PROVINCIA DE CATAMARCA
CONCURSO DE PRECIO N.º 9-0001-CPR22
MODALIDAD – COMPRA DETERMINADA
EX-2022-02217374- -CAT-DC#MEC

PLIEGO DE BASES Y CONDICIONES PARTICULARES

JURISDICCION LICITANTE:
JURISDICCION: MINISTERIO DE ECONOMÍA
UNIDAD LICITANTE (U.L.): DIRECCIÓN PROVINCIAL DE ADMINISTRACIÓN DE LA SECRETARÍA DE FINANZAS PÚBLICAS
DOMICILIO FISICO (U.L.): SARMIENTO 589, 5TO PISO - S.F.V. CATAMARCA (C.P. 4700)
DOMICILIO ESPECIAL ELETRONICO (U.L.): compras.saf9mecon@gmail.com

JURISDICCION SOLICITANTE
JURISDICCION: MINISTERIO DE ECONOMÍA
UNIDAD SOLICITANTE: SECRETARIA DE MODERNIZACION
SERVICIO ADMINISTRATIVO FINANCIERO (S.A.F.) N° 9 - DIRECCION PROVINCIAL DE ADMINISTRACION DE LA SECRETARIA DE FINANZAS PÚBLICAS
CUIT S.A.F. N° 30-71642193-3
DOMICILIO FÍSICO (U.S.): Av. VENEZUELA S/N – CAPE CAPELLON 21 - S.F.V. CATAMARCA (C.P. 4700)
DOMICILIO ESPECIAL ELECTRÓNICO (U.S.): compras.saf9mecon@gmail.com

ENCUADRE LEGAL:
Artículo 1º: La presente Contratación se regirá por, las disposiciones de la Ley N.º 4938 que establece y regula la Administración Financiera, las Contrataciones, la Administración de los Bienes y los Sistemas de Control del Sector Público Provincial, por el Anexo I –Reglamento Parcial N.º 2 de la Ley 4938– Decreto Acuerdo N.º 1127/2020 y su modificatorio Decreto Acuerdo 1573/2020 y Decreto Acuerdo N.º 2036/2020, por la Ley N.º 5038 "Compre y Contrate Preferentemente Catamarqueño" y sus Decretos Reglamentarios N.º 1122/01 y N.º 445/02, y por las disposiciones del Pliego Único de Bases y Condiciones Generales aprobado por Resolución RESOL-2020-28-E-CAT-CGP#MHF y de la presente Bases de Contratación. Normativas a las que el oferente con la presentación de su propuesta, implica que las conoce, acepta y se somete a ellas. La presentación de las propuestas sin observaciones a las presentes Bases, implica su conocimiento, aceptación y sometimiento a todas sus disposiciones. Igual tratamiento corresponde asignar en aquellos casos en que no se acompañen los pliegos a la propuesta o que aquellos no sean rubricados.

OBJETO DE LA CONTRATACIÓN:
Artículo 2º: La presente Contratación tiene por objeto **la "Adquisición de firewall con licenciamiento para la protección de los diferentes equipos y sistemas administrados por la Secretaria de Modernización"**, según el **ANEXO I** de la presente bases de contratación cargada al Proceso **N.º 9-0001-CPR22,** cuya publicación y difusión se realiza en el sistema COMPR.AR en el sitio web http://comprar.catamarca.gob.ar-.
El **Ítem 2 del ANEXO I** referido a la prestación del servicio de Licenciamiento podrá ser prorrogada por única vez por un plazo igual a la inicial a pedido expreso de la Secretaría de Modernización.

PRESUPUESTO OFICIAL:

Artículo 3º: PESOS CUATRO MILLONES CIENTO OCHENTA Y UN MIL SEISCIENTOS NOVENTA Y DOS CON 95/100 **($ 4.181.692,95).**

FECHA Y HORA DE APERTURA:

Artículo 4º: La apertura de ofertas se efectuará por acto público a través del Sistema Electrónico de Contrataciones COMPR.AR el día 25 de noviembre de 2022 a horas 10:00 am. En forma electrónica y automática se generará el Acta de Apertura de ofertas correspondiente.

AUTORIZADO POR:

Artículo 5º: El acto administrativo que autoriza el llamado, es la Disposición DISPO-2022-7-E-CAT-DPA#MEC de fecha 16 de noviembre de 2022.

MODALIDAD DE CONTRATACIÓN:

Artículo 6º: El presente Concurso de Precios se regirá por la modalidad Compra Determinada, según lo establecido en el Reglamento Parcial N.º 2 de la Ley N.º 4938 – Anexo I – Decreto Acuerdo N.º 1127/2020, Art. 22º inc. c), 25º, modificado por Decreto Acuerdo N.º 1573/2020, y Decreto Acuerdo N.º 2036/2020.-

MONEDA EN LA QUE SE ADMITIRÁN LAS OFERTAS:

Artículo 7º: Los importes que se oferten, podrán efectuarse en moneda de curso legal en nuestro país o en moneda extranjera siendo expresada en dólar estadounidense.

Al ser una contratación que permite la cotización en moneda extranjera (dólares) es de aplicación lo normado en el Articulo 14 –"CONVERSION DE LA MONEDA EXTRANJERA"- del Anexo I –Reglamento Parcial N.º 2 de la Ley 4938– Decreto Acuerdo N.º 1127/2020 y sus modificatorios. En todos los casos que corresponda la conversión se realizará al Tipo de Cambio Vendedor del Banco de la Nación Argentina (Fuente: Página oficial del Banco de la Nación Argentina "COTIZACIÓN DIVISAS")

RECEPCIÓN Y CONTENIDO DE LAS OFERTAS:

Artículo 8º: Serán admisibles únicamente las ofertas que se presenten hasta el día y hora que se indique en la convocatoria, a través del sistema electrónico de contrataciones COMPR.AR cuyo sitio de internet es: http://comprar.catamarca.gob.ar, utilizando el formulario electrónico que suministre el mismo y cumpliendo con todos los requerimientos de este Pliego de Bases y Condiciones Particulares, acompañando la documentación que la integre en soporte electrónico.

A fin de garantizar su validez, la oferta electrónicamente cargada deberá ser confirmada por el oferente quien podrá realizarla únicamente a través de un usuario habilitado para ello, conforme lo normado con el procedimiento de registración y autenticación de los usuarios de los proveedores. La presentación de la oferta significará de parte del oferente el pleno conocimiento y aceptación de las normas y cláusulas que rigen este procedimiento de selección. No será necesario acompañar este pliego firmado junto con la oferta.

Respecto al bien y servicio a proveer deberá indicar con la mayor precisión posible y sin lugar a interpretaciones ambiguas, las características técnicas que permitan individualizar lo cotizado; acompañar ficha técnica en idioma castellano e indicar expresamente Garantía Ofrecida; la Administración podrá requerir las aclaraciones que consideren necesarias.

La propuesta deberá indicar claramente Razón Social y CUIT del oferente. Cumpliendo asimismo con los siguientes requerimientos, acompañando la documentación que la integre en soporte electrónico:

a) Declaración Jurada de sometimiento expreso a la jurisdicción de los Tribunales Ordinarios de la Provincia de Catamarca con renuncia expresa al Fuero Federal y a cualquier otro fuero que pudiere corresponder, para la resolución de controversias motivadas por el contrato en cualquiera de sus etapas **(ANEXO II).**

b) Declaración Jurada del oferente, de no encontrarse incurso de ninguna de las causales de inhabilidad ni suspendido en el Registro de Proveedores del Estado Provincial para contratar con la provincia **(ANEXO III).**

c) Formulario de CONSTITUCIÓN DE DOMICILIO ESPECIAL ELECTRÓNICO que forma parte de estas bases como **(ANEXO IV)**.

d) Constancia de Inscripción vigente en los tributos nacionales ante la A.F.I.P.

e) Cédula Fiscal del Impuesto sobre los Ingresos Brutos o Convenio Multilateral vigente, en las que se acredite que se encuentra inscripto en la actividad/rubro objeto de la presente contratación.

f) Para las empresas locales que se encuentren inscriptas en el "Compre y Contrate Preferentemente Catamarqueño" deberán adjuntar Certificado de Empresa Local o Proveedor Local emitido por la Dirección Provincial de Comercio dependiente de la Subsecretaría de Industria y Comercio de la Provincia de Catamarca. En el supuesto de poseer trabajadores en relación de dependencia deberá agregar Certificado Compre Catamarqueño Anexo I- Punto II- Art 6° del Decreto Acuerdo N° 122/2001 Y 445/2002- Ley N° 5038, emitida por la Dirección de Inspección Laboral dependiente de la Subsecretaría de Trabajo y Previsión de la Provincia de Catamarca.

g) TASA RETRIBUTIVA DE SERVICIOS para el Concurso de Precios del CERO COMA CERO CINCO POR CIENTO (0,05%) calculado sobre el monto de la oferta de conformidad a lo establecido por el artículo 27º, I), b) de la Ley Impositiva Provincial Nº5734, vigente para el Ejercicio Fiscal 2022. El mismo se podrá generar y pagar en forma online a través de la de la página de Internet: https://dgrentas.arca.gob.ar/

h) Constitución de la GARANTÍA DE MANTENIMIENTO DE OFERTA por el plazo establecido en el artículo 10° del presente Pliego de Bases y Condiciones Particulares, o la constancia de haberla constituido. No podrá ser inferior al UNO POR CIENTO (1%) del monto mayor de la oferta y por todo el tiempo de mantenimiento de la oferta, la que deberá ser constituida de acuerdo a alguna de las formas que se establece en el artículo 23°.

La indicada Garantía debe ser acompañada con un sellado provincial equivalente al CERO COMA SEIS POR CIENTO (0,60%) sobre el monto de la Garantía de Mantenimiento de Oferta cuando esta sea constituida por medio de avales y demás garantías personales o seguro de caución, de conformidad a lo establecido por el artículo 19º Inc. 6 de la Ley Impositiva Provincial Nº5734 vigente para el Ejercicio Fiscal 2022. El mismo se podrá generar y pagar en forma online a través de la de la página de Internet: https://dgrentas.arca.gob.ar/.

La presente garantía no corresponderá en caso de presentarse alguna de las excepciones previstas en el artículo 24° del presente pliego.

i) Se constatará que el oferente se encuentre con estado Inscripto en el Registro de Proveedores del Estado Provincial, en el rubro que corresponda con el objeto de la presente contratación. La Comisión Evaluadora, verificará la vigencia y validez del estado de Inscripción en el Registro de Proveedores del Estado Provincial.

Además de los documentos digitales adjuntos en la oferta, el documento físico (cuando correspondiere) deberá ser presentado en Mesa de Entrada y Salidas de la Dirección Provincial de Administración de la Secretaría de Finanzas Públicas, Sarmiento 589, 5to piso -S.F.V. Catamarca,

dentro de los tres (3) días hábiles posteriores al día establecido para la apertura de ofertas, en el horario de 8:00 a 13:00hs., salvo las garantías suscriptas con firma digital o electrónica.

En caso de OFERENTES NO INSCRIPTOS, la sola presentación de oferta, implicará solicitud de inscripción en el Registro de Proveedores del Estado Provincial, debiendo el oferente completar la documentación pertinente dentro de los CINCO (5) días corridos posteriores a la fecha del acto de apertura. Si el oferente no cumpliera, se tendrá por no inscripto y la oferta como no presentada.

FORMA DE COTIZACIÓN:

Artículo 9º: Se deberá cotizar utilizando el Sistema Electrónico de Contrataciones de la Administración Provincial "COMPR.AR", cuyo sitio de internet es: http://comprar.catamarca.gob.ar, conforme al formulario electrónico que suministre dicho portal; y conforme a los ítems detallados en el ANEXO I adjunto al presente. La cotización será por ítem o renglón completo, especificando Precio Unitario y Total en números, y redactado en letras en idioma nacional. Si el total cotizado para cada ítem o renglón no respondieran al precio unitario, se tomará este último como precio cotizado.

Los precios establecidos en las propuestas serán invariables. Los proponentes estarán obligados a mantener sus ofertas durante el plazo que se establece en la presente Bases de Condiciones, Plazo que se empezará a contar desde la fecha de Apertura de las Propuestas. El precio cotizado será el precio final que deba pagar el organismo contratante por todo concepto.

En el caso que existan cotizaciones en monedas distintas se homogeneizaran las mismas, con el fin de poder hacer una comparación adecuada; el valor de cotización será el del Tipo de Cambio Vendedor del Banco de la Nación Argentina del día anterior al acto de apertura donde quede fijado el precio (Fuente: Página oficial del Banco de la Nación Argentina "COTIZACIÓN DIVISAS").

No se aceptará la posibilidad de presentar ofertas parciales.

Los descuentos que se ofrezcan por pago dentro de un plazo determinado, no serán considerados a los efectos de la comparación de las ofertas, debiendo no obstante ser tenidos en cuenta para el pago, si la cancelación de las facturas se efectúa dentro de los términos fijados.

MANTENIMIENTO DE LA OFERTA:

Artículo 10º: Los Oferentes están obligados a mantener sus ofertas por un plazo no inferior a **treinta (30) días hábiles** contados a partir del día de la apertura. El plazo otorgado por el oferente deberá especificarse en la oferta, caso contrario se considerará como aceptado el indicado en el presente Artículo. El plazo se considerará prorrogado automáticamente por igual periodo, siempre que el oferente no manifieste lo contrario con una antelación de cinco (5) días corridos de producirse el vencimiento del plazo de mantenimiento de oferta, mediante nota.

NOTIFICACIONES Y COMUNICACIONES:

Artículo 11º: Todas las notificaciones entre la entidad contratante y los interesados, oferentes, adjudicatarios o cocontratantes, deberán realizarse en el domicilio especial electrónico constituido, para el caso del proveedor el que sea publicada en el perfil del mismo en el sistema COMPR.AR. y para el caso de la administración a compras.saf9mecon@gmail.com. Dichas notificaciones serán válidas desde el día en que fueron enviadas, sirviendo de prueba suficiente la constancia que el correo electrónico genere para el emisor.

La no recepción oportuna de correos electrónicos de alerta que envía el Sistema Electrónico de Contrataciones COMPR.AR, no justificará ni se considerará como causal suficiente para eximir a los proponentes de sus cargas y responsabilidades.

PLAZO DE ENTREGA:

Artículo 12º: El plazo de entrega de los bienes (Ítem 1) y de inicio de prestación del servicio (Ítem 2), no podrá ser superior a los **SETENTA (70) días hábiles** a partir de la fecha de difusión de la respectiva Orden de Compra en el sitio https://comprar.catamarca.gob.ar o en el que en un futuro lo reemplace o su notificación a la casilla de correo electrónico publicada en el perfil del proveedor en el sistema COMPR.AR., constituido como domicilio especial electrónico por el mismo.

Cuando en una oferta no se fije expresamente el plazo de entrega, se entiende que se ajusta al plazo máximo admitido en la presente Base de Condiciones. Asimismo, cuando el oferente indicare un plazo de entrega sin indicar "hábiles", a todos los efectos y principalmente en la puntuación del factor y su comparación con las demás ofertas, se considerará que ofertó dicho plazo en días hábiles. -

LUGAR Y FORMA DE ENTREGA:

Artículo 13º: la entrega de los bienes (ítem 1) se efectuará en UNA (01) única provisión, para el servicio (ítem 2) durante DOCE (12) meses contados a partir de la fecha de inicio de la prestación del mismo, en la Secretaría de Modernización del Ministerio de Economía, sito en Av. Venezuela S/N° - C.A.P.E. Pabellón 21, San Fernando del Valle de Catamarca, en el horario de 08:00 a 12:00 hs., conforme al plazo ofrecido por el oferente adjudicado que se ajuste a lo solicitado, corriendo los gastos de flete, acarreo, carga, descarga y seguro por cuenta del adjudicatario. Se presentará Remito que deberá cumplimentar lo dispuesto por la R.G. AFIP 1415/03, sin excepción.

CAUSALES DE INADMISIBILIDAD:

Artículo 14º: Serán causales de inadmisibilidad de las propuestas, las siguientes:

a) Cuando la oferta no fuera remitida por el sistema electrónico de compras (COMPR.AR).

b) Que fuera formulada por personas inhabilitadas o suspendidas para contratar con la Provincia.

c) Que fuera condicionada.

d) Que contuviere cláusulas en contraposición con las normas que rigen la contratación.

e) Si el precio cotizado mereciera la calificación de vil o no serio.

f) No indicar marca comercial del ítem ofertado en el formulario del Sistema Electrónico de Contrataciones de la Administración Provincial COMPR.AR.

g) Que el oferente no estuviere inscripto en el Registro de Proveedores del Estado Provincial, a la fecha de emisión del Dictamen de Evaluación, salvo las excepciones expresamente previstas.

Los errores intrascendentes de forma no serán causales de inadmisibilidad de la oferta.

Cualquiera de las Causales de Inadmisibilidad establecidas, y que pasará inadvertida en el acto de Apertura de las propuestas, podrá surtir efecto durante el estudio de las mismas y hasta la adjudicación.

DE LA PREADJUDICACION:

Artículo 15º: La pre adjudicación será por total ofertado, es decir que la pre adjudicación total de ambos ítems será a un mismo oferente cuya oferta se ajuste a lo solicitado, considerando la evaluación y orden de mérito indicadas en el Art. 16° de las presentes bases de condiciones.

EVALUACION Y ORDEN DE MERITO:

Artículo 16º: Luego de presentada la propuesta será analizada por La Comisión Evaluadora, adjuntándose informe sobre el cumplimiento total de los requisitos solicitados, como así también el Informe Técnico correspondiente emitido por la Secretaría de Modernización.

Entre las ofertas que se ajusten a lo solicitado, se adjudicará la oferta más conveniente teniendo en cuenta:

PARÁMETROS DE EVALUACIÓN DE LAS OFERTAS:

A efectos de determinar la propuesta más conveniente, se elaborará el cuadro comparativo de las propuestas en función de los parámetros objetivos de valoración que se establecen a continuación, el máximo puntaje que se podrá obtener es de 100 puntos distribuidos en:

A) PRECIO DEL BIEN A PROVEER.....OCHENTA (80) PUNTOS
B) CALIDAD DE LOS BIENES A PROVEER ..... DIEZ (10) PUNTOS
C) ANTECEDENTES COMO PROVEEDOR EN EL REGISTRO DE PROVEEDORES LOCAL..... CINCO (05) PUNTOS
D) PLAZO DE ENTREGA..... CINCO (05) PUNTOS
TOTAL... CIEN (100) PUNTOS

A los fines de lo precedentemente mencionado, la metodología a emplear para la ponderación de los factores será la siguiente:

A) PRECIO DEL BIEN A PROVEER (80 PUNTOS): En lo que respecta a este factor, la cuantificación se realizará mediante el producto entre el menor precio ponderado computable por el mayor puntaje asignado al factor a que se hace referencia; el resultado obtenido se dividirá por cada uno de los precios ponderados computables presentados, siempre en relación con el precio unitario de cada uno de los elementos a proveer:

$$\frac{\text{Menor Precio Ponderado Computable x Mayor Puntaje Asignado al factor (80) Precio Ponderado Computable de cada Oferta a Considerar}}{}$$

En caso de corresponder, se aplicará lo establecido en el Anexo I del Decreto Acuerdo N° 445/02 - Instructivo para la aplicación de la Ley N 5038 "Compre y Contrate preferentemente catamarqueño" y Decreto Acuerdo Reglamentario N° 1122/01.

B) CALIDAD DE LOS BIENES A PROVEER (10 PUNTOS): En cuanto a este factor, la puntuación se realizará tomando como base la calidad de los bienes ofrecidos en cuanto a si cumple con las cualidades solicitadas, se calificará de acuerdo a la siguiente escala:

MUY BUENO…….10 PUNTOS
BUENO..... 04 PUNTOS

C) ANTECEDENTE COMO PROVEEDOR EN EL REGISTRO DE PROVEEDORES (05 PUNTOS)

LOCAL: Se atribuirá los puntajes en función de las penalidades y sanciones establecidas en el TÍTULO IV, CAPÍTULO I y II (artículos 110° a 123°) del Anexo I - Reglamento Parcial Nº 2 de la Ley 4938 - Decreto Acuerdo Nº 1127 y modificatorios, que informe oportunamente el Registro de Proveedores del Estado Provincial, en la siguiente forma:

1) A los oferentes y/o proveedores que no hayan incurrido en alguna de las penalidades y sanciones previstas en el TÍTULO IV, CAPÍTULO I y II (artículos 114° a 123°) del Anexo I - Reglamento Parcial Nº 2 de la Ley 4938 - Decreto Acuerdo Nº 1127 y modificatorios, se le otorgará: CINCO (5) PUNTOS.

2) A los que hayan incurrido en penalidades por aplicación de lo dispuesto en los artículos 110 y 111° del Anexo I - Reglamento Parcial Nº 2 de la Ley 4938 - Decreto Acuerdo Nº 1127 y modificatorios, se le otorgará: TRES (3) PUNTOS.

3) A los oferentes y/o proveedores que hayan incurrido en sanciones de suspensión y/o inhabilitación, conforme lo dispuesto en los artículos 114° a 123° del Anexo I – Reglamento Parcial

Nº 2 de la Ley 4938 - Decreto Acuerdo Nº 1127 y modificatorios, según lo informado oportunamente por el Registro de Proveedores del Estado Provincial: UNO (1) PUNTO.

D) PLAZO DE ENTREGA (05 PUNTOS): Se asignará el mayor puntaje a la oferta que, siendo formal y técnicamente admisible, indique menor plazo de entrega al establecido en el presente Pliego de Bases y Condiciones Particulares; y a las restantes ofertas el puntaje que resulte de aplicar una regla de tres simple, de acuerdo a la siguiente fórmula:

$$\frac{\text{Menor Plazo de Entrega x Mayor Puntaje Asignado al factor (05)}}{\text{Plazo de Entrega a Considerar}}$$

ADJUDICACIÓN

ARTÍCULO 17°: La adjudicación será decidida por la autoridad competente conforme lo establecido en el Anexo I -Reglamento Parcial Nº 2 de la Ley 4938- del Decreto Acuerdo N° 1127/20 y modificatorios, y sobre la base del dictamen de la Comisión Evaluadora. Si la adjudicación fuera distinta a la aconsejada por la Comisión, deberá fundamentar dicha decisión. Podrá adjudicarse aun cuando se haya presentado una sola oferta. La autoridad facultada para adjudicar podrá rechazar todas las propuestas, sin que el adjudicatario tenga derecho a exigir indemnización o diferencia de precio. Se resolverá dentro del plazo de mantenimiento de las propuestas y recaerá en la propuesta que sea considerada más conveniente, de acuerdo a la normativa aplicable. La adjudicación será notificada dentro de los TRES (3) DÍAS de dictado el acto respectivo, mediante la difusión en el sitio de internet es: http://comprar.catamarca.gob.ar y se enviarán los avisos pertinentes mediante el sistema de mensajería automático de COMPR.AR.

DE LA ORDEN DE COMPRA:

Artículo 18º: La Orden de Compra será emitida dentro de los Cinco (5) días corridos de resuelta la adjudicación y deberá contener las estipulaciones básicas de la contratación. En caso de errores u omisión, el adjudicatario deberá ponerlo en conocimiento del organismo que lo expidió, sin perjuicio de cumplir el Contrato conforme a las bases de contratación y a la oferta adjudicada.

Su notificación será mediante la difusión en el sitio https://comprar.catamarca.gob.ar o en el que en un futuro lo reemplace o en el domicilio especial electrónico constituido por el adjudicatario (ANEXO IV) lo que producirá el perfeccionamiento del contrato.

RECEPCIÓN DE LOS BIENES:

Artículo 19º: La recepción se considerará efectuada, y definitiva, una vez verificada la misma y comprobada la calidad del bien adjudicado, la que se acordará dentro de los diez (10) días, el que se contará a partir del día siguiente al de la fecha de entrega de los elementos, de conformidad a lo dictado en el Art. 95º del Anexo I - Reglamento Parcial Nº 2 de la Ley Nº 4938 aprobado por el Decreto Acuerdo N° 1127/2020.

PERFECCIONAMIENTO DEL CONTRATO - FACTURACION Y PAGO:

Artículo 20º: La facturación debe realizarse a la CUIT de la JURISDICCION SOLICITANTE, consignada en el encabezado de la presente Bases y serán presentadas para su cobro en el domicilio físico de la misma UNIDAD, juntamente con la Orden de Compra y constancia de la recepción definitiva de los bienes o servicios, según los plazos de normativa vigente. Dicha factura deberá reunir los requisitos legales que rigen su emisión.

El pago se realizará dentro de los TREINTA (30) días corridos de la recepción definitiva de los bienes solicitados.

El oferente en su oferta deberá adherir a la presente forma y plazo de pago, en el caso de no especificarla en su oferta se entiende que adhiere y ajusta a la forma y plazo de pago consignado en el presente artículo.

Si la facturación fuera en Moneda Extranjera, se convertirá al Tipo de Cambio Vendedor del Banco de la Nación Argentina del día anterior a la emisión de la Orden de Pago (Fuente: Página oficial del Banco de la Nación Argentina "COTIZACIÓN DIVISAS").

ANTICIPO FINANCIERO DEL ITEM N.º 2

ARTICULO 21º: El proveedor podrá solicitar al momento de realizar su oferta un anticipo financiero, indicando el monto del mismo. En caso que éste sea aprobado por la administración, deberá constituir una **CONTRAGARANTÍA** por el equivalente a los montos que reciba el co-contratante como adelanto, indicando como plazo "hasta la extinción de las obligaciones contractuales" conforme lo establece el artículo 84° inc. c) del Anexo I –Reglamento Parcial N.º 2 de la Ley 4938– Decreto Acuerdo N.º 1127 y modificatorios.

De corresponder deberá acompañar la constancia del pago del Impuesto a los Sellos equivalente al Cero coma sesenta por ciento (0,60%) sobre la Contragarantía cuando esta sea constituida por medio de avales y demás garantías personales o seguro de caución, de conformidad a lo establecido por el artículo 19º Inc. 6 de la Ley Impositiva Provincial N.º 5734 vigente para el Ejercicio Fiscal 2022. El mismo se podrá generar y pagar en forma online a través de la página de Internet: https://dgrentas.arca.gob.ar/

Para percibir el anticipo, el adjudicatario previamente debe presentar una factura o documento equivalente, por el importe acordado en concepto de anticipo, y la constancia de haber constituido la contragarantía, en la forma establecida por el artículo 23° de las presentes bases de condiciones. Los pagos anticipados serán descontados del total a pagar al momento de la cancelación del contrato.

GARANTÍA DE CUMPLIMIENTO DEL CONTRATO

Artículo 22º: Para afianzar el cumplimiento de todas las obligaciones, el oferente que hubiera resultado adjudicatario, deberá constituir, una GARANTÍA DE CUMPLIMIENTO DE CONTRATO del TRES POR CIENTO (3%) del valor total de la adjudicación, dentro de los CINCO (5) DÍAS contados a partir del perfeccionamiento del contrato. Conforme lo establece los artículos 83° y 84° inc. b) del Anexo I –Reglamento Parcial N.º 2 de la Ley 4938– Decreto Acuerdo N.º 1127 y modificatorios.

La indicada Garantía debe ser acompañada con un sellado provincial equivalente al CERO COMA SEIS POR CIENTO (0,60%) sobre el monto de la Garantía de Mantenimiento del Contrato cuando esta sea constituida por medio de avales y demás garantías personales o seguro de caución, de conformidad a lo establecido por el artículo 19º Inc. 6 de la Ley Impositiva Provincial Nº5734 vigente para el Ejercicio Fiscal 2022. El mismo se podrá generar y pagar en forma online a través de la de la página de Internet: https://dgrentas.arca.gob.ar/.

La integración de la GARANTÍA DE CUMPLIMIENTO DE CONTRATO prevista precedentemente, se realizará por alguno de los medios de garantía establecidos en el artículo 23° del presente pliego de condiciones particulares.

La garantía se deberá constituir en la misma moneda en que se hubiere hecho la oferta. Cuando la cotización se hiciere en moneda extranjera y la garantía se constituyera en efectivo o cheque, el importe de la garantía deberá consignarse en moneda nacional y se utilizará el Tipo de Cambio

Vendedor Banco de la Nación Argentina del día anterior a la constitución de la misma (Fuente: Página oficial del Banco de la Nación Argentina "COTIZACIÓN DIVISAS").

La presente garantía no corresponderá en caso de presentarse alguna de las excepciones previstas en el artículo 24° del presente pliego.

FORMAS DE PRESENTACIÓN DE LA GARANTÍA:

Artículo 23º: Las GARANTÍAS a las que hace referencia el presente Pliego de Bases y Condiciones Particulares, en el caso de corresponder, podrán constituirse de las siguientes formas, o combinaciones de ellas, según lo previsto por el Artículo 85º del Anexo I - Reglamento Parcial N.º 2 del Decreto Acuerdo N.º 1127/2020 y sus modificatorios:

a) En efectivo, exclusivamente mediante depósito o transferencia bancaria en la cuenta oficial de la Tesorería General de la Provincia N°46600695-38 del Banco de la Nación Argentina - Sucursal Catamarca (3155). CBU 0110466420046600695387 – CUIT 30-63651135-4

b) Con cheque certificado contra una entidad bancaria, que opere preferentemente en la ciudad de San Fernando del Valle de Catamarca. El organismo depositará el cheque dentro de los plazos que rijan para estas operaciones.

c) Con títulos públicos emitidos por el Estado Nacional y/o Provincial. Los mismos deberán ser depositados en una entidad bancaria a la orden del organismo contratante, identificándose el procedimiento de selección de que se trate. El monto se calculará tomando en cuenta la cotización de los títulos al cierre del penúltimo día hábil anterior a la constitución de la garantía en la Bolsa o Mercado correspondiente, lo que deberá ser certificado por las autoridades bancarias al recibir dicho depósito. En caso de liquidación de los valores a que se refiere este inciso, se formulará cargo por los gastos que ello ocasione. El eventual excedente quedará sujeto a las disposiciones que rigen la devolución de garantías.

d) Con fianza bancaria, constituyéndose el fiador en deudor solidario, liso y llano y principal pagador con renuncia a los beneficios de división y excusión en los términos del Artículo N° 1574 y concordantes del Código Civil y Comercial de la Nación, así como al beneficio de interpelación judicial previa.

e) Con seguro de caución, mediante pólizas aprobadas por la Superintendencia de Seguros de la Nación, extendidas a favor del organismo contratante.

f) Mediante la afectación de créditos que el proponente o adjudicatario tenga liquidados y al cobro en un organismo provincial, a cuyo efecto el interesado deberá presentar, en la fecha de la constitución de la garantía, la cesión pertinente.

g) Con pagaré sin protesto suscriptos por quienes tengan el uso de la firma social o actuaren con poder suficiente, cuando el monto de la garantía no supere el valor de VEINTE (20) MÓDULOS.

h) Toda otra garantía que, a propuesta del Organismo contratante, disponga por acto administrativo la Contaduría General de la Provincia.

Se deberá tener en cuenta lo establecido en la Ley Impositiva Provincial N.º 5734 vigente para el Ejercicio Fiscal 2022, impuesto de sellos. El mismo se podrá generar y pagar en forma online a través de la de la página de Internet: https://dgrentas.arca.gob.ar/. Cuando estos sean repuestos en estampillas fiscales, y el soporte físico de las garantías establecidas precedentes, deberán ser presentados en forma digital junto a la oferta y además físicamente en Mesa de Entrada y Salidas de la Dirección Provincial de Administración de la Secretaría de Finanzas Públicas, Sarmiento 589, 5to piso -S.F.V. Catamarca, dentro de los TRES (3) días hábiles posteriores al día establecido para la presentación de la garantía, en el horario de 8:00 a 12:30hs.

EXCEPCIONES A LA OBLIGACIÓN DE PRESENTAR GARANTÍAS DE MANTENIMIENTO DE OFERTA Y DE CUMPLIMIENTO DE CONTRATO:

Artículo 24º: Conforme lo establece el artículo 87° del Decreto Acuerdo N.º 1127, Anexo I y sus modificatorios –Reglamento Parcial N.º 2 de la Ley 4938:

a) En la adquisición de publicaciones periódicas.

b) En las contrataciones de avisos publicitarios.

c) En las locaciones de inmuebles o leasings, cuando la provincia actúe como locatario.

d) Cuando el monto de la garantía no fuere superior a DIEZ (10) Módulos. Siendo el Valor Actual de cada Módulo $18.032 (Res. CGP 29/2022).

e) Ejecución de la prestación dentro del plazo de integración de la garantía.

f) Cuando el oferente o adjudicatario sea un organismo nacional, provincial o municipal o Sociedades del Estado Provincial.

g) Cuando se abonen anticipos utilizando medios electrónicos de pago que garanticen por sí la devolución del dinero en caso de incumplimiento del tercero receptor de los fondos, en los casos específicos que autorice el Órgano Rector del Sistema de Contrataciones.

SANCIONES:

Artículo 25º: El incumplimiento de las obligaciones contraídas por los proponentes o adjudicatarios a la Contratación en particular y el reglamento de contrataciones en su caso, dará lugar a la aplicación de las penalidades y sanciones, previstas en el Titulo IV - Anexo I - Reglamento Parcial N.º 2 de la Ley 4938 del Decreto Acuerdo N.º 1127/2020.

PROVINCIA DE CATAMARCA
CONCURSO DE PRECIO N.º 9-0001-CPR22
MODALIDAD – COMPRA DETERMINADA
EX-2022-02217374- -CAT-DC#MEC

ANEXO I
DETALLE DE BIENES SOLICITADOS Y ESPECIFICACIONES TECNICAS

ITEM	DESCRIPCION (CODIGO)	DETALLE	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA
01	4.3.6 - 6186.116	SERVIDORES; TIPO: PARA FIREWALLS (CORTAFUEGOS), CODIGO ETAP: SR-005, VERSION ETAP: 23.0	UNIDAD	1
02	4.8.1-1748.1115	LICENCIAS; NOMBRE DEL PRODUCTO: FORTINET, VERSION: 600E, CANT. DE USUARIOS: SEGÚN PLIEGO	SERVICIO	12

LUGAR DE ENTREGA: Secretaría de Modernización (Ministerio de Economía), Av. Venezuela S/N – CAPE Pabellón 21.

ADQUISICIÓN DE FIREWALL CON LICENCIAMIENTO PARA LA PROTECCIÓN DE LOS DIFERENTES EQUIPOS Y SISTEMAS ADMINISTRADOS POR LA SECRETARIA DE MODERNIZACION

- El equipamiento ofrecido deberá estar acompañado de Folletos ilustrativos o ficha técnica en idioma castellano con características y especificaciones técnicas, y todo otro detalle que permita individualizar lo cotizado, manuales, imágenes, etc.
- La totalidad de los gastos relacionados al embalaje, transporte, manipulación y la logística de los materiales a entregar en la presente Contratación, serán por cuenta y cargo del adjudicatario.
- Queda bajo responsabilidad del adjudicatario los daños que se produjeran como consecuencias del traslado o embalajes defectuosos.
- Condición de calidad: los bienes requeridos para dar cumplimiento al objeto del presente anexo deberán ser nuevos, sin uso, libre de defectos en el diseño, materiales o de fabricación de acuerdo a las especificaciones técnicas descriptas. –
- *Aclaración:* Cuando en el presente anexo se mencione "marca" o "tipo" (s/art. 38°- Decreto Acuerdo N° 1127/20 Reglamento Parcial Nº 2 de la Ley Nº 4938), será al solo efecto de señalar características generales del objeto pedido sin que ello implique que no podrán proponerse artículos similares de otras marcas o tipos.

ITEM 01: DISPOSITIVO FIREWALL

INDICAR MARCA COMERCIAL Y MODELO DE PRODUCTO COTIZADO POR ÍTEM. No indicar la marca comercial del producto cotizado hará que la oferta formulada para el ítem en cuestión se la considere como que **"NO SE AJUSTA A LO SOLICITADO"** e implicará la **DESESTIMACIÓN** de la oferta.
Con respecto a la Garantía: Ofrecer **GARANTÍA** de buen funcionamiento: Mínima de DOCE (12) meses, sobre fallas o problemas de fabricación.

a) CARACTERÍSTICAS DEL EQUIPAMIENTO
El equipamiento debe permitir el rackeo en racks estándar de 19 pulgadas, con fuentes AC 220V, 50Hz y cables de energía norma IRAM, fuentes de alimentación redundantes, al menos, en esquema 1+1 o superior.
Al menos dos (2) interfaces de 10Gbps SFP+, al menos ocho (8) interfaces de 1Gbps SFP, al menos ocho (8) interfaces de 1Gbps 1000baseTX.
Al menos uno (1) interfaz de consola RS232
Performance y dimensionamiento de los equipamientos remotos
El equipamiento deberá poder conmutar al menos, 36 Gbps de tráfico del tipo IPv4 con paquetes de un tamaño de 1514 bytes y políticas de firewall activas.
El equipamiento deberá poder establecer al menos 450.000 nuevas sesiones TCP por segundo.
El equipamiento deberá poder mantener al menos 8.000.000 de sesiones activas establecidas.
El equipamiento deberá poder establecer y mantener al menos, 2000 túneles IPSec y soportar al menos 20Gbps IPSec AES256-SHA256.

b) REQUISITOS MÍNIMOS DE FUNCIONALIDAD
Características Generales
1. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo;
2. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
3. Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
4. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
5. La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
6. Los dispositivos de protección de red deben soportar:
- 4094 VLANsTags 802.1q;
- agregación de enlaces 802.3ad y LACP;
- Policy based routing y policy based forwarding;
- encaminamiento de multicast (PIM-SM y PIM-DM);
7. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
8. Debe ser compatible con NAT64 y NAT46;

9. Debe implementar el protocolo ECMP;
10. Debe soportar SD-WAN de forma nativa;
11. Debe soportar el balanceo de enlace hash por IP de origen;
12. Debe soportar el balanceo de enlace por hash de IP de origen y destino;
13. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
14. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
15. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
16. Enviar logs a sistemas de gestión externos simultáneamente a través de TCP y SSL;
17. Debe soporta protección contra la suplantación de identidad (anti-spoofing);
18. Implementar la optimización del tráfico entre dos dispositivos;
19. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
20. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
21. Soportar OSPF gracefulrestart;
22. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
23. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
24. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
25. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
26. Debe soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
27. Debe soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
28. Debe soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster;
29. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
30. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
31. La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
32. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
33. Debe soportar la creación de sistemas virtuales en el mismo equipo;
34. Para una alta disponibilidad, el uso de clústeres virtuales debe de ser posible, ya sea activo-activo
o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
35. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
36. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
37. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados

directamente en los sistemas virtuales (contextos);
38. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
39. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
40. Debe existir la opción de un servicio de soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
41. La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.
42. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas
43. Control por Política de Firewall:
* Debe soportar controles de zona de seguridad;
* Debe permitir la creación de políticas de control por puerto y protocolo;
* Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
* Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
* Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
* Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, e implementar acciones (notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública).
* Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato CommonEventFormat (CEF);
* Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, VmwareESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
* Debe soportar el protocolo estándar de la industria VXLAN;
* La solución debe permitir la implementación sin asistencia de SD-WAN
* En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
* La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.
44. Control de Aplicación:
* Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
* Detección de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
* Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpcover http, gotomeeting, webex, evernote, googledocs;

* Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
* Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
* Actualización de la base de firmas de la aplicación de forma automática;
* Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
* Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
* Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
* El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
* Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
* Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
* Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
* Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
45. Prevención de Amenazas
* Deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo, las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
* Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
* Deber permitir el bloqueo de vulnerabilidades y exploitsconocidos, protección contra ataques de denegación de servicio;
* Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, Análisis para detectar anomalías de protocolo, Desfragmentación IP, Reensamblado de paquetes TCP, Bloqueo de paquetes con formato incorrecto (malformedpackets);
* Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;
* Detectar y bloquear los escaneos de puertos de origen, (worms) conocidos ,dos y ddos
* Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
* Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
* Identificar y bloquear la comunicación con redes de bots;
* Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
* Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
* Los eventos deben identificar el país que origino la amenaza;

* Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
* Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
* Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
* En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
* Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
46. Filtrado de URL
* Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
* Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
* Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
* Tener por lo menos 75 categorías de URL;
* Debe tener la funcionalidad de exclusión de URLs por categoría;
* Permitir página de bloqueo personalizada;
* Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
* Además del Explicit Web Proxy, soportar proxy web transparente;
47. Identificación de Usuarios
* Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
* Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;
* Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
* Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;
* Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basados en usuarios y grupos de usuarios;
* Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);

* Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
* Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP/AD;
* Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
* Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
48. QoS TrafficShaping
* Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
* Soportar la creación de políticas de QoS y TrafficShaping por dirección de origen;
* Soportar la creación de políticas de QoS y TrafficShaping por dirección de destino;
* Soportar la creación de políticas de QoS y TrafficShaping por usuario y grupo;
* Soportar la creación de políticas de QoS y TrafficShaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
* Soportar la creación de políticas de calidad de servicio y TrafficShaping por puerto;
* En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
* En QoS debe permitir la definición de tráfico con máximo ancho de banda;
* En QoS debe permitir la definición de colas de prioridad;
* Soportar marcación de paquetes DiffServ, incluso por aplicación;
* Soportar la modificación de los valores de DSCP para Diffserv;
* Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
* Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;
49. Filtro de Datos
* Permite la creación de filtros para archivos y datos predefinidos;
* Los archivos deben ser identificados por tamaño y tipo;
* Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
* Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
* Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
* Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;
50. Geo Localización
* Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
* Debe permitir la visualización de los países de origen y destino en los registros de acceso;
51. VPN
* Soporte VPN de sitio-a-sitio y cliente-a-sitio;

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

52. Wireless Controller

* Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);
* Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
* La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;
* El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;
* La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;
* Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;
* El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;
* Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;
* Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;
* Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación

entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;

* La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;

* La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;

* La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;

* La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;

* La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;

* La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;

* La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;

* La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Backgroundscanning. Cuando se realiza a través de Off-channel / Backgroundscanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;

* La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;

* La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;

* La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;

* La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;

* La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;

* Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;

* La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como FastRoaming;
* La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;
* La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectado mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
* La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;
* La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;
* La solución debe implementar técnicas de CallAdmission Control para limitar el número de llamadas simultáneas;
* La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;
* Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;
* La solución debe permitir la configuración de los datarates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;
* La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;
* La solución debe soportar la característica que ignore ProbeRequests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los ProbeRequests sean ignorados;
* La solución debe permitir la configuración del valor de Short GuardInterval para 802.11n y 802.11ac en 5GHz;
* La solución debe implementar una característica conocida como AirtimeFairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;
* La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;
* La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;
* La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep PacketInspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y

la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;
* La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;
* La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps ou Bps) para las aplicaciones reconocidas a través de la técnica de DPI;
* La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;
* La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:
- Ataques de flood contra el protocolo EAPOL (EAPOL Flooding);
- Los siguientes ataques de denegación de servicio: AssociationFlood, AuthenticationFlood, BroadcastDeauthentication y SpoofedDeauthentication;
- ASLEAP, Null Probe Response / Null SSID Probe Response, Long Duration, Ataques contra Wireless Bridges, Weak WEP, Invalid MAC OUI.
* La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication
* La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;
* La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;
* Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;
* Debe implementar la autenticación administrativa a través del protocolo RADIUS;
* En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
* En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;
* La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;
* Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;
* La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;
* La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;
* La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAPSIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
* La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocida como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;
* La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;

* La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;
* La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;
* La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;
* La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;
* La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;
* La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;
* Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;
* La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;
* La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;
* La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;
* La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;
* La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;
* La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;
* La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;
* La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;
* La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;
* La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);
* La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato.pcap;
* La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD; La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;
* La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;
* La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;
* La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;

* La solución debe tener herramientas de diagnóstico y depuración;
* La solución debe soportar la comunicación con elementos externos a través de las API;
* La solución deberá ser compatible y administrar los puntos de acceso de este proceso.

53. La solución deberá incluir el soporte para la transferencia de conocimientos para aplicar los siguientes requerimientos:

* Configuración básica del equipamiento.
* Registración del servicio.
* Actualización de SO.
* 3 interfaces, una WAN, LAN y DMZ
* 3 VLAN una por cada interface.
* Una zona de OSFP.
* 5 rutas estáticas.
* 5 zonas.
* 10 objetos de red/dispositivos.
* Reglas de Firewall, una de NAT para LAN, otra para DMZ, una de PAT y 5 reglas de publicación de servicios y 5 reglas de navegación a internet con 5 perfiles de seguridad.
* Un perfil de VPN con autenticación local, después el cliente realiza la integración con AD.
* 3 enlaces punto a punto.
* Testing de toda la solución.
* Documentación de toda la implementación con doce (12) horas de transferencia de conocimientos sobre las configuraciones aplicadas para cuatro (4) personas en modalidad remoto.
* Diez (10) horas de consultoría y soporte post implementación en horario laboral para consultas, resolución de problemas, etc.

54.Garantía de funcionamiento

* 12 meses

<u>ITEM 02:</u> LICENCIA PARA FIREWALL

Se requiere un servicio de primera calidad, por DOCE (12) meses con opción a prórroga a final del mismo, por igual periodo de tiempo.

* Durante un (1) año se deberá garantizar la actualización automática de la base de firmas/vulnerabilidades y vacunas en forma periódica o cuando la situación así lo amerite.
* Cuando se publique alguna nueva forma de ataque/vulnerabilidad deberá ser aplicada inmediatamente sobre este equipo en forma automática y sin interrupción del servicio.
* Deberá tener protección por un (1) año basada en servicios de reputación IP, categorización de URLs, geolocalización, aplicaciones y DNS para detectar y eliminar conexiones de origen maliciosas con verificación diaria de nuevas actualizaciones.

ANEXO II
DECLARACIÓN JURADA DE DOMICILIO Y FUERO

San Fernando del Valle de Catamarca, ……

Por la presente, para todas las cuestiones judiciales, nos sometemos a los tribunales ordinarios de la Provincia de Catamarca, con renuncia expresa a cualquier otro fuero o jurisdicción. Para ello, deberemos agotar los reclamos de la vía administrativa.

Manifiesto:

☐ Domicilio Real: ……..
☐ Domicilio Comercial: ……

Asimismo, aclaramos que constituimos domicilio especial en la ciudad de San Fernando del Valle de Catamarca en…….

Firma del oferente: ……

Aclaración: …….

ANEXO III
DECLARACIÓN JURADA DE INEXISTENCIA DE CAUSALES DE INHIBICIÓN

San Fernando del Valle de Catamarca, …….

Declaramos bajo juramento que la Firma ……

1. No se encuentra inhibida para disponer y gravar bienes registrables; ni en Concurso Preventivo, Quiebra o Liquidación.

2. Asimismo, manifiesto en carácter de declaración jurada, de no estar incurso en ninguna de las causales de inhabilidad para contratar con la Provincia, ni suspendido en el Registro de Proveedores del Estado Provincial para contratar con la provincia, conforme a la normativa vigente.

Firma del oferente: ……

Aclaración: …….

ANEXO IV

CONSTITUCIÓN DE DOMICILIO ESPECIAL ELECTRÓNICO

En mi carácter de…… de la firma.....CUIT/CUIL/CDI Nº ……..……, constituyo como domicilio especial electrónico…… conforme a lo dispuesto en el 4° párrafo Artículo 104 BIS Ley 4938 y sus modificatorias; y artículo 15° del Anexo I - Reglamento Parcial Nº 2 de la Ley 4938- del Decreto Acuerdo N° 1127/20. A tal efecto, declaro aceptar en todos sus términos y condiciones que se indican a continuación:

PRIMERA: El domicilio especial electrónico constituido es de uso exclusivo de la razón social....., constituyéndome en custodio de la confidencialidad de la clave de acceso al mismo, obligándome a no ceder, transferir o comunicar bajo ninguna circunstancia la misma, asumiendo la autoría y plena responsabilidad por las ofertas, documentos y presentaciones que bajo esta casilla ingresen en el domicilio especial constituido por la administración provincial para la presente contratación. Por lo tanto, asumo las consecuencias de su divulgación a terceros, liberando a la PROVINCIA DE CATAMARCA de toda responsabilidad que de ello derive. Renuncio expresamente a oponer defensas basadas en la inexistencia o defecto del uso del domicilio especial electrónico constituido, o en la acreditación de la existencia de la información electrónica que provenga de su uso.

SEGUNDA: En los términos del 4° párrafo Artículo 104 BIS Ley 4938, sus modificatorias y del artículo 15° del Anexo I -Reglamento Parcial Nº 2 de la Ley 4938- del Decreto Acuerdo N° 1127/20; reconozco que el domicilio especial electrónico que constituyo en el presente formulario goza de validez y plena eficacia jurídica, y producirá en el ámbito administrativo los efectos del domicilio constituido; siendo válidos y plenamente eficaces las notificaciones, emplazamientos y comunicaciones practicadas allí.

TERCERA: Las presentaciones electrónicas por medio del domicilio especial electrónico constituido, no podrán revocarse bajo ninguna forma o medio a mi alcance.

CUARTA: Asumo la responsabilidad por el uso indebido o inadecuado del domicilio especial electrónico constituido, haciéndome cargo de todos los daños y perjuicios correspondientes, sin que ello obste la facultad de la Administración a implementar las sanciones o penalidades respectivas.

QUINTA: La PROVINCIA DE CATAMARCA no asume ninguna responsabilidad por los inconvenientes que tuviera con el software, hardware, servidores o nodos ajenos al mismo.

SEXTA: Acepto la prueba de la existencia de la documentación y comunicaciones electrónicas que surjan de los domicilios especiales electrónicos constituidos tanto por la Administración de la PROVINCIA DE CATAMARCA como el constituido en la presente declaración.

SEPTIMA: Dejo expresa constancia que de mi parte renuncio expresamente a oponer, en sede administrativa o judicial, defensas relacionadas con la inexistencia de firma ológrafa de todos los documentos que se envíen desde el domicilio especial electrónico que constituyo por la presente; considerándose que dichos documentos que son enviados desde el mismo contienen mi rubrica y por lo tanto tienen los mismos efectos que la firma ológrafa en papel.

Firma:

Apellido y Nombre completo:

Lugar y fecha:

Documento:

CUIT/CUIL/CDI:

***IMPORTANTE: EL PRESENTE ANEXO DEBERÁ ADJUNTARSE DE MANERA DIGITAL A LA PROPUESTA PRESENTADA, RUBRICADA (FIRMA Y ACLARACIÓN) DE PUÑO Y LETRA POR EL PROPIETARIO O REPRESENTANTE LEGAL DE LA FIRMA PROPONENTE.**

Gobierno de Catamarca
2022

Hoja Adicional de Firmas
Pliego Bases Cond Part

Número: PLIEG-2022-02239008-CAT-DC#MEC

SAN FERNANDO DEL VALLE DE CATAMARCA, CATAMARCA
Miércoles 16 de Noviembre de 2022

Referencia: Pliego de Bases y Condiciones Particulares - Adquisición de firewall con licenciamiento para la Sec. de Modernizacion - Concurso Precio - Modalidad Det.- Proceso 9-0001-CPR22

El documento fue importado por el sistema GEDO con un total de 26 pagina/s.

Digitally signed by GDECatamarca
DN: cn=GDECatamarca, c=AR, o=Tesoreria General de la Provincia, ou=Secretaria de Modernizacion del Estado de Catamarca, serialNumber=CUIT 30636511354
Date: 2022.11.16 10:07:48 -03'00'

Guillermo Salas
Director
Dirección de Compras - Dirección Provincial de Administración- Secretaria de Finanzas Públicas - MEC
Ministerio de Economía

Digitally signed by GDECatamarca
DN: cn=GDECatamarca, c=AR, o=Tesoreria General de la Provincia, ou=Secretaria de Modernizacion del Estado de Catamarca, serialNumber=CUIT 30636511354
Date: 2022.11.16 10:07:50 -03'00'