprobado de manera independiente en cada campaña.
- Debe permitir la configuración de envío de recordatorios automáticos.
- Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña pero aún no la han finalizado.
- Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
- Debe mostrar, dentro de la interfaz de usuario del usuario final:
    - Exámenes asignados al usuario final dentro de una campaña.
    - Exámenes completados por el usuario final.
- Debe permitir configurar si el usuario final podrá ver en su interfaz los exámenes que ha completado previamente junto con su resultado.
- Debe permitir configurar, por cada campaña, si se presentará al usuario final un feedback por cada pregunta del examen.
- Debe permitir configurar, de manera general, el mensaje final de aprobación o desaprobación de los exámenes.
- Debe permitir el uso de contenidos que cumplan con las siguientes características:
    - Contener preguntas de opción múltiple con orden aleatorio de respuestas.
    - Posibilidad de agregar una imagen a cada pregunta.
- Debe permitir su visualización en un reproductor de exámenes diseñado especialmente para su correcta visualización dentro de la plataforma.

- El reproductor de exámenes no debe permitir al usuario final avanzar hacia la siguiente pregunta de un examen, hasta no responder la pregunta actual.
- El reproductor de exámenes debe permitir al usuario final cambiar las respuestas a las diferentes preguntas de un examen mientras no lo finalice.
- El reproductor de exámenes debe informar de manera constante al usuario final el tiempo disponible para finalizar el examen.
- El reproductor de exámenes debe informar al usuario final su calificación al finalizar el examen.
- El reproductor de exámenes debe guardar las respuestas del usuario final de manera que, si abandona el examen, al retomarlo conserve sus respuestas realizadas anteriormente.
- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.
- Debe ser posible descargar el certificado correspondiente a cada usuario en particular en formato PDF.

- Encuestas
  - Debe permitir su asignación a usuarios finales por medio de campañas.
  - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
    - Encuesta enviada.
    - Encuesta comenzada.
    - Encuesta finalizada.
    - Respuestas realizadas en cada actividad.
  - Debe permitir la creación de campañas anónimas:
    - Este tipo de campañas no deben permitir al usuario administrador conocer a qué usuario corresponden cada una de las respuestas realizadas en la encuesta.
    - Deben informar al usuario final que la encuesta que le ha sido asignada es anónima.
  - Debe permitir la configuración de envío de recordatorios automáticos.

- Los recordatorios se deben enviar a aquellos usuarios que han sido asignados a una campaña pero aún no la han finalizado.
- Los recordatorios deben ser enviados a mitad de la duración de una campaña y el día antes de su expiración.
- Debe mostrar, dentro de la interfaz de usuario del usuario final:
    - Encuestas asignadas al usuario final dentro de una campaña.
    - Encuestas completadas por el usuario final.
- Debe permitir configurar si el usuario final podrá ver en su interfaz las encuestas que ha completado previamente.
- Debe permitir el uso de preguntas de opción múltiple con orden aleatorio de respuestas.
- Debe brindar la posibilidad de configurar si el usuario final podrá seleccionar una única respuesta o bien, respuestas múltiples por cada una de las preguntas.
- Debe permitir añadir, por cada pregunta, la opción “Otro” que permita el ingreso de una respuesta abierta a modo de texto por parte del usuario final.
- Debe posibilitar agregar una imagen a cada pregunta.
- Preguntas abiertas que posibiliten al usuario final el ingreso de texto.
- El contenido predefinido debe estar desarrollado de manera de ser visualizado en su completitud por el usuario final en un tiempo máximo de diez minutos.
- Debe permitir su visualización en un reproductor de encuestas diseñado especialmente para su correcta visualización dentro de la plataforma.
- El reproductor de encuestas debe guardar las respuestas del usuario final de manera que, si el mismo abandona la encuesta, al retomarla conserve sus respuestas realizadas anteriormente.
- Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.

Instancia de Usuarios Externos

- La plataforma debe contar con el licenciamiento progresivo, de forma tal de permitir integrar 5.000 usuarios externos al Consejo de la Magistratura de la C.A.B.A. en el primer año, 15.000 en el segundo y 25.000 en el tercero
- Newsletters de concientización
    - Debe permitir su asignación a usuarios finales por medio de campañas.
    - Las campañas deben guardar los siguientes datos estadísticos por cada usuario asignado:
        - Newsletter enviado.
        - Newsletter abierto.
    - Debe permitir el uso de contenidos que cumplan con las siguientes características:
        - El contenido predefinido debe estar desarrollado para ser visualizado en su completitud por el usuario final en un tiempo no superior a dos minutos.
        - Debe permitir añadir preguntas al final de cada newsletter para validar la lectura y comprensión de los contenidos.
    - El contenido debe seguir patrones de diseño responsivos válidos para cualquier cliente de correo electrónico de uso extendido.
        - Debe permitir crear una campaña desde la galería de contenidos y poder acceder a la vista de creación de una nueva campaña.

Servicio de implementación

El adjudicatario deberá realizar la implementación de las soluciones requeridas, debiendo 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 RENGLONES 2, 4, 6 Y 8

El oferente deberá proveer un servicio de garantía y soporte técnico ante incidentes y consultoría proactiva, con la respectiva actualización tecnológica de todas las soluciones provistas en los renglones 1, 3, 5 y 7, por el plazo de treinta y seis (36) meses desde la fecha indicada en el Parte de Recepción Definitiva de la provisión, implementación y puesta en funcionamiento de las soluciones requeridas.

Servicio de soporte técnico reactivo/proactivo

- El servicio de soporte técnico deberá brindarse al personal del Consejo de la Magistratura. El Consejo de la Magistratura suministrará al adjudicatario una lista con la identificación de aquellas personas que se encuentran autorizadas a reportar incidentes o solicitar el soporte.
- Ante cada evento de soporte técnico el adjudicatario deberá realizar y presentar al Consejo de la Magistratura, si éste así lo requiriese, un informe que contendrá como mínimo la siguiente información:
    - Descripción detallada del problema, su causa y solución.
    - Documentación adjunta de los cambios hechos.
    - Recomendaciones.
    - Fecha y hora de resolución.
- Cada vez que se genere una solicitud de soporte técnico, según lo establecido en las cláusulas precedentes, el Adjudicatario deberá entregar un número de orden registrable por tal reclamo en el que deberá dejarse constancia cómo mínimo, de la fecha y horario en el que se realizó tal orden y el problema reportado.
- Las resoluciones a los problemas e incidentes reportados deberán ser informadas (por cualquier medio) al Consejo de la Magistratura por el personal del proveedor que brinde el soporte técnico en el menor tiempo posible. El personal del Consejo de la Magistratura verificará la solución propuesta por el proveedor y evaluará el resultado.

Si el resultado es satisfactorio se considerará el incidente como solucionado, en caso contrario se considerará el incidente como pendiente de solución.

- El servicio de soporte técnico no podrá ser modificado bajo ningún concepto de forma tal que se vea afectado el nivel de los servicios exigidos en estas especificaciones y comprometidos en la oferta.
- Si alguno de los productos objeto del contrato tuviese fecha de discontinuidad o si alguno de los servicios contratados tuviese fecha de vencimiento de soporte durante la vigencia del contrato, el Adjudicatario deberá, además de informarlo en forma escrita al Consejo de la Magistratura, asumir el compromiso de continuar con el servicio contratado, sin limitaciones o condicionantes, hasta la fecha de finalización del contrato.
- El Oferente en su propuesta deberá tener presente que a lo largo de la vigencia del contrato deberá a su vez cumplir con los siguientes requisitos:
    - Deberá incluir un servicio de garantía y soporte técnico por un plazo de treinta y seis (36) meses. El oferente deberá explicar el alcance y detalle del mismo cubriendo software y hardware.
    - Deberá incluir en la suma de todos los renglones 2 recursos full time con nivel Senior, dedicado a la gestión de las soluciones ofertadas por el lapso del contrato, pudiendo trabajar en forma remota sobre la plataforma de CMCABA.
    - Deberá incluir en la suma de todos los renglones 3 recursos full time con nivel SemiSenior, dedicado a la gestión de las soluciones ofertadas por el lapso del contrato, pudiendo trabajar en forma remota sobre la plataforma de CMCABA.
- Este servicio de garantía y soporte técnico deberá incluir como mínimo:
    - El reemplazo de equipos/partes que presenten fallas:
    - El soporte técnico local 7x24 para diagnóstico de fallas:
    - La posibilidad de actualizar el firmware/software a la última versión disponible.
    - Deberá incluir el mantenimiento proactivo de la solución de forma tal de prevenir incidentes, asegurar el cumplimiento de las buenas prácticas del fabricante y optimizar el rendimiento de la tecnología.
    - La movilización del personal o cualquier costo asociado que surgiera del servicio a prestar correrá por exclusiva cuenta del adjudicatario para cada vez que se requiera.
    - Los requerimientos se podrán efectuar telefónicamente, por correo electrónico o vía web. El oferente deberá detallar en su oferta económica el procedimiento a

realizar en caso de tener que reportar incidentes, tal como número de teléfono de asistencia, personas de contactos, etc.

- No deberá existir un límite en el número de casos de soporte que puede solicitar el Consejo de la Magistratura de la C.A.B.A.
- El servicio deberá contemplar el reemplazo parcial o total (RMA) de componentes de la solución que presenten fallas sin incurrir en gastos adicionales por parte del Consejo de la Magistratura de la C.A.B.A.

- Los Oferentes deberán presentar, para la solución que proponen, un contrato de nivel de servicio. Se deja constancia que éste último no forma parte del criterio de evaluación. A tales efectos se deberá tener presente los siguientes grados de severidad:

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

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

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

  - **Tiempos de atención/resolución de las solicitudes:** En función del grado de Severidad de la solicitud se le asociará una prioridad relacionada con los tiempos

de atención y resolución de la misma. En la siguiente tabla se detallan los tiempos que el proveedor deberá comprometer.

SLA	SEVERIDAD 1	SEVERIDAD 2	SEVERIDAD 3	SEVERIDAD 4
Tiempo de respuesta del registro de la Solicitud	15 minutos	30 minutos	60 minutos	60 minutos
Tiempo Solución Temporal	12 horas	24 horas	72 horas	--
Tiempo Solución Definitiva	40 horas	80 horas	1 mes	A convenir (Ej. Próximo reléase)

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

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

Servicio de actualización tecnológica

- Se entenderá que ha ocurrido una actualización tecnológica cuando se presente una nueva versión o release del/los mismo/s producto/s objeto de este contrato en el mercado, así como también reparaciones disponibles (en general denominadas comercialmente como patches, temporary fixes, etc.) para la generalidad de los clientes.
- Se deberán entregar sin cargo adicional todas las actualizaciones tecnológicas que, según se indica en la definición anterior, sean liberadas al mercado durante la vigencia del contrato.

- Las actualizaciones tecnológicas de los productos de software deberán estar disponibles para el Consejo de la Magistratura dentro de los treinta (30) días de liberadas al mercado.
- La obligación del adjudicatario en la entrega de actualizaciones tecnológicas surgidas dentro del período de contrato no se extinguirá con la finalización del mismo, sino hasta la efectiva entrega de las actualizaciones liberadas durante el período de contrato.

7. ESPECIFICACIONES TÉCNICAS RENGLÓN 9

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

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

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

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

Si bien las capacitaciones podrán ser brindadas en forma virtual (mediante soluciones de colaboración tales como Zoom, Microsoft Teams, Google Meets, etc.), en caso de ser presenciales, las mismas deberán ser dictadas en la Ciudad Autónoma de Buenos Aires.

El oferente brindará un certificado de asistencia a las capacitaciones a cada uno de los agentes que participen en las mismas.

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

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

FIRMAS DIGITALES

DIAZ Gaston Federico
DIRECTOR
CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTONOMA DE BUENOS AIRES