CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

CONTRATO DE COMPRAVENTA PARA **LA RENOVACIÓN DEL LICENCIAMIENTO PARA LA SEGURIDAD PERIMETRAL POR VEINTICUATRO MESES QUE INCLUYA PUESTA EN SITIO (PARTIDA "A") Y UN LICENCIAMIENTO DE ANTIVIRUS ENDPOINT DE SEGURIDAD PARA EL TRIBUNAL SUPERIOR DE JUSTICIA DEL ESTADO (PARTIDA "B")**, QUE CELEBRAN, POR UNA PARTE, EL **PODER JUDICIAL DEL ESTADO A TRAVÉS DEL TRIBUNAL SUPERIOR DE JUSTICIA,** REPRESENTADO POR LA **LICENCIADA EN ADMINISTRACIÓN MARIA CRISTINA SANCHEZ TELLO ZAPATA** TITULAR DE LA UNIDAD DE ADMINISTRACIÓN DEL TRIBUNAL SUPERIOR DE JUSTICIA DEL ESTADO DE YUCATÁN, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ **"EL TRIBUNAL SUPERIOR DE JUSTICIA"** Y, POR LA OTRA PARTE LA EMPRESA **AXTEL, S.A.B. DE C.V.,** REPRESENTADA POR EL CIUDADANO **MARCOS RODRIGO BAEZA MALDONADO** AL QUE SE NOMBRARÁ **"EL PROVEEDOR".**

DECLARACIONES

1. "EL TRIBUNAL SUPERIOR DE JUSTICIA" Declara:

1.1. Que de conformidad con lo establecido en el artículo 64 de la Constitución Política del Estado de Yucatán y 21 de la Ley Orgánica del Poder Judicial del Estado de Yucatán, el Tribunal Superior de Justicia es la autoridad máxima del Poder Judicial del Estado de Yucatán.

1.2. Que para la prestación del servicio de impartición de justicia, el Tribunal Superior de Justicia requiere la renovación del licenciamiento para la seguridad perimetral por veinticuatro meses que incluya puesta en sitio (partida "A") y un licenciamiento de antivirus endpoint de seguridad para el Tribunal Superior de Justicia del Estado (partida "B").

1.3. Que en la **Décimo Segunda** sesión **Ordinaria** del Comité de Adquisiciones, Arrendamientos, Servicios y Obra Pública del Tribunal Superior de Justicia del Estado de Yucatán, celebrada el día veinte de diciembre de dos mil veintitrés, en relación con la licitación pública número "PODJUDTSJ-CA 18/2023", se adjudicó a la empresa AXTEL, S.A.B. DE C.V. el contrato para la renovación del licenciamiento para la seguridad perimetral por veinticuatro meses que incluya puesta en sitio (partida "A") y un licenciamiento de antivirus endpoint de seguridad para el Tribunal Superior de Justicia del Estado (partida "B") de total conformidad con el Reglamento de Adquisiciones, Arrendamientos, Servicios y Obra Pública del Tribunal Superior de Justicia del Estado de Yucatán.

1.4. Que la adjudicación de este contrato de compraventa, se hizo mediante el procedimiento de **Licitación Pública**, con fundamento en los artículos 1, 3, 13, 16, 28, 29, 30, 35, 36 y 39 del Reglamento de Adquisiciones, Arrendamientos, Servicios y Obra Pública del Tribunal Superior de Justicia del Estado de Yucatán y conforme al artículo segundo del Acuerdo General Número **OR01-230104-32**, por el que se establecen los montos para la procedencia de los procedimientos de obra pública y servicios conexos, adquisiciones, arrendamientos y contratación de servicios durante el ejercicio fiscal 2023, publicado en el Diario Oficial del Gobierno del Estado en su edición del diecisiete de enero de dos mil veintitrés.

1.5. Que la Licenciada en Derecho María Carolina Silvestre Canto Valdés es Presidenta del Tribunal Superior de Justicia y del Consejo de la Judicatura del Poder Judicial del Estado de Yucatán como consta en el acta de la Décimo Sexta Sesión Extraordinaria correspondiente al día dieciséis de diciembre de dos mil veintidós, por el término comprendido del primero de enero del año dos mil veintitrés al treinta y uno de diciembre de dos mil veintiséis y cuenta con las facultades legales para suscribir este contrato en representación del Tribunal Superior de Justicia del Estado de Yucatán.

[redacted]

1.6. Que con fundamento en el Artículo 40, fracción IV de la Ley Orgánica del Poder Judicial del Estado, la Licenciada en Administración María Cristina Sánchez Tello Zapata cuenta con poder para actos de administración de conformidad con el acta doscientos cuarenta y uno, tomo nueve, libro quinto, folio doscientos diecisiete, de fecha treinta y uno de agosto del año dos mil veintidós pasada ante la fe de la Abogada Verónica del Carmen Moguel Esperón, Notario Público del Estado de Yucatán en ejercicio, Titular de la Notaria treinta y cuatro con residencia en la ciudad de Mérida, Yucatán.

1.7. Que el Tribunal Superior de Justicia cuenta con la suficiencia presupuestal disponible proveniente del presupuesto autorizado para el ejercicio fiscal 2023. Asimismo, dichos recursos quedarán comprometidos durante el ejercicio fiscal 2023 y una vez que se obtenga la recepción de conformidad y a entera satisfacción de los bienes y servicios contratados, según el calendario de ejecución establecido en el presente instrumento, durante el ejercicio fiscal 2024 se reconocerán las obligaciones que deriven y se realizarán los pagos correspondientes, en cumplimiento de la Ley de Disciplina Financiera.

1.8. Que sus datos fiscales son: denominación **Poder Judicial del Estado,** Registro Federal de Contribuyente es **PJE 860206913,** sede la **calle 59 letra "A" (Avenida Jacinto Canek), número 605, por calle 90, Colonia Inalámbrica, C.P. 97069**, y domicilio fiscal **calle 35, número 501 letra "A" entre 62 y 62 letra "A", colonia Centro, C.P. 97000,** Mérida, Yucatán.

2. "EL PROVEEDOR" a través de su representante legal declara:

2.1. Que es una sociedad de naturaleza mercantil, legalmente constituida de conformidad con lo establecido con las leyes mexicanas en la materia, lo que se comprueba con la copia certificada de la escritura pública número tres mil seiscientos ochenta de fecha veintidós de julio de mil novecientos noventa y cuatro, pasada ante la fe del Notario Público número ochenta del Estado de Nuevo León, Licenciado Rodolfo Vela de León, cuya copia certificada por la Secretaría General de Acuerdos obra en los registros del Padrón de Proveedores de este Tribunal.

2.2. Que tiene capacidad jurídica para contratar, como acredita con la copia certificada del testimonio de la escritura pública número tres mil ochocientos noventa y cuatro de fecha quince de mayo de dos mil veintitrés, pasada ante la fe del Notario Público número dieciocho; Licenciado Salvado Martínez Martínez del Estado de Nuevo León, y al respecto manifiesta bajo protesta de decir verdad que dicho poder no le ha sido revocado ni modificado a la fecha, cuya copia certificada por la Secretaría General de Acuerdos obra en los registros del Padrón de Proveedores de este Tribunal.

2.3. Que entre su objeto social y su actividad empresarial se encuentra los marcados en el objeto de este contrato y que cuenta con los recursos humanos, técnicos, económicos y materiales necesarios para cumplir las obligaciones derivadas de este contrato.

2.4. Que se encuentra inscrito como contribuyente ante la Secretaría de Hacienda y Crédito Público con el Registro Federal de Contribuyentes **AXT940727FP8**.

2.5. Que conoce y se sujeta voluntaria y plenamente, a las disposiciones contenidas en el Reglamento de Adquisiciones, Arrendamientos, Servicios y Obra Pública del Tribunal Superior de Justicia del Estado de Yucatán.

2.6. Que para los fines de este contrato y específicamente para los efectos de recibir notificaciones, señala como domicilio la calle 1, número 358, C.P. 97118, Colonia Gonzalo Guerrero de Mérida, Yucatán. Su domicilio fiscal es: Av. Munich, número 175, Colonia Cuauhtemoc entre Av. Guerrero y Av. Nogalar, C.P. 66450, de San Nicolás de los Garza, Nuevo León.

[redacted]

CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

CLÁUSULAS

Primera.- **Objeto**.- Mediante el presente contrato de compraventa, "El Tribunal Superior de Justicia" y "El Proveedor" dan cumplimiento al fallo recaído en la Licitación Pública Número **"PODJUDTSJ-CA 18/2023"**, respecto a la renovación del licenciamiento para la seguridad perimetral por veinticuatro meses que incluya puesta en sitio (partida "A") y un licenciamiento de antivirus endpoint de seguridad para el Tribunal Superior de Justicia del Estado (partida "B").

Segunda.- **Bienes y servicios objeto del contrato**.- "El Proveedor" se obliga y compromete a suministrar, instalar y poner en funcionamiento los bienes, que se señala en el **Anexo 1** de este contrato que se suscribe y adjunta como parte integrante del mismo.

Tercera.- "El Proveedor" se obliga y compromete a lo siguiente:

A) Prestar los servicios de soporte técnico y mantenimiento correctivo, durante el periodo de garantía y carta de servicio de los bienes, sin costo adicional alguno para "El Tribunal Superior de Justicia", conforme la carta de garantía proporcionada con los bienes.

B) Garantizar el buen funcionamiento y calidad de los bienes para la partida "A" por el término de **veinticuatro meses** en todas las partes, mano de obra y servicio de soporte técnico y para la partida "B" de **dos años** en mano de obra y servicio de soporte técnico.

C) Brindar toda la asistencia y soporte técnicos necesarios para la entrega, instalación, y operación inicial de los bienes, en el lugar que designe "El Tribunal Superior de Justicia".

D) A vender a los mismos precios y condiciones contratadas, a solicitud de "El Tribunal Superior de Justicia" hasta el 25% adicional al volumen de los bienes y servicios contratados y hasta por tres meses más contados a partir de que finalice la vigencia del contrato o plazo de ejecución según sea el caso, en cuyo caso se formalizará mediante un convenio de ampliación y el proveedor deberá realizar la modificación correspondiente a la fianza.

Cuarta.- **Monto del contrato**.- Las partes acuerdan que el importe total de la presente compraventa se desglosa de la siguiente manera: **$4,325,236.32** (cuatro millones trescientos veinticinco mil doscientos treinta y seis pesos 32/100 M.N.) monto que corresponde a la partida "A" y **$598,165.60** (quinientos noventa y ocho mil ciento sesenta y cinco pesos 60/100 M.N.) monto que corresponde a la partida "B", haciendo un gran total de **$4,923,401.92** (cuatro millones novecientos veintitrés mil cuatrocientos un pesos 92/100 M.N.) incluyendo a todas las cantidades el correspondiente Impuesto al Valor Agregado.

Quinta.- **Lugar para el suministro, instalación y puesta en funcionamiento de los bienes, objeto del contrato**.- El lugar para el suministro, instalación y puesta en funcionamiento de los bienes, objeto del contrato, es el Departamento de Informática del Poder Judicial del Estado, ubicado en la planta baja del edificio sede del Tribunal Superior de Justicia, sito en calle 59 letra "A" (Avenida Jacinto Canek), número 605, por calle 90, Colonia Inalámbrica de la ciudad de Mérida, Yucatán, en horario de 08:00 a 15:00 horas.

Sexta.- **Plazo para el suministro, instalación y puesta en funcionamiento de los bienes, objeto del contrato**.- El plazo para el suministro, instalación y puesta en funcionamiento de los bienes será a más tardar dentro de los **cuarenta y cinco días naturales,** contados a partir de la firma del contrato.

Séptima.- **Aceptación del objeto del contrato**.- El suministro e instalación de los bienes que son objeto de este contrato podrá ser aceptados o rechazados por "El Tribunal Superior de Justicia", en un plazo de quince días naturales contados a partir de su entrega y puesta en marcha; y un nivel del

[redacted]

cien por ciento de disponibilidad, contado a partir de la fecha en que fueron aprobados los rendimientos y la operación de los mismos.

Si alguno de los bienes no cumple con el cien por ciento de los requerimientos establecidos en las bases de la licitación pública número **"PODJUDTSJ-CA 18/2023"** o tienen daños o defectos, serán sustituidos por un nuevo bien en un plazo no mayor de **quince** días hábiles por parte de "El Proveedor", sin costo alguno para "El Tribunal Superior de Justicia", y se iniciará bajo los mismos términos, el período de aceptación, por lo que hace a los bienes sustituidos.

Cuando todos los bienes y servicios sean recibidos a satisfacción deberán hacerse constar en un acta suscrita por las partes de este contrato, que servirá para computar el inicio del plazo de vigencia de las garantías a que se refiere la **cláusula tercera, inciso B** de este contrato.

Octava.- Catálogos, manuales y equipo complementario.- "El Proveedor", se obliga a entregar, junto con los bienes a que se refiere el presente contrato:

A) Un juego completo de manuales originales y de las características de cada uno de los bienes objeto de este contrato.

B) Un juego de manuales completo por cada bien.

C) En caso de que los materiales impresos que proporcione "El Proveedor", se encuentren escritos en idioma distinto del español, deberá acompañarse una traducción simple en idioma español.

Novena.- Patentes, marcas y derechos de autor.- "El Proveedor" asume de manera expresa la responsabilidad total con "El Tribunal Superior de Justicia" en el caso de que al suministrar los bienes objeto del presente contrato, infrinja los derechos de tercero sobre patentes, franquicias, marcas o derechos de autor; asimismo, libera en este acto a "El Tribunal Superior de Justicia" de cualquier responsabilidad por estos conceptos.

Décima.- Forma y Lugar de Pago.- "El Tribunal Superior de Justicia" se obliga a pagar a "El Proveedor", el monto total pactado en este contrato, con el Impuesto al Valor Agregado incluido, dentro de los diez días hábiles siguientes a la entrega de la factura correspondiente, una fianza para garantizar el cumplimiento del contrato, los vicios ocultos y la calidad de los bienes y servicios conforme lo estipulado en la **cláusula décima primera** de este contrato y la aceptación de los bienes y servicios en los términos a que se refiere la **cláusula séptima** de este contrato.

"El Tribunal Superior de Justicia" y "El Proveedor" convienen que el pago de las facturas por el suministro de los bienes y la prestación del servicio objeto de este contrato, se hará mediante cheque por "El Tribunal Superior de Justicia" en sus oficinas ubicadas en calle 59 letra "A" (Avenida Jacinto Canek), número 605, por calle 90, Colonia Inalámbrica o mediante transferencia electrónica de fondos con abono a la cuenta bancaria del beneficiario, previa presentación del formato de solicitud.

Décima Primera.- Garantías.- Para asegurar el cumplimiento de todas y cada una de las obligaciones a que se refiere el presente contrato, los vicios ocultos y la calidad de los bienes y servicios "El Proveedor" se obliga a entregar dentro de los diez días hábiles siguientes al fallo, una fianza en moneda nacional, a favor de "El Poder Judicial del Estado - Tribunal Superior de Justicia del Estado", con un importe igual al 10% (diez por ciento) del monto total del contrato, esto es, incluido el impuesto al valor agregado, otorgada por una institución legalmente autorizada para tal efecto. Esta fianza tendrá una vigencia para las partidas "A" y "B" de **dos años**, contados a partir de la firma de este contrato.

La garantía a que se refiere esta cláusula se hará efectiva parcial o totalmente, en caso de

[redacted]

incumplimiento de cualquiera de las obligaciones a cargo de "El Proveedor", establecidas en este contrato.

La póliza de fianza deberá prever, como mínimo, las siguientes declaraciones:

I. Que la fianza garantiza el fiel cumplimiento del contrato.

II. Que la fianza se otorga atendiendo a todas las estipulaciones contenidas en el contrato.

III. Que la fianza permanecerá vigente durante el cumplimiento de la obligación que garantice y continuará vigente en caso de que se otorgue prórroga al cumplimiento del contrato, así como durante la substanciación de todos los recursos legales o juicios que se interpongan y hasta que se dicte resolución definitiva que quede firme.

Adicionalmente, "El Proveedor" se obliga a entregar las cartas de garantía conforme al **punto 1.2.5 de las bases de licitación**, junto con la entrega de los bienes y el **inciso B** de la **cláusula tercera** de este contrato.

Décima Segunda.- Penas convencionales.- Las partes fijan de común acuerdo las penas convencionales siguientes:

En el caso de mora en el cumplimiento del plazo del suministro, instalación y puesta en funcionamiento de los bienes a que se refiere la **cláusula sexta** de este contrato, "El Proveedor" deberá pagar una pena convencional consistente en el **cinco al millar** sobre el monto de los bienes no entregados y los servicios no prestados oportunamente, por cada día natural de retraso, hasta el día que se cumpla con esta obligación.

Para determinar la aplicación de las sanciones estipuladas en esta cláusula, no se tomarán en cuenta las demoras motivadas por caso fortuito o de fuerza mayor, ya que, en tal caso, "El Tribunal Superior de Justicia", podrá autorizar las prórrogas necesarias, a solicitud de "El Proveedor".

Los montos que resulten de la aplicación de las penas convencionales que se impongan a "El Proveedor", deberán ser pagados al área correspondiente del Tribunal Superior de Justicia dentro de los cinco días hábiles siguientes a que sea requerido para ello y, en caso contrario, se harán efectivos con cargo a la fianza a que se refiere la **cláusula décima primera** de este contrato.

El monto de las penas convencionales no excederá en su aplicación del monto de la garantía de cumplimiento del contrato, los vicios ocultos y la calidad de los bienes y servicios.

"El Proveedor" otorga su conformidad en el sentido de que "El Tribunal Superior de Justicia" podrá aplicar las penalidades pactadas en este contrato, mediante deducciones al importe de la factura autorizada a "El Proveedor" correspondiente a este contrato. Si estas fueran insuficientes o no existen pagos pendientes, las penas se aplicarán incluso a cualquier otro derecho de cobro pendiente que tuviese "El Proveedor" a su favor derivado de otro u otros contratos celebrados con "El Tribunal Superior de Justicia", y si lo pendiente de pagarse a "El Proveedor" no alcanzare para cubrir el importe total de las sanciones, se hará uso de la fianza otorgada.

Décima Tercera.- Supervisión del contrato.- "El Tribunal Superior de Justicia" designa como supervisores del presente contrato, a las personas titulares de la Subjefatura del Departamento de Informática y la Jefatura del Departamento de Servicios Generales y Mantenimiento ambos de "El Tribunal Superior de Justicia" quiénes controlarán, verificarán y revisarán que el contrato se cumpla de conformidad con lo pactado en el mismo y en las bases de la licitación, y que se cumpla con las órdenes de "El Tribunal Superior de Justicia", dadas por escrito, en la inteligencia de que esta facultad

[redacted]

de supervisión no implica la conformidad tácita o expresa del cumplimiento ni releva a "El Proveedor" de las obligaciones que contrae bajo este contrato.

Décima Cuarta.- **Modificaciones al contrato**.- Las partes convienen en que por caso fortuito o fuerza mayor, o por causas atribuibles al Tribunal Superior de Justicia, este podrá modificar el contrato a efectos de prorrogar la fecha o plazo para la entrega de los bienes y la prestación de los servicios, formalizándose el convenio modificatorio respectivo, no procediendo la aplicación de penas convencionales por atraso. Tratándose de causas imputables al Tribunal Superior de Justicia no se requerirá de la solicitud del proveedor.

Décima Quinta.- **Procedimiento y causas de la rescisión del contrato**.- "El Tribunal Superior de Justicia" podrá rescindir administrativamente el contrato en caso de incumplimiento de las obligaciones a cargo de "El Proveedor", en cuyo caso el procedimiento iniciará dentro de los quince días naturales siguientes a aquel en que se hubiere agotado el monto límite de las penas convencionales. Si antes de la determinación de dar por rescindido el contrato, se hiciere entrega de los bienes y servicios, el procedimiento iniciado quedará sin efecto.

Asimismo, en caso de que "El Proveedor" se coloque en algunos de los supuestos que más adelante se señalan o contravenga las disposiciones, o incumpla cualquiera de las obligaciones estipuladas en este contrato, "El Tribunal Superior de Justicia" podrá rescindir éste administrativamente.

Esta rescisión operará de pleno derecho y sin necesidad de declaración judicial y, para efectuarla, "El Tribunal Superior de Justicia" comunicará por escrito a "El Proveedor" las razones que tuviere para iniciar el procedimiento de rescisión, para que "El Proveedor", dentro del término de 5 (cinco) días hábiles contados a partir de la fecha en que reciba la comunicación antes mencionada, manifieste lo que a su derecho convenga, y exhiba las pruebas con que acredite sus argumentaciones; "El Tribunal Superior de Justicia" resolverá lo procedente dentro del plazo de 15 (quince) días hábiles siguientes a la fecha que hubiere recibido el escrito de contestación de "El Proveedor" o de que hubiere vencido el plazo para que éste contestara.

En caso de emitirse resolución de rescisión administrativa por causas imputables a "El Proveedor", "El Tribunal Superior de Justicia" procederá a hacer efectivas las garantías y se abstendrá de cubrir los importes resultantes de los bienes y servicios aún no liquidados hasta que se otorgue el finiquito correspondiente, lo que deberá efectuarse dentro de los 30 (treinta) días naturales siguientes a la fecha de la comunicación de dicha resolución.

Cuando sea "El Proveedor" quien decida dar por rescindido este contrato, será necesario que acuda ante la autoridad judicial y obtenga la declaración correspondiente.

Las partes convienen en que el contrato podrá ser rescindido, por cualquiera de las causas siguientes:

1. Si "El Proveedor" suspende injustificadamente el objeto de este contrato.
2. Si "El Proveedor" se niega a reponer el bien y servicio que hubiera sido rechazados por "El Tribunal Superior de Justicia".
3. Si "El Proveedor" no ejecuta el contrato de conformidad con lo estipulado en este mismo y sus anexos.
4. Si "El Proveedor" sin motivo justificado no acata las órdenes dadas por escrito por "El Tribunal Superior de Justicia" respecto de las obligaciones contraídas en virtud de este contrato.

5. Si "El Proveedor" es sujeto de algún procedimiento judicial para ser declarado en quiebra o suspensión de pagos.
6. Si "El Proveedor" cede los derechos de cobro derivados de este contrato, sin la previa autorización por escrito de "El Tribunal Superior de Justicia".
7. Si "El Proveedor" no da a "El Tribunal Superior de Justicia" y a las dependencias que tengan facultades de intervenir, las facilidades, datos necesarios para la inspección, vigilancia y supervisión del contrato.
8. Si "El Proveedor" no entrega a "El Tribunal Superior de Justicia" los certificados y/o documentación de conformidad con lo estipulado en este contrato, o si habiéndose entregado dicha documentación, ésta no se mantiene en vigor durante la vigencia del contrato.
9. Por negativa de "El Proveedor" a presentar denuncias o a ejercitar cualquier otra acción legal, de acuerdo a los términos establecidos en este acuerdo de voluntades.
10. Si "El Proveedor" intenta transmitir o transmite total o parcialmente bajo cualquier título a un tercero los derechos y obligaciones estipulados en este contrato.
11. Si "El Proveedor" no cumple con la entrega de la fianza a que se refiere la **cláusula décima primera** de este contrato, a más tardar a los diez días hábiles siguientes al fallo, o bien, no entrega la modificación de la póliza en el caso del convenio de ampliación a que se refiere la **cláusula tercera inciso D** de este contrato.
12. Que "El Proveedor" sea incluido en los listados definitivos a que se refiere el artículo 69-B del Código Fiscal de la Federación.
13. En general, por incumplimiento por parte de "El Proveedor" a cualesquiera de las obligaciones derivadas del contrato y sus anexos, a las leyes y reglamentos aplicables, o a las órdenes por escrito de "El Tribunal Superior de Justicia".

"El Tribunal Superior de Justicia" queda expresamente facultado para optar entre exigir el cumplimiento del contrato o rescindirlo administrativamente; si "El Tribunal Superior de Justicia" opta por la rescisión, "El Proveedor", se obliga a pagar como pena convencional, el importe del 10% (diez por ciento) del monto total contratado, esto es, incluido el Impuesto al Valor Agregado o bien, se hará efectiva la garantía que se refiere la **cláusula décima primera** de este contrato.

Décima Sexta.- Impuestos.- Cada parte conviene en pagar todas y cada una de las contribuciones y demás cargas fiscales que conforme a las leyes federales, estatales y municipales, tengan la obligación de cubrir durante la vigencia, ejecución y cumplimiento de éste contrato y sus anexos.

Décima Séptima.- Responsabilidad laboral.- "El Proveedor", será el único patrón del personal que utilice con motivo del suministro de los bienes y de la prestación de los servicios objeto del presente contrato, y será el único responsable de las obligaciones legales y demás ordenamientos en materia de trabajo y seguridad social, y responderá de todas las reclamaciones que sus trabajadores presenten en su contra, incluida la muerte, sin responsabilidad alguna para "El Tribunal Superior de Justicia".

Décima Octava.- De la jurisdicción y competencia.- las partes contratantes se someten expresamente para todo lo relacionado con la interpretación, cumplimiento y, en su caso, ejecución del presente contrato, así como para todo aquello que no esté establecido en el mismo, a la jurisdicción y competencia de los jueces y tribunales de la ciudad de Mérida, Yucatán, Estados Unidos

[redacted]

CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

Mexicanos, renunciando "El Proveedor" al fuero que por razón de su domicilio o cualquier otra causa, pudiera corresponderle.

Leído que fue el presente contrato que consta de ocho fojas útiles y su anexo que consta de cuarenta fojas útiles y enteradas las partes de su valor y alcance legales, manifiestan su total conformidad y aceptación con todas y cada una de las obligaciones a que se contrae el presente documento y para debida constancia y validez, lo firman por triplicado quedando dos ejemplares en poder del "Tribunal Superior de Justicia" y uno en poder del "Proveedor" en la ciudad de Mérida, capital del Estado de Yucatán, Estados Unidos Mexicanos, a veintiocho de diciembre de dos mil veintitrés.

Por "El Tribunal Superior de Justicia"

Supervisora del Contrato

L.A. Maria Cristina Sánchez Tello Zapata
Titular de la Unidad de Administración del Tribunal Superior de Justicia del Poder Judicial del Estado.

L.A. Karina Osorio Morales
Jefa del Departamento de Servicios Generales y Mantenimiento del Tribunal Superior de Justicia del Poder Judicial del Estado.

Supervisor del Contrato

C. Francisco Arturo Pacheco Reyes
Subjefe del Departamento de Informática del Tribunal Superior de Justicia del Poder Judicial del Estado.

Por "El Proveedor"

[redacted]

Marcos Rodrigo Baeza Maldonado
AXTEL, S.A.B. DE C.V.

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

PARTIDA	CANTIDAD	UNIDAD MEDIDA	DESCRIPCIÓN	PRECIO UNITARIO	IMPORTE
A	1	SERVICIO	**RENOVACIÓN DEL LICENCIAMIENTO PARA LA SEGURIDAD PERIMETRAL DE ALTA DISPONIBILIDAD** **AXTEL, S.A.B. DE C.V.** oferta la renovación de Seguridad Perimetral, los cuales cumplen con las siguientes especificaciones: Renovación del licenciamiento para la seguridad perimetral de alta disponibilidad que incluye lo siguiente: **Marca:** Check Point **Licenciamiento/ modelo:** 12 meses de servicios Check Point Suscripción de seguridad paquete SandBlast (Security Suscription Package SandBast), el licenciamiento incluye 2 equipos Gateway de seguridad 6700 plus, con una configuración de 10 puertos de 1GbE RJ-45, 4 slots SFP+, 4 tranceptores SFP+ SR multimodo, 1 disco SSD, 2 fuentes de poder AC, rieles. Actualización de Memoria RAM a 32 Gb. **Garantía:** 12 meses de soporte Check Point Empresarial directo premium (Enterprise Direct Premium) Paquete de servicios SandBlast incluye: • Firewall, VPN, Mobile Access • Content Awareness • Control de aplicaciones • IPS • Filtrado URL • Antivirus y Anto-bot • DNS Security • Threat Emulation (Sandboxing) • Threat Extractin (CDR) • Zero Phishing Renovación de Consola existente propiedad de la Convocante. **Marca:** Check Point **Licenciamiento/modelo:** Renovación de Consola de Administración de Seguridad basada en Software de próxima generación para 5 equipos (Next Generation Security Management Software for 5 gateways - SmartEvent & Compliance) incluye los servicios de administración Eventos y Reporteo (SmartEvent & SmartReporter) por 12 meses.	$ 3,728,652.00	$ 3,728,652.00

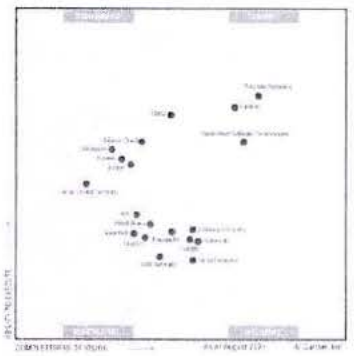
[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Garantía: 12 meses de soporte Check Point empresarial directo premium (Enterprise Direct Premium) **CARACTERÍSTICAS GENERALES** • Check Point, fabricante del sistema de seguridad perimetral tiene más de 20 años de experiencia en el Mercado de seguridad informática. • Check Point proporciona exclusivamente soluciones de seguridad de Internet. • Check Point proporciona evidencia de las posiciones de liderazgo año tras año en firewall empresarial, firewalls UTM y prevención de intrusiones basadas en datos independientes de la industria de la seguridad. Figure 1. Magic Quadrant for Network Firewalls  Source: Gartner (December 2022) • Check Point proporciona evidencia de la posición de liderazgo año tras año del Cuadrante Mágico de Gartner para las soluciones de Prevención de Intrusión y / o el Cuadrante Mágico Gartner del firewall de la red empresarial.		

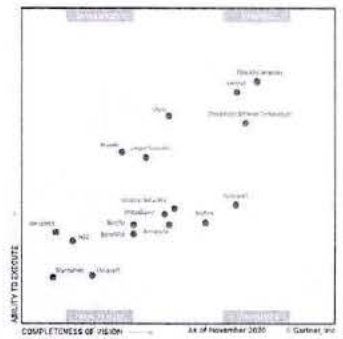
[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

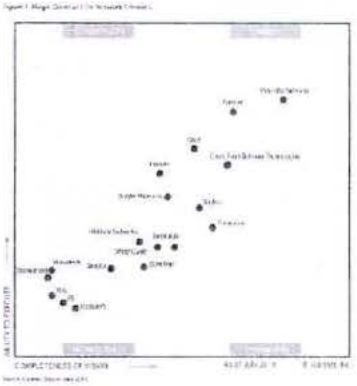


Source: Gartner (November 2021)

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)



- Es capaz de soportar estas aplicaciones de seguridad de próxima generación en una plataforma unificada: Stateful Inspection Firewall, Sistema de Prevención de Intrusos, Adquisición de Identidad de Usuario, Control de Aplicación y Filtrado de URL, Anti-Bot y Anti-Virus, Emulación de Amenazas

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			(Sandboxing), Extracción de Amenazas (depuración), Anti-Spam, VPN IPSec y acceso móvil. • Para la protección de la red perimetral, se oferta un clúster (2 appliances) de ciberseguridad, los cuales cuentan con las siguientes capacidades: • El cluster se gestiona de manera centralizada por un Servidor de Administración Centralizada de Seguridad. • La solución de Check Point provee un mecanismo para constantemente educar al usuario final de la política de seguridad en tiempo real. • Check Point otorga todas las certificaciones de la solución. • Check Point tiene la capacidad para proveer una solución para mitigar ataques de tipo denegación de servicio. • Los Gateways de seguridad usan Stateful Inspection basada en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de la red. • La solución admite el control de acceso para 150 servicios o protocolos predefinidos. • La solución soporta control de acceso usando objetos de tipo data centers genéricos. • La solución soporta un ilimitado número de lenguajes en los objetos de tipo Check de Usuarios. • La solución soporta la instalación de políticas aceleradas. • La solución soporta la instalación de políticas de seguridad de manera concurrente. • La solución soporta el recuento de aciertos en las reglas de NAT. • La solución soporta objetos de dominio, actualizables, zonas de seguridad, roles de acceso y centro de datos. • Proporciona estadísticas de recuento de aciertos de reglas de seguridad a la Consola de administración. • Permite que las reglas de seguridad se apliquen en intervalos de tiempo que se configurarán con una fecha / hora de caducidad.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La comunicación entre las consolas de administración y los Gateways de seguridad están encriptada y autenticada con Certificados PKI. • Los Gateways de seguridad soportan métodos de autenticación usuario, cliente y sesión. • Los Gateways de seguridad soportan el siguiente esquema de autenticación de usuario a nivel Gateway y a nivel módulo de VPN: tokens, TACACS, RADIUS y certificados digitales. • La solución incluye una base de datos local para aceptar la autenticación y autorización por usuario sin la necesidad de un dispositivo externo. • La solución soporta DHCP en modo server y relay. • La solución soporta HTTP y HTTPS Proxy. • La solución incluye la facilidad para trabajar en modo transparente y modo puente. • La solución admite Alta disponibilidad de Gateways e intercambio de carga con sincronización de estado. • La solución es compatible con la integración de terceros (API pública). • Motor de comparación de firmas que permite contrastar el contenido del tráfico de una sesión contra patrones de firmas de virus, ataques de intrusión, reconocimiento de aplicaciones u otros patrones sin comprometer el rendimiento de la red. • Soporta protocolos: TCP, UDP, ARP, ICMP, IPv4, IPv6, OSPF, IPSec, RIP. • La solución soporta 6 a 4 NAT o 6 a 4 Tunnel. • La solución soporta integración al Directorio activo utilizando tráfico IPV6. • La solución soporta ver el log del tráfico de IPV6. • La plataforma soporta la habilidad para desplegar la tabla de enrutamiento de IPV6 • Para el presente esquema se requiere una arquitectura de un clúster, es decir, dos gateways. • Los componentes de la Solución de Seguridad Perimetral tienen la capacidad individual de:		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			○ Brinda soporte de 7 millones de sesiones o conexiones concurrentes. ○ Brinda soporte de 160,000 sesiones o conexiones por segundo. ○ Brinda soporte de 35 Gbps de throughput ideal de Firewall y 4 Gbps de VPN AES-128. ○ Brinda soporte de 18 Gbps de Inspección y prevención de tráfico malicioso (IPS) y 5 Gbps para Amenazas Avanzadas. ○ Cuenta con una interfaz de 1G dedicado para administración remota, adicional a una de sincronía. ○ Cuenta con 8 interfaces de 1G de cobre ○ Cuenta con 4 interfaces de 10G SFP+ y 4 transceivers SR ○ Cuenta con memoria RAM de 32GB ○ Fuente de poder redundante AC ○ 1 Unidad de Rack **VPN** • La solución admite cifrado 3DES y AES-256 para IKE Phase I y II IKEv2 más "Suite-B-GCM-128" y "Suite-B-GCM-256" para Fase II. • La solución admite los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20 • La solución es compatible con la integridad de los datos con md5, sha1 SHA-256, SHA-384 y AES-XCBC. • Se admite CA interna y CA externa de terceros. • La solución incluye soporte para VPN de sitio a sitio en las siguientes topologías: ○ Full Mesh (todo para todos), ○ Estrella (oficinas remotas al sitio central) ○ Hub and Spoke (sitio remoto a través del sitio central a otro sitio remoto). • La solución soporta encripción SHA/512 • La solución es compatible con la configuración de VPN con una GUI mediante		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			la adición de objetos de arrastrar y soltar a las comunidades de VPN • La solución admite VPN SSL sin cliente para el acceso remoto. • La solución soporta autenticación de máquina. **IDENTIFICACIÓN DE USUARIOS** • Puede adquirir la identidad del usuario al consultar Microsoft Active Directory en función de los eventos de seguridad. • Tiene un método de autenticación de identidad de usuario basado en el navegador para usuarios o activos que no sean de dominio • Provee múltiples métodos de identificación de usuarios: Consulta de AD, basada en navegador o agentes de identidad, Autenticación transparente de Kerberos, portal captivo. • Soporta entornos de servidor de terminal. • La solución se integra perfectamente con los servicios de directorio, IF-MAP y Radius. • El impacto en los controladores de dominio es inferior al 3%. • La solución de identidad admite servidores de terminal y Citrix. • Puede adquirir la identidad del usuario de Microsoft Active Directory sin ningún tipo de agente instalado en los controladores de dominio. • Tiene integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios; • Tiene la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios. • La solución soporta integración de portal cautivo con SAML 2.0 y proveedores de identidad de terceros. **IPS**		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• Check Point provee evidencia de que año tras año aparece como líder en el cuadrante mágico de Gartner para la categoría de Firewall de Red Empresarial, dicha información la puede consultar en la sección de características generales. • Se suministra el servicio de IPS brindándose con el mismo Appliance, en una configuración de alta disponibilidad, para la protección de ataques orientados a conexiones internas y externas. • IPS se basa en los siguientes mecanismos de detección: firmas de explotación, anomalías de protocolo, controles de aplicaciones y detección basada en el comportamiento. • IPS y el módulo de firewall se integra en una plataforma. • IPS tiene un mecanismo de fail-open basado en software, configurable basado en umbrales de CPU de Gateways de seguridad y uso de memoria. • IPS proporciona un mecanismo automático para activar o administrar nuevas firmas a partir de actualizaciones. • IPS admite excepciones de red basadas en la fuente, el destino, el servicio o una combinación de los tres. • IPS incluye un modo de solución de problemas que establece el perfil en uso para detectar solo, con un clic sin modificar las protecciones individuales. • IPS es capaz de detectar y prevenir las siguientes amenazas: uso indebido de protocolos, comunicaciones de malware, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas. • Para cada protección, la solución incluye el tipo de protección (relacionada con el servidor o con el cliente), la gravedad de la amenaza, el impacto en el rendimiento, el nivel de confianza y la referencia de la industria. • IPS puede detectar y bloquear los ataques a la red y a la capa de aplicaciones, protegiendo los siguientes servicios:		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			servicios de correo electrónico, DNS, FTP, servicios de Windows (redes de Microsoft). • Se proporciona evidencia de liderazgo para proteger las vulnerabilidades de Microsoft. • IPS y/ o Application Control incluye la capacidad de detectar y bloquear aplicaciones P2P y evasivas. • La solución protege contra el envenenamiento de caché de DNS e impide que los usuarios accedan a las direcciones de dominio bloqueadas. • La solución proporciona protecciones de protocolos VOIP • IPS detecta y bloquear las aplicaciones de controles remotos, incluidas aquellas que son capaces de crear túneles a través del tráfico HTTP. • La solución permite al administrador bloquear fácilmente el tráfico entrante y / o saliente en función de los países, sin la necesidad de administrar manualmente los rangos de IP correspondientes al país. • Actualizaciones periódicas durante la vigencia del contrato de nuevas definiciones, las actualizaciones se realizan de forma automática, programada por fecha y hora. • Se integra protección basada en firmas contra ataques de inyección de SQL. • Sincroniza las firmas de IPS, antivirus, anti-spyware cuando se despliega en alta disponibilidad; **CONTROL DE APLICACIONES Y FILTRADO DE URLS** • La base de datos de control de aplicaciones contiene 10,000 aplicaciones conocidas. • La solución tiene una clasificación de URL que supera los 200 millones de URL y cubre más del 85% de los principales sitios de 1M de Alexa. • La solución es capaz de crear una regla de filtrado con múltiples categorías. • La solución es capaz de crear un filtro para un solo sitio que sea compatible con múltiples categorías. • La solución tiene granularidad de usuarios y grupos con reglas de seguridad.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• El caché local del Gateway de seguridad da respuesta al 99% de las solicitudes de categorización de URL dentro de las 4 semanas de producción. • La solución tiene una interfaz de búsqueda fácil de usar para aplicaciones y URL. • La solución clasifica las aplicaciones y las URL y las aplicaciones por Factor de riesgo. • El control de la aplicación y la política de seguridad URLF pueden definirse por las identidades del usuario. • El control de la aplicación y la base de datos URLF son actualizados por un servicio basado en la nube. • La solución tiene un control de aplicación unificado y reglas de seguridad URLF. • La solución proporciona un mecanismo para informar o solicitar a los usuarios en tiempo real que los eduquen o confirmen acciones basadas en la política de seguridad. • Permite especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora); • Es posible crear políticas para usuarios, IPs, redes, o zonas de seguridad • Tiene la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory, y la base de datos local. • Permite página de bloqueo personalizada. • Permite el bloqueo y continuación (que permite al usuario acceder a un sitio bloqueado potencialmente informándole en la pantalla de bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio). • Tiene la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo • Es posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos. • La solución admite el control de acceso para 150 servicios o protocolos predefinidos.		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			ANTI-BOT y ANTIVIRUS • Check Point tiene una aplicación integrada Anti-Bot y Anti-Virus en el firewall de próxima generación. • La aplicación Anti-Bot es capaz de detectar y detener el comportamiento anormal sospechoso de la red. • La aplicación Anti-Bot usa un motor de detección de niveles múltiples, que incluye la reputación de direcciones IP, URL y DNS, y detectar patrones de comunicaciones de bots. • Las protecciones anti-Bot pueden escanear en busca de acciones de bots. • La solución es compatible con la detección y prevención de virus y variantes de Cryptors y ransomware (por ejemplo, Wannacry, Cryptlocker, CryptoWall) mediante el uso de análisis estáticos y / o dinámicos. • La solución tiene mecanismos para proteger contra los ataques de spear phishing. • Ataques basados en DNS • La solución tiene capacidades de detección y prevención para los escondites DNS de C&C. • La solución busca patrones de tráfico C&C, no solo en su destino DNS. • Invierte malware de ingeniería para descubrir su DGA (Generación de nombres de dominio). • Característica de captura de DNS como parte de nuestra prevención de amenazas, ayudando a descubrir hosts infectados generando comunicación C&C. • La solución tiene capacidades de detección y prevención para los ataques de túnel DNS. • La política Anti-Bot y Anti-Virus se administra desde una consola central. • La aplicación Anti-Bot y Anti-Virus tiene un mecanismo centralizado de correlación e informe de eventos. • La aplicación de antivirus puede evitar el acceso a sitios web maliciosos. • La aplicación antivirus puede inspeccionar el tráfico cifrado SSL.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• Anti-Bot y Anti-Virus tiene actualizaciones en tiempo real de servicios de reputación basados en la nube. • Anti-Virus es capaz de detener los archivos maliciosos entrantes. • Anti-Virus puede escanear archivos archivados. • Las políticas de antivirus y anti-Bot se administran de forma centralizada con la configuración de políticas granulares y su aplicación. • El Anti-Virus admite más de 50 motores AV basados en la nube. • El Anti-Virus es compatible con el escaneo de enlaces dentro de los correos electrónicos. • El Anti-Virus escanea archivos que están pasando el protocolo CIFS. **INSPECCIÓN SSL (INBOUND / OUTBOUND)** • La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas. • La solución es compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites). • La solución aprovecha la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular. • La solución inspecciona el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL. • Soporte TLS 1.3 **PROTECCIÓN CONTRA AMENAZAS DESCONOCIDAS (DIA CERO)** • La solución ofrece soporte para la inspección / descifrado SSL con un rendimiento líder en todas las tecnologías de mitigación de amenazas. • La solución es compatible con Perfect Forward Secrecy (PFS, ECDHE Cipher Suites).		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución es compatible con AES-NI, AES-GCM para mejorar el rendimiento. • La emulación de amenazas / sandboxing se integra con SSL Inspection. • La solución se aprovecha de la base de datos de filtrado de URL para permitir al administrador crear una política de inspección https granular. • La solución puede inspeccionar el filtrado de URL basado en HTTPS sin necesidad de descifrado SSL. • La solución proporciona la capacidad de proteger contra ataques de malware desconocidos y de día cero antes de que se hayan creado protecciones de firma estática. • Prevención en tiempo real: malware desconocido paciente-0 en la navegación web. • Prevención de malware desconocido en tiempo real paciente-0 en el correo electrónico. • La solución es capaz de emular 53 tipos de archivos como ejecutables, documentos, JAVA y flashear específicamente: 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk (android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh. • La solución es capaz de emular ejecutable, documentos, JAVA y flash específicamente dentro de varios protocolos: HTTP, HTTPS, FTP, SMTP, CIFS (SMB), SMTP, TLS. • El motor de emulación es compatible con varios sistemas operativos, como XP y Windows7, 8,10 32 / 64bit, incluidas las imágenes personalizadas. • La solución soporta el análisis estático para Windows, Mac OS-X, Linux o cualquier plataforma x86. • El motor de emulación puede inspeccionar, emular, prevenir y compartir los resultados del evento de sandboxing en la infraestructura antimalware.		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución permite la emulación de archivos con un tamaño superior a 80 Mb en todos los tipos que admita. • Las soluciones son compatibles con los motores de detección basados en el aprendizaje automático de máquinas. • El motor de emulación supera el 90% de tasa de captura en las pruebas de Virus Total donde los archivos .PDF y .exe maliciosos conocidos se modifican con encabezados "no utilizados" para demostrar la capacidad de las soluciones para detectar malware nuevo y desconocido. • La solución detecta el tráfico de C&C de acuerdo con la reputación dinámica de ip / url. • La solución es capaz de emular y extraer archivos incrustados en documentos. • La solución puede escanear documentos que contienen URL. • La solución tiene capacidades anti-evasión que detecten la ejecución de sandbox. • La solución entrega reportes basados en el framework de MITRE. • La solución soporta administración autónoma de la prevención de amenazas. • La solución soporta la actualización automática de los perfiles de la política de prevención de amenazas. **GESTIÓN DE SEGURIDAD** • **AXTEL, S.A.B. DE C.V.** considera la extensión del licenciamiento y soporte de la solución de gestión de seguridad actual, propiedad de la Convocante. • El licenciamiento para renovar incluye las funcionalidades de vistas de eventos de seguridad y generación de reportes personalizados, de los hallazgos más relevantes. • **AXTEL, S.A.B. DE C.V.** realiza todas las gestiones con el fabricante Check Point para unificar todos las productos, licencias y servicios bajo un único identificador de cuenta a nombre de la Convocante.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Las funciones que la solución de gestión de seguridad realiza son: • Tras la detección de archivos maliciosos, se genera un informe detallado para cada uno de los archivos maliciosos. • El informe detallado incluye: capturas de pantalla, líneas de tiempo, creación / modificaciones de clave de registro, creación de archivos y procesos, actividad de red detectada. • La aplicación de administración de seguridad puede coexistir en la puerta de enlace de seguridad como una opción. • La solución incluye la capacidad de distribuir de forma centralizada y aplicar nuevas versiones de software de puerta de enlace • La solución incluye una herramienta para administrar centralmente las licencias de todas las puertas de enlace controladas por la estación de administración • La GUI de administración tiene la capacidad de excluir fácilmente la dirección IP de la definición de firma IPS. • El Visor de registro tiene la capacidad de excluir fácilmente la dirección IP de los registros de IPS cuando se detecta como falso positivo • La GUI de administración tiene la capacidad de acceder fácilmente a la definición de firmas IPS a partir de los registros de IPS • La solución combina la configuración de políticas y el análisis de registros en un solo panel, para evitar errores y lograr la confianza del cambio. • La solución de administración de políticas proporciona registros de reglas similares para el usuario a medida que crea o modifica reglas (registros de contenido) • La GUI de la solución proporciona una navegación fácil entre cientos de políticas, cada una con hasta 1 millón de reglas. Se proporciona saltos entre sub políticas y títulos de sección, así como una búsqueda exhaustiva. **REGISTRO Y MONITOREO**		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• El registro central es parte del sistema de gestión. • La solución proporciona la opción de ejecutarse en el servidor de administración o en un servidor dedicado. • El visor de registro tiene la capacidad de realizar búsquedas indexadas. • La solución tiene la capacidad de registrar todas las aplicaciones de seguridad integradas en la puerta de enlace e incluir IPS, Control de aplicaciones, Filtrado de URL, Antivirus, Anti-Bot, Antispam, Identidad del usuario, Acceso móvil. • La solución incluye un mecanismo automático de captura de paquetes para que los eventos IPS proporcionen un mejor análisis forense. • La solución proporciona diferentes registros para la actividad regular del usuario y registros relacionados con la administración. • La solución proporciona la siguiente información del sistema para cada puerta de enlace: Sistema Operativo, uso de CPU, uso de memoria, todas las particiones de disco y porcentaje de espacio libre en el disco duro. • La solución incluye el estado de todos los túneles VPN, sitio a sitio y cliente a sitio. • La solución incluye una configuración de umbral personalizable para realizar acciones cuando se alcanza un determinado umbral en una puerta de enlace. Las acciones incluyen: Iniciar sesión, alerta, enviar una captura SNMP, enviar un correo electrónico y ejecutar una alerta definida por el usuario. • La solución incluye gráficos pre-configurados para monitorear la evolución en el tiempo del tráfico y los contadores del sistema: las principales reglas de seguridad, los principales usuarios de P2P, los túneles VPNs, el tráfico de red y otra información útil. La solución proporciona la opción de generar nuevos gráficos personalizados con diferentes tipos de gráficos. • La solución incluye la opción de registrar el tráfico y las vistas del sistema en un archivo		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			para su posterior visualización en cualquier momento. **VIGENCIA** La solución completa, considera una vigencia de Licenciamiento y Soporte directo por parte de Check Point de 12 meses, iniciando del 01 de enero de 2024 al 31 de diciembre de 2024. La solución de seguridad cuenta con un soporte de Check Point con los siguientes alcances: • Soporte de Check Point 24x7, con opción de que la Convocante puede solicitar soporte de manera directa. • Soporte telefónico y por correo electrónico • Solicitudes de soporte ilimitado • Acceso a la base de datos de conocimientos • Acceso a actualizaciones mayores y mejoras • Acceso a Hot Fixes y paquetes de servicio • Solicitud de refacciones bajo proceso (RMA) "Autorización de devolución de mercancía". La solución de seguridad perimetral cuenta con los siguientes servicios de seguridad para descarga de firmas y actualizaciones: • Control de aplicaciones • IPS • Filtrado de contenido • Antibot • Antivirus • Anti-spam • Anti Phising • Sandbox en la nube La solución de gestión cuenta con los siguientes servicios: • Cumplimiento • Correlacionador de eventos • Reportes **CURSOS** **AXTEL, S.A.B. DE C.V.** considera un curso oficial en un centro autorizado de entrenamiento autorizado por Check Point, es un curso básico para la administración de los equipos de seguridad Firewall y Solución de Gestión para 2 asistentes. • Se incluye curso para dos personas, curso Check Point Administrador de Seguridad		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Certificado (Certified Security Administrator CCSA) • Duración 3 días • Modalidad virtual • Curso en español • Material digital en idioma inglés certificado por el fabricante • Instructor certificado • Diploma de participación • Incluye examen de certificación el cual la Convocante deberá presentar en un centro de evaluación autorizado por el fabricante. **SERVICIO DE INSTALACIÓN PARA EQUIPOS DE SEGURIDAD** Se incluye todo lo necesario para la correcta instalación y operación de los equipos de seguridad. • Previo al inicio de los servicios de instalación, **AXTEL, S.A.B. DE C.V.** realizará mesas de trabajo en conjunto con la Convocante para realizar la identificación de requerimientos, arquitecturas de comunicación existentes, redes y recursos que son necesarios proteger con el fin de definir las políticas de seguridad que serán necesarias establecer en la solución de seguridad. • Se incluye suministro, colocación, puesta a punto de la infraestructura solicitada. • **AXTEL, S.A.B. DE C.V.** considera que la Convocante cuenta con una infraestructura de seguridad la cual **AXTEL, S.A.B. DE C.V.** retirará de los racks de comunicaciones para poder realizar correctamente la instalación de los nuevos equipos. • Configuración de los equipos Firewall en alta disponibilidad. • Configuración de políticas de ruteo, seguridad y acceso a los recursos DMZ. • Configuración de funcionalidades de balanceo de enlaces WAN para permitir la navegación de usuarios a través de una red privada de enlaces inalámbricos y/o internet, y en caso de pérdida de la comunicación primaria se cambie a la ruta de salida alterna de manera		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			automática sin afectar la disponibilidad de los servicios. • Establecimiento de una red de comunicaciones VPN site-to-site o client-to-site según requiera la Convocante. • Configuración de acceso por medio de restricción origen/destino de puertos TCP/UDP/ICMP y direcciones IP. • Configuración de NAT/PAT • Configuración de funcionalidad de firewall con validación de estados de conexión • Activación y configuración de las funciones de seguridad. • **AXTEL, S.A.B. DE C.V.** realizará la configuración de todos los módulos o funcionalidades de seguridad incluidos en el licenciamiento del equipo. • **AXTEL, S.A.B. DE C.V.** realizará una instalación nueva de la Consola de Gestión solicitada a renovar. La Consola será puesta en operación sobre una infraestructura de servidor virtual que será proporcionada por la Convocante. **AXTEL, S.A.B. DE C.V.** proporciona la lista de requerimientos que son necesarios y validar la infraestructura proporcionada para el correcto funcionamiento de la solución. • **AXTEL, S.A.B. DE C.V.** dará de alta todos los firewalls de seguridad solicitados en este Anexo Técnico en la Consola de Gestión, así como configurar todos los módulos de servicios para proporcionar a la Convocante información en tiempo real y generar reportes. • **AXTEL, S.A.B. DE C.V.** realizará las pruebas de funcionamiento necesarias para asegurar correctamente la operación de los equipos de seguridad. • **AXTEL, S.A.B. DE C.V.** incluye como parte de los servicios la entrega de una memoria técnica al finalizar los servicios. • **AXTEL, S.A.B. DE C.V.** entrega el licenciamiento y las garantías/pólizas de soporte técnico de Check Point.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• **AXTEL, S.A.B. DE C.V.** considera que los equipos serán instalados en edificio dentro de la ciudad de Mérida, y como parte de su propuesta considera todos los gastos necesarios para la correcta implementación en sitio. La información y ubicación de dicho edificio será acordado con **AXTEL, S.A.B. DE C.V.** en caso de resultar ganador. Con el fin de garantizar la correcta ejecución de los servicios, **AXTEL, S.A.B. DE C.V.** incluye como parte de su propuesta técnica el certificado que avala a la persona que realizará funciones de Administrador de Proyectos con las capacidades de Project Management Professional (PMP). Dicho certificado podrá ser localizado en el **Apéndice 1** de la presente propuesta técnica. **AXTEL, S.A.B. DE C.V.** integra dentro de su propuesta técnica los certificados de 1 ingeniero con un nivel de certificación a nivel asociado, 1 ingeniero con un nivel de certificación a nivel experto o su equivalente, 1 ingeniero con un nivel de certificación a nivel experto en resolución de problemas, a fin de demostrar que cuenta con las capacidades técnicas de implementación, configuración y puesta en servicio de los equipos para el proyecto. Dichos certificados podrán ser localizados en el **Apéndice 2** de la presente propuesta técnica. **SOPORTE TÉCNICO PARA EQUIPOS DE SEGURIDAD** El servicio será por 12 meses. • Los equipos contarán con soporte técnico durante la vigencia del servicio con atención las 24 horas del día los 7 días de la semana, en caso de requerirse el reemplazo de partes, **AXTEL, S.A.B. DE C.V.** considera un nivel de servicio de 8x5xNBD siguiente día hábil y gestionar las refacciones con Check Point para el restablecimiento del servicio. • **AXTEL, S.A.B. DE C.V.** mantendrá actualizada la solución de seguridad durante la vigencia del servicio. • **AXTEL, S.A.B. DE C.V.** proporcionará soporte técnico a través de un centro SOC (Security Operation Center) propietario. El documento que		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			comprueba la pertenencia del SOC podrá ser localizada en el **Apéndice 3** de la presente propuesta técnica. • Alineará todos sus procesos a las mejores prácticas ITIL, ISO27001:2013, 20000-1:2018, ISO 37001:2016 y 9001:2015. **AXTEL, S.A.B. DE C.V.** proporcionará como parte de su propuesta técnica los certificados que demuestran el cumplimiento de dichos estándares. Dichos certificados podrán ser localizados en el **Apéndice 4** de la presente propuesta técnica. • El SOC pertenece al grupo de respuesta de incidencias FIRST. • https://www.first.org/members/teams/axtel-csirt • Atención del SOC en un esquema 24x7x365. • Alineará todos sus procesos a las mejores prácticas ITIL, incluye como parte de su propuesta los certificados de 3 personas que cuenten con certificación ITIL Foundation e ITIL OSA. Dichos certificados podrán ser localizados en el **Apéndice 5** de la presente propuesta técnica. • El servicio cuenta con mesa de ayuda para la recepción y canalización de tickets de soporte técnico o para reportar incidencias. • Incluye soporte técnico por medio telefónico, remoto y email. • Considera soporte técnico en sitio para la atención de fallas y el restablecimiento del servicio.		
				Subtotal Partida	$ 3,728,652.00
				I.V.A.	$596,584.32
				Total Partida	$4,325,236.32
PARTIDA	CANTIDAD	UNIDAD MEDIDA	DESCRIPCIÓN	PRECIO UNITARIO	IMPORTE
B	295	SERVICIO	**SUMINISTRO DE LICENCIAS ENDPOINT** **AXTEL S.A.B. de C.V.** proporciona una solución de protección de punto final que cumple con las siguientes características técnicas:	$ 1,748.00	$ 515,660.00

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

Marca: Check Point
Modelo - Licenciamiento: 2 años Harmony endpoint avanzado (Endpoint Advanced) con paquete de servicios.
Garantía: 2 años de soporte Check Point tipo Directo Empresarial Premium (Enterprise software subscription Direct Premium)

CHECK POINT HARMONY	AVANZADO
Reducir la superficie de ataque	✓
Cortafuegos del host	
Control de aplicaciones	
Cumplimiento	
NGAV: Prevenga los ataques antes de que se ejecuten	✓
Antimalware	
NGAV basado en ML	
NGAV: Detección y protección en tiempo de ejecución	✓
Antiransomware	
Guardia de comportamiento	
Antibot	
Antiexplotación	
protección web	✓
Protección de sitios de phishing de día cero	
Protección de reutilización de contraseñas corporativas	
Filtrado de URL	
Protección contra sitios maliciosos	
Investigación y respuesta a ataques	✓
Recopilación y detección de análisis forenses	
Informe forense: visibilidad de incidentes, mapeo MITRE	
Esterilización completa de la cadena de ataque automatizada	
Restauración de archivos cifrados de ransomware	
Búsqueda de amenazas	
Acceso VPN	✓
VPN de acceso remoto	
Inteligencia sobre amenazas	✓
Desarrollado por ThreatCloud AI™	
Intercambio automatizado de IoC y de IoA	
Administración centralizada	

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Gestión de la nube ✓ **Desarmado y reconstrucción de contenido (CDR) a través del correo electrónico y la web** ✓ Emulación de amenazas (sandBox) Extracción de amenazas (desinfecta archivos en 1,5 segundos) Con el fin de contar con una estrategia de seguridad integrada en los firewalls perimetrales y la protección final de equipos, ambas soluciones pertenecen al fabricante Check Point. **ADMINISTRACIÓN** **Operacional** • La política puede definir listas blancas para implementar excepciones a la política base. • La solución es compatible con clientes locales y remotos independientemente de la red. • La solución tiene una API profundamente funcional y documentada para admitir la integración y la automatización en toda la plataforma y con otras plataformas. • La solución tiene una consola central para definir políticas, crear grupos de sistemas/usuarios, iniciar sesión, implementar actualizaciones, generar informes. • La solución tendrá soporte de fabricante. • Proporciona acceso basado en roles a la consola. • Tiene capacidad para excluir archivos y carpetas de los análisis. (Ejemplo: Exenciones para carpetas de bases de datos específicas). • Tiene capacidad para detener completamente el antivirus/EPP durante la instalación de la aplicación. • Control granular de la funcionalidad. • La solución es capaz de realizar operaciones de inserción en los clientes finales.		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución puede proporcionar una recopilación remota de registros de resolución de problemas. • La solución permite ejecutar un script de PowerShell remoto en el cliente. • La solución es "Network Aware" y tiene la capacidad de cambiar la política del cliente según su ubicación de red. • La solución tiene soporte para importar y prevenir IOC personalizados. • El acceso a la consola es compatible con el uso de autenticación de sistemas de terceros. **Despliegue** • La solución proporciona métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos). • La solución tiene la capacidad para la instalación remota nativa y la implementación del cliente sin el uso de herramientas de terceros. • La solución utiliza un "token de autenticación" para registrar de forma segura una nueva instalación de cliente en el servidor de gestión. • La solución permite gestionar la versión del agente y los componentes desde la interfaz de gestión. **Nube** • La solución proporciona gestión como un servicio. • La solución permite la selección de la región de la nube. • La solución tiene copias de seguridad proporcionadas como parte del servicio. • La solución cumple con el RGPD. • La solución tiene una separación total de datos entre clientes. • La solución de gestión es compatible con un cliente completo o un cliente ligero basado en web. • La solución tiene autenticación de dos factores para el inicio de sesión del administrador.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La autenticación web admite la autenticación SAML. • La Convocante contará con una sola consola de gestión en la nube, por lo que el **AXTEL S.A.B. de C.V.** realizará las actividades necesarias para crear, unificar, transferir o eliminar consolas de gestión, con fin que el licenciamiento sea administrado en una sola Consola a nombre de la Convocante. **Registro e informes** • La solución puede proporcionar alertas de correo electrónico en tiempo real. **CLIENTE** **Soporte de SO y VDI** • SO compatibles: Clientes Windows a partir del Windows 7 SP1 Pro +; Servidores Windows a partir del Windows 2008 R2 + Mac OS: 10.15 + (compatible con M1 completamente nativo) Linux: Debian v10, Ubuntu 18.04, CentOS 8, Red Hat Enterprise Linux 8.1 • La solución admite entornos VDI, tanto persistentes (flotantes) como no persistentes (dedicados). Los proveedores de Microsoft Terminal Server, Vmware Horizon y Citrix PVS/MCS son totalmente compatibles. • La solución esta alineada y es compatible con las últimas versiones del sistema operativo. • Esta solución permite implementar el cliente y proteger las máquinas que se ejecutan en servidores de terminales y cajeros automáticos. • Esta solución permite ejecutar funciones de protección de dispositivos habilitadas: HVCI, Credentials Guard y Windows Defender App Control. **Características del cliente** • El agente es liviano. • La solución es configurable para una utilización mínima de los recursos del sistema.		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución proporciona la capacidad de ejecutarse en un hipervisor. • La solución proporciona métodos modernos y sencillos de implementación/instalación/desinstalación remota (incluida la compatibilidad con secuencias de comandos). • La solución permite actualizar a versiones más nuevas sin realizar un reinicio. • El tamaño del paquete de la solución incluye solo los componentes relevantes para implementar en un solo instalador. • La solución proporciona capacidades de proxy para clientes que están fuera de línea y para limitar el uso del ancho de banda. • La solución puede recuperar actualizaciones de firmas para Internet mediante un proxy NTLM autenticado con las credenciales de un usuario conectado. • Al realizar actualizaciones, la solución descargará solo los cambios acumulados de la versión instalada. **Detección** • La solución recopila continuamente los eventos del sistema necesarios para la detección y el análisis. Elementos específicos se recopilan en tiempo real. (Los datos recopilados a través de secuencias de comandos posteriores al evento o la interacción en vivo con el host se tratan en un requisito separado). Los ejemplos incluyen, entre otros, eventos de proceso, modificaciones de archivos y registros, conexiones de red, actividad entre procesos, argumentos de línea de comando, eventos de Windows, consultas y respuestas de DNS. • La solución monitorea continuamente e informa los hallazgos lo más rápido posible. Si un endpoint no puede informar inmediatamente sobre los resultados, los resultados se almacenan localmente hasta que puedan cargarse		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			en el sistema de gestión central de la solución. • La solución permite alertas en tiempo real o registro de eventos notables basados en contenido personalizado (comportamientos) o indicadores atómicos de compromiso basados en tipos de datos identificados por la solución. • La solución proporciona una forma de garantizar que la información del proceso, los metadatos, las solicitudes de DNS, las conexiones de red, los archivos binarios o cualquier otra información recopilada no se comparta con el proveedor o un tercero (por ejemplo, VirusTotal) sin una suscripción explícita. • La solución puede demostrar gráficamente la actividad del sistema (árboles de procesos u otro tipo de interfaz de mapeo) para ayudar en las investigaciones. • La solución captura metadatos detallados sobre archivos binarios y procesos que se ejecutan en puntos finales. Los detalles incluyen, entre otros, el hash del binario (MD5, SHA-256), la información del editor, los detalles de la firma del código, la frecuencia observada en nuestro entorno, la información de la versión y el propietario del sistema de archivos. • La solución tiene la capacidad de cambiar la marca de las notificaciones de los usuarios. • La solución tiene la capacidad de controlar el nivel de mensajes para mostrar a los usuarios. **Respuesta** • La solución proporciona una forma de aislar un sistema que asegura que los controles preventivos se mantengan durante los reinicios. La configuración de aislamiento esta preestablecida para permitir que el punto final se aísle de las		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			amenazas, pero pueda conectarse a los sistemas de investigación/remediación. • La solución es capaz de aplicar inmediatamente controles preventivos (bloquear actividad específica o maliciosa conocida, etc.). • La solución tiene una capacidad de respuesta en vivo que permite la capacidad de interactuar de forma remota con el sistema. • La solución proporciona la capacidad de escribir una respuesta en vivo de forma condicional (es decir, si sucede X, entonces sucede Y). • La solución tiene una sólida comunidad de intercambio de socios. • La solución permite a los analistas la capacidad de alternar rápidamente entre diferentes actividades observadas en un punto final y proporcionar información contextual si está disponible. • La solución tiene la capacidad de buscar en todos los puntos finales los IOC u otros atributos del sistema que no se capturan en los datos de telemetría en tiempo real. **Informes** • La solución no expone la actividad de un usuario a otro usuario que esté usando la misma máquina. **PROTECCIÓN DE DATOS Y DISPOSITIVOS** **Protección de puertos** • La solución brinda administración de todos los puertos de punto final, con registro centralizado de la actividad del puerto para auditoría y cumplimiento. • La solución permite notificaciones de mensajes de usuario personalizados al conectar un dispositivo según el escenario. **Cumplimiento** • La solución obliga a los terminales a cumplir con las reglas de seguridad definidas para la organización. Los equipos que no cumplan se mostrarán		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			como no conformes y se les pueden aplicar políticas restrictivas. • La solución hará cumplir las aplicaciones y los archivos requeridos en función de la configuración de cumplimiento al monitorear la presencia de archivos específicos, valores de registro y procesos que deberán estar ejecutándose o presentes en las computadoras finales. • La solución hará cumplir las aplicaciones y los archivos prohibidos en función de la configuración de cumplimiento mediante la supervisión de la presencia de archivos específicos, valores de registro y procesos cuya ejecución o presencia está prohibida en los equipos terminales. • La solución aplicará una verificación Anti-Malware para verificar que las computadoras tengan un programa anti-malware instalado y actualizado. • La solución admite la integración con Windows Server Update Services (WSUS). **Cortafuegos** • La solución hace cumplir las reglas del cortafuegos para permitir o bloquear el tráfico de red a las computadoras finales en función de la información de conexión, como direcciones IP, puertos y protocolos. • La solución se utilizará para determinar si los usuarios pueden conectarse a redes inalámbricas mientras se encuentran en la LAN de su organización para proteger la red de las amenazas asociadas con las redes inalámbricas. • La solución definirá si los usuarios pueden conectarse a la red de la organización desde puntos de acceso en lugares públicos, como hoteles o aeropuertos. • La solución se utilizará para restringir o permitir el tráfico de red IPV6. • El Firewall del cliente de la solución permanece activo durante la actualización del cliente.		[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución incluye una opción para que Aislamiento de host aísle o permita un host específico (acceso a la red) que está bajo ataque de malware y presenta un riesgo de propagación. **Control de aplicaciones** • La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos. • La solución puede incluir aplicaciones en la lista blanca o en la lista negra. • La solución admite la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux"). • La solución se utilizará para restringir el acceso a la red para aplicaciones específicas. El administrador de Endpoint Security define políticas y reglas que permiten, bloquean o cancelan aplicaciones y procesos. • La solución incluye aplicaciones en la lista blanca o en la lista negra. • La solución admite la habilitación/deshabilitación del tráfico originado por los procesos WSL ("Subsistema de Windows para Linux"). **AntiMalware** • La solución es capaz de identificar la similitud de un archivo malicioso con una familia de malware conocida. • La solución permite el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles. • En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos. • La solución proporciona una interfaz de línea de comandos para iniciar el análisis de malware.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución proporciona una interfaz de línea de comandos para actualizar la base de datos de firmas antimalware. • La solución es compatible con un Anti-malware compatible con DHS. • La solución AV es capaz de proporcionar pruebas de que el escaneo se ha realizado en la mayoría de los archivos .DAT actuales o proporcionar un método de prueba igualmente eficaz que satisfaga los requisitos de auditoría para las soluciones AV sin DAT. • La solución protege la computadora de todo tipo de amenazas de malware, desde gusanos y troyanos hasta adware y registradores de pulsaciones de teclas. La solución gestionará de forma centralizada la detección y el tratamiento de malware en los equipos finales. • La solución permite el escaneo programado de unidades locales, mensajes de correo. Unidades ópticas y dispositivos extraíbles. • Las soluciones descargan firmas de un proxy NTLM autenticado con las credenciales de un usuario conectado. • La solución puede usar un cliente dedicado como proxy para actualizaciones de firmas antimalware para clientes que están fuera de línea y no tienen una conexión directa a Internet o para limitar el uso de ancho de banda. • En caso de detección de malware, la solución aislará los archivos del sistema operativo, pero no se eliminarán de forma permanente. El usuario puede restaurar archivos en cuarentena, si no son maliciosos. **Protección contra ransomware** • La solución protege contra ransomware existente y de día cero sin requerir actualizaciones de firmas. • La solución reparará y restaurará los archivos que se cifraron durante un ataque de ransomware. • La solución anti-ransomware tiene validación de terceros.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Protección conductual • La solución aprovecha múltiples sensores para identificar de manera efectiva y única los comportamientos de malware genérico, así como los comportamientos específicos de la familia de malware. • La solución previene o detiene inmediatamente comportamientos maliciosos sin importar si la máquina está en línea o fuera de línea. • La solución detecta y evita ataques sin archivos utilizando únicamente procesos de Windows. • La solución detecta y evita ataques sin archivos basados en secuencias de comandos. • La solución protege contra la técnica "Pass The Hash" para el robo de credenciales. • La solución detecta archivos LNK (acceso directo de Windows) maliciosos. • La solución detecta la escalada de privilegios locales (LPE) de día cero. • La solución se integra con la interfaz de análisis antimalware (AMSI) de Microsoft para recibir y analizar scripts decodificados. **Modelos ML para análisis estático** • La solución es capaz de identificar archivos de día cero incluso si no están familiarizados con ningún servicio de reputación. • El modelo de ML utilizado por el endpoint se actualiza con frecuencia para protegerlo contra nuevos ataques de día cero. • La solución impide que el usuario use archivos hasta que se verifiquen y se determine que son benignos. • El Motor de Detección Estática de la solución monitorea el acceso a los archivos. • La solución comprueba la reputación de los archivos en función del hash ssdeep/Fuzzy. **Anti-robot** • La solución identifica y bloquea la comunicación saliente a sitios C&C maliciosos. • Los recursos de inteligencia de amenazas en la nube se utilizarán para actualizaciones e identificación de ataques C&C de día cero.		[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• Tras un ataque de bot identificado, la solución remediará completamente el ataque dejando el punto final limpio e ileso. **Protección de navegación web** • Navegadores compatibles, Windows: Chrome, Edge (cromo), FireFox. Sistema operativo Mac: Safari, Chrome, FireFox. • La solución tiene capacidades de limpieza sin hardware adicional. Los archivos entrantes se extraen de todo el contenido malicioso potencial, como secuencias de comandos, macros y contenido activo. • Al realizar la limpieza, el usuario final puede acceder al archivo original si el sandbox lo considera benigno. • Los archivos entrantes se emularán mediante sandboxing para contenido potencialmente malicioso. • La solución detectará sitios de phishing de día cero que solicitan credenciales de usuario, incluso si los motores de reputación no los conocen. • La solución impide que el usuario explore direcciones URL o dominios maliciosos conocidos. • La solución impide que el usuario utilice sus credenciales corporativas en un sitio que no pertenezca al dominio corporativo. • La solución proporciona filtrado de URL basado en categorías con una lista adicional en blanco y negro. • La solución aplica la función "Búsqueda segura" cuando emplean los motores de búsqueda de Google, Bing y Yahoo. • El usuario no puede eliminar la protección de navegación de ninguna manera. **Sandboxing** • Todos los archivos escritos en el sistema de archivos son monitoreados y analizados estáticamente. Si se encuentran como potencialmente maliciosos, los archivos son emulados por sandboxing y puestos en cuarentena si se encuentran como maliciosos. • La solución es capaz de limpiar completamente el endpoint de cualquier		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			resto del ataque en caso de que el sandbox encontrara que el archivo es malicioso. **Prevención de exploits** • La solución detecta y evita técnicas de explotación de software confiable. • La solución tiene la capacidad de bloquear los nuevos ataques RDP RCE como BlueKeep en sistemas sin parches. **EDR** **Análisis forense** • La solución creará automáticamente un análisis de incidentes para cada detección/prevención que ocurra. Este análisis incluye árboles de ejecución de procesos incluso entre arranques si es relevante. • El informe forense identifica automáticamente el punto de entrada de la actividad maliciosa y resaltará el daño potencial, la acción de remediación y toda la cadena de ataque. • La solución mejora las detecciones de seguridad o antimalware de terceros mediante la creación y visualización automáticas de un informe de incidentes. • El informe forense registra, presenta y quita la ofuscación de los scripts de PowerShell utilizados durante un ataque. • La solución enumerará el análisis de reputación de los archivos, las URL y las IP utilizadas durante un ataque. La solución muestra la geolocalización de IP como parte de la información de reputación. • La solución puede seguir métodos indirectos de ejecución utilizados por malware como llamadas WMI e inyecciones para poder rastrear la actividad de malware más avanzado. • La solución incluye los siguientes sensores: Servicio de ejecución remota Descubrimiento del proceso de creación Descubrimiento de la ventana de la aplicación Tarea programada Captura de pantalla Captura de entrada DDE (intercambio dinámico de datos).		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• La solución crea un informe de incidentes que muestra el incidente en términos de Mitre ATT&CK Matrix. • La solución permite la búsqueda de múltiples tipos de datos de sensores no detectados, incluidos datos de archivo, proceso, red, registro, inyección y usuario. • La solución permite la remediación de cualquier archivo o proceso que se encuentre a través de la plataforma EDR. • La solución permite el análisis forense y el informe de cualquier indicador encontrado a través de la plataforma EDR. • La solución proporciona múltiples opciones de remediación manual, como Cuarentena, Proceso de eliminación y Análisis forense con remediación. • La solución proporciona una capacidad de gestión central para aislar las máquinas de forma remota. • La solución permite la búsqueda de incidencias mediante técnicas de Mitre Att&ck. • La solución tiene la capacidad de ver las direcciones MAC de cada computadora que envíe datos. • La solución EDR proporciona datos relacionados con periféricos y dispositivos de almacenamiento externo. • La solución enriquecerá automáticamente los resultados de búsqueda con reputación. **REGISTRO E INFORMES** **Informes** • La solución genera informes periódicos sobre tipos de malware, tipos de vulnerabilidades explotadas, etc. • La solución tiene la capacidad de generar informes visuales. • La solución proporciona el estado de salud del agente. **Registros** • La solución muestra el proceso afectado, las claves de registro afectadas y los archivos afectados en el entorno del sistema operativo.		

[redacted]

			• La solución muestra capturas de pantalla y videos de emulación de archivos maliciosos en el entorno Sandbox. • La solución puede registrar la comunicación de C&C desde el archivo BOT emulado. **CUMPLIMIENTO DE LA NORMATIVA** La solución cumple con: • Reglamento Internacional de Tráfico de Armas (ITAR). • Ley Federal de Gestión de la Seguridad de la Información (FISMA). • Marco de gestión de riesgos del Departamento de Defensa (RMF). • Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). • Normas de seguridad de la industria de tarjetas de pago (PCI). • Directiva de la comunidad de inteligencia (ICD) 503. • La solución deberá cumplir con las regulaciones de GDPR. **Inteligencia de amenazas** **Nube** • La solución se actualiza dinámicamente en función de una red global de sensores de amenazas mediante el intercambio de datos de amenazas. **VIGENCIA** Se considera una vigencia de Licenciamiento y Soporte directo por parte del fabricante de 24 meses. La solución de seguridad cuenta con un soporte de fabricante con los siguientes alcances: • Soporte de fabricante 24x7, con opción de que la Convocante pueda solicitar soporte de manera directa. • Soporte telefónico y por correo electrónico • Solicitudes de soporte ilimitado • Acceso a la base de datos de conocimientos • Acceso a actualizaciones mayores y mejoras • Acceso a Hot Fixes y paquetes de servicio **CURSOS** **AXTEL S.A.B. de C.V.** considera un curso oficial en un centro autorizado de entrenamiento autorizado por el fabricante Check Point, es un curso básico		

[redacted]

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			para la administración de la solución de protección de punto final para 1 asistente. • Se incluye curso para una persona, curso Check Point Harmony Endpoint Specialist (CCES). • Duración 2 días • Modalidad virtual • Curso en español • Material digital en idioma inglés certificado por el fabricante • Instructor certificado • Diploma de participación • Incluye examen de certificación el cual la Convocante deberá presentar en un centro de evaluación autorizado por el fabricante. **SERVICIO DE INSTALACIÓN** **AXTEL S.A.B. de C.V.** incluye todo lo necesario para la correcta instalación y operación de la solución de protección de punto final. • Incluye suministro, configuración, puesta a punto del licenciamiento solicitado. • **AXTEL S.A.B. de C.V.** considera los servicios profesionales para la instalación, configuración y puesta en funcionamiento de la solución de protección de punto final. • Activación y configuración de las funciones de seguridad. • La Convocante proporcionará a **AXTEL S.A.B. de C.V.** en caso de resultar ganador el inventario de equipos de cómputo y servidores sobre los cuales desplegará la solución de protección. • **AXTEL S.A.B. de C.V.** creará los paquetes de instalación adecuados para realizar la instalación de todos los equipos de cómputo o servidores. • **AXTEL S.A.B. de C.V.** realizará la validación de los sistemas operativos y versiones al fin de asegurar el 100% de la compatibilidad de la solución antes de realizar la instalación del agente. • **AXTEL S.A.B. de C.V.** creará una estrategia de despliegue masivo, en caso de no poder realizarse, **AXTEL**		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			S.A.B. de C.V. realizará la instalación manual de 50 agentes. • **AXTEL S.A.B. de C.V.** realizará la configuración de la Consola de Administración en la nube del fabricante Check Point. • **AXTEL S.A.B. de C.V.** proporcionará la documentación con el proceso para ejecutar la instalación manual para que la Convocante finalice el despliegue de la solución de seguridad. • Se considera: o Configuración de hasta 10 políticas. (Web & Files Protection) o Configuración de Behavioral Protection. (Best Practice) o Configuración de Análisis y Remediciones. (Best Practice) • El servicio considera una sesión remota para las pruebas de comunicación entre los componentes, agentes de la consola y aplicación de políticas. • **AXTEL S.A.B. de C.V.** realizará la configuración de todos los módulos o funcionalidades de seguridad incluidos en el licenciamiento. • **AXTEL S.A.B. de C.V.** previo al inicio de los trabajos realizará un plan de trabajo en conjunto con la Convocante a fin de garantizar la correcta ejecución de los trabajos y la mínima afectación de los equipos de cómputo o servidores. • **AXTEL S.A.B. de C.V.** realizará las pruebas de funcionamiento necesarias para asegurar correctamente la operación de los equipos de seguridad. • **AXTEL S.A.B. de C.V.** incluye como parte de los servicios la entrega de una memoria técnica al finalizar los servicios profesionales. • **AXTEL S.A.B. de C.V.** entregará el licenciamiento y las garantías/pólizas de soporte técnico del fabricante. Con el fin de garantizar la correcta ejecución de los servicios, **AXTEL S.A.B. de C.V.** incluye como parte de su propuesta técnica el certificado que avala a la persona que realizará funciones de Administrador de		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			Proyectos con las capacidades de Project Management Professional (PMP). Dicho certificado puede ser localizado en el **Apéndice 1** de la presente propuesta técnica. **SOPORTE TÉCNICO PARA LICENCIAS ENDPOINTS** **AXTEL S.A.B. de C.V.** brindará soporte técnico a solución de protección de puntos finales por 2 años, los alcances del soporte técnico cumplen con: • Cuenta con una mesa de ayuda para la recepción de solicitudes de atención con un esquema de atención 24x7. • Cuenta con soporte técnico durante la vigencia del servicio con atención en un esquema de tipo 5x8. • Incluye soporte técnico por medio telefónico, remoto y email. • Incluye soporte técnico en las configuraciones y resolución de dudas sobre la administración de la solución de seguridad. • Incluye acciones correctivas y resolución de problemas para incidencias. • Apertura de casos y seguimiento puntual con fabricante para incidencias. • **AXTEL S.A.B. de C.V.** mantiene actualizada la solución de seguridad durante la vigencia del servicio. • **AXTEL S.A.B. de C.V.** proporciona soporte técnico a través de un centro SOC (Security Operation Center) propietario. El documento que comprueba la pertenencia del SOC podrá ser localizada en el **Apéndice 3** de la presente propuesta técnica. • **AXTEL S.A.B. de C.V.** alinea todos sus procesos a las mejores prácticas ITIL, ISO27001:2013, 20000-1:2018, ISO 37001:2016 y 9001:2015. **AXTEL S.A.B. de C.V.** proporciona como parte de su propuesta técnica los certificados que demuestran el cumplimiento de dichos estándares. Dichos certificados podrán ser localizados en el **Apéndice 4** de la presente propuesta Técnica.		

ANEXO 1 DEL CONTRATO No. PODJUDTSJ-CA 18/2023-PA-PB

			• El SOC de **AXTEL S.A.B. de C.V.** pertenece al grupo de respuesta de incidencias FIRST. • https://www.first.org/members/teams/axtel-csirt • **AXTEL S.A.B. de C.V.** alinea todos sus procesos a las mejores prácticas ITIL, incluye como parte de su propuesta los certificados de 3 personas que cuentan con certificación ITIL Foundation e ITIL OSA. Dichos certificados podrán ser localizados en el **Apéndice 5** de la presente propuesta Técnica		
				Subtotal Partida	**$ 515,660.00**
				I.V.A.	**$ 82,505.60**
				Total Partida	**$ 598,165.60**
				Subtotal general	**$4,244,312.00**
				I.V.A.	**$679,089.92**
				Total general propuesta	**$4,923,401.92**

Importe en letras: Cuatro millones novecientos veinte y tres mil cuatrocientos un pesos 92/100 Moneda nacional IVA incluido

* PLAZO Y LUGAR DE ENTREGA: LOS ESTABLECIDOS EN LOS PUNTOS 1.2.6. Y 1.2.7. DE LAS BASES DE LICITACIÓN.

* CONDICIÓN DE ENTREGA: NO SE OFERTAN FECHAS DE ENTREGA POSTERIORES, NI PERIODOS O TIEMPOS DE GRACIA, TAMPOCO SE SOLICITARÁN PRÓRROGAS SALVO POR CASO FORTUITO O FUERZA MAYOR O CAUSAS ATRIBUIBLES A EL TRIBUNAL SUPERIOR DE JUSTICIA.

AXTEL S.A.B. de C.V. EN CASO DE RESULTAR GANADOR, ENTREGARÁ JUNTO CON LOS BIENES POR PARTIDA CONTRATADA, LAS GARANTÍAS DEL FABRICANTE, LAS CUALES VENDRÁN A NOMBRE DEL: PODER JUDICIAL DEL ESTADO - TRIBUNAL SUPERIOR DE JUSTICIA DEL ESTADO, LO ANTERIOR AUNADO A LA FIANZA DE GARANTÍA DE CUMPLIMIENTO DEL CONTRATO, LOS VICIOS OCULTOS Y LA CALIDAD DE LOS BIENES Y SERVICIOS VIGENTE POR UN PLAZO PARA LA PARTIDA "A" DE DOCE MESES Y PARA LA PARTIDA "B" DE DOS AÑOS, CONTADOS A PARTIR DE LA FECHA DEL CONTRATO.

RECEPTORES: LAS PERSONAS TITULARES DE LA SUBJEFATURA DEL DEPARTAMENTO DE INFORMÁTICA Y LA JEFATURA DEL DEPARTAMENTO DE SERVICIOS GENERALES Y MANTENIMIENTO AMBOS DE "EL TRIBUNAL SUPERIOR DE JUSTICIA".

Estos importes estarán vigentes por 30 días naturales a partir de la fecha del acto de entrega y apertura de propuestas y corresponden a la descripción técnica de los bienes y servicios contenida en el formato UDAP 03.

Dentro de los diez días hábiles siguientes a la fecha del fallo, entregaré una garantía de cumplimiento del contrato, los vicios ocultos y la calidad de los bienes y servicios de acuerdo con las condiciones del contrato, otorgando una fianza del 10% sobre el monto total adjudicado a mi favor en el contrato, incluido el Impuesto al Valor Agregado.

En adición a la propuesta solicitada oferto continuar con el servicio por 12 meses más de lo contemplado para esta licitación de la partida A, es decir del 01 de enero 2024 al 31 de diciembre del 2025

AXTEL S.A.B. de C.V. expresa su aceptación de todas las condiciones establecidas en las bases de esta licitación y en el modelo de contrato.

[redacted]