CONTRATO NO. UAF-ST-001/2020

CONTRATO ABIERTO PARA LA PRESTACIÓN DEL SERVICIO DE INFRAESTRUCTURA, SERVICIOS PROFESIONALES Y MANTENIMIENTO DE EQUIPOS Y APLICACIONES DE INTERNET Y EXTRANET (HOSTING CENTRO DE DATOS EXTERNO) 2020, QUE CELEBRAN POR UNA PARTE EL INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS, EN LO SUCESIVO "EL INEA", REPRESENTADO POR ANTONIO QUINTAL BERNY, EN SU CARÁCTER DE TITULAR DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS Y APODERADO LEGAL, ASISTIDO EN ESTE ACTO POR OSCAR ULISES CONTRERAS LUNA, SUBDIRECTOR TÉCNICO, QUIEN FUNGIRÁ COMO ADMINISTRADOR DEL CONTRATO, ASÍ TAMBIÉN POR ROBERTO RAMÍREZ GUZMÁN, JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO Y SERVICIOS, QUIEN SERÁ EL SUPERVISOR DEL CONTRATO; Y POR LA OTRA PARTE, SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V., REPRESENTADA POR JUAN CARLOS MARTÍNEZ VALDÉS, EN SU CARÁCTER DE APODERADO LEGAL, EN LO SUCESIVO "EL PROVEEDOR", A QUIENES ACTUANDO CONJUNTAMENTE SE LES DENOMINARÁ "LAS PARTES" AL TENOR DE LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

ANTECEDENTES

I. Para cubrir las erogaciones derivadas del presente Contrato se cuenta con disponibilidad de recursos, mediante la autorización de suficiencia presupuestaria número ST/01/2020, emitida por la Dirección de Prospectiva, Acreditación y Evaluación, a través de la Subdirección de Planeación, Programación y Presupuesto, en la partida 31602 (Servicios de telecomunicaciones), del Presupuesto de Egresos autorizado a **"EL INEA"** Asimismo se cuenta con Requisición de Bienes y Servicios número ST-001/2020 de fecha 07 de enero de 2020.

II. El presente Contrato fue otorgado mediante el procedimiento de adjudicación directa, con fundamento en los artículos, 22, fracción II, 26 fracción III, 40, 41 fracción III y 47, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; artículo 71 y72 fracción III y 85, de su Reglamento, y el capítulo IV.17 y IV.17.1 de **"LAS POBALINES"**, habiéndose notificado a **"EL PROVEEDOR"** de dicha adjudicación mediante carta de aceptación de servicios de fecha 14 de enero de 2020.

III. Asimismo, a través de escrito de fecha 7 de enero de 2020, signado por el Titular de la Subdirección Técnica, se justifica la contratación del servicio.

IV. Mediante oficio número ST/015/2020 de fecha 08 de enero de 2020, el Titular del área requirente solicita la contratación del servicio, motivo del presente Contrato.

CONTRATO NO. UAF-ST-001/2020

DECLARACIONES

"EL INEA" declara por conducto de su Apoderado Legal que:

I.1 Es un Organismo Descentralizado de la Administración Pública Federal, agrupado en el sector coordinado por la Secretaría de Educación Pública, con personalidad jurídica y patrimonio propio, con domicilio en la Ciudad de México, creado por Decreto Presidencial del 28 de agosto de 1981, publicado en el Diario Oficial de la Federación (DOF) el 31 del mismo mes y año, así como el que se reformó por Decreto Presidencial el 17 de agosto de 2012, publicado el 23 de los siguientes.

I.2 Que su Registro Federal de Contribuyentes número INE-810901-CP4.

I.3 Tiene por objeto promover y realizar acciones para organizar e impartir la educación para adultos, a través de la prestación de los servicios de alfabetización, educación primaria y secundaria, la formación para el trabajo y las demás que determinen las disposiciones jurídicas y los programas aplicables, apoyándose en la participación y la solidaridad social, de conformidad al artículo 2 del Decreto por el que se reforma el diverso por el que se crea el Instituto Nacional para la Educación de los Adultos, publicado en el DOF el 23 de agosto de 2012.

I.4 En los términos señalados en la fracción VII del artículo 22 de la Ley Federal de las Entidades Paraestatales, el Director General de este Organismo Descentralizado de la Administración Pública Federal tiene, entre otras facultades, la de otorgar poderes a nombre de **"EL INEA"**, así como nombrar representantes.

I.5 Antonio Quintal Berny, Apoderado Legal, cuenta con las facultades necesarias para formalizar el presente Contrato, lo cual se acredita con el testimonio del Poder General, número 169,253 de fecha 22 de enero de 2019, otorgado ante la Fé del Notario Público número 42 de la Ciudad de México, Lic. Salvador Godínez Viera, que le confiere entre otras facultades, poderes generales para Actos de Administración, mismos que no le han sido modificadas ni disminuidas a la presente fecha.

I.6 Para los efectos del presente Contrato, señala como su domicilio legal el ubicado en la Calle Francisco Márquez número 160, colonia Condesa, Demarcación Territorial Cuauhtémoc, Código Postal 06140, Ciudad de México.

"EL PROVEEDOR" declara por conducto de su apoderado legal que:

II.1 Es una persona moral, legalmente constituida conforme a las leyes mexicanas, lo que acredita con la Escritura Pública número 95, 987 de fecha 23 de marzo de 2001, otorgada ante la fe del Lic. Arturo Sobrino Franco, Titular de la Notaría Pública número 49 del Distrito Federal, ahora Ciudad de México, y con Registro Federal de Contribuyentes SNM010323EB5.

II.2 Cuenta con las facultades suficientes para contratar y obligarse a nombre de su representada, como se acredita con la Escritura Pública número 77, 500 de fecha 25 de agosto de 2016, otorgada ante la fe del Lic. Roberto Núñez y Bandera, titular de la Notaría Pública número 1, del Distrito Federal, ahora Ciudad de México, mismas que no le han sido modificadas ni disminuidas a la presente fecha.

II.3 Cuenta con facultades suficientes para contratar y obligarse conforme a lo establecido en el presente Contrato.

II.4 Dentro de su actividad económica, brinda servicios de Hosting, alojamiento de páginas de Internet.

II.5 Conoce plenamente el contenido de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, declarando bajo protesta de decir verdad que no se encuentra en ninguno de los supuestos que señalan los artículos 50 y 60 de este ordenamiento.

II.6 Cuenta con la experiencia, capacidad jurídica, material y económica, así como con la organización y los elementos técnicos y humanos necesarios para cumplir con las obligaciones derivadas del presente Contrato.

II.7 Manifiesta bajo protesta de decir verdad, que **"EL INEA"** no es su único cliente.

II.8 Para los efectos del presente Contrato, señala como su domicilio fiscal el ubicado en Paseo de la Reforma No. 5287, Colonia Cuajimalpa, Demarcación Territorial Cuajimalpa de Morelos, Código Postal 05000, Ciudad de México.

Declaran "LAS PARTES" que:

III.1 Las actividades que realicen de manera conjunta no involucran relaciones de carácter administrativo, laboral o cualquier otra que implique subordinación o que impida el libre desarrollo de sus objetivos.

III.2 El presente Contrato constituye el acuerdo entre **"LAS PARTES"** en relación con su objeto y deja sin efecto cualquier otra negociación, obligaciones o comunicación entre éstas ya sea verbal o escrita, efectuada con anterioridad en que se firme el mismo.

III.3 Se reconocen recíprocamente la calidad con que comparecen y están de acuerdo con los antecedentes y las declaraciones, por lo que manifiestan su conformidad para suscribir el presente instrumento.

REVISIÓN JURÍDICA

III.4 Se deberá considerar que de conformidad con el artículo 54 bis, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su reglamento, se procederá a la terminación anticipada, cuando concurran razones de interés general o cuando por causas justificadas se extinga la necesidad de requerir el servicio o se determine la nulidad total o parcial de los actos que dieron origen al Contrato con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública, o de así ser necesario conforme a las disposiciones de contratación o el Instituto Nacional Para la Educación de los Adultos.

Expuesto lo anterior, **"LAS PARTES"** otorgan las siguientes:

CLÁUSULAS

PRIMERA. - OBJETO.
"EL PROVEEDOR" se obliga con **"EL INEA"** a prestar el de **"Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting Centro de Datos Externo) 2020**".

La contratación del servicio antes referido se desarrollará de acuerdo con la programación que determine **"EL INEA"** a través del administrador y/o supervisor del Contrato, y que se enuncia con mayor amplitud en el Anexo Único que se integra por el anexo técnico y cotización. **"LAS PARTES"** convienen en agregar éste Anexo Único al Contrato como parte íntegra del mismo.

SEGUNDA. - MONTO.
"LAS PARTES" acuerdan que el monto mínimo por la prestación del servicio objeto del presente Contrato, es por la cantidad de **$4´352,469.67 (Cuatro millones trescientos cincuenta y dos mil cuatrocientos sesenta y nueve pesos 67/100 M.N.)**, y un monto máximo por la cantidad de **$10´881,174.18 (Diez millones ochocientos ochenta y un mil ciento setenta y cuatro pesos 18/100 M.N.)**, que incluye el Impuesto al Valor Agregado, que se cubrirá contra entrega de los servicios contratados como se detalla en el Anexo Único.

Así mismo convienen **"LAS PARTES"** que por ninguna circunstancia el precio pactado variará durante la vigencia del presente Contrato.

Si **"EL PROVEEDOR"** recibiera pagos en exceso deberá reintegrar las cantidades entregadas más los intereses que se calcularán conforme a una tasa que será igual a la establecida en la Ley de Ingresos de la Federación 2020, como si se tratara del supuesto de prórroga para el pago de créditos fiscales. Los cargos se calcularán sobre las cantidades pagadas en exceso en cada caso y se computará por días naturales, desde la fecha del pago hasta que se ponga a disposición de **"EL INEA"**.

"EL INEA" se obliga a realizar el pago como se detalla en el Anexo Único, por los servicios realizados conforme a las características y especificaciones contratadas.

TERCERA. - OBLIGACIONES DE "EL PROVEEDOR".
Prestar los servicios objeto de este Contrato, de acuerdo con las normas, tiempos, requerimientos, instrucciones, programas, especificaciones y datos que le indique **"EL INEA"** a través del administrador del Contrato y/o del supervisor del mismo y en su caso, ajustarse a las indicaciones que éstos le otorguen por escrito.

Aceptar, de ser el caso, que **"EL INEA"** efectúe las retenciones, deducciones o descuentos previstos en las disposiciones fiscales aplicables.

Entregar al administrador y/o al supervisor del Contrato, en caso de que se lo soliciten, un informe del avance de la prestación del servicio.

CUARTA. - CONDICIONES DE PAGO.
"EL INEA" realizará el pago a través depósito bancario, mediante una transferencia electrónica de recursos a la cuenta bancaria señalada por **"EL PROVEEDOR"**, por el importe del servicio proporcionado. **"EL PROVEEDOR"** deberá presentar un Comprobante (s) Fiscal (es) Digital (es) por Internet (CFDI) en el cual especificará el importe mensual del Contrato.

El pago se realizará en 11 exhibiciones contra entrega de los resultados e informes de actividades que se estipulan en el Anexo Único y conforme a las características y especificaciones contratadas, en un plazo que no podrá exceder de veinte días naturales contados a partir de la entrega del (los) CFDI previa prestación de los servicios en los términos establecidos en el Contrato. El plazo señalado no incluye aclaraciones o demoras atribuibles a **"EL PROVEEDOR"** o carencia de documentos comprobatorios para la emisión del pago.

El (los) CDFI, deberá (n) cumplir con los requisitos fiscales vigentes, indicando el número de Contrato, la descripción completa del servicio prestado, el costo unitario, el desglose del Impuesto al Valor Agregado, el importe total y los datos de **"EL PROVEEDOR"**.

El Titular del Departamento de Control Presupuestal validará el (los) CDFI, y será el responsable de devolver a **"EL PROVEEDOR"** los comprobantes que tengan errores, deficiencias o falta de requisitos dentro de los dos días hábiles siguientes a la fecha de su recepción, indicando por escrito a **"EL PROVEEDOR"** las deficiencias que deberá corregir.

Las obligaciones fiscales vigentes que resulten con motivo del presente Contrato serán cumplidas puntualmente por cada una de **"LAS PARTES"** en lo que les corresponda.

QUINTA. - CONSTANCIA DE CUMPLIMIENTO.
Una vez cumplidas las obligaciones por parte de **"EL PROVEEDOR"** conforme a las características y especificaciones contratadas, se procederá a extender la constancia de cumplimiento de obligaciones por parte del área requirente.

SEXTA. - FINIQUITO.
"EL PROVEEDOR" otorgará, al momento de efectuarse el último pago, el finiquito más amplio que en derecho proceda en el que expresamente manifieste que **"EL INEA"** cumplió con todas y cada una de las obligaciones contraídas, sin reservarse acción ni derecho alguno por ejercitar con posterioridad.

SÉPTIMA. - COMPROBACIÓN, SUPERVISIÓN Y VERIFICACIÓN.
"EL INEA", por conducto del Administrador y del Supervisor del Contrato, serán los responsables de verificar, comprobar y supervisar que se cumplan con los derechos y obligaciones establecidas en el presente Instrumento.

Las funciones del Administrador del Contrato son: interactuar con el Supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Las funciones del Supervisor del Contrato son: interactuar con el Administrador y **"EL PROVEEDOR"**, para dar seguimiento y verificar que el servicio se cumpla con las especificaciones, actividades y entregas a entera satisfacción conforme a lo establecido en el Anexo Único.

El Administrador del Contrato será Oscar Ulises Contreras Luna, Subdirector Técnico, y el Supervisor será Roberto Ramírez Guzmán, Jefe de Departamento de Soporte Técnico y Servicios, o quienes en el futuro les sustituyan.

OCTAVA. - VIGENCIA.
La vigencia del Contrato será del 17 de enero al 31 de diciembre de 2020.

Esta vigencia es voluntaria para **"EL INEA"** y forzosa para **"EL PROVEEDOR"**, por lo que el primero podrá dar por terminado anticipadamente el presente Instrumento cuando concurran razones de interés general, o por causas justificadas se extinga la necesidad del objeto requerido.

NOVENA. - DEFECTOS Y VICIOS OCULTOS.
"EL PROVEEDOR" se obliga ante el **"EL INEA"** a responder de los defectos y vicios ocultos en la calidad de los servicios, así como de cualquier responsabilidad en que hubiera incurrido, en los términos señalados en el presente Contrato y en la legislación aplicable.

DÉCIMA. - CONFIDENCIALIDAD.
"LAS PARTES", acuerdan en tratar como clasificada toda la información intercambiada o acordada con motivo del presente instrumento, excepto aquella que deba considerarse pública según lo dispuesto por los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública, los artículos 97, 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información, así como para la elaboración de Versiones Públicas, la Ley

Federal de Protección de Datos Personales en Posesión de los Particulares y demás disposiciones aplicables, no se podrá divulgar salvo que sea autorizado por escrito y de forma expresa por el área competente de **"EL INEA"**.

Toda la información impresa, audiovisual, en archivo magnético o que pueda almacenarse por algún otro medio técnico o científico que los adelantos de la ciencia lo permitan, que se proporcionen entre sí **"LAS PARTES"** para el debido cumplimiento del objeto del presente Contrato, se considera estrictamente reservada y se prohíbe su divulgación a terceros con cualquier carácter, hasta por el tiempo de cinco años, excepto en los casos y condiciones que establezca la ley.

DÉCIMA PRIMERA. - SUSPENSIÓN.
"EL INEA" podrá suspender los efectos de este Contrato, por razones de austeridad presupuestal o de orden público. En este caso, **"EL INEA"** se compromete a notificar por escrito a **"EL PROVEEDOR"** en el domicilio señalado en su declaración II.8, con tres días de anticipación y, por lo tanto, **"EL INEA"** cubrirá el o los pagos por los servicios recibidos, conforme a las características y especificaciones requeridas, procediendo a la suscripción del finiquito correspondiente.

DÉCIMA SEGUNDA. - TERMINACIÓN ANTICIPADA.
"EL INEA" podrá dar por terminado anticipadamente sin su responsabilidad el presente Instrumento, cuando por causas justificadas se extinga la necesidad de requerir los servicios recibidos, originalmente contratados, o se determine la nulidad total o parcial de los actos que dieron origen al Contrato.

La terminación anticipada del Contrato se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma en términos del artículo 54 bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su Reglamento y demás normatividad aplicable, dando aviso a **"EL PROVEEDOR"** con tres días naturales de anticipación.

DÉCIMA TERCERA. - RESCISIÓN.
"EL INEA" podrá rescindir administrativamente el presente Instrumento cuando **"EL PROVEEDOR"** incurra en incumplimiento de sus obligaciones, en términos del artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículo 98 de su Reglamento y las disposiciones de la Ley Federal de Procedimiento Administrativo.

"EL PROVEEDOR" no podrá ceder en forma parcial o total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del presente Contrato, en caso que llegara a suceder será causa de rescisión.

DÉCIMA CUARTA. - PROCEDIMIENTO DE RESCISIÓN.
En caso de que se actualice la hipótesis de incumplimiento mencionada en la Cláusula anterior, **"EL INEA"** comunicará por escrito a **"EL PROVEEDOR"** el probable incumplimiento en que haya incurrido, para que en un término de tres días hábiles exponga lo que a su derecho convenga y aporte en su caso, las pruebas que estime pertinentes para desvirtuar el posible incumplimiento.

Transcurrido el término a que se refiere el párrafo anterior, se resolverá considerando los argumentos y pruebas que **"EL PROVEEDOR"** hubiere hecho valer.

La determinación final de dar o no por rescindido el Contrato deberá ser fundada y motivada, la cual será notificada a **"EL PROVEEDOR"** dentro de los quince días hábiles siguientes al término señalado en el párrafo primero de esta Cláusula, y cuando se rescinda el Instrumento se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL INEA"** por concepto de los servicios recibidos, hasta el momento de la rescisión.

DÉCIMA QUINTA. - LEGISLACIÓN APLICABLE.
"EL INEA" y **"EL PROVEEDOR"** convienen en someterse a las disposiciones que señala la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás legislación aplicable.

DÉCIMA SEXTA. - PENA CONVENCIONAL.
"LAS PARTES" convienen que en el caso de incumplimiento en el tiempo de la prestación de los servicios **"EL INEA"** procederá a calcular la pena convencional conforme al 1% por cada día natural de atraso, en el inicio de la prestación del servicio sobre el monto total del presente Contrato. **"EL INEA"** notificará a **"EL PROVEEDOR"** dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor de **"EL INEA"** en el domicilio establecido en la declaración I.6 de **"EL INEA"**.

Así mismo se aplicarán penas deductivas conforme al 1% del monto total de la factura por cada día natural de la prestación del servicio de forma parcial y/o deficiente, conforme se establece en el Anexo Único. **"EL INEA"** notificará a **"EL PROVEEDOR"** dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque certificado o cheque de caja a favor de **"EL INEA"** en el domicilio establecido en la declaración I.6 de **"EL INEA"**.

El cálculo de las penas convencionales y deductivas es responsabilidad del área requirente a través del Administrador y/o Supervisor del Contrato, así como de cualquier incumplimiento y deberá avisar en tiempo y en forma a la Unidad de Administración y Finanzas.

"EL PROVEEDOR" queda obligado ante **"EL INEA"**, de responder por la calidad de los servicios, así como de cualquier otra responsabilidad en que incurra en los términos del presente Contrato y su Anexo Único.

DÉCIMA SÉPTIMA. - GARANTÍA DE CUMPLIMIENTO.
"EL PROVEEDOR" para asegurar el debido cumplimiento de este Contrato, se obliga a entregar a **"EL INEA"**, dentro de los diez días naturales siguientes a la fecha de su firma, preferentemente una **FIANZA** que tendrá carácter de **GARANTÍA DE CUMPLIMIENTO INDIVISIBLE**, expedida por compañía legalmente autorizada por la Secretaría de Hacienda y Crédito Público, a favor de **"EL INEA"**, por un importe equivalente al 10% del monto total del costo del servicio, sin considerar el Impuesto al Valor Agregado, de conformidad con el artículo 48, último párrafo y 49, fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Al término de la vigencia del presente Contrato, de no existir reclamación por parte de **"EL INEA"** sobre el cumplimiento de las obligaciones de **"EL PROVEEDOR"**, este deberá solicitar por escrito la liberación de la fianza ante el Administrador del Contrato de **"EL INEA"**, quien a su vez solicitará a la Subdirección de Recursos Materiales, exprese por escrito la procedencia de la devolución y cancelación de la fianza.

DÉCIMA OCTAVA. - CASO FORTUITO O FUERZA MAYOR.
Ninguna de **"LAS PARTES"** será responsable de cualquier retraso o incumplimiento de este Instrumento que resulte directa o indirectamente de caso fortuito o fuerza mayor, la que de invocarse deberá acreditarse fehacientemente.

DÉCIMA NOVENA. - RELACIÓN CONTRACTUAL.
La relación existente entre **"EL INEA"** y **"EL PROVEEDOR"** es de carácter estrictamente administrativa, por lo que **"EL PROVEEDOR"** es el único responsable de las obligaciones de carácter civil, laboral y de cualquier otra naturaleza para con las personas con quien se auxilie en el cumplimiento del presente Contrato, por lo que expresamente reconoce y acepta lo que dispone el artículo 13 de la Ley Federal del Trabajo, por ser el único y exclusivo patrón de los elementos que comisione, quienes no tienen ni tendrán vínculo laboral de alguna clase con **"EL INEA"** y por lo tanto, en ningún momento se considera a **"EL INEA"** como intermediario.

Por lo anterior, **"EL PROVEEDOR"** se obliga a dejar a salvo a **"EL INEA"** de cualquier reclamación o acción instaurada en su contra, o de cualquier juicio o procedimiento que se instaure con motivo del presente Contrato, así como a pagar en su caso los daños y perjuicios que se le causen.

VIGÉSIMA. - RESPONSABILIDAD.
"EL PROVEEDOR" exenta a **"EL INEA"** de toda responsabilidad legal que pudiera surgir, derivada como consecuencia directa o indirecta de la prestación de los servicios.

VIGÉSIMA PRIMERA. - DATOS PERSONALES.
Para efectos de lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y las disposiciones que de ella emanen, **"EL PROVEEDOR"** reconoce y acepta expresamente que la forma y términos en que cualquier información que se considere como datos personales serán protegidos y tratados de conformidad con lo que se establece y se regula en la Ley mencionada y en el **"Aviso de Privacidad"** correspondiente.

VIGÉSIMA SEGUNDA. - DE LA INFORMACIÓN A LOS ÓRGANOS DE CONTROL.
"EL INEA" y **"EL PROVEEDOR"** se obligan a entregar a la Secretaría de la Función Pública y/o al Órgano Interno de Control en **"EL INEA"**, en el momento que se les requiera, toda la información relacionada con el presente Contrato.

VIGÉSIMA TERCERA. - DE INTEGRIDAD Y COMBATE A LA CORRUPCIÓN.
"EL PROVEEDOR" se obliga a que durante la ejecución de este Instrumento, ni él ni sus socios, directivos o empleados, por sí o por interpósita persona:

a) Solicitarán o promoverán la realización, el otorgamiento o la contratación indebidos de los servicios objeto del Contrato;

b) Promoverán ante las personas que detenten la calidad de servidores públicos la gestión, la tramitación o la resolución ilícita de negocios públicos relacionados con la administración del Contrato, y

c) Ofrecerán, prometerán o darán dinero o cualquier otra dádiva, a los servidores públicos encargados de la administración del presente instrumento.

"EL INEA" y **"EL PROVEEDOR"** acuerdan que durante la vigencia del Contrato se comprometen a actuar con estricto apego a las anteriores reglas de conducta para combatir el cohecho, el tráfico de influencia y el uso indebido de atribuciones y facultades.

VIGÉSIMA CUARTA. - PATENTES, MARCAS Y DERECHOS DE AUTOR.
"EL PROVEEDOR" asumirá la responsabilidad total para el caso que se infrinjan patentes o marcas, o violen derechos de autor, tanto en el ámbito nacional como internacional con respecto de la prestación de servicios objeto de este Contrato, por lo que de presentarse alguna reclamación a **"EL INEA"** con ese motivo, durante la vigencia de este, o posterior a ella, **"EL PROVEEDOR"** conviene desde ahora en pagar cualquier importe que de ello se derive y sacar a salvo y en paz de tales reclamaciones a **"EL INEA"** a más tardar a los quince días naturales a partir de que sea notificado de ello este último.

"EL PROVEEDOR", por tratarse de un trabajo por el que recibe remuneración, reconoce que **"EL INEA"** es el titular de los derechos patrimoniales, conforme al artículo 83 de la Ley Federal del Derecho de Autor.

VIGÉSIMA QUINTA. - DEL COMBATE A LAS PRÁCTICAS MONOPÓLICAS ABSOLUTAS Y RELATIVAS.
"EL PROVEEDOR" se obliga a que, durante la vigencia del presente Instrumento, se abstendrán de celebrar acuerdos, por sí o a través de interpósita persona, entre sí o con otros agentes económicos, que tengan por finalidad o efecto, en relación con los servicios objeto de este Contrato:

a) Fijar, elevar, concertar o manipular el precio de dichos servicios;

b) Restringir o limitar la prestación de los servicios;

c) Dividir, distribuir, asignar o imponer porciones o segmentos del mercado gubernamental;

d) Establecer, concertar o coordinar posturas o la abstención en los procedimientos de contratación realizados conforme a lo dispuesto en el Contrato, o

e) Intercambiar información cuyo propósito o efecto corresponda a los referidos en los numerales anteriores.

"EL PROVEEDOR" se abstendrá de incurrir en prácticas monopólicas relativas, como están definidas en los artículos 54 a 56 de la Ley Federal de Competencia Económica.

VIGÉSIMA SEXTA. - DEL PROCEDIMIENTO DE CONCILIACIÓN.
En cualquier momento **"EL PROVEEDOR"** y **"EL INEA"** podrán presentar ante la Secretaría de la Función Pública, solicitud de conciliación, por desavenencias derivadas del cumplimiento del Contrato, cuyo procedimiento se substanciará conforme a lo dispuesto en el Título Sexto "De la solución de las controversias", Capítulo Segundo, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, así como de su reglamento.

En el supuesto de que **"LAS PARTES"** lleguen a un acuerdo durante la conciliación, el convenio respectivo obligará a las mismas, y su cumplimiento podrá ser demandado por la vía judicial; en caso contrario, podrán optar por cualquier vía de solución a su controversia.

VIGÉSIMA SÉPTIMA. - MODIFICACIONES AL CONTRATO.
El presente Instrumento podrá ser modificado o adicionado por voluntad de **"LAS PARTES"**, siempre y cuando medie causa justificada o superviniente. Siempre que el monto total de las modificaciones no rebase en conjunto, el 20% del monto o cantidad de los conceptos y volúmenes establecidos originalmente en el mismo y el precio sea igual al pactado originalmente; así como que se cuente con la disponibilidad presupuestal correspondiente.

VIGÉSIMA OCTAVA. - CESIÓN DE DERECHOS.
"EL PROVEEDOR" no podrá ceder en forma parcial o total a favor de cualquier otra persona, los derechos y obligaciones que se deriven del presente Contrato, con excepción de los derechos de cobro, en cuyo caso deberá contar con el consentimiento previo por escrito de **"EL INEA"**, a través de la Unidad de Administración y Finanzas.

Los derechos de cobro, podrán cederse cuando **"EL PROVEEDOR"** opte por adherirse a las cadenas productivas de **"EL INEA"** en la página web https://cadenasnafin.com.mx, de conformidad con las disposiciones emitidas por la Secretaría de Hacienda y Crédito Público publicadas en el Diario Oficial de la Federación el 28 de febrero de 2007.

VIGÉSIMA NOVENA. - AUSENCIA DE VICIOS.
"LAS PARTES" manifiestan que a la firma del presente Contrato no media dolo, violencia, mala fe o cualquier otro vicio de consentimiento que pudiera invalidar.

TRIGÉSIMA. - ENCABEZADOS Y DEFINICIONES.
Los encabezados y definiciones señalados en las Cláusulas del presente Contrato se han utilizado únicamente para una rápida localización e identificación de su contenido, por lo que en ningún momento se entenderá que dichos encabezados y definiciones limitan o alteran el acuerdo de **"LAS PARTES"**.

TRIGÉSIMA PRIMERA.- JURISDICCIÓN.
Para la interpretación y cumplimiento de este Contrato, **"LAS PARTES"** se someterán expresamente a la jurisdicción y competencia de los Tribunales Federales con residencia en la Ciudad de México, renunciando a cualquier otro fuero que pudiera corresponderles en razón de sus respectivos domicilios presentes o futuros.

Leído el presente Contrato y enteradas **"LAS PARTES"** del valor, alcance y fuerza legal de sus Cláusulas, lo firman al calce y al margen, constante de 12 fojas, por triplicado para constancia y validez, en la Ciudad de México, a los 31 días del mes de enero del año dos mil veinte, conservando dos ejemplares **"EL INEA"** y uno **"EL PROVEEDOR"**.

Por "EL INEA"	**Por "EL PROVEEDOR"**
Antonio Quintal Berny **Titular de la Unidad de Administración y Finanzas y Apoderado Legal**	**Juan Carlos Martínez Valdés** **Apoderado Legal**
Administrador	**Supervisor**
Oscar Ulises Contreras Luna **Subdirector Técnico**	**Roberto Ramírez Guzmán** **Jefa de Departamento de Soporte Técnico y Servicio**

Las firmas que aparecen en esta hoja, forman parte del Contrato de Prestación de Servicios de fecha 31 de enero de 2020, celebrado entre este Instituto Nacional para la Educación de los Adultos y SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V., cuyo objeto es la prestación del Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting Centro de Datos Externo) 2020.

ANEXO TÉCNICO

CONTRATACIÓN DEL SERVICIO DE INFRAESTRUCTURA, SERVICIOS PROFESIONALES Y MANTENIMIENTO DE EQUIPOS Y APLICACIONES DE INTERNET Y EXTRANET (HOSTING CENTRO DE DATOS EXTERNO) 2020

Antecedentes

El cliente ha realizado contratos plurianuales para el servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting). La infraestructura mencionada se encuentra actualmente alojada en un Centro de Datos de alta especialización, en el cual están hospedadas las diferentes aplicaciones informáticas que apoyan a los procesos sustantivos enfocados a cumplir los servicios que demandan los usuarios del CLIENTE.

I. Requerimientos Funcionales

Descripción General del Servicio Requerido

El CLIENTE requiere de un contrato de servicios que provea la infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de internet y extranet de la entidad.

El contrato de servicios debe contemplar como mínimo el servicio de hospedaje dedicado de aplicaciones en infraestructura y servidores dedicados, lo cual permitirá alojar aplicaciones críticas para tener acceso vía internet. Se deberá incluir todo el soporte necesario en hardware, software, servicios y recursos humanos especializados de acuerdo a la tarea a desarrollar para implementar, instalar, reinstalar las aplicaciones del CLIENTE durante todo el tiempo que dure el contrato y soporte e instalación de equipo de comunicaciones y almacenamiento solicitado en este documento. Así mismo deberá contar con el personal dedicado y especializado de acuerdo a la tarea a desarrollar para el CLIENTE en servicio 7x24 los 365 días para soporte y asesoría de todas las plataformas de hardware, software (en todas las aplicaciones integradas).

A través de los servicios solicitados el CLIENTE contará con una infraestructura dedicada de alta calidad para hospedar de forma remota aplicaciones complejas de uso crítico alojadas en el centro de datos.

Este documento describe las especificaciones técnicas que en materia de hospedaje y/o co-ubicación de la plataforma tecnológica, procesamiento, almacenamiento,

seguridad, licenciamiento de software, soporte y comunicaciones del ambiente de producción de la información que soporta las aplicaciones de misión crítica que requiere el Instituto, en un esquema de servicios administrados.

Objetivos generales

1. Obtener una solución en la cual el licitante integrará todo lo requerido para alojar, instalar, migrar, operar, monitorear, soportar y mantener las aplicaciones en los servidores, equipos de comunicaciones y seguridad especificados en este documento.
2. Obtener altos niveles de servicio bajo un solo modelo de operación de acuerdo a lo establecido en este documento.

1. CANTIDAD Y ESPECIFICACIONES GENERALES.

La descripción general por partida es la siguiente:

PARTIDA	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
1	SERVICIO DE INFRAESTRUCTURA, SERVICIOS PROFESIONALES Y MANTENIMIENTO DE EQUIPOS Y APLICACIONES DE INTERNET Y EXTRANET (HOSTING CENTRO DE DATOS EXTERNO) 2020	1	Servicio

Lugar de prestación de los servicios

El servicio se brindará desde el Centro de Datos externo propuesto por el licitante y los sistemas y servicios hospedados serán accesibles desde cualquier lugar con internet y dentro de la República Mexicana.

Los entregables se presentarán a la Subdirección Ténica del CLIENTE, ubicada en la Calle Francisco Márquez # 160, Colonia Condesa, C. P. 06140, Cuauhtémoc, Ciudad de México.

Horario de servicio

Las 24 horas del día durante la vigencia del instrumento jurídico.

2. DESCRIPCIÓN Y ESPECIFICACIONES TÉCNICAS APLICABLES A LOS BIENES O SERVICIOS.

CARACTERÍSTICAS TÉCNICAS PARA LA PARTIDA 1.

Infraestructura

El centro de datos propuesto por el licitante, deberá contar con una infraestructura de alojamiento diseñado para operar como un centro de datos de alta disponibilidad y garantizar de acuerdo al Anexo I, una disponibilidad sin rebasar los minutos de indisponibilidad indicados en dicho anexo. El licitante deberá incluir los documentos que comprueben la certificación ICREA Nivel 4 o TIER III del Uptime Institute. Las instalaciones del licitante deberán estar diseñadas específicamente para el hospedaje de aplicaciones de misión crítica con características de seguridad y operación como las que se mencionan a continuación:

- Contar con medidas de protección física externa que lo mantenga seguro contra robo y actos vandálicos, así mismo deberá contar con estacionamiento para el resguardo de vehículos y deberá permitir el acceso al personal identificado y autorizado por el INEA.
- Estar ubicado en región geológica de terreno firme zona A (bajo) o B (moderado) de peligro sísmico de acuerdo a la clasificación de regionalización sísmica publicada por el Servicio Sismológico Nacional.
- La superficie o áreas donde se encuentren en operación los equipos de procesamiento y almacenamiento que contengan las aplicaciones e información del INEA, deberán estar delimitadas de otras instalaciones y áreas comunes a través de una estructura de aislamiento perimetral (jaula o equivalente, gabinetes cerrados o una solución auto contenida), de tal forma que el acceso físico a la infraestructura sólo pueda realizarlo personal autorizado por el licitante o el INEA, mediante rigurosos procedimientos de control de acceso, como detector de huellas, tarjetas de proximidad.
- Contar con cámara plena entre loza y piso falso con la altura suficiente no menor a 60 cm.
- Piso firme con revestimiento epóxico de alta conductividad eléctrica con características capacitivas, conductivas, disipativas y aislantes.

2019

- Contar con una acometida eléctrica dimensionada para garantizar la demanda y operación de las aplicaciones del CLIENTE alojadas en el centro de datos propuesto, y garantizar la disponibilidad indicada en el Anexo I.
- Contar con sub-estación de alta a baja tensión con sistemas de transferencia.
- Contar con equipos de energía ininterrumpida (UPS's) redundantes con las protecciones correspondientes de supresión de transitorios y entrega de los circuitos eléctricos monofásicos, bifásicos o trifásicos necesarios para la infraestructura integral de servicios dentro del centro de datos.
- El sistema de tierra interno deberá permitir aterrizar los dispositivos de cómputo y telecomunicaciones, racks y/o gabinetes y demás equipos necesarios.
- El sistema eléctrico en su totalidad deberá tener un arreglo al menos 2N y estará dimensionado para garantizar la demanda y operación de las aplicaciones del CLIENTE alojadas en el centro de datos propuesto y garantizar la disponibilidad indicada en el anexo I. Deberá contar con un arreglo de generadores que, en el caso de una interrupción prolongada de energía, deberá tener la capacidad de operar de manera autónoma y sin recargar combustible al menos 4 días.
- La interconexión de los dispositivos que integren la infraestructura asignada, se realizará a través de cableado estructurado que, dependiendo de la Interface de red de los equipos y su funcionalidad, deberá al menos ser del tipo UTP cat 6A (que soporte velocidades de transferencia del orden de 10/100/1000 MBPS), soporte de 10GE:10G base SR y 10G base LR, o fibra óptica, según sea el caso.
- No existirá cableado expuesto, ni tendidos de cableado mezclados de suministro eléctrico y datos.
- Contar con la capacidad instalada para recibir servicios de comunicaciones a través de fibra óptica y a través de infraestructuras independientes, de por lo menos 3 de los principales proveedores de telecomunicaciones (carriers) de la República Mexicana.
- Contar con al menos dos conexiones robustas y redundantes a la red de internet mediante accesos de alta velocidad y contener la funcionalidad de trafico seguro (clean pipes), para garantizar que contará con la suficiente capacidad de ancho de banda de tal suerte que, en caso de que cualquiera de ellos no

proporcione el servicio por alguna contingencia, el medio de acceso que permanezca en operación soporte la totalidad del tráfico del centro de datos.

- Contar con un arreglo de aires acondicionados de precisión al menos de n+1 dentro de las instalaciones donde se alberguen los equipos con controles automáticos de humedad y temperatura para mantener el rango de temperatura de operación de la infraestructura conforme a las especificaciones de los diversos fabricantes de los equipos que la compongan. El licitante incluirá el monitoreo de estos parámetros dentro del sistema de monitoreo integral del centro de datos.
- El licitante soportará los BTU's adicionales incurridos por la instalación de la infraestructura integral común de servicios, así como cualquier ampliación de infraestructura requerida para la prestación del servicio.
- Deberá considerar arreglos en rack para la optimización de espacios y crecimiento vertical, así como contar con la posibilidad de ampliación de superficie de al menos el 50% de la superficie asignada.

Procesamiento y Virtualización

El procesamiento propuesto por el licitante deberá llevarse a cabo fundamentalmente en servidores basados en tecnología x86 con soporte a x64, en formato rack en plataforma virtualizada, dedicados para el servicio requerido por el CLIENTE.

El licitante proporcionará la infraestructura necesaria para llevar a cabo el soporte físico para la operación del servicio de punta a punta, considerando el servicio de procesamiento correspondiente, el cual deberá estar acorde con las especificaciones del servicio de centro de datos en base a su oferta. Deberá considerar el cableado tanto para LAN, SAN, configuraciones, seguridad física y lógica; como para los periféricos necesarios para el correcto funcionamiento de toda la infraestructura.

El licitante será responsable de proporcionar las licencias de software de virtualización solicitados por el CLIENTE.

El equipo de cómputo deberá contar con soporte garantizado durante la vigencia del contrato, la solución deberá reflejar que se contará con alta disponibilidad en todos sus componentes y en el centro de datos.

La solución de virtualización deberá soportar como guest los sistemas operativos mencionados en el Anexo I.

El equipamiento que proporcionará el licitante deberá contar con los antivirus necesarios y el licenciamiento requerido para su operación a nivel sistemas operativos, bases de datos, aplicaciones y todo aquello requerido para la operación de la plataforma del INEA.

El equipo deberá contar con garantía durante la vigencia del contrato en todos los componentes; con soporte técnico en línea y telefónico, y cobertura de servicio de soporte en sitio los 7 días de la semana, las 24 horas del día (7x24); y asistencia en sitio en un máximo de cuatro (4) horas en caso de requerirse.

Se deberá considerar en la propuesta el licenciamiento del software necesario para soportar los servicios detallados, así como la administración y/o implementación de los mismos.
Se iniciará la migración de su información a los servidores proporcionados por el licitante iniciando con la aplicación SASA, la cual es la aplicación core de CLIENTE, una vez probada se realizarán la migración de las aplicaciones satélite. Las versiones de los sistemas operativos deberán ser respetadas ya que algunos de sus aplicativos tienen codependencias. El licitante ganador deberá de garantizar la continuidad de la operación.

Adicionalmente deberá considerar una solución en alta disponibilidad y comprender todos sus componentes de manera dedicada. Esto es derivado de la criticidad de su operación y con la finalidad de brindar el nivel de servicio esperado por parte de INEA

Cableado estructurado, comunicaciones y almacenamiento

Cableado estructurado:

La interconexión de los dispositivos que integren la infraestructura propuesta, se realizará respetando la norma de cableado estructurado, que dependiendo de la interface de red de los equipos deberá ser mínimo del tipo UTP categoría 6A o 10GE:10G base SR y 10G base LR, según sea el caso.

El cableado estará debidamente identificado, tanto en el panel de distribución como en los cables de interconexión.

El licitante proporcionará todos los cables, tableros, conectores y dispositivos de interconexión para todos y cada uno de los servidores, equipos de comunicaciones y seguridad descritos en este documento.

La velocidad de transferencia en la red del centro de datos entre los servidores del instituto será de 10 GB.
El licitante considera una red independiente para el monitoreo de los servidores.

Comunicaciones:

Equipamiento de conectividad para la red LAN

El licitante proveerá el equipamiento de switching necesario para la interconexión de toda la infraestructura del centro de datos CLIENTE; y la disponibilidad en la misma será de al menos la solicitada en el anexo I de acuerdo a la infraestructura solicitada en este documento.

El esquema de conexión será coordinado por el área técnica del licitante, de tal forma que la solución sea la óptima para el desempeño de las aplicaciones.

El licitante contará con personal técnico capacitado en el equipo propuesto, el licitante dará las facilidades al instituto para que en cualquier momento pueda solicitar cambio del personal técnico asignado al instituto, si se considera necesario.

El licitante será el responsable de la configuración, monitoreo y mantenimiento de este servicio con el objetivo de cumplir con los niveles de servicio solicitados.

El equipo de switching de la solución, tendrá al menos las siguientes características:

Puertos 10GB a velocidad nominal, puertos GIGABIT SFP y/o 10/100/1000 necesarios para la solución propuesta y equipo dedicado al INEA considerando todas las conexiones de los servidores a los switches, servidores y firewalls, incluyendo todos los conectores y componentes necesarios para su conexión.
Fuente de poder redundante.
Capa 3 con manejo de VLANS y calidad de servicio, listas de acceso y validación vía RADIUS o TACACS+.
Posibilidad de limitar el ancho de banda por cada puerto del switch.

Fr... ...áuez 160, Col. ... C.P. 06140, Cuauhtémoc, Ciudad de México.
Tel: ... 52 41 28 00 · 52 41 29 00

El equipo debe ser de capacidad no bloqueable.
Soportar UDP, IP, ICMP y TCP.
Administración vía web, telnet.
Switching debe ser totalmente compatible con la infraestructura propuesta para la operación de los servicios.
Procesadores y fuentes de poder redundantes.

Acceso a la red de internet

El nivel de servicio mínimo comprometido por El licitante para este servicio deberá ser de 99.80%.

Este servicio será entregado a través del centro de datos del licitante en esquema redundante.

La solución propuesta proveerá un ancho de banda garantizado para el INEA de 70 MB en forma continua y será capaz de absorber picos hasta 110 MBPS de entrega continua de contenido de los portales y los sistemas hospedados. El hoster deberá tener establecido en México acuerdos de interconexión (Peering agreements) con por lo menos dos (2) proveedores de servicios de internet con capacidad destinada en infraestructura de medios de transmisión y ancho de banda para su operación del orden de 1 GBPS con cada uno de ellos como mínimo y con la finalidad de optimizar el intercambio de tráfico entre los distintos proveedores de internet nacionales los cuales deberán estar conectados por lo menos a dos nodos "CORE" del licitante , mismos que se deberán encontrar en diferentes zonas geográficas, por lo cual El licitante deberá presentar carta bajo protesta de decir verdad que confirme el cumplimiento de este punto.
En todo momento que se requiera el INEA deberá tener garantizado un ancho de banda mínimo de 70 MBPS soportando picos de hasta 110 MBPS

Las conexiones que tendrán con al menos dos de los principales proveedores de servicios de internet de la República mexicana, tendrán a su vez las siguientes características:

Los prestadores de servicios de internet tendrán conexión directa a por lo menos dos puntos de acceso a la red de internet en Estados Unidos y/o NAP'S (Network Access Points, por sus siglas en inglés) con una capacidad del orden de un Gbps como mínimo.

Cobertura a nivel nacional mediante infraestructura robusta con esquemas de alta disponibilidad y redundancia automática entre sus puntos de presencia POP'S (Points of Presence, por sus siglas en inglés) y ubicación.

El acceso al backbone de Internet del licitante debe ser exclusivo para el tráfico de Internet y no deberá compartir el tráfico con otros protocolos o servicios (frame relay, mpls, x.25, servicios de voz, etc.).

La red de Internet del licitante deberá ofrecer redundancia y diversidad de rutas.

La arquitectura de la red deberá estar basada en un diseño de red jerárquico (nodos de backbone, acceso al servicio y CPE), dentro de esta arquitectura, las capas se usan para aislar estratos de la red, cada capa debe tener un propósito específico y cada elemento se clasifica como un miembro de la capa basado en la función que está realizando.

La red de Internet del licitante deberá estar diseñada de tal manera que el transporte de los paquetes sea de una manera eficiente, además debe contar con la redundancia necesaria que le permita ofrecer un alto rendimiento a través de una red pública.

El licitante ofrecerá el servicio de conexión a Internet simétrico con redundancia.

El licitante deberá entregar el servicio mediante dos cableados en donde el primero es para internet activo y el segundo para la redundancia de este, estos cableados son Ethernet los protocolos que se utilizan para este servicio son anti loop y redundancia de ruteo.

Direccionamiento IP

- El licitante proporcionará al INEA un rango de direcciones IP homologadas para los servidores descritos en el Anexo I, equipos de comunicaciones y seguridad.
- Las direcciones homologadas así como las direcciones IP internas deberán de mantenerse con la misma numeración en cualquier proceso de migración.

Servicio DNS

- El licitante será responsable de ofrecer el registro de dominios y controlar la información de los DNS y todos los trámites ante el NIC o el INTERNIC, así como su mantenimiento anual correspondiente.

Servicio de almacenamiento, respaldo y recuperación

- El licitante será responsable de la configuración, administración y dispositivos necesarios para la conexión de los servidores de aplicaciones del instituto al sistema de almacenamiento.
- El licitante deberá ofrecer el servicio integral de almacenamiento SAN (STORAGE AREA NETWORK), para tener espacio adicional para almacenamiento de información a través de líneas de fibra canal (FC-SWITCH O FC-AL) FC8, para la aplicación control de gestión, este deberá poder crecer con solo incluir discos para poder proveer crecimiento.
- El licitante integrará las Interfaces de comunicación y componentes necesarios para la conexión entre los servidores del Anexo I y el sistema de almacenamiento SAN.
- La bóveda en la cual se resguardarán las cintas o medios de respaldos históricos deberá estar ubicada fuera de las instalaciones del centro de datos propuesto, con un ambiente físico controlado para garantizar el resguardo de los medios o las cintas. y se darán las facilidades aplicables para que personal autorizado del INEA pueda realizar visitas para validar y evaluar el servicio de resguardo.
- El acceso a la bóveda deberá contar con control de accesos biométricos y controles de acceso en el edificio donde se encuentre.
- El equipamiento por incorporar deberá contar como mínimo con las siguientes características y composición de partes en hardware y software:

  Controladoras:

  - Contemplar la incorporación de al menos 2 controladoras.
  - La conectividad de las controladoras al sistema de almacenamiento SAN a través de Fibre Channel, de al menos 8 GBPS. Y deberá soportar conectividad a 10GBE
  - Las controladoras deben ser redundantes e interconectadas.
  - Memoria cache
  - Cada controlador debe tener cache independiente.
  - Gabinetes de disco
  - Al menos gabinetes para discos de 2,5" o 3.5"
  - Discos
  - Capa de almacenamiento de alto rendimiento de 25 TB de espacio útil después de aplicar raid 5, que deberá estar

compuesta por discos SAS de 450/600 GB de 10K RPM como mínimo.

- Fuentes de alimentación eléctrica redundantes
- Ventiladores redundantes
- El equipamiento estará instalado en un rack standard de 19", incorporando las PDU'S necesarias para la energización del almacenamiento propuesto, dispondrá de líneas de alimentación redundantes y debe ser conectado a la red eléctrica.

Las propuestas que se presenten para este punto deben incluir necesariamente las siguientes funcionalidades:

Aprovisionamiento delgado (THIN PROVISIONING)

- Esta funcionalidad permite crear volúmenes con un tamaño inicial reducido, presentarlo al servidor con un tamaño superior y aumentar el tamaño del volumen en forma automática a medida que sea necesario.
- Copia instantánea de volúmenes de datos (snapshots).
- Esta funcionalidad permite tanto duplicar un volumen de datos como tomar una imagen de un volumen en un determinado momento sin impactar la performance de los servicios que entrega el volumen.

Deduplicación.

- Esta funcionalidad permite la optimización en la utilización del espacio a nivel SAN, es a nivel de bloques de máximo 4KB. Debe ser independiente de las aplicaciones. Permitir la integración con otras tecnologías de eficiencia del almacenamiento propuesto.

Compresión

- Esta funcionalidad es complementaria con la función de deduplicación, puede ser realizada en línea o posteriormente.

Copias livianas

- Esta característica permite la creación de copias de datos en forma instantánea (snapshots) que puedan ser utilizadas en entornos de desarrollo, QA y en ambientes virtuales, sin necesidad de duplicar la capacidad de almacenamiento haciendo una gestión eficiente.

Manejo de múltiples protocolos.

- El almacenamiento es capaz de utilizar múltiples protocolos de almacenamiento considerando al menos FCP, FCOE, ISCSI, CIFS/SMB, NFS/PNFS, estos protocolos pueden ser utilizados sin la incorporación de appliances:
- Sistema operativo de tipo Scale-Out.
- Almacenamiento en caché inteligente
- Esta tecnología permite acelerar las operaciones I/O para la virtualización de servidores y escritorios. Esta tecnología al igual que las anteriormente mencionadas, permite su utilización en ambientes NAS y SAN utilizando cualquiera de los protocolos asociados.
- El licitante proveerá todo el licenciamiento necesario para el uso de las herramientas y aplicaciones que se requieran para la operación y administración de la solución de almacenamiento propuesta.
- Para estas y todas las funcionalidades que se propongan, se deberá detallar el esquema de licenciamiento.
- También se deberán enumerar y describir claramente las herramientas de administración necesarias, así como la posibilidad de incorporación de módulos opcionales. para estas herramientas, se deberá detallar:
- Características del servidor necesario para la instalación de estas herramientas.
- Esquema de licenciamiento necesario de administración, así como las opciones de incorporación de módulos adicionales.

Respaldo y recuperación.

- Licenciamiento de software de 20 TB para respaldo y recuperación además del almacenamiento en disco necesario (independiente del espacio ocupado por los sistemas en producción). La unidad deberá considerar los agentes de software necesarios para respaldar sistemas operativos, file systems y aplicaciones que residan en cada servidor.

- El software propuesto deberá ser capaz de respaldar las plataformas enlistadas en el Anexo I.
- El software propuesto deberá ser capaz de respaldar en línea las siguientes aplicaciones: MICROSOFT SQL, MICROSOFT EXCHANGE, ORACLE, DB2 y MICROSOFT SHAREPOINT
- El software tendrá la capacidad de habilitar al usuario de poder recuperar su información mediante una ventana de visualización, con la introducción de un usuario y una clave.
- El software llevará la administración desde una consola centralizada pudiendo lanzar los respaldos desde esta consola de manera programada o en demanda, adicional podrá habilitarse al usuario a iniciar un proceso de respaldo en demanda.
- El software utilizará tecnología de de-duplicación en el origen y de manera global para optimizar la infraestructura de red y de almacenamiento de los datos respaldados.
- Permitirá crear calendarios de respaldo de acuerdo con las necesidades del usuario o del cliente.
- En caso de presentarse una disrupción en el servicio se requiere que la solución propuesta, deberá cumplir con un RTO y un RPO máximo de 12 hrs.

Restauración y recuperación.

- El software propuesto deberá ser capaz de realizar procesos de restauración y recuperación tanto de máquina virtuales completas, file systems, bases de datos o configuraciones de las plataformas enlistadas en el Anexo I.
- Permitirá realizar las pruebas necesarias para corroborar la veracidad de la información recuperada y que garantice la continuidad de las operaciones.

Servicios técnicos profesionales integrados al servicio solicitado

Servicios profesionales y personal capacitado.

- El licitante será responsable, técnica y administrativamente de migrar todas las aplicaciones cargadas actualmente en los servidores de web, aplicaciones, base de datos y servicios con que cuenta el instituto descritas en Anexo I, a su centro de datos. Lo anterior no considera modificaciones necesarias a las aplicaciones desarrolladas por el CLIENTE por parte del licitante ganador.

- El licitante será responsable por la correcta instalación y configuración de nuevas aplicaciones que adquiera el instituto durante la vigencia del contrato.
- Asesoría telefónica en horario 7x24x365 para el personal del CLIENTE y en el centro de datos cuando se requiera, dando soporte especializado sobre: Windows Server, Linux, VMware o Hyper-V, así como del software de aplicaciones y sistemas operativos que se instalen en los servidores hospedados, equipo de comunicaciones propuesto y seguridad.
- El CLIENTE se reserva el derecho de exigir en cualquier momento de la vigencia del contrato o pedido que el proveedor del servicio cuente con el personal técnico integrado en su propuesta técnica y avalado por los documentos presentados del personal.
- Se dará asesoría en reingeniería y control de aplicaciones para asegurar siempre el mejor desempeño dentro de los sistemas en la red del licitante y en la red de internet.
- El licitante ofrecerá un centro de atención telefónica con un control de llamadas y reportes de seguimiento y solución de los mismos. Los reportes de seguimiento contendrán como mínimo lo siguiente:
  - Número de reporte
  - Fecha
  - Hora
  - Tipo de falla
  - Tipo de escalamiento
  - Fecha y hora de solución
  - Quién reporta la falla y quién atendió
- Se contará con soporte 24 horas al día, los 7 días de la semana, todo el año. Con un número 01 800.
- Contar con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7x24 los 365 días del año.
- Atención del técnico asignado en forma directa para la solicitud de servicios y asesoría técnica, de forma inmediata.
- Asegurar un tiempo de respuesta a falla de máximo 30 minutos.
- La mesa de ayuda formará parte primordial de un mecanismo de recepción, canalización, atención, coordinación, seguimiento, registro y reporte de incidentes, cambios solicitados, requerimientos en general y comunicación.

- El licitante dedicará un contacto encargado de toda la relación con el CLIENTE, con el poder suficiente para ordenar cualquier modificación en configuración, programación y/o control de los dispositivos hospedados en el centro de datos. Este contacto podrá, de así requerirse a petición del personal del cliente, sostener reuniones periódicas para informar sobre estatus y calidad de los servicios prestados, así como entregar los reportes de desempeño de todos los elementos de la solución. El contacto asignado por el licitante tendrá capacidad para dirigir el proyecto apegándose a estándares de ITIL, por lo que el licitante deberá incluir en su propuesta copia de certificado de "ITIL V3 Expert" y Curriculum del contacto encargado.
- Así mismo, el personal de operación del licitante que preste el servicio al CLIENTE contará al menos con certificación ITIL Foundations, deberán incluirse al menos 5 certificados de ITIL Foundations v3 de su personal que atiende la mesa de ayuda.
- El INEA requiere de un personal especializado en virtualización de la plataforma VMware o Hyper-V, para asesoría e implementación de al menos 40 horas, que podrán utilizarse durante la vigencia del contrato.

Monitoreo del servicio

El servicio de Monitoreo comprenderá lo siguiente:

- Para todos los servidores del Anexo I de aplicaciones migradas a la arquitectura deberá contar con monitoreo en hardware y software.
- Generará reportes de uso y monitoreo de los servicios en línea mediante una ventana gráfica accesible por internet (web), la cual brindará información sobre los siguientes parámetros:
  - Utilización de recursos de hardware.
  - Utilización de ancho de banda de salida y de entrada.
  - Reportes de tráfico y desempeño en cada uno de los puertos de acceso a internet.
  - Filtros de reportes por día, semana y mes.
  - Monitoreo de los servidores de base de datos del sistema SASA en línea y SIGA.
- El licitante deberá contar con personal técnico que tenga por lo menos un año de experiencia trabajando para un Hosting center de un ISP o carrier de internet.
- El licitante estará en la disposición de interactuar con el personal de la Subdirección Técnica del Instituto.

- El licitante informará inmediatamente sobre problemas detectados en el funcionamiento de servidores y el servicio al personal designado por el INEA y catalogará este procedimiento como de alta prioridad.
- Reportes de incidentes de seguridad al detectar una falla.
- Todo el monitoreo será realizado mediante una red dedicada independiente para la cual el licitante proporcionará todos los componentes necesarios (Interfaces de red, switches, etc.).
- Se deberá monitorear el desempeño de la red, emitiendo alertas cuando el comportamiento de la misma se desvíe de los patrones establecidos, mediante el análisis detallado de todas y cada una de las aplicaciones alojadas en el centro de datos.
- El licitante proporcionará una cuenta de usuario de solo lectura para todos los equipos de comunicaciones y seguridad.
- Como parte de los entregables mensuales, el licitante entregará el monitoreo de la infraestructura y el estatus de todos los incidentes reportados.
- El licitante deberá proporcionar el servicio de monitoreo a través de un ambiente gráfico orientado a objetos donde se puede observar el estado de los recursos en un ambiente definido.

Soporte telefónico (Contact Center)

- Soporte 24 horas al día, los 7 días de la semana, todo el año, con un número 01 800.
- El servicio del proveedor deberá tener las siguientes características distintivas:
  - A través del sitio web del licitante ganador del servicio se podrá solicitar en línea cualquier servicio de ayuda y apoyo técnico, opciones adicionales y modificaciones a sus servicios, así como verificar el estatus de sus órdenes.
- Contar con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7x24 los 365 días del año.
- Compromiso de atención de forma directa e inmediata del técnico especializado asignado para la solicitud de servicios y asesoría técnica.
- Asegurar un tiempo de respuesta a falla de máximo 30 minutos.

Soporte en el Centro de Datos

El proveedor debe brindar soporte técnico especializado de acuerdo a la solución propuesta (especialistas en todas las plataformas de hardware y software propuestos en su solución) a personal del Instituto, de acuerdo al personal técnico solicitado en estas bases, en el centro de datos con soporte 7x24x365.

Servicios administrados

Servicio de Administración de Sistemas Operativos

El licitante ofrecerá la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de los sistemas operativos de plataformas distribuidas. Este servicio complementará al de Monitoreo de Sistemas para ofrecer al CLIENTE una experiencia integral en la atención de sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que debe considerar la administración de Sistema Operativo:

- Soporte al sistema operativo
  - Actualización de parches
  - Reinstalación del Sistema Operativo
  - Instalación de nuevos volúmenes y particiones.
  - Asignación de almacenamiento para la creación de nuevos volúmenes.
  - Configuración del sistema operativo de acuerdo a las necesidades del cliente.
  - Configuración de ambientes de clúster si así lo requiere el cliente.
  - Configuración de Servicios de Acceso Remoto.
- Soporte al Hardware
  - Instalación de discos.
  - Instalación de memoria.
  - Instalación de procesadores.
  - Instalación de CPU's. (con asesoría de terceros).
  - Configuración del hardware de acuerdo a las necesidades del cliente.
- Asistencia en Actualizaciones.
  - Niveles de parches que requiera las aplicaciones.
- Administración del Sistema de Archivos.

- Creación de nuevos volúmenes.
- Creación y modificación de particiones.
- Modificaciones al sistema de archivos de acuerdo a las necesidades del cliente.

- Administración de Usuarios.
  - Alta de nuevas cuentas
  - Baja de cuentas
  - Modificación de perfiles
  - Asignación de prioridades.
  - Cambio de contraseñas.
  - Asignación de grupos.
  - Asignación de permisos.
  - Asignación de Dominios.
- Configuración de permisos de los usuarios dentro del dominio.

- Emisión de reportes en caso de falla de algún servicio
  - Contacto telefónico del licitante hacia CLIENTE para dar avances en la tarea.
  - Entrega de reporte del licitante hacia CLIENTE por escrito, al final de la tarea con los resultados obtenidos.
  - Entrega del plan de trabajo al CLIENTE previo a la tarea. El plan de trabajo deberá de incluir los siguientes puntos:
    - Objetivo
    - Prioridad
    - Impacto
    - Tiempo de duración
    - Fecha Inicio
    - Fecha Término

- Descripción
- Puntos de Contacto
- Entrega y validación de orden de cambios

Administración de VMWare o Hyper-V

El licitante ofrecerá la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de VMware o Hyper-V que contienen los equipos proporcionados. Este servicio complementará al de Administración de Sistemas Operativos para ofrecer al cliente una experiencia integral en la atención de sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que el licitante deberá considerar para la Administración de VMware o Hyper-V:

- Instalación de ESX
- Configuración de ESX
- Ambientes de alta disponibilidad (HA, V-Motion, Switches Distribuidos)
- Creación de máquinas virtuales
- Configuración y administración de sistemas operativos
- Instalación de aplicativos dentro de las virtuales
- Adición de recursos (vCPU's, RAM, espacio en disco)
- Eliminación de Máquinas virtuales
- Configuración de Storage.
- Monitoreo de disponibilidad de los equipos virtuales
- Graficas de consumo de recursos (CPU, Memoria RAM, Utilización de Disco y Red)

Servicio de Administración de Bases de Datos

El licitante deberá ofrecer la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de base de datos de plataformas distribuidas del CLIENTE. Este servicio complementará al de Monitoreo de Base de Datos para ofrecer al cliente una experiencia integral en la atención de las bases de datos alojadas en sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que el licitante deberá de considerar para la administración de Base de Datos:

- Manejo de Incidentes/Operaciones
    - Mantener información programada en las herramientas de "Job Scheduling"
    - Monitorear, cancelar o programar la ejecución de un "batch job"
    - Restaurar la ejecución de un "batch job" en caso de fallas
    - Recuperar "rollbacks" de "batch jobs" fallidos
    - Manejos de logs
    - Monitorear el status de la base de datos
    - Restaurar base de datos en caso de fallas
    - Ejecución de Imports y/o Exports no riesgosos de Base de Datos
    - Crear tablespace de base de datos
    - Aumentar o disminuir el tablespace de base de datos
    - Eliminar / Borrar tablespace de base de datos

- Manejo de Problemas/Cambios/Configuraciones
    - Diseñar un ambiente de base de datos
    - Crear el cascaron de una base de datos
    - Ejecución de Imports de Base de Datos
    - Ejecución de Exports de Base de Datos
    - Copia de Base de Datos
    - Diagnosticar y arreglar problemas de lentitud o fallas de base de datos
    - Crear "scripts" para base de datos
- Manejo de Capacidades/Rendimiento
    - Detectar problemas de capacidades en los sistemas
    - Generar reportes de capacidad de recursos para los clientes

<u>Servicio de Administración de Respaldos</u>

El alcance mínimo que el licitante deberá contemplar para la Administración de respaldos:

Se deberán respaldar 20 TB en total para los servidores (independiente a la recuperación y respaldo). Deberá incluir licenciamiento de respaldos para file systems y Bases de Datos.

Política de respaldos:

- Respaldos Diarios con retención de 7 Días
- Respaldos Semanales con retención de 1 mes (De acuerdo al número de semanas en el mes)
- Respaldos Mensuales con retención de 3 Meses
- Respaldos Anuales con retención de 1 año.

Servicio de Administración de Restauraciones

El alcance mínimo que el licitante deberá contemplar para la Administración de restauraciones considera entre otros los siguientes puntos:

- El INEA podrá solicitar en cualquier momento, la restauración de algunos de los servidores, ya sea parcialmente (solo datos o archivos específicos) o servidores completos que incluyan la configuración
- El licitante notificará al INEA el tiempo esperado para realizar las restauraciones solicitadas y notificará oportunamente al INEA el avance de estas o cualquier imprevisto que se presente durante el proceso
- El licitante en coordinación con el INEA, realizará de manera aleatoria pruebas de restauración de los servidores en el alcance del contrato. El licitante presentará al INEA una propuesta de calendario de ejecución de restauraciones el cual deberá considerar escenarios aleatorios.

Servicio de Administración de Almacenamiento

El licitante proporcionará el servicio de Almacenamiento dedicado para la atención de INEA

Estos servicios de almacenamiento deberán contemplar la implementación de la infraestructura y los procesos operativos necesarios para resguardar la información en un sistema de almacenamiento dedicado para el INEA. Este servicio operará mediante canales de fibra redundantes.

- Se considera como parte del alcance lo siguiente: Configuración y puesta a punto del almacenamiento en disco en el arreglo de discos
- El alcance mínimo de los servicios es:
  - Administración, operación y monitoreo de la infraestructura en la que opera el servicio de almacenamiento.
  - Actualización de micro-código en el hardware de las plataformas de almacenamiento en disco.

- Aprovisionamiento de nuevos requerimientos.
- Actualización de parches de seguridad.

El servicio de almacenamiento deberá estar compuesto por los siguientes rubros:

Almacenamiento en SAN: 20 TB utilizables por el INEA
Conexión a la red: 2 Puertos por cada servidor físico

Cada servidor físico deberá estar conectado de manera redundante al sistema de almacenamiento, considerando doble tarjeta de puerto y doble cableado.

La administración consiste en asegurarse de que el servidor permanezca conectado al sistema de almacenamiento de manera redundante, cualquier re-configuración por falla en dispositivos como puertos de directores, HBA's, puertos del arreglo de discos estará considerada dentro de la administración.

- Revisión de estatus de controladoras.
- Revisión de volúmenes.
- Creación y borrado de volúmenes
- Creación y borrado de hosts.
- Administración de los switches del sistema de administración.
- Atención a incidentes.
- Revisión de volúmenes libres.
- Validación de rutas de acceso a disco.
- Revisión del estado de arreglo de discos.
- Revisión de bitácoras en los switches.
- Asignación de volúmenes a los servidores.
- Liberación de volúmenes que están asignados.
- Generación de reportes para seguimiento a fallas.
- Supervisión del reemplazo de componentes relacionados con la infraestructura.

- Validación de tamaño de los volúmenes asignados
- Reasignación en línea de LUNS
- Elaboración de reporte de uso de espacio asignado en el sistema de almacenamiento.
- El licitante considera un crecimiento 20% por lo que en caso de que el CLIENTE requiera de este espacio se podrá habilitar de manera inmediata.

Servicio de migración de aplicaciones y servicios

El licitante deberá tener instalados y configurados todos los servicios a los que se refiere este documento, a más tardar el 12 de enero de 2020.

La migración deberá estar concluida a más tardar el 12 de enero de 2020. El licitante deberá considerar que durante el periodo de migración la operación de las aplicaciones del CLIENTE continuará en producción y a cargo del proveedor actual. El plan de migración del licitante deberá ser diseñado de modo que no cause interrupción a la operación normal de las aplicaciones del CLIENTE.

El licitante será responsable de la migración de todos los sistemas y aplicaciones del Instituto, por lo que debe contar con toda la infraestructura, personal especializado (de acuerdo a los requerimientos técnicos de Hardware, software y servicios indicados en anexo) requerido por el INEA, gastos de operación y vehículos para el traslado de equipos, necesarios para cumplir con este punto en su totalidad. Por lo que el licitante deberá contar con el personal especialista y certificado en el hardware y software propuesto por la empresa y solicitado en este documento durante toda la vigencia del contrato para resolver cualquier petición de soporte en sitio, previa solicitud del INEA.

El licitante migrará los servicios indicados en el Anexo I, por lo que deberá contar con el licenciamiento, equipos, herramientas y personal para realizar esta migración y para atender incidentes o nuevas solicitudes que surjan durante la vigencia del contrato.

Para esta etapa de migración el licitante realizará estas actividades bajo la dirección de un líder de proyecto que cuente con certificaciones aplicables; el líder de proyecto deberá elaborar las bitácoras de actividades para llevar las memorias de los servicios en sitio.

... Condesa, C.P. 06140 ...
... 41 29 00

Así mismo el licitante observará las reglas mínimas relacionadas con la seguridad de la información, ordenadas por objetivo de control según el marco del MAAGTICSI, para lo cual se requiere que la empresa esté certificada en ISO 27001.

El licitante presentará un plan que abarcará desde la etapa de planeación hasta la puesta en marcha de las aplicaciones del INEA. El costo derivado de los especialistas en sistemas operativos, aplicaciones comerciales y base de datos será cubierto en su totalidad por el licitante. Este plan será presentado junto con su propuesta.

El CORE del negocio del CLIENTE lo tienen las aplicaciones SASA y SIGA, los demás son sistemas de gestión educativa. El CLIENTE entregará una lista con el orden de migración por grupo de servidores y por aplicación, la primera aplicación a migrar será el grupo de servidores que integran al SASA. La gestión de servicio de tecnologías de la información será totalmente compatible con el esquema ITIL (Information Technology Infrastructure Library) v3, además la operación en el centro de datos del licitante deberá estar certificada bajo la norma ISO 20000. Para lo cual el licitante deberá incluir en su oferta copia de dicha certificación.

La gestión de servicio de tecnologías de la información será totalmente compatible con el esquema ITIL (Information Technology Infrastructure Library) v3, además la operación en el centro de datos del licitante deberá estar certificada bajo la norma ISO 20000. Para lo cual el licitante deberá incluir en su oferta copia de dicha certificación.

En caso de retraso, por parte del licitante ganador, en la ejecución del calendario de migración que se establezca, el licitante ganador cubrirá la renta al actual proveedor del servicio, hasta que la migración haya concluido y se aplicará la pena correspondiente que se señala en el contrato.

Especificaciones al término de la implantación e inicio del servicio

Deberá ser entregado al Instituto el manual de operación y memoria técnica de la instalación. Deberá contener la configuración de todos y cada uno de los componentes que incluyen la solución.

Vigencia

La vigencia del servicio será a partir del 13 de enero al 31 de diciembre de 2020.

II. Requerimientos no Funcionales

Ubicación

El centro de datos propuesto por el licitante estará construido para operar como un centro de datos de alta disponibilidad, debe estar construido en la República Mexicana. En caso de estar fuera del área Metropolitana de la Ciudad de México el licitante deberá considerar los viáticos para al menos 3 personas del Instituto dos veces al mes, y visitas extraordinarias que sean necesarias en caso de recuperación de respaldos, incidentes o requerimientos especiales.

Certificaciones del Centro de Datos.

El licitante deberá de presentar por lo menos las siguientes certificaciones vigentes del centro de datos propuesto para garantizar los niveles de servicio solicitados,

- ISO 9001:2015 o posterior (Sistema de administración de calidad)
- ISO 20000:2011 o posterior (Sistema de Gestión de Servicio de TI)
- ISO 22301:2012 o posterior (Sistema de gestión de Continuidad de Negocio)
- ISO 27001:2013 o posterior (Sistema de administración de la seguridad de la información)

Niveles de servicio y Garantía de disponibilidad en el Centro de Datos

El nivel de servicio solicitado para el Centro de Datos deberá de ser ICREA Nivel 4 o TIER III, con lo cual se garantiza un nivel de servicio del 99.80% de disponibilidad, en caso de incumplimiento el proveedor del servicio se hará acreedor a la pena convencional correspondiente. En razón de lo anterior el licitante deberá garantizar alta disponibilidad operativa de las aplicaciones que se indican en el Anexo II.

Controles de Seguridad, Seguridad Lógica

- La solución propuesta debe ser exclusiva para el INEA y en esquema redundante.

- El licitante deberá describir detalladamente en su oferta técnica la solución propuesta para el esquema de seguridad lógica, es decir, se deben mencionar marcas, equipos, modelos, esquema de configuración e interconexión entre los mismos, para lograr la solución deseada y la protección de los servicios del Instituto.

- La solución de seguridad lógica propuesta deberá ser realizada con equipos de propósito específico, de última generación y en una configuración de alta disponibilidad (activo-activo).

- La solución propuesta no deberá ser un factor de latencia adicional en las redes por razones de su desempeño, por lo cual deberá de garantizar la latencia igual o menor a la de los equipos de red propuestos.

- Los equipos o dispositivos que integren la solución propuesta, serán completamente compatibles entre sí; de tal manera que no existan problemas de desempeño por incompatibilidad entre ellos y los equipos deben ser configurados por el licitante ganador hasta su puesta en marcha.

- La configuración de este sistema de seguridad, deberá ser coordinado en todo momento por personal del licitante ganador. El CLIENTE podrá solicitar las adecuaciones que considere necesarias según las necesidades del Instituto.

- Del punto anterior el tiempo máximo para atender un requerimiento de configuración de seguridad será de 30 minutos en un esquema de 7x24x365, por lo que el licitante deberá contar con el personal capacitado y autorizado para efectuar movimientos en las configuraciones de estos equipos cuales quiera que estas sean.

- El licitante deberá presentar el currículum de los ingenieros que serán responsables del diseño, quienes deberán tener las certificaciones CISSP y CISM. Adicionalmente para la coordinación de la operación de la seguridad lógica de la solución durante la vigencia del contrato, se deberá acreditar la certificación CISSP.

- El licitante deberá detallar en la oferta técnica, una arquitectura de seguridad la cual cumpla con el modelo de seguridad para proteger de forma integral la infraestructura de los servicios del Instituto, ocupando para ello los dispositivos de propósito específico, esquemas en alta disponibilidad y configuraciones de seguridad; tales como:

  - Firewalls en alta disponibilidad,
  - Sistema de detección y prevención de intrusos de red,
  - Switches,
  - Antimalware
  - Antispam

- Todo esto en base a políticas y procesos de administración documentados, mismos que deberán de ser proporcionados al CLIENTE.

- El licitante será el encargado de instalar, administrar, monitorear, mantener y actualizar, todos los equipos antes mencionados con personal especializado para ello, asignando al personal que el CLIENTE designe, una cuenta de solo lectura para verificar el servicio y contar con acceso a los sistemas de monitoreo para visualización de información.
- El centro de datos deberá contar con línea de defensa, que al menos ofrezca servicios de firewall, antivirus, antispam, VPN, detección y prevención de intrusos. Estos servicios deberán contar con las siguientes características:

Firewall

- Dispositivo de propósito específico.
- Firewall en esquema de alta disponibilidad y con balanceo de cargas con interfaces de red 10/100/1000 suficientes para la conectividad de la solución propuesta en firewall.
- Soportar puertos 10G.
- Soportar la creación de VPN'S. usando los algoritmos de cifrado, firmado y hashing más comunes, así como los más modernos y seguros.
- Capaz de manejar al menos 2, 000,000 de conexiones concurrentes.
- Al menos 1.2 GBPS de IPS Throughput.
- Al menos soportar 50 mil nuevas conexiones por segundo.
- Los servicios de firewall deben de ser de estado completo (statefull).
- Capaz de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con Timeout.
- Deberá prevenir IP spoofing, debiendo tener mecanismos de protección contra ataques DoS y DDoS.
- Deberá ser capaz de implementar mecanismos de calidad de servicio; tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- La solución ofertada deberá estar certificada por ICSA LABS como Enterprise firewall, con el objetivo de garantizar que la solución ofertada cumpla con las especificaciones de un firewall empresarial.

Sistema de detección y prevención de intrusos

- El licitante deberá ofrecer un sistema de detección y prevención de intrusos el cual deberá considerar en una plataforma independiente que permita la correcta y oportuna identificación de ataques, que por lo menos proporcionen lo siguiente:
- El sistema de prevención y detección de intrusos estará en un esquema de alta disponibilidad y de balanceo de cargas con interfaces suficientes para la solución propuesta.
- Detección de ataques e intrusos: basada en firmas, anomalías estadísticas, protocolos de situaciones de negación de servicio.
- La solución ofertada deberá estar certificada por ICSA LABS como Network IPS (NIPS por sus siglas en inglés,) para garantizar que la solución cumpla con las especificaciones necesarias para un IPS de red empresarial.
- La solución deberá contar con un performance mínimo de 1 GBPS.
- La solución deberá contar con la capacidad de detección de más de 5000 ataques y deberá permitir la actualización constante de su base de detección de ataques.
- La plataforma de IPS debe contar con protección contra ataques en capas aplicativas con filtros contra PHP (Include, inyección, evasión etc.), filtros contra Cross Site Scriptiing y filtros contra inyección de SQL, además deberá contar con capacidades de detección y prevención de los "OWASP Top 10 Most Critical Web Application Security Risks.
- Rechazo de intrusos: posibilidad de configurar el sistema para rechazar o eliminar automáticamente las conexiones no deseadas.
- Soporte a configuración en modo transparente en la red.
- Proveer de capacidad de auto aprendizaje para adaptar las políticas basadas en comportamiento del tráfico en tiempo real.

Protección contra ataque de negación de servicios

El licitante deberá incluir en el alcance de la solución, protección contra ataque de negación de servicios con las siguientes características:

- Formato tipo "appliance" de propósito específico para el servicio de protección contra ataques de negación de servicio distribuido.
- No se aceptan equipos de propósito genérico (PCS o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como MICROSOFT WINDOWS, FREEBSD, SUN SOLARIS, APPLE OS-X O GNU/LINUX.
- Soporte al análisis de comportamiento basado en ASICS para detectar y bloquear ataques de anomalías, reconocimiento y mitigación anti DDOS.
- Soporte a configuración en modo transparente en la red.

- Soporte en modo de operación transparente, el no requerir de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- Proveer de capacidad de auto aprendizaje para adaptar las políticas basadas en comportamiento del tráfico en tiempo real.
- Realizar análisis de comportamiento de red (NBA, por sus siglas en inglés).

En seguridad

El licitante deberá incluir en la solución, Seguridad con las siguientes características:

- Filtrado de direcciones IP por país (protección con geo-localización).
- Servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.
- Bloqueo de tráfico dirigido a puertos restringidos.
- Aprovisionar una lista de nodos o dispositivos infectados para su bloque
- Mitigación de sobre flujo de paquetes.
- Verificación de protocolos.
- Filtrado de paquetes fuera de estado e inspección del estado de los paquetes.
- Determinación heurística de tráfico malicioso (tipo botnet) y prevenirlo automáticamente.
- Filtrado basado en algoritmos.
- Análisis de comportamiento de red.
- Deberá de contar con procesos de Multi-verificación, la cual se refiere a que la solución pueda realizar múltiples procesos de verificación para identificar anomalías en el tráfico, como ser filtrado dinámico, verificación activa, reconocimiento de anomalías, verificación de protocolos.
- Mitigación de ataques en capa 3, 4 y 7.
- Capacidad de mostrar diagnósticos en tiempo real.
- La prevención contra ataques de día 0.
- Latencia permitida será de microsegundos.
- Rastreo de los dispositivos origen del ataque.
- Identificación de URL´S dentro de paquetes de http.
- Aprendizaje en base a patrones de tráfico desde y hacia los sistemas protegido; auto aprendizaje para determinación de umbrales dinámicos para diferenciación de tráfico legítimo.
- En alcance sobre la protección ante ataques de negación de servicio distribuida.
- Comprobación de direcciones IP legítimas.

- Excesivas conexiones TCP por destino.
- Sobre flujo de conexiones.
- Activación de políticas en base a umbrales de comportamiento.
- Verificación de encabezado incorrecta.
- Combinación inválida de banderas TCP.
- Versión inválida de http.

En capacidad

- Throughput 1.2 GBPS.
- Conexiones simultáneas 2,000,000.
- Establecimiento/cierre de sesiones 200,000 / segundo.
- Respuesta de mitigación de un ataque DDOS menor a 2 segundos.
- Puertos LAN necesarios para la conexión.
- Puertos WAN necesarios.
- Fuente de alimentación redundante.

Servicio de Análisis de Vulnerabilidades

- El licitante deberá identificar y administrar vulnerabilidades de la infraestructura a los que se encuentra expuesto el INEA por medio de escaneos recurrentes (trimestral), con el fin de establecer medidas adecuadas para mitigarlas o reducirlas a un nivel aceptable.
- Se deberá de identificar y administrar vulnerabilidades de la infraestructura del INEA por medio de escaneos recurrentes; y se deberá de dar un seguimiento para la mitigación de dichas desviaciones de seguridad.
- El servicio se deberá de prestar mediante la administración de una solución tecnológica de escaneo y administración de vulnerabilidades, el cual debe considerar hasta 10 ip´s
- El licitante deberá operar, administrar, monitorear y dar mantenimiento a la solución tecnológica de escaneo y administración de vulnerabilidades. esta solución tecnológica deberá de cubrir los siguientes requerimientos mínimos:
  - Debe de ser un software o equipo(s) de tipo appliance.
  - Debe ser actualizado frecuentemente para incluir vulnerabilidades recientes.
  - Debe permitir generar reportes con formato flexible ya sean técnicos o directivos.
  - Debe realizar una clasificación de riesgos: altos, medios o bajos.

- Proporcionar recomendaciones de mitigación sobre las vulnerabilidades encontradas, así como su aplicación en el ámbito de competencia del licitante.
- Debe permitir generar plantillas de escaneos de acuerdo a los diferentes dispositivos a escanear (ej. windows, linux, cisco, etc) o normas de cumplimiento de seguridad (ej. pci, etc.).

- El licitante ganador llevará a cabo la detección y administración de las vulnerabilidades de la infraestructura del INEA por medio de una solución de escaneo.
- Las actividades que deberá de llevar a cabo el licitante se mencionangestión de servicio de tecnologías de la información será totalmente compatible con el esquema ITIL (Information Technology Infrastructure Library) v3, además la operación en el centro de datos del licitante deberá estar certificada bajo la norma ISO 20000. Para lo cual el licitante deberá incluir en su oferta copia de dicha certificación a continuación, las cuales deben de ser de manera continua durante los tiempos definidos con el INEA:
  - Operar la herramienta en los siguientes rubros:
  - Alta, baja y cambios de las direcciones ip a escanear.
  - Actualizaciones automáticas y manuales en la herramienta.
  - Escaneos de vulnerabilidades a través de la herramienta de acuerdo al calendario acordado.
  - Identificar y reducir falsos positivos de las vulnerabilidades identificadas.
  - Dará recomendaciones y seguimiento a la mitigación de las vulnerabilidades identificadas.
  - El licitante dará atención a fallas de los dispositivos de seguridad de forma remota:
  - Soporte primer nivel
  - Analizar la posible falla en el dispositivo de seguridad.
  - Re-establecer la configuración inicial o un estado anterior para su funcionamiento.
  - Soporte segundo nivel
  - En caso de que no se pueda resolver dicha falla, se escalará al proveedor para dar solución.

Los entregables que se deberán de generar serán de forma trimestral, los cuales deberán incluir los siguientes puntos:

- Resumen ejecutivo.
- Reporte técnico con base en la herramienta.

Servicio de Protección de Aplicaciones

Además de los firewalls de seguridad perimetral el licitante deberá considerar un WAF (Web Application Firewall por sus siglas en inglés), con el propósito de robustecer la seguridad a nivel aplicación. La conectividad considerada debe ser 10Gb, con la finalidad de robustecer y agilizar el procesamiento de los aplicativos.

El objetivo de este servicio será proteger las aplicaciones de ataques y amenazas en tiempo real; como, por ejemplo: SQL INJECTION, CROSS SITE SCRIPTING (XSS), denegación de servicios (dos), denegación de servicios distribuidos (DDOS) y cross site request forgery (CSRF), etc.

El servicio será prestado mediante una solución tecnológica para protección de aplicaciones web.

El licitante será responsable de operar, administrar, monitorear y dar mantenimiento al firewall de aplicaciones que cubra con los siguientes requerimientos mínimos:

- Estar basada en equipo o equipos de tipo appliance.
- Puedan configurarse (por capacidad) al menos 50 (cincuenta) aplicativos en este dispositivo.
- Aprender y entender la estructura de las aplicaciones, elementos y comportamientos normales de usuarios aplicativos, así como los cambios a través del tiempo que se dé en éstos.
- Permitir configurar y actualizar los métodos, cookies, parámetros, y URLS de las aplicaciones.
- Contar con una base de políticas predefinidas, granulares y personalizables, así como firmas de protección a nivel aplicativo para protección contra ataques basados a aplicaciones.
- Contar con un módulo de reporteo personalizable. Los reportes deben permitir sacar gráficas y deberán poderse generar en una base de tiempo semanal, mensual o de manera diaria.
- Cumplimiento de estándares http para prevenir explotaciones del protocolo y técnicas de evasión.
- Contar con un bypass en caso de un apagado o falla inesperada del o los equipos.
- Aprender automáticamente las aplicaciones y el comportamiento del usuario sobre estas.
- Contar con un módulo para la actualización de las firmas de manera automática.

- Identificar y detener fuentes de ataques conocidos.
- Mitigar ataques a gran escala integrando direcciones IP de atacantes, BOTS, y servicios anónimos.
- Realizar la protección de acuerdo a los estándares de seguridad al menos vs OWASP top 10.
- Soportar alta disponibilidad.
- Salvaguardar la infraestructura de las aplicaciones incluyendo servidores web, políticas de seguridad de xml y web 2.0.
- Permitir la correlación de políticas para la reducción de falsos positivos permitiendo la validación de ataques correlacionados mediante la capacidad de examinar múltiples atributos, violaciones de los perfiles de las aplicaciones, caracteres especiales, etc.
- Contar con un módulo de tablero (dashboard) que permita conocer el estatus en tiempo real de las aplicaciones y de los eventos generados.
- Deberá permitir el aprendizaje de la operación de las aplicaciones de manera que en un principio sólo se monitoree la actividad y posteriormente permitir los bloqueos en tiempo real.
- Protección a nivel aplicativo según el top ten del estándar OWASP.
- Implementación de modo monitoreo.
- Implementación de modo en línea para bloqueos en tiempo real.
- Implementación de modo en línea sin bloquear, con el fin de aprender la actividad normal de las aplicaciones, antes de bloquear.
- El licitante deberá considerar en su propuesta los siguientes requerimientos mínimos:
  - Las características de las herramientas para la protección de aplicaciones (WAF) donde realizará la administración, operación, monitoreo y reportes.
  - El monitoreo en tiempo real de las aplicaciones, que permita prevenir incidentes que afecten los niveles de servicio.
  - El monitoreo será con una disponibilidad de 24x7x365

- El sistema de monitoreo deberá tener capacidad de acceso vía web con mecanismos de autenticación segura, para visualizar las métricas, proporcionar una cuenta de acceso para realizar consultas.
- Definirá junto con el INEA las aplicaciones y los parámetros y eventos a ser monitoreados por el WAF.
- Definir procedimientos de notificación y escalación de acuerdo a la estructura organizacional del CLIENTE.
- Mantenimiento de bitácoras históricas y registro de incidencias (hasta 15 días), desde el inicio del contrato jurídico hasta su conclusión.
- Deberá permitir el análisis de eventos en tiempo real, histórico y análisis forenses. Así como contar con la capacidad de poder integrarse a la mesa de ayuda propuesta mediante la apertura de tickets vía correo electrónico; en paralelo y de acuerdo a la severidad de la alarma notificar al personal adecuado para su pronta solución.

- Monitorear los eventos de seguridad detectados por el WAF en el horario establecido.
- Analizar eventos de seguridad para identificar y reducir falsos positivos de las alertas generadas.
- Generar notificaciones por evento de incidencias detectadas (vía correo electrónico o llamada telefónica).
- Dar recomendaciones generales de seguridad informática relacionada con el WAF y los incidentes detectados.
- Configurar el WAF para enviar alertas de los eventos de seguridad.
- Revisar el estado actual del WAF en licencias, actualizaciones, firmas de ataque, hotfix, performance y capacidad de almacenamiento.
- Dar atención a fallas de los dispositivos WAF en sitio o en forma remota:

Soporte primer nivel

- Analizar la posible falla en el dispositivo de seguridad
- Re-establecer la configuración inicial o un estado anterior para su funcionamiento

Soporte segundo nivel

- En caso de que no se pueda resolver dicha falla, se contactará al proveedor para dar solución
- Registrar todos los eventos (tickets) en bitácora ya sea de:
- Control de cambios
- Incidentes
- Reporte mensual de las actividades de servicio administrado de WAF que incluye:
  - Resumen ejecutivo.
  - Detalle técnico con ayuda de la herramienta.

Seguridad Física

•Contar con medidas de protección física externa que lo mantenga seguro contra robo y actos vandálicos, así mismo deberá contar con estacionamiento para el resguardo de vehículos y deberá permitir el acceso al personal identificado y autorizado por el CLIENTE.

•Estar ubicado en región geológica de terreno firme zona a (bajo) o b (moderado) de peligro sísmico de acuerdo a la clasificación de regionalización sísmica publicada por el Servicio Sismológico Nacional

•Contar con un sistema de seguridad física mediante personal de vigilancia especializado con cobertura 7x24, los cuales deberán registrar mediante bitácora diaria soportada por un sistema automatizado, los accesos que realice personal a las instalaciones administrativas y en especial a quien acceda al centro de datos.

•El centro de datos del licitante deberá contar con un sistema de circuito cerrado de televisión CCTV o de grabación digital, el cual mantenga monitoreo permanente 7x24 al centro de datos, tanto en el interior como en el exterior y perímetro. La grabación de los videos estará a disposición del CLIENTE, por 30 días naturales contados a partir de la fecha de grabación, plazo en el cual el CLIENTE podrá solicitarlos, si así fuera necesario.

•Contar con acceso restringido al centro de datos mediante sistemas automatizados, marcos detectores de metales y permitiendo acceso únicamente mediante tarjetas de proximidad o equivalente y, adicionalmente, un sistema integral de acceso con control biométrico (lectoras de iris, reconocimiento facial, huella dactilar) o la combinación de ellos, que registre el acceso del personal a la misma, hora de entrada y hora de salida.

•Para tener acceso al área del centro de datos donde resida la infraestructura de cómputo y almacenamiento asignada al CLIENTE, habrá al menos 3 puntos de control de acceso.

•Deberá contar con un procedimiento y sistema implantado para garantizar al CLIENTE, la acreditación y autorización de acceso al centro de datos y a las áreas asignadas al CLIENTE de los servidores públicos que ésta designe las 24 horas del día los 365 días del año.

•Contar con sistemas de alarmas de seguridad y salidas de emergencia con alarmas sonoras.

•El centro de datos propuesto por el licitante deberá contar con un sistema de prevención y detección de incendio altamente zonificado, de modo que ubique y aplique específicamente en el área de riesgo detectada en caso necesario.

•Contar con los elementos necesarios y redundantes para detectar y extinguir incendios, con elementos de detección zonificada que detecten partículas de humo y calor en todo el centro de datos, así mismo con extintores manuales y automáticos.

Matriz de trazabilidad

Consideraciones generales que se deberán tomar en cuenta necesariamente en la propuesta

La plataforma de procesamiento, comunicación interna y seguridad que actualmente tiene el CLIENTE está virtualizada, por lo que el licitante tendrá que contemplar las configuraciones actuales de los servidores virtuales respetando los sistemas operativos y aplicaciones instaladas.

El licitante integrará todo lo requerido para alojar, instalar, migrar, operar, monitorear, soportar y mantener en condiciones óptimas de operación las aplicaciones en los servidores especificados en la tabla del Anexo I en la arquitectura que proponga el licitante durante la vigencia del contrato, por lo cual deberá contar con el personal técnico con los conocimientos necesarios de acuerdo a la solución de su propuesta.

Las especificaciones y configuraciones que se solicitan en este documento, Anexo I, se consideran mínimas.

El CLIENTE con el fin de asegurar que el servicio que está solicitando sea de la más alta calidad solicita que el equipo que el licitante provea sea equipo dedicado, vigente y con garantía de soporte durante la vigencia del contrato. Las licencias de software y sus actualizaciones de versiones de sistemas operativos, bases de datos (SQL server), software de virtualización (VMware o Hyper-V) asi como las necesarias

para la operación de los sistemas y aplicaciones deberán ser proporcionadas por el proveedor sin costo adicional para el Instituto. En el caso del licenciamiento de Microsoft, se podrá utilizar el contrato actual de licenciamiento Select Académico suscrito actualmente con la empresa Microsoft de México por el CLIENTE.

Se deberá permitir el acceso de personal técnico autorizado del CLIENTE al centro de datos propuesto, para supervisar los procesos realizados, tanto en la etapa de migración como de operación de los servicios, dentro del área que el licitante destine al CLIENTE.

En el caso específico el MAAGTICSI (Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información), El licitante deberá conocer y trabajar de acuerdo al mismo integrando la documentación que se le solicite por parte del CLIENTE en el momento que se le requiera.

Al término del contrato el licitante se obliga, en su caso, a prestar al CLIENTE las facilidades necesarias para la migración del servicio a otro centro de datos, dichas facilidades consistirán en lo siguiente:

- Entregará memoria técnica actualizada de la infraestructura en que operan las aplicaciones, especificando características y capacidades de los equipos, versiones de sistemas operativos, bases de datos y demás software ambiental necesario para el servicio. Deberá incluir también la información de configuración aplicable, tales como los parámetros de configuración de sistemas operativos. Esta memoria técnica deberá ser entregada al CLIENTE a más tardar el 30 de abril de 2020.

- Migración Tecnológica de fin de contrato: el proveedor actual deberá coordinar la transferencia tecnológica del servicio objeto de este contrato con futuros proveedores de servicios, por lo que el proveedor actual de manera conjunta con el proveedor entrante elaborarán la logística de transición así como los mecanismos e infraestructura a utilizar para tal efecto sin costo adicional para el INEA, considerando que el inicio de la migración tecnológica deberá iniciar al menos 30 días naturales antes de la conclusión del contrato actual para quedar totalmente concluida al término de contrato actual. El prestador del servicio saliente estará obligado a colaborar y facilitar las labores de transferencia del servicio objeto de este contrato al nuevo prestador del servicio.

Los servidores del Anexo I deberán conservar la virtualización de acuerdo a la arquitectura propuesta por el licitante o podrá variar conforme a las necesidades del CLIENTE dentro del total de las capacidades propuestas.

Debido a la criticidad del servicio se requiere que el centro de datos propuesto cumpla con al menos la disponibilidad, de cada uno de sus elementos, solicitada en el Anexo I y II.

El centro de datos propuesto deberá ubicarse dentro de la República Mexicana. En caso de encontrarse fuera de la Zona Metropolitana de la Cd. De México, el Licitante deberá considerar en su propuesta, los costos por concepto de viáticos y traslados del personal del CLIENTE al menos 2 veces por mes para dos personas (Hospedaje, Alimentos y Traslados).

IV. Niveles de servicio.

Los niveles de servicio se consideran por cada uno de los servidores virtuales donde se hospedan las aplicaciones críticas del Instituto, los cuales se pueden observar de manera detallada en la tabla del Anexo II.

Penalizaciones en la operación de los servicios

Con fundamento en lo dispuesto por el artículo 53 de la Ley en la materia y el 95 y 96 de su reglamento, el Instituto aplicará penas convencionales al proveedor del servicio, de la siguiente manera:

Se precisa que el instituto requiere la totalidad de los conceptos del servicio que indica en la partida 1.

•**Pena convencional**: En el caso de incumplimiento en el tiempo de la prestación del servicio, el personal del cliente procederá a calcular la pena convencional conforme al 1% del monto total del monto total del contrato, por cada día de retraso en la prestación del servicio, la que no excederá del monto de la garantía de cumplimiento. Dicha pena tendrá como límite la aplicación un equivalente al 5% considerando que el porcentaje de la fianza es del 10% del monto total del contrato y/o pedido antes de I.V.A.. no podrá exceder del monto de la garantía de cumplimiento del contrato y/o pedido, una vez transcurridos una vez alcanzado el 5% el inea podrán iniciar el procedimiento de rescisión del instrumento jurídico respectivo y se hará efectiva la garantía de cumplimiento del mismo, el pago de las penalizaciones deberá hacerse a favor del inea mediante cheque certificado, de caja o dinero en efectivo en el departamento de tesorería.

Asimismo, notificará a la Dirección de Administración y Finanzas, para que le notifique al prestador de servicios dicha pena, para que éste realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor de INEA.

•**Penalización por deductivas**: En el caso de cumplimiento deficiente en la prestación del servicio, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del entregable, la que no excederá del monto de la garantía de cumplimiento. Adicionalmente, notificará al prestador de servicios mediante oficio para que, en un término no mayor a 5 días hábiles posteriores a la notificación, se realice la reposición del servicio; en caso de que el prestador de servicios no realice dicha reposición, la Subdirección Técnica procederá a calcular, de forma adicional, la deductiva conforme al 1% del monto total de la factura del entregable, la que no excederá del monto de la garantía de cumplimiento.

En caso de que el proveedor de servicio dentro de los primeros 5 días naturales del mes siguiente no entregue el Reporte mensual de operaciones, el cual incluye: el Reporte de atención de tickets y CRQ´s, el Reporte de monitoreo de servidores, el Reporte de uso de enlaces de Internet y el Reporte WAF, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del mes correspondiente por cada día natural de atraso en la entrega del reporte mensual, la que no excederá del monto de la garantía de cumplimiento. En caso de alguna instrucción de carácter de cierre presupuestal lo anterior puede ser modificado conforme a la naturaleza de la solicitud.

Una vez entregado el Reporte mensual de operaciones, el cual incluye: el Reporte de atención de tickets y CRQ´s, el Reporte de monitoreo de servidores, el Reporte de uso de enlaces de Internet y el Reporte WAF, la Subdirección Técnica procederá a su revisión en un máximo de 2 días naturales, y en el supuesto que tenga comentarios u observaciones sobre el mismo, notificará al proveedor por correo electrónico para que realice las correcciones, por lo que el proveedor contará con 3 días naturales para realizar las correcciones, en caso de que el proveedor exceda los 3 días naturales, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del mes correspondiente por cada día natural de atraso en la entrega del reporte mensual corregido, la que no excederá del monto de la garantía de cumplimiento.

Asimismo, se notificará a la Dirección de Administración y Finanzas, para que le notifique al prestador de servicios dicha deductiva y éste realice el pago de la deductiva mediante efectivo, cheque de caja o certificado a favor de INEA.

V. Terminos y condiciones de entrega y de aceptación.

Plazos, condiciones de entrega y forma de pago:

Se realizará el pago a mensualidades vencidas contra entrega del Reporte Mensual de operación documento que respalda los servicios aplicables durante la vigencia, que será validado y a entera satisfacción del anexo técnico para que el personal de la Subdirección Técnica, sea quien realice la liberación de pago correspondiente.

El licitante ganador deberá presentar los primeros días de cada mes el Reporte Mensual de Operación (entregable) del servicio prestado en el período inmediato anterior, el cual será revisado y validado por el personal de la Subdirección Técnica, el cual estará integrado por:

- Reporte de tickets y CRQ´s en el período
- Reporte de monitoreo de las máquinas virtuales
- Uso de Enlaces de Internet
- Reporte del WAF

VI. Tiempos de respuesta de soporte y de servicio.

Soporte 24 horas al día, los 7 días de la semana, durante la vigencia del instrumento jurídico con un número 01 800. El servicio del proveedor deberá tener las siguientes características distintivas:

- A través del sitio web del licitante ganador del servicio se podrá solicitar en línea cualquier servicio de ayuda y apoyo técnico, opciones adicionales y modificaciones a sus servicios, así como verificar el estatus de sus órdenes.
- Contar con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7x24.
- Compromiso de atención de forma directa e inmediata del técnico especializado asignado para la solicitud de servicios y asesoría técnica.
- Asegurar un tiempo de respuesta a falla de máximo 30 minutos.

VII. Cláusula de Confidencialidad

•El licitante se obliga a que toda la información suministrada por el CLIENTE o a la que tenga acceso, sea o no confidencial o reservada, es propiedad del CLIENTE; por consiguiente, está expresamente prohibido transmitir, divulgar o comercializar total o

parcialmente dicha información, y esta será manejada con carácter estrictamente confidencial o reservada.

•El licitante guardará absoluta confidencialidad respecto del contenido de la documentación y/o información a la que tenga acceso, en el supuesto de que se incumpla con esta obligación, se deberá pagar al CLIENTE los daños y perjuicios que se le ocasione.

•El licitante adoptará las precauciones necesarias para proteger la información confidencial o reservada del CLIENTE. Por tal motivo, el licitante asume expresamente cualquier responsabilidad que se derive del incumplimiento por parte de sus respectivos empleados a las obligaciones de confidencialidad descritas en el presente documento. Cuando la información confidencial o reservada ya no sea necesaria, se devolverá al CLIENTE o se destruirá si esta así lo solicita.

•El licitante notificará inmediatamente al CLIENTE en caso de descubrir un uso, revelación o divulgación no autorizados de información confidencial o reservada, y cooperará con el CLIENTE para ayudarla a retomar posesión e impedir usos no autorizados adicionales de su información confidencial o reservada.

VIII. Supervisión del servicio contratado

Administración, supervisión y vigilancia.

El administrador del instrumento jurídico será el Titular de la Subdirección Técnica y el Supervisor será el Titular del Departamento de Soporte Técnico y Servicios.

Funciones del administrador: responsable de interactuar con el supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Funciones del supervisor: responsable de interactuar con el administrador y el proveedor, para dar seguimiento y verificar que el servicio cumpla con las especificaciones, actividades y entregas puntuales del servicio.

El INEA a través del administrador y supervisor del contrato realizarán la comprobación y verificación en cualquier tiempo y lugar del desarrollo de los servicios y el cumplimiento en tiempo y forma de la presentación de los entregables por parte del licitante ganador, otros elementos que se deberán de tomar en consideración:

- Monitoreo cotidiano del servicio.
- Seguimiento a tickets:
  - Levantados.
  - Resueltos.
  - En proceso.
- Revisión del entregable mensual

TABLA DE SUPERVISIÓN

Elemento a supervisar	Descripción	Documento de supervisión	Comentarios
Servidores	Que los servidores estén disponibles y operables con respecto a procesamiento, memoria y almacenamiento	Gráficas mensuales de uso de procesador, memoria y disco	En caso de incumplimiento o cumplimiento parcial por parte del proveedor de servicio se aplicará la pena convencional o deductiva correspondiente
Proteccion de aplicaciones Web	Que los sitios web estén protegidos de posibles ataques de seguridad.	Reporte mensual de intentos de ataque de los siguientes sitios web: www.inea.gob.mx www.conevyt.org.mx www.cursosinea.conevyt.org.mx	
Registro y seguimiento de incidentes	Que la mesa de servicio proporcione el seguimiento de los incidentes presentados	Reporte mensual de incidentes y cambios solicitados.	
Enlaces de internet	Que se tenga disponible el ancho de banda solicitado	Gráfica mensual de uso de enlaces	

Entregables

El licitante ganador está obligado a presentar los siguientes entregables durante la prestación del servicio.

Reporte	Fecha	Observaciones
Reportes sobre el inicio y fin de la migración de aplicaciones	Primera semana de iniciada la migración y hasta concluir la actividad satisfactoriamente	

Reporte mensual de operaciones: Reporte de atención de tickets y CRQ´s Reporte de monitoreo de servidores Reporte de uso de enlaces de Internet	Los primeros 5 días del mes siguiente	
Reporte mensual	Los primeros 5 días del mes	Reporte WAF

Otros resultados, aportaciones y compromisos

- El prestador de servicios acudirá a las reuniones que se le soliciten vía correo electrónico, por parte del personal adscrito a la Subdirección Técnica del CLIENTE, ubicada en la Calle Francisco Márquez # 160, Colonia Condesa, C. P. 06140, Cuauhtémoc, Ciudad de México; con la finalidad de validar los avances del proyecto.

ATENTAMENTE

Oscar Ulises Contreras Luna
Subdirector Técnico

EDUCACIÓN

INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS

ANEXO I

TABLA DE SERVIDORES, CARACTERÍSTICAS MÍNIMAS

No.	Name	Plataforma	Tipo de servicio	Procesadores	HD (GB)	RAM (GB)	Motor de BD	Nivel de criticidad	Minutos máximos de indisponibilidad en el mes	Observaciones
1	Arp_Mevyt	Red Hat Enterprise Linux 6.4 Santiago(64-bit)	Web Server	8	150	32		2	60 minutos	
2	[illegible]	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	4	100	16		2	60 minutos	
3	[illegible]	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	90	2		2	60 minutos	
4	[illegible]	Microsoft Windows Server 2003 (32 bit)	Base de datos	8	558	32	SQL Server 2005	1	30 minutos	
5	[illegible]	Red Hat Enterprise Linux 6.6 Santiago (64-bit)	Web Server	4	170	16		2	60 minutos	
6	[illegible]	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	130	1		2	60 minutos	
7	[illegible]	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1487	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
8	[illegible]	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1340	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
9	DBPRIOMX05	Microsoft Windows Server 2008 R2 (64 bit)	Base de datos	40	620	160	SQL Server 2016 Enterprise Edition	1	30 minutos	
10	DBPRIOMX06	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	478	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
11	dborkiosasa	Microsoft Windows Server 2012 (64-bit)	Base de datos	8	230	8	SQL Server 2016 Enterprise Edition	1	30 minutos	
12	FILENET	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	240	4	SQL Server 2000 Enterprise	2	60 minutos	
13	FTPJXKIOMX01	Ubuntu Linux 8.04 Hardy (64-bit)	Web Server	4	135.97	4		2	60 minutos	
14	HDVRKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	8	245	16	SQL Server 2008 R2	1	30 minutos	
15	ineavcliente	Microsoft Windows 8 (64-bit)	Web Server	4	54	4		2	60 minutos	
16	INEA-WEB	Microsoft Windows Server 2003 Standard (32-bit)	Web Server	4	78	4		1	30 minutos	
17	ineawad01	Microsoft Windows Server 2008 R2 (64-bit)	Administración	4	100	4		1	30 minutos	
18	ineawad02	Microsoft Windows Server 2003	Administración	8	100	8		1	30 minutos	
19	ineawbd01	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	50	4	SQL Server 2014	2	60 minutos	
20	ineawbd02	Microsoft Windows Server 2012 (64-bit)	Base de datos	32	642	128	SQL Server 2008 R2, SQL Server 2012, SQL Server 2014	1	30 minutos	
21	ineawbd03	Microsoft Windows Server 2012 (64-bit)	Base de datos	4	442	4	SQL Server 2008 R2, SQL Server 2012, SQL Server 2014	2	60 minutos	
22	ineawws01	Microsoft Windows Server 2012 (64-bit)	Web Server	4	150	32		2	60 minutos	
23	ineawws02	Microsoft Windows Server 2003 Enterprise x64 SP2	Web Server	2	50	4		2	60 minutos	
24	ineawws03	Microsoft Windows Server 2012 (64-bit)	Web Server	32	1155	32		1	30 minutos	
25	ineawws04	Microsoft Windows Server 2012 (64-bit)	Web Server	4	405	4		2	60 minutos	
26	ineawws05	Microsoft Windows Server 2012 R2(64-bit)	Web Server	16	150	4		1	30 minutos	
27	MEVYTVK	Red Hat Enterprise Linux 5.4 Tikanga (32-bit)	Web Server	2	118	4		2	60 minutos	
28	mevyt-ol	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	4	100	8		2	60 minutos	
29	mevytusa	Red Hat Enterprise Linux 5 Tikanga (64-bit)	Web Server	16	207	32		2	60 minutos	
30	MICROINEA	Red Hat Enterprise Linux 6.1 - Santiago (64-bit)	Web Server	1	136	1		2	60 minutos	
31	MINDVRKIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	8	180	32	SQL Server 2005	2	60 minutos	
32	msuxinea01	Linux Red Hat 7.0	Web Server	4	130	8		2	60 minutos	
33	MSUXKIOMXPCONE	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	8	180	32		2	60 minutos	
34	MSUXKIOMXPINEA	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	8	119	32		2	60 minutos	
35	POWERBI	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	100	4	SQL Server 2008 R2, SQL Server 2014	2	60 minutos	
36	RUBYAELKIOMX	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	64	130	128	SQL Server 2008 R2	1	30 minutos	
37	[illegible]	Microsoft Windows Server 2003 (32 bit)	Base de datos	4	250	32	SQL Server 2000	1	30 minutos	Se requiere licencia para Crystal Reports XI Release 1, BussinesObjects Enterprise Release 2
38	[illegible]	Microsoft Windows Server 2003 (32 bit)	Base de datos	4	230	32	SQL Server 2000	1	30 minutos	Se requiere licencia para Crystal Reports XI Release 1, BussinesObjects Enterprise Release 2
39	SIVEFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	4	200	24		2	60 minutos	SAP Crystal Reports, BusinessGbjects
40	SIVESQL	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	4	300	16	SQL Server 2008 R2	2	60 minutos	
41	SPLAZAS	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	8	456	16	SQL Server 2008 R2	2	60 minutos	
42	VCSRV-INEA01	Microsoft Windows Server 2012 (64-bit)	Administración	8	228	8		2	60 minutos	
43	vsalNEA-BAAS	Other (32-bit)	Administración	2	158	2		2	60 minutos	
44	WSPDKIOMX02	Microsoft Windows Server 2003 (32-bit)	Web Server	16	200	32		1	30 minutos	
45	wspdkiomx03	Microsoft Windows Server 2003 (32-bit)	Web Server	32	200	32		1	30 minutos	
46	WSPDKIOMX04	Microsoft Windows Server 2003 (32-bit)	Web Server	2	100	32		1	30 minutos	
47	WSPDKIOMX06	Microsoft Windows Server 2003 (32-bit)	Web Server	16	200	32		1	30 minutos	
48	WSPDKIOMX07	Microsoft Windows Server 2003 (32-bit)	Web Server	16	220	32		1	30 minutos	
49	WSPDKIOMX09	Microsoft Windows Server 2003 (32-bit)	Web Server	16	215	32		1	30 minutos	
50	WSSAELKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	32	200	64		1	30 minutos	

ANEXO II
NIVELES DE SERVICIO

No.	Name	Plataforma	Tipo de servicio	Nivel de criticidad	Minutos máximos de indisponibilidad en el mes
1	App_Mevyt	Red Hat Enterprise Linux 6.4 Santiago(64-bit)	Web Server	2	60 minutos
2	app-mevyt	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	2	60 minutos
3	APPRKIOCFE01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	60 minutos
4	BITVRKIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	1	30 minutos
5	CURSOS_INEA	Red Hat Enterprise Linux 6.6 Santiago (64-bit)	Web Server	2	60 minutos
6	DBPRKIOINAP01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
7	DBPRKIOMX03	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
8	DBPRKIOMX04	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
9	DBPRKIOMX05	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
10	DBPRKIOMX06	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
11	dbprkiosasa	Microsoft Windows Server 2012 (64-bit)	Base de datos	1	30 minutos
12	FLEXNET	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	60 minutos
13	FTPUXKIOMX01	Ubuntu Linux 8.04 Hardy (64-bit)	Web Server	2	60 minutos
14	HDVRKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
15	ineavcliente	Microsoft Windows 8 (64-bit)	Web Server	2	60 minutos
16	INEA-W16	Microsoft Windows Server 2003 Standard (32-bit)	Web Server	1	30 minutos
17	ineawad01	Microsoft Windows Server 2008 R2 (64-bit)	Administración	1	30 minutos
18	ineawad02	Microsoft Windows Server 2003	Administración	1	30 minutos
19	ineawbd01	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
20	ineawbd02	Microsoft Windows Server 2012 (64-bit)	Base de datos	1	30 minutos
21	ineawbd03	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
22	ineawws01	Microsoft Windows Server 2012 (64-bit)	Web Server	2	60 minutos
23	ineawws02	Microsoft Windows Server 2003 Enterprise x64 SP2	Web Server	2	60 minutos
24	ineawws03	Microsoft Windows Server 2012 (64-bit)	Web Server	1	30 minutos
25	ineawws04	Microsoft Windows Server 2012 (64-bit)	Web Server	2	60 minutos
26	ineawws05	Microsoft Windows Server 2012 R2(64-bit)	Web Server	1	30 minutos
27	MEVYTMX	Red Hat Enterprise Linux 5.4 Tikanga (32-bit)	Web Server	2	60 minutos
28	mevyt-pl	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	2	60 minutos
29	mevytusa	Red Hat Enterprise Linux 5 Tikanga (64-bit)	Web Server	2	60 minutos
30	MICROINEA	Red Hat Enterprise Linux 6.1 - Santiago (64-bit)	Web Server	2	60 minutos
31	MINDVRKIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	60 minutos
32	msuxinea01	Linux Red Hat 7.0	Web Server	2	60 minutos
33	MSUXKIOMXPCONE	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	2	60 minutos
34	MSUXKIOMXPINEA	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	2	60 minutos
35	POWERBI	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
36	RDBSAELKIOMX	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
37	rppdkiomx02	Microsoft Windows Server 2003 (32-bit)	Base de datos	1	30 minutos
38	rppdkiomx03	Microsoft Windows Server 2003 (32-bit)	Base de datos	1	30 minutos
39	SIVEFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	60 minutos
40	SIVESQL	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
41	SPLAZAS	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
42	VCSRV-INEA01	Microsoft Windows Server 2012 (64-bit)	Administración	2	60 minutos
43	vsaINEA-BAAS	Other (32-bit)	Administración	2	60 minutos
44	WSPDKIOMX02	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
45	wspdkiomx03	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
46	WSPDKIOMX04	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
47	WSPDKIOMX06	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
48	WSPDKIOMX07	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
49	WSPDKIOMX09	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
50	WSSAELKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	1	30 minutos

EDUCACIÓN

INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS

FORMATO DE PROPOSICIÓN ECONÓMICA

NOMBRE DE LA EMPRESA:

DOMICILIO FISCAL

R.F.C. **TELÉFONO:**

No. de partida	Descripción	Concepto	A Costo del 13 al 31 de enero de 2020	B Costo mensual	C Costo por 11 meses (febrero a diciembre 2020)	Costo total del servicio (A + C)
1	Servicio de infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y extranet (hosting centro de datos externo) 2020	Servicio de migración de aplicaciones y servicios				
		Servicios de hospedaje				
		Infraestructura y servidores				
		Servicios técnicos profesionales integrado				
		Servicios administrados				
		Licenciamiento				
		Servicio de análisis de vulnerabilidades				
		Servicio de protección aplicaciones Web (WAF)				
		Respaldo y recuperación de información				
		SUBTOTAL				
		I.V.A.				
		TOTAL INCLUYENDO I.V.A				
TOTAL CON LETRA INCLUYENDO I.V.A.						

NOTAS:

1. LOS IMPORTES DEBEN ESTAR EN MONEDA NACIONAL CON DOS DECIMALES.
2. LA COTIZACIÓN DEBERÁ CONTENER LA FECHA DE VIGENCIA
3. ES REQUISITO INDISPENSABLE COTIZAR LA TOTALIDAD DE LOS CONCEPTOS CONTENIDOS EN LA PARTIDA.
4. EL CONCEPTO "SERVICIO DE MIGRACIÓN DE APLICACIONES Y SERVICIOS" DEBERÁ CONCLUIRSE EN LA FECHA INDICADA EN LAS ESPECIFICACIONES TÉCNICAS, NO OBSTANTE QUE EL COSTO TOTAL DEL MISMO SERÁ PAGADO A MENSUALIDAD JUNTO CON LOS DEMÁS CONCEPTOS.

NOMBRE Y FIRMA DE LA EMPRESA O REPRESENTANTE LEGAL

Ciudad de México a, _____ de _____ de _____.

ATENTAMENTE

Oscar Ulises Contreras Luna
Subdirector Técnico

KIO Networks

Ciudad de México a enero 3 2020.

Instituto Nacional para la Educación de los Adultos INEA
Francisco Márquez No. 160
Col. Condesa
Ciudad de México., C.P. 06140

Subdirección Técnica

Atención: **Lic. Oscar Ulises Contreras Luna**

Estimado Lic. Oscar Contreras

En respuesta a su solicitud realizada a través del oficio número ST/009/2020 de fecha 03 de enero del 2020, le comunico que Sixsigma Networks México S.A. de C.V. (KIO Networks), sí está en condiciones de otorgar el servicio de Infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de internet y extranet (hosting centro de datos externo) 2020 al Instituto Nacional para la Educación de los Adultos (INEA) conforme a lo solicitado en su Anexo Técnico el cual corresponde a los alcances, términos y condiciones del contrato que actualmente tenemos celebrado con el Instituto. Lo anterior, conforme a su solicitud aceptamos realizarlo bajo un esquema de adhesión al contrato de prestación de servicios No. SG/CPS/85/2016-2019, mediante el cual proveemos servicios a la Secretaría de Gobernación – RENAPO, el cual es derivado de licitación pública No. LA-004000998-E51-2016.

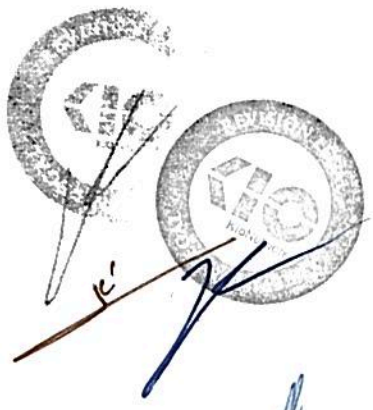
El precio total del servicio sería de $10,220,558.74 (M.N.), IVA incluido, durante 11 meses 15 días, a partir del 17 de enero del 2020 al 31 de diciembre de 2020.

Se anexa propuesta económica y técnica que cubren la totalidad del requerimiento del INEA descrito en el Anexo Técnico.

Sin más por el momento, quedo a sus órdenes y le envío un cordial saludo.

Atentamente,

Juan Carlos Martínez Valdés
Representante Legal
Sixsigma Networks México, S.A. de C.V.



SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
Prol. Paseo de la Reforma No. 5287
Col. Cuajimalpa, México D.F. 05000
SNM010323EB5

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS

FORMATO DE PROPOSICIÓN ECONÓMICA DE LA EMPRESA

KIO Networks

NOMBRE DE LA EMPRESA: Sixsigma Networks México S.A. de C.V.

DOMICILIO FISCAL: Prol. Paseo de la Reforma No. 5287 Col. Cuajimalpa, México D.F. 05000

R.F.C.: SNM010323E85 **TELÉFONO:** (52) 55 85032600 Ext. 3931

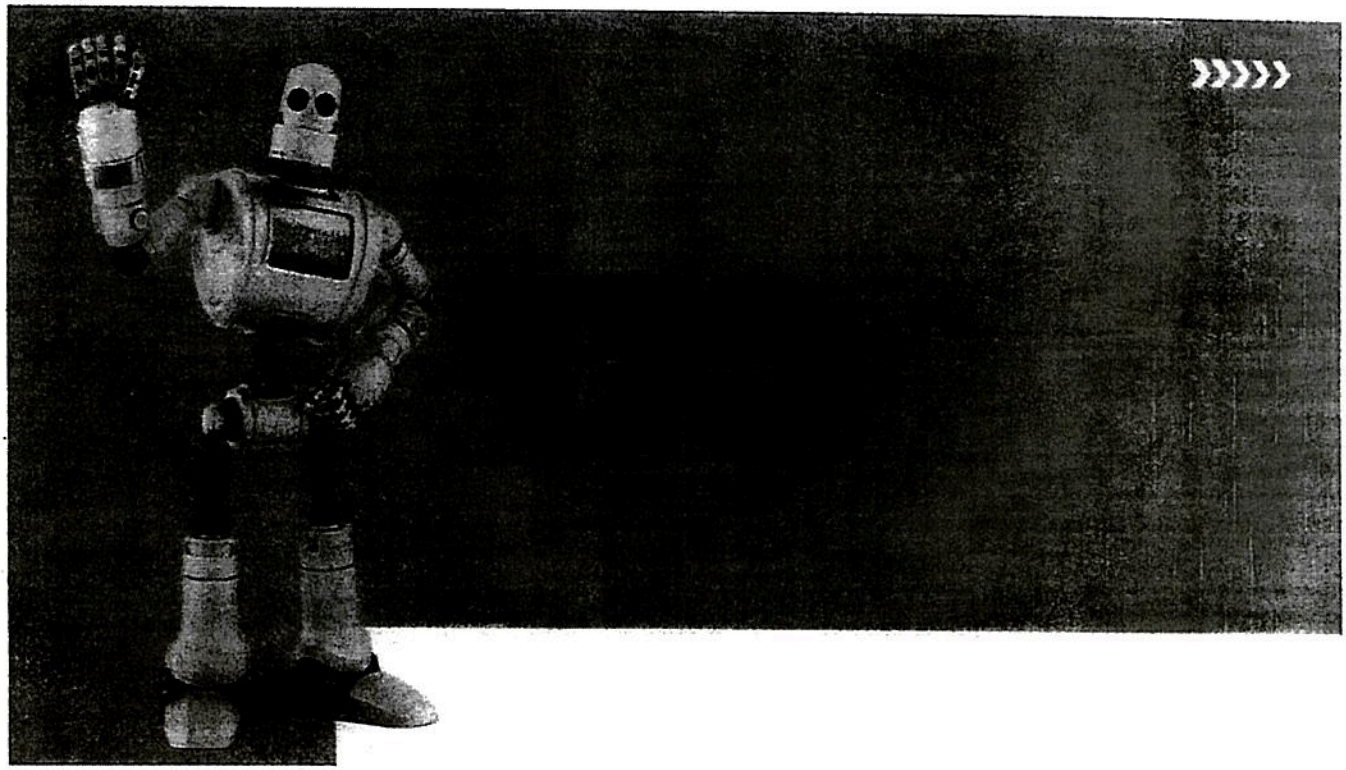
			A	B	C	
No. de Partida	**Descripción**	**Concepto**	**Costo del 17 al 31 de enero de 2020**	**Costo mensual**	**Costo por 11 meses (febrero a diciembre 2020)**	**Costo total del servicio (A + C)**
1	*Infraestructura servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y Extranet (hosting centro de datos externo) 2020*	SERVICIO DE MIGRACIÓN DE APLICACIONES Y SERVICIOS	$ -	$ -	$ -	$ -
		SERVICIOS DE HOSPEDAJE	$ 15,250.99	$ 31,518.71	$ 346,705.80	$ 361,956.79
		INFRAESTRUCTURA Y SERVIDORES	$ 153,309.79	$ 316,840.23	$ 3,485,242.54	$ 3,638,552.32
		SERVICIO DE TÉCNICOS PROFESIONALES INTEGRADOS	$ 29,874.66	$ 61,840.96	$ 680,250.60	$ 710,125.26
		SERVICIOS ADMINISTRADOS	$ 37,622.50	$ 77,753.16	$ 855,284.76	$ 892,907.26
		LICENCIAMIENTO	$ 41,716.29	$ 86,213.67	$ 948,350.37	$ 990,066.66
		SERVICIO DE ANALISIS DE VULNERABILIDADES	$ 6,077.99	$ 12,511.30	$ 137,624.30	$ 143,702.29
		SERVICIO DE PROTECCIÓN DE APLICACIONES WEB (WAF)	$ 48,642.98	$ 100,528.82	$ 1,105,817.00	$ 1,154,459.98
		RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	$ 38,724.27	$ 80,030.15	$ 880,331.67	$ 919,055.94
		SUBTOTAL	**$ 371,219.46**	**$ 767,237.00**	**$ 8,439,607.04**	**$ 8,810,826.50**
		I.V.A	**$ 59,395.11**	**$ 122,757.92**	**$ 1,350,337.13**	**$ 1,409,732.24**
		TOTAL INCLUYENDO I.V.A	**$ 430,614.58**	**$ 889,994.92**	**$ 9,789,944.17**	**$ 10,220,558.74**
		TOTAL CON LETRA INCLUYENDO I.V.A	*Diez millones doscientos veinte mil quinientos cincuenta y ocho pesos 74/100 M.N.*			

NOTAS:

1. LOS IMPORTES ESTAN EXPRESADOS EN MONEDA NACIONAL CON DOS DECIMALES.
2. LA COTIZACIÓN CORRESPONDE A UNA CONTRATACIÓN DE 11 MESES Y 15 DÍAS
3. LA VIGENCIA DE LA PROPUESTA ECONÓMICA ES DE 60 DÍAS.

Juan Carlos Martínez Valdés
Representante Legal

03 de enero de 2020



Propuesta Técnica

Contratación del Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting Centro de Datos Externo) 2020

03/ene.2020

ESPECIFICACIONES TÉCNICAS

Contratación del Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting Centro de Datos Externo) 2020.

Antecedentes

El INEA ha realizado contratos plurianuales para el servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting centro de datos externo) 2020. La infraestructura mencionada se encuentra actualmente alojada en un Centro de Datos de alta especialización, en el cual están hospedadas las diferentes aplicaciones informáticas que apoyan a los procesos sustantivos enfocados a cumplir los servicios que demandan los usuarios del INEA.

Propuesta para requerimientos Funcionales solicitados por el INEA

Descripción General del Servicio Requerido

Sixsigma Networks México, SA de CV, en adelante KIO Networks presenta la siguiente propuesta al INEA.

El INEA requiere de un contrato de servicios que provea la infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de internet y extranet de la entidad.

El contrato de servicios ofertado por KIO Networks contempla como mínimo el servicio de hospedaje dedicado de aplicaciones en infraestructura y servidores dedicados, lo cual permitirá alojar aplicaciones críticas para tener acceso vía internet. Se incluye todo el soporte necesario en hardware, software, servicios y recursos humanos especializados de acuerdo con la tarea a desarrollar para implementar, instalar, reinstalar las aplicaciones del INEA durante todo el tiempo que dure el contrato y soporte e instalación de equipo de comunicaciones y almacenamiento solicitado en este documento. Así mismo, contará con el personal dedicado y especializado de acuerdo con la tarea a desarrollar para el INEA en servicio 7x24 los 365 días para soporte y asesoría de todas las plataformas de hardware, software (en todas las aplicaciones integradas).

A través de los servicios solicitados el INEA contará con una infraestructura dedicada de alta calidad para hospedar de forma remota aplicaciones complejas de uso crítico alojadas en el centro de datos.

Este documento describe las especificaciones técnicas que en materia de hospedaje y/o coubicación de la plataforma tecnológica, procesamiento, almacenamiento, seguridad, licenciamiento de software, soporte y comunicaciones del ambiente de producción de la información que soporta las aplicaciones de misión crítica que KIO Networks oferta al Instituto, en un esquema de servicios administrados.

Objetivos generales.

- KIO Networks oferta una solución en la cual integrará todo lo requerido para alojar, instalar, migrar, operar, monitorear, soportar y mantener las aplicaciones en los servidores, equipos de comunicaciones y seguridad especificados en este documento.
- KIO Networks propone altos niveles de servicio bajo un solo modelo de operación de acuerdo con lo establecido en este documento.

SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
Prol. Paseo de la Reforma No. 5287
Col. Cuajimalpa, Ciudad de México, C.P. 05000
SNM010323 EB5

1. CANTIDAD Y ESPECIFICACIONES GENERALES.

La descripción general de la partida ofertada es la siguiente:

Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (Hosting centro de datos externo) 2020

Lugar de prestación de los servicios.

KIO Networks brindará el Servicio desde el Centro de Datos de KIO Networks (externo), ubicado en Santa Fe, Ciudad de México, los sistemas y servicios hospedados serán accesibles desde cualquier lugar a través del Servicio de Salida de Internet y dentro de la República Mexicana.

Los entregables se presentarán a la Subdirección Técnica del INEA, ubicada en la Calle Francisco Márquez # 160, Colonia Condesa, C. P. 06140, Cuauhtémoc, Ciudad de México.

Horario de servicio

El servicio se brindará las 24 horas del día los 365 días del año.

2. DESCRIPCIÓN Y ESPECIFICACIONES TÉCNICAS APLICABLES A LOS BIENES O SERVICIOS.

CARACTERÍSTICAS TÉCNICAS PARA LA PARTIDA 1.

Infraestructura

El centro de datos propuesto por KIO Networks contará con una infraestructura de alojamiento diseñado para operar como un centro de datos de alta disponibilidad y garantizar de acuerdo con el Anexo técnico, una disponibilidad sin rebasar los minutos de indisponibilidad indicados en dicho anexo KIO Networks incluye los documentos que comprueban la certificación ICREA Nivel 5 (superior al nivel 4 de ICREA solicitado por el INEA). Las instalaciones del Centro de Datos ofertado por KIO están diseñadas específicamente para el hospedaje de aplicaciones de misión crítica con características de seguridad y operación como las que se mencionan a continuación:

- Cuenta con medidas de protección física externa que lo mantiene seguro contra robo y actos vandálicos, así mismo cuenta con estacionamiento para el resguardo de vehículos y permite el acceso al personal identificado y autorizado por el INEA.

- Esta ubicado en región geológica de terreno firme zona A (bajo) o B (moderado) de peligro sísmico de acuerdo con la clasificación de regionalización sísmica publicada por el Servicio Sismológico Nacional.

- La superficie o áreas donde se encontrarán en operación los equipos de procesamiento y almacenamiento que contengan las aplicaciones e información del INEA, estarán delimitadas de otras instalaciones y áreas comunes a través de una estructura de aislamiento perimetral (jaula o equivalente, gabinetes cerrados o una solución auto contenida), de tal forma que el acceso físico a la infraestructura sólo podrá realizarlo personal autorizado por KIO Networks o el INEA, mediante rigurosos procedimientos de control de acceso, como detector de huellas, tarjetas de proximidad.

- Cuenta con cámara plena entre loza y piso falso con la altura suficiente no menor a 60 cm.

- Tiene piso firme con revestimiento epóxico de alta conductividad eléctrica con características capacitivas, conductivas, disipativas y aislantes.

- Cuenta con una acometida eléctrica dimensionada para garantizar la demanda y operación de las aplicaciones del INEA alojadas en el centro de datos propuesto y garantiza la disponibilidad indicada en el Anexo técnico.

- Cuenta con subestación de alta a baja tensión con sistemas de transferencia.

- Cuenta con equipos de energía ininterrumpida (UPS'S) redundantes con las protecciones correspondientes de supresión de transitorios y entrega de los circuitos eléctricos monofásicos, bifásicos o trifásicos necesarios para la infraestructura integral de servicios dentro del centro de datos.

- El sistema de tierra interno permitirá aterrizar los dispositivos de cómputo y telecomunicaciones, racks y/o gabinetes y demás equipos necesarios.

- El sistema eléctrico en su totalidad tiene un arreglo al menos 2N y estará dimensionado para garantizar la demanda y operación de las aplicaciones del INEA, alojadas en el centro de datos propuesto por KIO Networks, y garantizará la disponibilidad indicada en el Anexo técnico. Cuenta con un arreglo de generadores que, en el caso de una interrupción prolongada de energía, tendrá la capacidad de operar de manera autónoma y sin recargar combustible al menos 4 días.

- La interconexión de los dispositivos que integren la infraestructura ofertada se realizará a través de cableado estructurado que, dependiendo de la Interface de red de los equipos y su funcionalidad, será al menos ser del tipo UTP cat 6A (que soporta velocidades de transferencia del orden de 10/100/1000 MBPS), soporte de 10GE:10G base SR y 10G base LR, o fibra óptica, según sea el caso.

- No existirá cableado expuesto, ni tendidos de cableado mezclados de suministro eléctrico y datos.

- Cuenta con la capacidad instalada para recibir servicios de comunicaciones a través de fibra óptica y a través de infraestructuras independientes, de por lo menos 3 de los principales proveedores de telecomunicaciones (carriers) de la República Mexicana.

- Cuenta con al menos dos conexiones robustas y redundantes a la red de internet mediante accesos de alta velocidad y contendrá la funcionalidad de tráfico seguro (clean pipes), para garantizar que contará con la suficiente capacidad de ancho de banda de tal suerte que, en caso de que cualquiera de ellos no proporcione el servicio por alguna contingencia, el medio de acceso que permanezca en operación soporte la totalidad del tráfico del centro de datos.

- Cuenta con un arreglo de aires acondicionados de precisión al menos de N+1 dentro de las instalaciones donde se alberguen los equipos con controles automáticos de humedad y temperatura para mantener el rango de temperatura de operación de la infraestructura conforme a las especificaciones de los diversos fabricantes de los equipos que la compongan.

- KIO Networks incluye como parte de su propuesta el monitoreo de estos parámetros dentro del sistema de monitoreo integral del centro de datos.

- El servicio ofertado por KIO Networks soportará los BTU'S adicionales incurridos por la instalación de la infraestructura integral común de servicios, así como cualquier ampliación de infraestructura requerida para la prestación del servicio.

- KIO Networks considera como parte de su propuesta los arreglos en rack para la optimización de espacios y crecimiento vertical, así como contar con la posibilidad de ampliación de superficie de al menos el 50% de la superficie asignada.

- KIO Networks considera como parte de su propuesta posiciones de trabajo, al menos 4 posiciones de manera eventual, de así requerirlo el INEA, para que servidores públicos puedan acceder a administrar los aplicativos en sitio. Estarán equipadas con mesa, silla, teléfono y acceso a internet, provistos por KIO Networks (podrán estar en el centro de datos ofertado por KIO Networks o en un centro de negocios con el que cuente, dentro del mismo conjunto donde se ubique el inmueble del centro de datos), con acceso completo en el mismo segmento a los sistemas del INEA, restringido al acceso lógico asignado.

Procesamiento y Virtualización

El procesamiento considerado por KIO Networks para brindar el servicio se proporcionará a través de servidores basados en tecnología x86 con soporte a x64, en formato rack en plataforma virtualizada, dedicados para el servicio requerido por el INEA.

KIO Networks considera la infraestructura necesaria para llevar a cabo el soporte físico para la operación del servicio de punta a punta, considerando el servicio de procesamiento correspondiente, el cual estará acorde con las especificaciones del servicio de centro de datos ofertado.

KIO Networks considera el cableado tanto para LAN, SAN, configuraciones, seguridad física y lógica; como para los periféricos necesarios para el correcto funcionamiento de toda la infraestructura.

KIO Networks considera las licencias de software de virtualización solicitados por el INEA.

El equipo de cómputo considerado por KIO Networks contará con soporte garantizado durante la vigencia del contrato, la solución ofertada se encontrará en posibilidades de contar con alta disponibilidad en todos sus componentes y en el centro de datos.

La solución de virtualización soportará como guest los sistemas operativos mencionados en el Anexo técnico.

El equipamiento considerado por KIO Networks para brindar el servicio contará con antivirus necesario y el licenciamiento a nivel sistemas operativos, bases de datos y aplicaciones y todo aquello requerido para la operación de la plataforma del INEA.

El equipo considerado por KIO Networks para brindar el servicio ofertado contará con garantía durante la vigencia del contrato en todos los componentes por parte del fabricante; con soporte técnico en línea y telefónico, y cobertura de servicio de soporte en sitio los 7 días de la semana, las 24 horas del día (7x24); y asistencia en sitio en un máximo de cuatro (4) horas en caso de requerirse.

KIO Networks considera el licenciamiento del software necesario para soportar los servicios detallados, así como la administración y/o implementación de estos.

Actualmente las aplicaciones del INEA operan en el centro de datos propuesto por KIO Networks, por lo que no se espera tener que hacer una migración de ambientes y/o aplicaciones. Sin embargo, durante esta etapa KIO Networks realizará una revisión de la infraestructura e información actual, por si fuera necesario realizar algunos ajustes o cambios para mantener la operación durante los dosmeses de servicio que cubre esta propuesta. Durante la revisión de iniciará la aplicación SASA, la cual es la aplicación core del INEA, una vez probada se realizará la revisión de las aplicaciones satélite. Las versiones de los sistemas operativos actuales serán respetadas ya que algunos de sus aplicativos tienen codependencias. KIO Networks garantizará la continuidad de la operación a través de la infraestructura considerada para brindar el servicio.

Adicionalmente la solución ofertada por KIO Networks podrá tener alta disponibilidad y todos sus componentes de manera dedicados para el servicio ofertado al INEA. Esto es derivado de la criticidad de su operación y con la finalidad de brindar el nivel de servicio esperado por parte del INEA.

Cableado estructurado, comunicaciones y almacenamiento.
Cableado estructurado:

La interconexión de los dispositivos que integren la infraestructura considerada por KIO Networks se realizará respetando la norma de cableado estructurado, que dependiendo de la interface de red de los equipos será mínimo del tipo UTP categoría 6A o 10GE:10Gb base SR y 10G base LR, según sea el caso.

El cableado estará debidamente identificado, tanto en el panel de distribución como en los cables de interconexión.

KIO Networks considerará todos los cables, tableros, conectores y dispositivos de interconexión para todos y cada uno de los servidores, equipos de comunicaciones y seguridad descritos en este documento.

La velocidad de transferencia en la red del centro de datos entre los servidores considerados por KIO Networks para brindar el servicio al instituto será de 10Gb.

KIO Networks considerará una red independiente para el monitoreo de los servidores.

Comunicaciones:
Equipamiento de conectividad para la red LAN.

KIO Networks considera el equipamiento de switching necesario para la interconexión de toda la infraestructura a implementar en el centro de datos ofertado; y la disponibilidad en la misma será de al menos la solicitada en el Anexo técnico de acuerdo con la infraestructura solicitada por el INEA.

El esquema de conexión será coordinado por el área técnica de KIO Networks, de tal forma que la solución sea la óptima para el desempeño de las aplicaciones.

KIO Networks contará con personal técnico capacitado en el equipo considerado para brindar el servicio y dará las facilidades al instituto para que en cualquier momento pueda solicitar cambio del personal técnico asignado al instituto, si se considera necesario.

KIO Networks será el responsable de la configuración, monitoreo y mantenimiento de este servicio con el objetivo de cumplir con los niveles de servicio solicitados.

El equipo de switching considerado para brindar el servicio, tendrá al menos las siguientes características:

- Puertos 10Gb a velocidad nominal, puertos GIGABIT SFP y/o 10/100/1000 necesarios para la solución propuesta y equipo dedicado al INEA considerando todas las conexiones de los servidores a los switches, servidores y firewalls, incluyendo todos los conectores y componentes necesarios para su conexión.
- Fuente de poder redundante.
- Capa 3 con manejo de VLANS y calidad de servicio, listas de acceso y validación vía RADIUS o TACACS+.
- Posibilidad de limitar el ancho de banda por cada puerto del switch.
- El equipo será de capacidad no bloqueable.
- Soportar UDP, IP, ICMP y TCP.
- Administración vía web, telnet.
- Switching será totalmente compatible con la infraestructura propuesta para la operación de los servicios.
- Procesadores y fuentes de poder redundantes.

Acceso a la Red de Internet.

El nivel de servicio mínimo comprometido por KIO Networks para este servicio será de 99.80%.

Este servicio será entregado a través del centro de datos de KIO Networks en esquema redundante.

La solución propuesta por KIO Networks proveerá un ancho de banda de Servicio de Salida de Internet garantizado para el INEA de 70 Mb en forma continua y será capaz de absorber picos hasta 110 Mbps de entrega continua de contenido de los portales y los sistemas hospedados.

KIO Networks tendrá establecido en México acuerdos de interconexión (Peering agreements) con por lo menos dos (2) proveedores de servicios de internet con capacidad destinada en infraestructura de medios de transmisión y ancho de banda para su operación del orden de 1 Gbps con cada uno de ellos como mínimo y con la finalidad de optimizar el intercambio de tráfico entre los distintos proveedores de internet nacionales los cuales deberán estar conectados por lo menos a dos nodos "CORE" de KIO Networks , mismos que se encontrarán en diferentes zonas geográficas.

En todo momento el INEA tendrá garantizado un ancho de banda mínimo de 70 Mbps soportando picos de hasta 110 Mbps.

Las conexiones tendrán con al menos dos de los principales proveedores de servicios de internet de la República mexicana, tendrán a su vez las siguientes características:

Los prestadores de servicios de internet tendrán conexión directa a por lo menos dos puntos de acceso a la red de internet en Estados Unidos y/o NAP'S (Network Access Points, por sus siglas en inglés) con una capacidad del orden de un Gbps como mínimo.

Cobertura a nivel nacional mediante infraestructura robusta con esquemas de alta disponibilidad y redundancia automática entre sus puntos de presencia POP'S (Points of Presence, por sus siglas en inglés) y ubicación.

El acceso al backbone de Internet será exclusivo para el tráfico de Internet y no compartirá el tráfico con otros protocolos o servicios (frame relay, mpls, x.25, servicios de voz, etc.).

La red de Internet del KIO Networks contará con redundancia y diversidad de rutas.

La arquitectura de la red estará basada en un diseño de red jerárquico (nodos de backbone, acceso al servicio y CPE), dentro de esta arquitectura, las capas se usan para aislar estratos de la red, cada capa tendrá un propósito específico y cada elemento se clasifica como un miembro de la capa basado en la función que está realizando.

La red de Internet de KIP Networks estará diseñada de tal manera que el transporte de los paquetes sea de una manera eficiente, además contará con la redundancia necesaria que le permitirá ofrecer un alto rendimiento a través de una red pública.

KIO Networks considerá como parte de su propuesta el servicio de conexión a Internet simétrico con redundancia.

KIO Networks entregará el servicio mediante dos cableados en donde el primero es para internet activo y el segundo para la redundancia de este, estos cableados son Ethernet, los protocolos que se utilizarán para este servicio son anti loop y redundancia de ruteo.

Direccionamiento IP

- KIO Networks proporcionará al INEA un rango de direcciones IP homologadas para los servidores descritos en el Anexo técnico, equipos de comunicaciones y seguridad.
- Las direcciones homologadas, así como las direcciones IP internas se mantendrán con la misma numeración en cualquier proceso de migración.

Servicio DNS

- KIO Networks será responsable de ofrecer el registro de dominios y controlar la información de los DNS y todos los trámites ante el NIC o el INTERNIC, así como su mantenimiento anual correspondiente.

Servicio de almacenamiento, respaldo y recuperación

- KIO Networks considera la configuración, administración y dispositivos necesarios para la conexión de los servidores de aplicaciones del instituto al sistema de almacenamiento.

- KIO Networks considera como parte del servicio integral ofertado, el almacenamiento SAN (STORAGE AREA NETWORK) para tener espacio adicional para almacenamiento de información a través de líneas de fibra canal (FC-SWITCH O FC-AL) FC8, para la aplicación control de gestión, este podrá crecer con solo incluir discos para poder proveer crecimiento.

- KIO Networks considerará integrar las Interfaces de comunicación y componentes necesarios para la conexión entre los servidores del Anexo técnico y el sistema de almacenamiento SAN.

- KIO Networks podrá ofertar el servicio de bóveda en la cual se podrán resguardar las cintas o medios de respaldos históricos el cual podrá estar ubicado fuera de las instalaciones del centro de datos propuesto, con un ambiente físico controlado para garantizar el resguardo de los medios o las cintas y se darán las facilidades aplicables para que personal autorizado del INEA para que pueda realizar visitas para validar y evaluar el servicio de resguardo.

- El acceso a la bóveda podrá contar con control de accesos biométricos y controles de acceso en el edificio donde se encuentre.

- El equipamiento considerado contará como mínimo con las siguientes características y composición de partes en hardware y software:

Controladoras:

- KIO Networks contemplará la incorporación de al menos 2 controladoras.
- La conectividad de las controladoras al sistema de almacenamiento SAN a través de Fiber Channel, de al menos 8 Gbps, y soportarán conectividad a 10GbE
- Las controladoras serán redundantes e interconectadas.
- Memoria cache
- Cada controlador tendrá cache independiente.
- Gabinetes de disco
- Al menos gabinetes para discos de 2,5" o 3.5"
- Discos
- Capa de almacenamiento de alto rendimiento de 25 TB de espacio útil después de aplicar RAID 5, que estará compuesta por discos SAS de 450/600 GB de 10K RPM como mínimo.
- Fuentes de alimentación eléctrica redundantes
- Ventiladores redundantes
- El equipamiento considerado podrá ser instalado en un rack standard de 19", incorporando las PDU'S necesarias para la energización del almacenamiento propuesto, dispondrá de líneas de alimentación redundantes y será conectado a la red eléctrica.

La propuesta ofertada por KIO Networks incluirá las siguientes funcionalidades:

Aprovisionamiento delgado (THIN PROVISIONING)

- Esta funcionalidad permite crear volúmenes con un tamaño inicial reducido, presentarlo al servidor con un tamaño superior y aumentar el tamaño del volumen en forma automática a medida que sea necesario.

- Copia instantánea de volúmenes de datos (snapshots).

- Esta funcionalidad permite tanto duplicar un volumen de datos como tomar una imagen de un volumen en un determinado momento sin impactar la performance de los servicios que entrega el volumen.

Deduplicación.

- Esta funcionalidad permite la optimización en la utilización del espacio a nivel SAN, es a nivel de bloques de máximo 4Kb. Podrá ser independiente de las aplicaciones. Permitirá la integración con otras tecnologías de eficiencia del almacenamiento propuesto.

Compresión

- Esta funcionalidad será complementaria con la función de deduplicación, podrá ser realizada en línea o posteriormente.

Copias livianas

- Esta característica permite la creación de copias de datos en forma instantánea (snapshots) que pueden ser utilizadas en entornos de desarrollo, QA y en ambientes virtuales, sin necesidad de duplicar la capacidad de almacenamiento haciendo una gestión eficiente.

SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
Prol. Paseo de la Reforma No. 5287
Col. Cuajimalpa, Ciudad de México, C.P. 05000
SNM010323 EB5

Manejo de múltiples protocolos.

- El almacenamiento es capaz de utilizar múltiples protocolos de almacenamiento considerando al menos FCP, FCOE, ISCSI, CIFS/SMB, NFS/PNFS, estos protocolos podrán ser utilizados sin la incorporación de appliances:
- Sistema operativo de tipo Scale-Out.
- Almacenamiento en caché inteligente
- Esta tecnología permitirá acelerar las operaciones I/O para la virtualización de servidores y escritorios. Esta tecnología al igual que las anteriormente mencionadas, permite su utilización en ambientes NAS y SAN utilizando cualquiera de los protocolos asociados.
- KIO Networks considera como parte de su propuesta todo el licenciamiento necesario para el uso de las herramientas y aplicaciones que se requieran para la operación y administración de la solución de almacenamiento propuesta.
- Para estas y todas las funcionalidades que se propongan, se detallará el esquema de licenciamiento.
- También se enumerará y describirá claramente las herramientas de administración necesarias, así como la posibilidad de incorporación de módulos opcionales para estas herramientas, se detallará:
- Características del servidor necesario para la instalación de estas herramientas.
- Esquema de licenciamiento necesario de administración, así como las opciones de incorporación de módulos adicionales.

Respaldo y recuperación.

- Licenciamiento de software de 20Tb para respaldo y recuperación además del almacenamiento en disco necesario (independiente del espacio ocupado por los sistemas en producción). La unidad considerará los agentes de software necesarios para respaldar sistemas operativos, file systems y aplicaciones que residan en cada servidor.
- El software considerado por KIO Networks para brindar el servicio será capaz de respaldar las plataformas enlistadas en el Anexo técnico.
- El software considerado por KIO Networks será capaz de respaldar en línea las siguientes aplicaciones: MICROSOFT SQL, MICROSOFT EXCHANGE, ORACLE, DB2 y MICROSOFT SHAREPOINT
- El software considerado por KIO Networks tendrá la capacidad de habilitar al usuario de poder recuperar su información mediante una ventana de visualización, con la introducción de un usuario y una clave.
- El software considerado por KIO Networks llevará la administración desde una consola centralizada pudiendo lanzar los respaldos desde esta consola de manera programada o en demanda, adicional podrá habilitarse al usuario a iniciar un proceso de respaldo en demanda.
- El software considerado por KIO Networks utilizará tecnología de deduplicación en el origen y de manera global para optimizar la infraestructura de red y de almacenamiento de los datos respaldados.
- Permitirá crear calendarios de respaldo de acuerdo con las necesidades del usuario o del INEA.
- En caso de presentarse una disrupción en el servicio se requiere, el software considerado por KIO Networks cumplirá con un RTO y un RPO máximo de 12 hrs.

Restauración y recuperación.

- El software considerado por KIO Networks será capaz de realizar procesos de restauración y recuperación tanto de máquina virtuales completas, file systems, bases de datos o configuraciones de las plataformas enlistadas en el Anexo técnico.
- Permitirá realizar las pruebas necesarias para corroborar la veracidad de la información recuperada y que garantice la continuidad de las operaciones.
- Servicios técnicos profesionales integrados al servicio solicitado

Servicios profesionales integrados al servicio ofertado por KIO Networks.
Servicios Profesionales y personal capacitado.

- KIO Networks será responsable, técnica y administrativamente de migrar todas las aplicaciones cargadas actualmente en los servidores de web, aplicaciones, base de datos y servicios con que cuenta el instituto descritas en Anexo técnico, a su centro de datos. Lo anterior no considera modificaciones necesarias a las aplicaciones desarrolladas por el INEA, por parte de KIO Networks en caso de resultar adjudicado.
- KIO Networks podrá ser responsable por la correcta instalación y configuración de nuevas aplicaciones que adquiera el instituto durante la vigencia del contrato.
- Asesoría telefónica en horario 7x24x365 para el personal del INEA y en el centro de datos cuando se requiera, dando soporte especializado sobre:
  Windows Server, Linux, VMware, así como del software de aplicaciones y sistemas operativos que se instalen en los servidores hospedados, equipo de comunicaciones propuesto y seguridad.
- El INEA se reserva el derecho de exigir en cualquier momento de la vigencia del contrato o pedido que KIO Network en caso de resultar adjudicado, como proveedor cuente con el personal técnico integrado en su propuesta técnica y avalado por los documentos presentados del personal.
- Se podrá dar asesoría en reingeniería y control de aplicaciones para asegurar siempre el mejor desempeño dentro de los sistemas en la red de KIO Networks y en la red de internet.

- KIO Networks considera como parte del servicio propuesto un centro de atención telefónica con un control de llamadas y reportes de seguimiento y solución de estos. Los reportes de seguimiento contendrán como mínimo lo siguiente:

  - Número de reporte
  - Fecha
  - Hora
  - Tipo de falla
  - Tipo de escalamiento
  - Fecha y hora de solución
  - Quién reporta la falla y quién atendió

- Se contará con soporte 24 horas al día, los 7 días de la semana, todo el año. Con un número 01 800.
- Contará con un centro de monitoreo NOC (Network Operation Center) que monitoreará el estado de la red 7x24 los 365 días del año.
- Atención del técnico asignado en forma directa para la solicitud de servicios y asesoría técnica, de forma inmediata.
- Asegurará un tiempo de respuesta a falla de máximo 30 minutos.
- La mesa de ayuda formará parte primordial de un mecanismo de recepción, canalización, atención, coordinación, seguimiento, registro y reporte de incidentes, cambios solicitados, requerimientos en general y comunicación.

- KIO Networks dedicará un contacto encargado de toda la relación con el INEA, con el poder suficiente para ordenar cualquier modificación en configuración, programación y/o control de los dispositivos hospedados en el centro de datos. Este contacto podrá, de así requerirse a petición del personal del INEA, sostener reuniones periódicas para informar sobre estatus y calidad de los servicios prestados, así como entregar los reportes de desempeño de todos los elementos de la solución. El contacto asignado por KIO Networks tendrá capacidad para dirigir el proyecto apegándose a estándares de ITIL, "ITIL V3 Expert".
- KIO Networks considera como parte de su propuesta personal especializado en virtualización de la plataforma VMware, para asesoría e implementación de al menos 40 horas, que podrán utilizarse durante la vigencia del contrato.

Monitoreo del Servicio

El servicio de Monitoreo considerado como parte de la propuesta de KIO Networks comprenderá lo siguiente:

- Para todos los servidores del Anexo técnico de aplicaciones migradas a la arquitectura contará con monitoreo en hardware y software.
- Generará reportes de uso y monitoreo de los servicios en línea mediante una ventana gráfica accesible por internet (web), la cual brindará información sobre los siguientes parámetros:
    - Utilización de recursos de hardware.
    - Utilización de ancho de banda de salida y, de entrada.
    - Reportes de tráfico y desempeño en cada uno de los puertos de acceso a internet.
    - Filtros de reportes por día, semana y mes.
    - Monitoreo de los servidores de base de datos del sistema SASA en línea y SIGA.
- KIO Networks contará con personal técnico que tenga por lo menos un año de experiencia trabajando para un Hosting center de un ISP o carrier de internet.
- KIO Networks estará en la disposición de interactuar con el personal de la Subdirección Técnica del Instituto.
- KIO Networks informará inmediatamente sobre problemas detectados en el funcionamiento de servidores y el servicio al personal designado por el INEA y catalogará este procedimiento como de alta prioridad.
- Reportes de incidentes de seguridad al detectar una falla.
- Todo el monitoreo será realizado mediante una red dedicada independiente para la cual el KIO Networks proporcionará todos los componentes necesarios (Interfaces de red, switches, etc.).
- Se monitoreará el desempeño de la red, emitiendo alertas cuando el comportamiento de esta se desvíe de los patrones establecidos, mediante el análisis detallado de todas y cada una de las aplicaciones alojadas en el centro de datos.
- KIO Networks proporcionará una cuenta de usuario de solo lectura para todos los equipos de comunicaciones y seguridad.
- Como parte de los entregables mensuales, KIO Networks entregará el monitoreo de la infraestructura y el estatus de todos los incidentes reportados.
- KIO Networks proporcionará el servicio de monitoreo a través de un ambiente gráfico orientado a objetos donde se puede observar el estado de los recursos en un ambiente definido.

Soporte telefónico (Contact Center)

- Brindará soporte 24 horas al día, los 7 días de la semana, todo el año, con un número 01 800.
- El servicio de KIO Networks tendrá las siguientes características distintivas:

    - A través del sitio web de KIO Networks en caso de resultar adjudicado, se podrá solicitar en línea cualquier servicio de ayuda y apoyo técnico, opciones adicionales y modificaciones a sus servicios, así como verificar el estatus de sus órdenes.
    - Contará con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7x24 los 365 días del año.
    - Tendrá el compromiso de atención de forma directa e inmediata del técnico especializado asignado para la solicitud de servicios y asesoría técnica.
    - Asegurará un tiempo de respuesta a falla de máximo 30 minutos.

Soporte en el Centro de Datos.

KIO Networks brindará soporte técnico especializado de acuerdo con la solución propuesta (especialistas en todas las plataformas de hardware y software propuestos en su solución) a personal del Instituto, de acuerdo con el personal técnico solicitado por el INEA, en el centro de datos con soporte 7x24x365.

Servicios administrados

Servicio de Administración de Sistemas Operativos

KIO Networks considera como parte del servicio ofertado la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de los sistemas operativos de plataformas distribuidas. Este servicio complementará al de Monitoreo de Sistemas para ofrecer al INEA una experiencia integral en la atención de sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que considera KIO Networks para la administración de Sistema Operativo es lo siguiente:

Soporte al sistema operativo

- Actualización de parches
- Reinstalación del Sistema Operativo
- Instalación de nuevos volúmenes y particiones.
- Asignación de almacenamiento para la creación de nuevos volúmenes.
- Configuración del sistema operativo de acuerdo con las necesidades del cliente.
- Configuración de ambientes de clúster si así lo requiere el cliente.
- Configuración de Servicios de Acceso Remoto.

Soporte al Hardware

- Instalación de discos.
- Instalación de memoria.
- Instalación de procesadores.
- Instalación de CPU's. (con asesoría de terceros).
- Configuración del hardware de acuerdo con las necesidades del cliente.
- Asistencia en Actualizaciones.
    - Niveles de parches que requiera las aplicaciones.

Administración del Sistema de Archivos.

- Creación de nuevos volúmenes.
- Creación y modificación de particiones.
- Modificaciones al sistema de archivos de acuerdo con las necesidades del cliente.

Administración de Usuarios.

- Alta de nuevas cuentas
- Baja de cuentas
- Modificación de perfiles
- Asignación de prioridades.
- Cambio de contraseñas.
- Asignación de grupos.
- Asignación de permisos.
- Asignación de Dominios.
- Configuración de permisos de los usuarios dentro del dominio.

Emisión de reportes en caso de falla de algún servicio

- Contacto telefónico de KIO Networks hacia el INEA para dar avances en la tarea.
- Entrega de reporte de KIO Networks hacia el INEA por escrito, al final de la tarea con los resultados obtenidos.
- Entrega del plan de trabajo al INEA previo a la tarea. El plan de trabajo incluirá los siguientes puntos:
    - Objetivo
    - Prioridad
    - Impacto
    - Tiempo de duración
    - Fecha Inicio
    - Fecha Término
    - Descripción
    - Puntos de Contacto
    - Entrega y validación de orden de cambios

Administración de VMWare

KIO Networks considera como parte de su propuesta la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de VMware que contienen los equipos proporcionados. Este servicio complementará al de Administración de Sistemas Operativos para ofrecer al INEA una experiencia integral en la atención de sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que el licitante deberá considerar para la Administración de VMware:

- Instalación de ESX
- Configuración de ESX
- Ambientes de alta disponibilidad (HA, V-Motion, Switches Distribuidos)
- Creación de máquinas virtuales
- Configuración y administración de sistemas operativos

- Instalación de aplicativos dentro de las virtuales
- Adición de recursos (vCPUs, RAM, espacio en disco)
- Eliminación de Máquinas virtuales
- Configuración de Storage
- Monitoreo de disponibilidad de los equipos virtuales
- Graficas de consumo de recursos (CPU, Memoria RAM, Utilización de Disco y Red)

Servicio de Administración de Bases de Datos.

KIO Networks considera como parte de su propuesta la asistencia de personal altamente calificado para ejecutar las tareas básicas de administración de base de datos de plataformas distribuidas del INEA. Este servicio complementará al de Monitoreo de Base de Datos para ofrecer al INEA una experiencia integral en la atención de las bases de datos alojadas en sus servidores, tomando la responsabilidad de la operación y soporte de los equipos.

El alcance mínimo que KIO Networks considera para la administración de Base de Datos es:

Manejo de Incidentes/Operaciones
- Mantener información programada en las herramientas de "Job Scheduling"
- Monitorear, cancelar o programar la ejecución de un "batch job"
- Restaurar la ejecución de un "batch job" en caso de fallas
- Recuperar "rollbacks" de "batch jobs" fallidos
- Manejos de logs
- Monitorear el status de la base de datos
- Restaurar base de datos en caso de fallas
- Ejecución de Imports y/o Exports no riesgosos de Base de Datos
- Crear tablespace de base de datos
- Aumentar o disminuir el tablespace de base de datos
- Eliminar / Borrar tablespace de base de datos

Manejo de Problemas/Cambios/Configuraciones
- Diseñar un ambiente de base de datos
- Crear el cascaron de una base de datos
- Ejecución de Imports de Base de Datos
- Ejecución de Exports de Base de Datos
- Copia de Base de Datos
- Diagnosticar y arreglar problemas de lentitud o fallas de base de datos
- Crear "scripts" para base de datos

Manejo de Capacidades/Rendimiento
- Detectar problemas de capacidades en los sistemas
- Generar reportes de capacidad de recursos para los clientes

Servicio de Administración de Respaldos.

El alcance mínimo que KIO Networks contempla para la Administración de respaldos es:

- Se respaldarán 20Tb en total para los servidores (independiente a la recuperación y respaldo). El servicio ofertado por KIO Networks Incluirá licenciamiento de respaldos para file systems y Bases de Datos.

Política de respaldos:

- Respaldos Diarios con retención de 7 Días
- Respaldos Semanales con retención de 1 mes (De acuerdo con el número de semanas en el mes)

- Respaldos Mensuales con retención de 3 Meses
- Respaldos Anuales con retención de 1 año

Servicio de Administración de Restauraciones

El alcance mínimo que KIO Networks contempla para la Administración de restauraciones considera entre otros los siguientes puntos:

- El INEA podrá solicitar en cualquier momento, la restauración de algunos de los servidores ya sea parcialmente (solo datos o archivos específicos) o servidores completos que incluyan la configuración.
- KIO Networks notificará al INEA el tiempo esperado para realizar las restauraciones solicitadas y notificará oportunamente al INEA el avance de estas o cualquier imprevisto que se presente durante el proceso.
- KIO Networks en coordinación con el INEA, realizará de manera aleatoria pruebas de restauración de los servidores en el alcance del contrato. KIO Networks presentará al INEA una propuesta de calendario de ejecución de restauraciones el cual deberá considerar escenarios aleatorios.

Servicio de Administración de Almacenamiento.

KIO Networks proporcionará el servicio de almacenamiento dedicado para la atención del INEA. Estos servicios de almacenamiento contemplarán la implementación de la infraestructura y los procesos operativos necesarios para resguardar la información en un sistema de almacenamiento dedicado para el INEA. Este servicio operará mediante canales de fibra redundantes.

Se considera como parte del alcance lo siguiente:

- Configuración y puesta a punto del almacenamiento en disco en el arreglo de discos

El alcance mínimo del servicio será:

- Administración, operación y monitoreo de la infraestructura en la que opera el servicio de almacenamiento
- Actualización de microcódigo en el hardware de las plataformas de almacenamiento en disco
- Aprovisionamiento de nuevos requerimientos
- Actualización de parches de segurida
-

El servicio de almacenamiento considerado como parte de la propuesta está compuesto por los siguientes rubros:

- Almacenamiento en SAN para 20Tb utilizables por el INEA
- Conexión a la red con 2 Puertos por cada servidor físico
- Cada servidor físico deberá estará conectado de manera redundante al sistema de almacenamiento, considerando doble tarjeta de puerto y doble cableado.

La administración consistirá en asegurarse de que el servidor permanezca conectado al sistema de almacenamiento de manera redundante, cualquier reconfiguración por falla en dispositivos como puertos de directores, HBA's, puertos del arreglo de discos estará considerada dentro de la administración.

- Revisión de estatus de controladoras
- Revisión de volúmenes.
- Creación y borrado de volúmenes

- Creación y borrado de hosts
- Administración de los switches del sistema de administración
- Atención a incidentes con escalación al fabricante
- Revisión de volúmenes libres
- Validación de rutas de acceso a disco
- Revisión del estado de arreglo de discos
- Revisión de bitácoras en los switches
- Asignación de volúmenes a los servidores
- Liberación de volúmenes que están asignados
- Generación de reportes para seguimiento a fallas
- Supervisión del reemplazo de componentes relacionados con la infraestructura
- Validación de tamaño de los volúmenes asignados
- Reasignación en línea de LUNS
- Elaboración de reporte de uso de espacio asignado en el sistema de almacenamiento
- KIO Networks considerará un crecimiento 20% por lo que en caso de que el INEA requiera de este espacio se podrá habilitar de manera inmediata.

Servicio de migración de aplicaciones y servicios.

KIO Networks tendrá instalados y configurados todos los servicios a los que se refiere este documento para el 13 de enero del 2020.

La gestión de servicio de tecnologías de la información será totalmente compatible con el esquema ITIL (Information Technology Infrastructure Library) v3, además la operación en el centro de datos del KIO Networks está certificada bajo la norma ISO 20000.

Especificaciones al término de la implantación e inicio del servicio.

En caso de haber cambios en la operación de las aplicaciones que actualmente se encuentran en producción en el centro de datos de KIO Networks, se entregará al Instituto el manual de operación y memoria técnica de la instalación actualizados. Lo cual contendrá la configuración de todos y cada uno de los componentes que incluyen la solución.

Vigencia.

La vigencia del servicio ofertado por KIO Networks será a partir del 13 de enero del 2020 al 31 de diciembre de 2020.

Requerimientos no Funcionales.

Ubicación

El centro de datos propuesto por KIO Networks está construido para operar como un centro de datos de alta disponibilidad, está construido en la República Mexicana. En caso de estuviera fuera del área Metropolitana de la Ciudad de México KIO Networks considerará los viáticos para al menos 3 personas del Instituto dos veces al mes, y visitas extraordinarias que sean necesarias en caso de recuperación de respaldos, incidentes o requerimientos especiales.

Certificaciones del Centro de Datos.

KIO Networks cuenta con las siguientes certificaciones vigentes del centro de datos propuesto para garantizar los niveles de servicio solicitados:

- ISO 9001:2015 o posterior (Sistema de administración de calidad)
- ISO 20000:2011 o posterior (Sistema de Gestión de Servicio de TI)

- ISO 22301:2012 o posterior (Sistema de gestión de Continuidad de Negocio)
- ISO 27001:2013 o posterior (Sistema de administración de la seguridad de la información)

Niveles de servicio y Garantía de disponibilidad en el Centro de Datos.

El nivel de servicio considerado por KIO Networks para el Centro de Datos es ICREA Nivel 5 con lo cual se garantizará un nivel de servicio del 99.80% de disponibilidad, en caso de incumplimiento del servicio KIO Networks se hará acreedor a la pena convencional correspondiente. Debido a lo anterior KIO Networks garantizará alta disponibilidad operativa de las aplicaciones que se indican en el Anexo técnico.

Controles de Seguridad, Seguridad Lógica.

La solución propuesta por KIO Networks será exclusiva para el INEA y en esquema redundante según corresponda.

KIO Networks describe más adelante la solución propuesta para el esquema de seguridad lógica, es decir, se mencionan marcas, equipos, modelos, esquema de configuración e interconexión entre los mismos, para lograr la solución deseada y la protección de los servicios del Instituto.

- La solución de seguridad lógica propuesta por KIO Networks será realizada con equipos de propósito específico, de última generación y en una configuración de alta disponibilidad (activo-activo) según corresponda.
- La solución propuesta no será un factor de latencia adicional en las redes por razones de desempeño, por lo cual garantizará la latencia igual o menor a la de los equipos de red propuestos.
- Los equipos o dispositivos que integren la solución propuesta por KIO Networks serán completamente compatibles entre sí; de tal manera que no existan problemas de desempeño por incompatibilidad entre ellos y los equipos estarán configurados por KIO Networks hasta su puesta en marcha.
- La configuración de este sistema de seguridad será coordinada en todo momento por personal del KIO Networks. El INEA podrá solicitar las adecuaciones que considere necesarias según las necesidades del Instituto.
- Del punto anterior el tiempo máximo para atender un requerimiento de configuración de seguridad será de 30 minutos en un esquema de 7x24x365, por lo que KIO Networks contará con el personal capacitado y autorizado para efectuar movimientos en las configuraciones de estos equipos cuales quiera que estas sean.
- Adicionalmente para la coordinación de la operación de la seguridad lógica de la solución durante la vigencia del contrato, se deberá acreditar la certificación CISSP.
- KIO Networks detalla en la presente propuesta técnica, una arquitectura de seguridad la cual cumplirá con el modelo de seguridad para proteger de forma integral la infraestructura de los servicios del Instituto, ocupando para ello los dispositivos de propósito específico, esquemas en alta disponibilidad y configuraciones de seguridad; tales como:

- Firewalls en alta disponibilidad
- Sistema de detección y prevención de intrusos de red
- Switches
- Antimalware
- Antispam

Todo esto en base a políticas y procesos de administración documentados, mismos que serán proporcionados al INEA.

KIO Networks en caso de resultar adjudicado instalará, administrará, monitoreará, mantendrá y actualizará, todos los equipos antes mencionados con personal especializado para ello, asignando al personal que el INEA designe, una cuenta de solo lectura para verificar el servicio y contar con acceso a los sistemas de monitoreo para visualización de información.

El centro de datos contará con línea de defensa, que ofrece servicios de firewall, antivirus, antispam (que será proporcionado en caso de que el Servicio de Correo Electrónico sea solicitado como un proyecto por parte del INEA), VPN, detección y prevención de intrusos. Estos servicios contarán con las siguientes características:

Firewall

- Dispositivo de propósito específico.
- Firewall en esquema de alta disponibilidad y con balanceo de cargas con interfaces de red 10/100/1000 suficientes para la conectividad de la solución propuesta en firewall.
- Soportar puertos 10Gb.
- Soportar la creación de VPN'S usando los algoritmos de cifrado, firmado y hashing más comunes, así como los más modernos y seguros.
- Capaz de manejar al menos 2,000,000 de conexiones concurrentes.
- Al menos 1.2Gbps de IPS Throughput.
- Al menos soportar 50 mil nuevas conexiones por segundo.
- Los servicios de firewall serán de estado completo (statefull).
- Capaz de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con Timeout.
- Prevenir IP spoofing, debiendo tener mecanismos de protección contra ataques DoS y DDoS.
- Será capaz de implementar mecanismos de calidad de servicio; tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- La solución ofertada por KIO Networks podrá estar certificada por ICSA LABS como Enterprise firewall, con el objetivo de garantizar que la solución ofertada cumpla con las especificaciones de un firewall empresarial.

Sistema de detección y prevención de intrusos.

KIO Networks considera como parte de su propuesta, tener un sistema de detección y prevención de intrusos el cual considerará en una plataforma independiente que permita la correcta y oportuna identificación de ataques, que por lo menos proporcionen lo siguiente:

- El sistema de prevención y detección de intrusos estará en un esquema de alta disponibilidad y de balanceo de cargas con interfaces suficientes para la solución propuesta.
- Detección de ataques e intrusos: basada en firmas, anomalías estadísticas, protocolos de situaciones de negación de servicio.
- La solución ofertada podrá estar certificada por ICSA LABS como Network IPS (NIPS
- por sus siglas en inglés,) para garantizar que la solución cumpla con las especificaciones necesarias para un IPS de red empresarial.
- La solución ofertada contará con un performance mínimo de 1Gbps.
- La solución ofertada contará con la capacidad de detección de más de 5,000 ataques y permitirá la actualización constante de su base de detección de ataques.
- La plataforma de IPS contará con protección contra ataques en capas aplicativas con filtros contra PHP (Include, inyección, evasión etc.), filtros contra Cross Site Scripting y filtros

contra inyección de SQL, además contará con capacidades de detección y prevención de los "OWASP Top 10 Most Critical Web Application Security Risks.

- Rechazo de intrusos: posibilidad de configurar el sistema para rechazar o eliminar automáticamente las conexiones no deseadas.
- Soporte a configuración en modo transparente en la red.
- Proveerá de capacidad de auto aprendizaje para adaptar las políticas basadas en comportamiento del tráfico en tiempo real.

Protección contra ataque de negación de servicios.

KIO Networks incluirá en el alcance de la solución, protección contra ataque de negación de servicios con las siguientes características:

- Formato tipo "appliance" de propósito especifico para el servicio de protección contra ataques de negación de servicio distribuido.
- No se aceptarán equipos de propósito genérico (PCS o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como MICROSOFT WINDOWS, FREEBSD, SUN SOLARIS, APPLE OS-X O GNU/LINUX.
- Soportará el análisis de comportamiento basado en ASICS para detectar y bloquear ataques de anomalías, reconocimiento y mitigación Anti DDoS.
- Soporte a configuración en modo transparente en la red.
- Soporte en modo de operación transparente, el no requerir de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- Proveerá de capacidad de auto aprendizaje para adaptar las políticas basadas en comportamiento del tráfico en tiempo real.
- Realizará análisis de comportamiento de red (NBA, por sus siglas en inglés).

En seguridad.

KIO Networks incluye en la solución de seguridad con las siguientes características:

- Filtrado de direcciones IP por país (protección con geolocalización).
- Servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo con la configuración del administrador.
- Bloqueo de tráfico dirigido a puertos restringidos.
- Aprovisionar una lista de nodos o dispositivos infectados para su bloque
- Mitigación de sobre flujo de paquetes.
- Verificación de protocolos.
- Filtrado de paquetes fuera de estado e inspección del estado de los paquetes.
- Determinación heurística de tráfico malicioso (tipo botnet) y prevenirlo automáticamente.
- Filtrado basado en algoritmos.
- Análisis de comportamiento de red.
- Deberá de contar con procesos de Multi-verificación, la cual se refiere a que la solución pueda realizar múltiples procesos de verificación para identificar anomalías en el tráfico, como ser filtrado dinámico, verificación activa, reconocimiento de anomalías, verificación de protocolos.
- Mitigación de ataques en capa 3, 4 y 7.
- Capacidad de mostrar diagnósticos en tiempo real.
- La prevención contra ataques de día 0.

- Latencia permitida será de microsegundos.
- Rastreo de los dispositivos origen del ataque.
- Identificación de URL'S dentro de paquetes de http.
- Aprendizaje en base a patrones de tráfico desde y hacia los sistemas protegido; auto aprendizaje para determinación de umbrales dinámicos para diferenciación de tráfico legítimo.
- En alcance sobre la protección ante ataques de negación de servicio distribuida.
- Comprobación de direcciones IP legítimas.
- Excesivas conexiones TCP por destino.
- Sobre flujo de conexiones.
- Activación de políticas en base a umbrales de comportamiento.
- Verificación de encabezado incorrecta.
- Combinación inválida de banderas TCP.
- Versión inválida de http.

En capacidad

- Throughput 1.2Gbps.
- Conexiones simultáneas 2,000,000.
- Establecimiento/cierre de sesiones 200,000 / segundo.
- Respuesta de mitigación de un ataque DDOS menor a 2 segundos.
- Puertos LAN necesarios para la conexión.
- Puertos WAN necesarios.
- Fuente de alimentación redundante.

Servicio de Análisis de Vulnerabilidades.

KIO Networks identificará y administrará vulnerabilidades de la infraestructura a los que se encuentra expuesto el INEA por medio de escaneos recurrentes (trimestral), con el fin de establecer medidas adecuadas para mitigarlas o reducirlas a un nivel aceptable.

Se identificarán y administrarán las vulnerabilidades de la infraestructura del INEA por medio de escaneos recurrentes; y se dará seguimiento para la mitigación de dichas desviaciones de seguridad.

El servicio se prestará mediante la administración de una solución tecnológica de escaneo y administración de vulnerabilidades, el cual debe considerar hasta 100 IP's.

KIO Networks operará, administrará, monitoreará y dará mantenimiento a la solución tecnológica de escaneo y administración de vulnerabilidades. Esta solución tecnológica cubrirá los siguientes requerimientos mínimos:

- Será un software o equipo(s) de tipo appliance.
- Será actualizado frecuentemente para incluir vulnerabilidades recientes.
- Permitirá generar reportes con formato flexible ya sean técnicos o directivos.
- Realizará una clasificación de riesgos: altos, medios o bajos.
- Proporcionará recomendaciones de mitigación sobre las vulnerabilidades encontradas, así como su aplicación en el ámbito de competencia de KIO Networks.
- Permitirá generar plantillas de escaneos de acuerdo con los diferentes dispositivos a escanear (ej. windows, linux, cisco, etc) o normas de cumplimiento de seguridad (ej. pci, etc.).

KIO Networks en caso de resultar adjudicado llevará a cabo la detección y administración de las vulnerabilidades de la infraestructura del INEA por medio de una solución de escaneo.

Las actividades que KIO Networks llevará a cabo se mencionan en el apartado de gestión de servicio de tecnologías de la información, el cual será totalmente compatible con el esquema ITIL (Information Technology Infrastructure Library) v3, además la operación en el centro de datos ofertado por KIO Networks está certificado bajo la norma ISO 20000.

- Operará la herramienta en los siguientes rubros:
- Realizará alta, baja y cambios de las direcciones IP a escanear.
- Realizará actualizaciones automáticas y manuales en la herramienta.
- Realizará escaneos de vulnerabilidades a través de la herramienta de acuerdo con el calendario acordado.
- Identificará y reducirá falsos positivos de las vulnerabilidades identificadas.
- Dará recomendaciones y seguimiento a la mitigación de las vulnerabilidades identificadas.

KIO Networks dará atención a fallas de los dispositivos de seguridad de forma remota:

- Soporte primer nivel
- Analizar la posible falla en el dispositivo de seguridad.
- Reestablecer la configuración inicial o un estado anterior para su funcionamiento.
- Soporte segundo nivel
- En caso de que no se pueda resolver dicha falla, se escalará a KIO Networks para dar solución.

Los entregables que se generarán serán de forma trimestral, los cuales incluirán los siguientes puntos:

- Resumen ejecutivo.
- Reporte técnico con base en la herramienta.

Servicio de Protección de Aplicaciones.

Además de los firewalls de seguridad perimetral, KIO Networks considera un WAF (Web Application Firewall por sus siglas en inglés), con el propósito de robustecer la seguridad a nivel aplicación. La conectividad considerada debe ser 10Gb, con la finalidad de robustecer y agilizar el procesamiento de los aplicativos.

El objetivo de este servicio será proteger las aplicaciones de ataques y amenazas en tiempo real; como, por ejemplo: SQL INJECTION, CROSS SITE SCRIPTING (XSS), denegación de servicios (dos), denegación de servicios distribuidos (DDOS) y cross site request forgery (CSRF), etc.

El servicio será prestado mediante una solución tecnológica para protección de aplicaciones web.

KIO Networks será responsable de operar, administrar, monitorear y dar mantenimiento al firewall de aplicaciones que cubra con los siguientes requerimientos mínimos:

- Estará basada en equipo o equipos de tipo appliance.
- Podrá configurarse (por capacidad) al menos 50 (cincuenta) aplicativos en este dispositivo.
- Aprenderá y entenderá la estructura de las aplicaciones, elementos y comportamientos normales de usuarios aplicativos, así como los cambios a través del tiempo que se dé en éstos.
- Permitirá configurar y actualizar los métodos, cookies, parámetros, y URLS de las aplicaciones.

- Contará con una base de políticas predefinidas, granulares y personalizables, así como firmas de protección a nivel aplicativo para protección contra ataques basados a aplicaciones.
- Contará con un módulo de reporteo personalizable. Los reportes permitirán sacar gráficas y podrán generar en una base de tiempo semanal, mensual o de manera diaria.
- Cumplimiento de estándares http para prevenir explotaciones del protocolo y técnicas de evasión.
- Contará con un bypass en caso de un apagado o falla inesperada del o los equipos.
- Aprender automáticamente las aplicaciones y el comportamiento del usuario sobre estas.
- Contará con un módulo para la actualización de las firmas de manera automática.
- Identificar y detener fuentes de ataques conocidos.
- Mitigará ataques a gran escala integrando direcciones IP de atacantes, BOTS, y servicios anónimos.
- Realizará la protección de acuerdo con los estándares de seguridad al menos vs OWASP top 10.
- Soportará alta disponibilidad.
- Salvaguardará la infraestructura de las aplicaciones incluyendo servidores web, políticas de seguridad de xml y web 2.0.
- Permitirá la correlación de políticas para la reducción de falsos positivos permitiendo la validación de ataques correlacionados mediante la capacidad de examinar múltiples atributos, violaciones de los perfiles de las aplicaciones, caracteres especiales, etc.
- Contará con un módulo de tablero (dashboard) que permita conocer el estatus en tiempo real de las aplicaciones y de los eventos generados.
- Permitirá el aprendizaje de la operación de las aplicaciones de manera que en un principio sólo se monitoree la actividad y posteriormente permitir los bloqueos en tiempo real.
- Protección a nivel aplicativo según el top ten del estándar OWASP.
- Implementación de modo monitoreo.
- Implementación de modo en línea para bloqueos en tiempo real.
- Implementación de modo en línea sin bloquear, con el fin de aprender la actividad normal de las aplicaciones, antes de bloquear.

KIO Networks considerará en su propuesta los siguientes requerimientos mínimos:

- Las características de las herramientas para la protección de aplicaciones (WAF) donde realizará la administración, operación, monitoreo y reportes.
- El monitoreo en tiempo real de las aplicaciones, que permita prevenir incidentes que afecten los niveles de servicio.
- El monitoreo será con una disponibilidad de 24x7x365
- El sistema de monitoreo tendrá capacidad de acceso vía web con mecanismos de autenticación segura, para visualizar las métricas, proporcionar una cuenta de acceso para realizar consultas.
- Definirá junto con el INEA las aplicaciones y los parámetros y eventos a ser monitoreados por el WAF.
- Definirá procedimientos de notificación y escalación de acuerdo con la estructura organizacional del INEA.
- Mantenimiento de bitácoras históricas y registro de incidencias (hasta 15 días), desde el inicio del contrato jurídico hasta su conclusión.
- Permitirá el análisis de eventos en tiempo real, histórico y análisis forenses. Así como contar con la capacidad de poder integrarse a la mesa de ayuda propuesta mediante la apertura de tickets vía correo electrónico; en paralelo y de acuerdo con la severidad de la alarma notificar al personal adecuado para su pronta solución.
- Monitoreará los eventos de seguridad detectados por el WAF en el horario establecido.
- Analizará eventos de seguridad para identificar y reducir falsos positivos de las alertas generadas.

- Generará notificaciones por evento de incidencias detectadas (vía correo electrónico o llamada telefónica).
- Dará recomendaciones generales de seguridad informática relacionada con el WAF y los incidentes detectados.
- Configurará el WAF para enviar alertas de los eventos de seguridad.
- Revisará el estado actual del WAF en licencias, actualizaciones, firmas de ataque, hotfix, performance y capacidad de almacenamiento.
- Dará atención a fallas de los dispositivos WAF en sitio o en forma remota:

Soporte primer nivel

- Analizará la posible falla en el dispositivo de seguridad
- Reestablecerá la configuración inicial o un estado anterior para su funcionamiento

Soporte segundo nivel

- En caso de que no se pueda resolver dicha falla, se contactará al proveedor y/o al fabricante para dar solución
- Registrar todos los eventos (tickets) en bitácora ya sea de:
  - Control de cambios
  - Incidentes
  - Reporte mensual de las actividades de servicio administrado de WAF que incluye:
  - Resumen ejecutivo.
  - Detalle técnico con ayuda de la herramienta.

Seguridad Física.

El Centro de Datos contará con medidas de protección física externa que lo mantenga seguro contra robo y actos vandálicos, así mismo contará con estacionamiento para el resguardo de vehículos y permitirá el acceso al personal identificado y autorizado por el INEA.

- Estará ubicado en región geológica de terreno firme zona a (bajo) o b (moderado) de peligro sísmico de acuerdo con la clasificación de regionalización sísmica publicada por el Servicio Sismológico Nacional.
- Contará con un sistema de seguridad física mediante personal de vigilancia especializado con cobertura 7x24, los cuales registrarán mediante bitácora diaria soportada por un sistema automatizado, los accesos que realice personal a las instalaciones administrativas y en especial a quien acceda al centro de datos.
- El centro de datos ofertado por KIO Networks contará con un sistema de circuito cerrado de televisión CCTV o de grabación digital, el cual mantenga monitoreo permanente 7x24 al centro de datos, tanto en el interior como en el exterior y perímetro. La grabación de los videos estará a disposición del INEA, por 30 días naturales contados a partir de la fecha de grabación, plazo en el cual el INEA podrá solicitarlos, si así fuera necesario.
- Contará con acceso restringido al centro de datos mediante sistemas automatizados, marcos detectores de metales y permitiendo acceso únicamente mediante tarjetas de proximidad o equivalente y, adicionalmente, un sistema integral de acceso con control biométrico (lectoras de iris, reconocimiento facial, huella dactilar) o la combinación de ellos, que registre el acceso del personal a la misma, hora de entrada y hora de salida.
- Para tener acceso al área del centro de datos donde resida la infraestructura de cómputo y almacenamiento asignada al INEA, habrá al menos 3 puntos de control de acceso.

- Contará con un procedimiento y sistema implantado para garantizar al INEA, la acreditación y autorización de acceso al centro de datos y a las áreas asignadas al INEA de los servidores públicos que ésta designe las 24 horas del día los 365 días del año.
- Contará con sistemas de alarmas de seguridad y salidas de emergencia con alarmas sonoras.
- El centro de datos propuesto por el INEA contará con un sistema de prevención y detección de incendio altamente zonificado, de modo que ubique y aplique específicamente en el área de riesgo detectada en caso necesario.
- Contará con los elementos necesarios y redundantes para detectar y extinguir incendios, con elementos de detección zonificada que detecten partículas de humo y calor en todo el centro de datos, así mismo con extintores manuales y automáticos.

Detalle del Alcance de Servicio de Seguridad

Alcance del Servicio.

Se contempla la administración y monitoreo 7x24x365 de las siguientes soluciones de seguridad:

1. WAF del fabricante IMPERVA:

- Protección de 6 dominios
- Tráfico constante, no mayor a 100 Mbps
- Soporte de un ataque de denegación de servicio distribuido (DDoS) de hasta 1Gbps.

2. Firewall del fabricante Fortinet:

- Esquema High availability (HA)
- Modelo: Fortigate 1000 C (2)
- Unified (UTM) Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud)

3. Administración de vulnerabilidades:

- 1 escaneo
- 50 direcciones IP

WAF en la Nube.

Servicio de WAF en la nube (Web Application Firewall) del fabricante IMPERVA, para mantener la seguridad de aplicaciones y sitios web en tiempo real con políticas basadas en alertas y bloqueos.

Funciones clave:

- Aprendizaje automático de la estructura de las aplicaciones y del comportamiento de los usuarios.
- Políticas de seguridad respaldadas por investigaciones.
- Protección adaptable contra ataques automatizados a gran escala.
- Parches virtuales mediante la integración con escáneres de vulnerabilidades.

- Protección de las redes y de las plataformas contra ataques.
- Protección del protocolo HTTP y de los servicios web (XML).
- Las políticas de correlación granular reducen los falsos positivos.
- Informes a la medida de la conformidad y de los análisis forenses.
- Monitorización para el análisis profundo de los ataques.

Objetivos del Servicio:

- Monitorear el tráfico web de las aplicaciones web para mitigar ataques.
- Detectar y bloquear peticiones de tipo Cross Site Scripting, SQL Injection, Remote y Local File Inclusion, etc.
- Proteger en tiempo real.
- Descubrir y reducir la exposición de ataques.
- Reducir los costos de las soluciones para esta capa de seguridad.

Firewall – Fortigate 1000C.

Servicio de Firewall para continuar brindando una solución unificada e integrada, sintonizada para ofrecer la máxima seguridad contra amenazas de quinta generación sin comprometer el rendimiento y proporcionando la seguridad de prevención de amenazas avanzadas para redes empresariales.

Con la administración de esta solución se obtiene una visibilidad detallada de los usuarios, grupos, equipos de cómputo y tipos de conexión en su red para que puedan asignar permisos a usuarios y dispositivos correctos

Actividades puntuales:

- Sanity Check de las soluciones que garanticen su correcto funcionamiento.
- Transición segura al SOC de KIO Cyber Security.
- 2 firewalls físicos hosteados en DC MEX2

Firewall	Fortinet	Fortigate 1000C	FW – Inea – Master/FGT1KC3913800294
Firewall	Fortinet	Fortigate 1000C	FW – Inea – Slave/FGT1KC3911800416

Servicios de administración de vulnerabilidades.

Se realizará un acompañamiento para la ejecución del análisis de vulnerabilidades a la infraestructura tecnológica, se apoyara para la revisión y mejora del nivel de la seguridad de la información, que permita conocer las vulnerabilidades técnicas a las que se encuentra expuesta la empresa, y poder así establecer medidas o recomendaciones adecuadas para mitigarlas o reducirlas a un nivel aceptable con base en las mejores prácticas, estándares y metodologías de seguridad de la información orientadas al negocio y a su operación

Alcance

El esquema de ejecución para este servicio tendrá el siguiente alcance:

1. Se llevará a cabo el análisis de vulnerabilidades de manera Trimestral con las capacidades de la herramienta proporcionada
2. El total de IPs son 50 internas, orientado a Infraestructura
3. Periodo 2 meses (1 ciclo de ejecución)

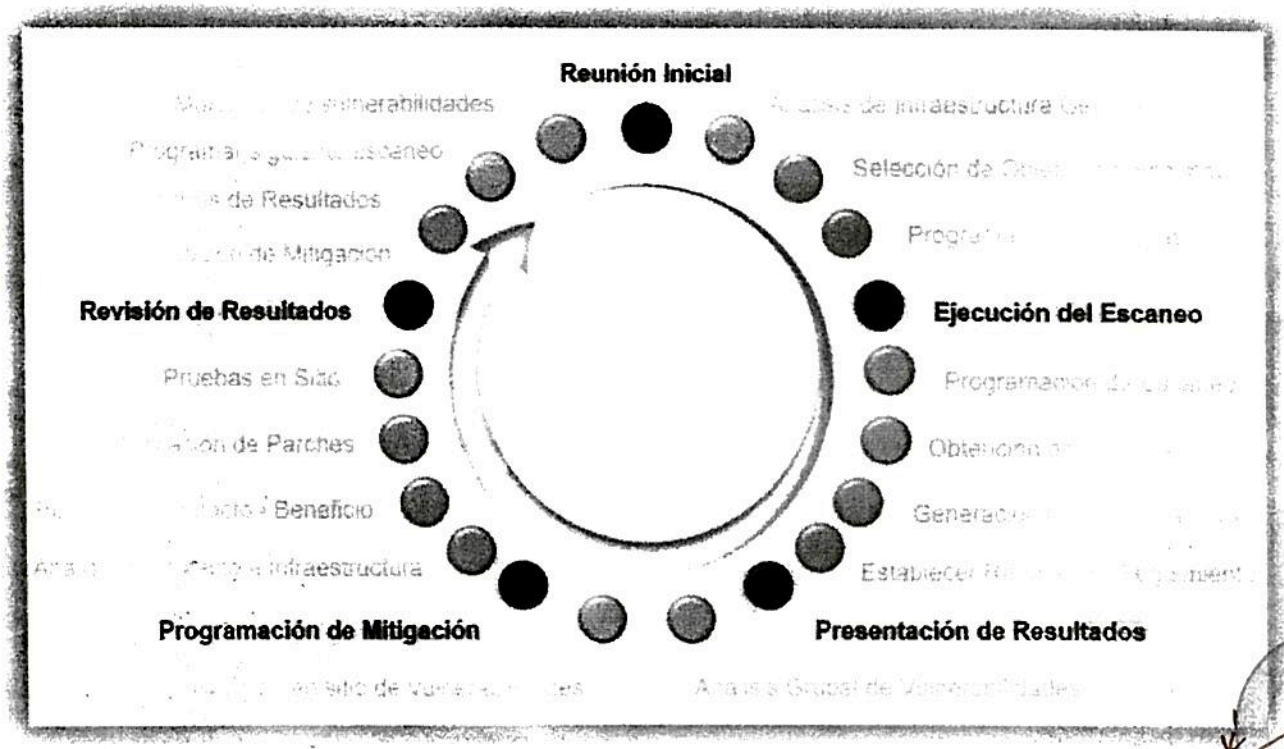
Actividades

A continuación, se detallan las actividades para el acompañamiento en la ejecución:

Análisis.

- Validación de las vulnerabilidades encontradas acorde con el tipo de activo escaneado.
- Detección y depuración de falsos positivos.
- Generación de recomendaciones para la mitigación de vulnerabilidades.
- Plan de seguimiento propuesto.

En el siguiente diagrama se muestran las fases de las que se compone el servicio de Análisis de vulnerabilidades



Metodología.

KIO Networks brindará un método para el análisis de vulnerabilidades que se describe a continuación:

1. Inicialización / Reunión Inicial

SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
Prol. Paseo de la Reforma No. 5287
Col. Cuajimalpa, Ciudad de México, C.P. 05000
SNM010323 EB5

Esta fase incluye actividades de presentación del servicio al cliente y encargados de gestionar las tecnologías a analizar, además de contextualizar los activos a analizar para poder enfocar de manera acertada los resultados de las pruebas para la adecuada generación de los reportes que les serán entregados.

Asimismo, se establece de ser necesario un acuerdo de confidencialidad con respecto a la información que se genera y entrega por ambas partes.

Esta etapa contempla las actividades de integración del equipo para el análisis y validación del alcance.

2. Ejecución de escaneo

KIO Networks procederá a coordinar los escaneos con la periodicidad indicada en el alcance.

Esta etapa contempla las actividades que permitan identificar y validar la arquitectura de red y una vez obtenidos los resultados proceder con la generación de los documentos entregables.

3. Presentación de resultados

Ya que los reportes han sido generados y entregados al personal pertinente, se agendan sesiones de seguimiento con los administradores de sistemas con la periodicidad acordada inicialmente y en las cuales se presentan las vulnerabilidades ya analizadas y agrupadas.

4. Mitigación

Durante la revisión de vulnerabilidades se determina quién será el responsable de realizar las acciones de mitigación en conjunto con la consultoría del personal asignado por el área de Administración de Vulnerabilidades. Adicionalmente, se determinan las fechas límite para realizar las mitigaciones y se realizan las minutas y acuerdos correspondientes. Las recomendaciones se realizan de forma puntual para facilitar la coordinación de la mitigación.

5. Revisión de resultados / Cierre del ejercicio

La fase final del Servicio de Administración de Vulnerabilidades implica dos actividades:

- Primera actividad: consta de la coordinación y ejecución de un re-escaneo para comparar los resultados iniciales con los obtenidos posteriores a las acciones de mitigación.
- Segunda actividad: refiere a la aceptación de las vulnerabilidades que no pueden ser mitigadas con ningún plan de acción.

El esquema de ejecución para este servicio tendrá el siguiente alcance:

- Se llevará a cabo el análisis de vulnerabilidades de manera Trimestral con las capacidades de la herramienta proporcionada
- El total de IPs son 50 internas, orientado a Infraestructura
- Período 2 meses

Matriz de trazabilidad

Consideraciones generales que KIO Networks tomó en cuenta para su propuesta.

La plataforma de procesamiento, comunicación interna y seguridad que actualmente tiene el INEA está virtualizada, por lo que KIO Networks contemplará las configuraciones actuales de los servidores virtuales respetando los sistemas operativos y aplicaciones instaladas.

KIO Networks integrará todo lo requerido para alojar, instalar, migrar, operar, monitorear, soportar y mantener en condiciones óptimas de operación las aplicaciones en los servidores especificados en la tabla del Anexo técnico en la arquitectura que proponga KIO Networks durante la vigencia del contrato, por lo cual contará con el personal técnico con los conocimientos necesarios de acuerdo con la solución de su propuesta.

Las especificaciones y configuraciones que se solicitan en este documento, Anexo técnico, se consideran mínimas.

El INEA con el fin de asegurar que el servicio que está solicitando sea de la más alta calidad solicita que el equipo que KIO Networks provea sea equipo dedicado, vigente y estará en el catálogo del fabricante y con garantía de soporte durante la vigencia del contrato.

Las licencias de software y sus actualizaciones de versiones de sistemas operativos, bases de datos (SQL server), software de virtualización (VMware) así como las necesarias para la operación de los sistemas y aplicaciones podrán ser proporcionadas por KIO Networks sin costo adicional para el Instituto. En el caso del licenciamiento de Microsoft, se utilizará el contrato actual de licenciamiento Select Académico suscrito actualmente con la empresa Microsoft de México por el INEA.

Se permitirá el acceso de personal técnico autorizado del INEA al centro de datos propuesto por KIO Networks, para supervisar los procesos realizados, tanto en la etapa de migración como de operación de los servicios, dentro del área que KIO Networks destine al INEA.

En el caso específico el MAAGTICSI (Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información), KIO Networks conocerá y trabajará de acuerdo con el mismo integrando la documentación que se le solicite por parte del INEA en el momento que se le requiera.

Al término del contrato KIO Networks se obligará, en su caso, a prestar al INEA las facilidades necesarias para la migración del servicio a otro centro de datos, dichas facilidades consistirán en lo siguiente:

- Entregará memoria técnica actualizada de la infraestructura en que operan las aplicaciones, especificando características y capacidades de los equipos, versiones de sistemas operativos, bases de datos y demás software ambiental necesario para el servicio. Incluirá también la información de configuración aplicable, tales como los parámetros de configuración de sistemas operativos. Esta memoria técnica será entregada al INEA a más tardar el 28 de febrero de 2020.

- Migración Tecnológica de fin de contrato: el proveedor actual deberá de otorgar las facilidades para la migración tecnológica del servicio objeto de este contrato para futuros proveedores de servicios, por lo que el proveedor actual de manera conjunta con el proveedor entrante elaborarán la logística de transición así como los mecanismos e infraestructura a utilizar para tal efecto sin costo adicional para el INEA, considerando que el inicio de la migración tecnológica deberá iniciar al menos 30 días naturales antes de la conclusión del contrato actual para quedar totalmente concluida al término de contrato actual. El proveedor entrante será responsable del plan de migración y su ejecución, el proveedor actual colaborará con el proveedor entrante dentro de los alcances de los servicios descritos en el presente documento.

Los servidores del Anexo técnico conservarán la virtualización de acuerdo con la arquitectura propuesta por KIO Networks o podrá variar conforme a las necesidades del INEA dentro del total de las capacidades propuestas.

Debido a la criticidad del servicio se requiere que el centro de datos propuesto cumpla con al menos la disponibilidad, de cada uno de sus elementos, solicitada en el Anexo técnico.

El centro de datos propuesto se ubica dentro de la República Mexicana. En caso de encontrarse fuera de la Zona Metropolitana de la Cd. De México, KIO Networks considerará en su propuesta, los costos por concepto de viáticos y traslados del personal del INEA al menos 2 veces por mes para dos personas (Hospedaje, Alimentos y Traslados).

Niveles de servicio.

Los niveles de servicio se consideran por cada uno de los servidores virtuales donde se hospedan las aplicaciones críticas del Instituto, los cuales se pueden observar de manera detallada en la tabla del Anexo técnico.

Penalizaciones en la operación de los servicios

Con fundamento en lo dispuesto por el artículo 53 de la Ley en la materia y el 95 y 96 de su reglamento, el Instituto aplicará penas convencionales al proveedor del servicio, de la siguiente manera:

Se precisa que el instituto requiere la totalidad de los conceptos del servicio que indica en la partida 1.

- Pena convencional:

En el caso de incumplimiento en el tiempo de la prestación del servicio, el personal del INEA procederá a calcular la pena convencional conforme al 1% del monto total del contrato, de la factura, por cada día de retraso en la prestación del servicio, la que no excederá del monto de la garantía de cumplimiento. Dicha pena tendrá como límite la aplicación un equivalente al 5% considerando que el porcentaje de la fianza es del 10% del monto total del contrato y/o pedido antes de IVA, no podrá exceder del monto de la garantía de cumplimiento del contrato y/o pedido, una vez transcurridos una vez alcanzado el 5% el INEA podrán iniciar el procedimiento de rescisión del instrumento jurídico respectivo y se hará efectiva la garantía de cumplimiento del mismo, el pago de las penalizaciones deberá hacerse a favor del INEA mediante cheque certificado, de caja o dinero en efectivo en el departamento de tesorería.

Asimismo, notificará a la Dirección de Administración y Finanzas, para que le notifique al prestador de servicios dicha pena, para que este realice el pago de la penalización mediante efectivo, cheque de caja o cheque certificado a favor del INEA.

- Penalización por deductivas:

En el caso de cumplimiento deficiente en la prestación del servicio, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del entregable, la que no excederá del monto de la garantía de cumplimiento. Adicionalmente, notificará al prestador de servicios mediante oficio para que, en un término no mayor a 5 días hábiles posteriores a la notificación, se realice la reposición del servicio; en caso de que el prestador de servicios no realice dicha reposición, la Subdirección Técnica procederá a calcular, de forma adicional, la deductiva conforme al 1% del monto total de la factura del entregable, la que no excederá del monto de la garantía de cumplimiento.

En caso de que el proveedor de servicio dentro de los primeros 5 días naturales del mes siguiente no entregue el Reporte mensual de operaciones, el cual incluye: el Reporte de atención de tickets y CRQ´s, el Reporte de monitoreo de servidores, el Reporte de uso de enlaces de Internet y el Reporte WAF, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del mes correspondiente por cada día natural de atraso en la entrega del reporte mensual, la que no excederá del monto de la garantía de cumplimiento. En caso de alguna instrucción de carácter de cierre presupuestal lo anterior puede ser modificado conforme a la naturaleza de la solicitud.

Una vez entregado el Reporte mensual de operaciones, el cual incluye: el Reporte de atención de tickets y CRQ´s, el Reporte de monitoreo de servidores, el Reporte de uso de enlaces de Internet y el Reporte WAF, la Subdirección Técnica procederá a su revisión en un máximo de 2 días naturales, y en el supuesto que tenga comentarios u observaciones sobre el mismo, notificará al proveedor por correo electrónico para que realice las correcciones, por lo que el proveedor contará con 3 días naturales para realizar las correcciones, en caso de que el proveedor exceda los 3 días naturales, la Subdirección Técnica procederá a calcular la deductiva conforme al 1% del monto total de la factura del mes correspondiente por cada día natural de atraso en la entrega del reporte mensual corregido, la que no excederá del monto de la garantía de cumplimiento.

Asimismo, se notificará a la Dirección de Administración y Finanzas, para que le notifique al prestador de servicios dicha deductiva y éste realice el pago de la deductiva mediante efectivo, cheque de caja o certificado a favor del INEA.

Términos y condiciones de entrega y de aceptación.

Plazos, condiciones de entrega y forma de pago:

Se realizará el pago a mensualidades vencidas contra entrega del Reporte Mensual de operación documento que respalda los servicios aplicables durante la vigencia, que será validado y a entera satisfacción del anexo técnico para que el personal de la Subdirección Técnica sea quien realice la liberación de pago correspondiente según el cronograma de actividades.

KIO Networks en caso de resultar adjudicado presentará los primeros días de cada mes el Reporte Mensual de Operación (entregable) del servicio prestado en el período inmediato anterior, el cual será revisado y validado por el personal de la Subdirección Técnica, el cual estará integrado por:

- Reporte de tickets y CRQ´s en el período
- Reporte de monitoreo de las máquinas virtuales
- Uso de Enlaces de Internet
- Reporte del WAF

Tiempos de respuesta de soporte y de servicio.

Soporte 24 horas al día, los 7 días de la semana, todo el año, con un número 01 800. El servicio de KIO Networks tendrá las siguientes características distintivas:

- A través del sitio web de KIO Networks en caso de resultar adjudicado del servicio se podrá solicitar en línea cualquier servicio de ayuda y apoyo técnico, opciones adicionales y modificaciones a sus servicios, así como verificar el estatus de sus órdenes.
- Contar con un centro de monitoreo NOC (Network Operation Center) que monitorea el estado de la red 7x24 los 365 días del año.
- Compromiso de atención de forma directa e inmediata del técnico especializado asignado para la solicitud de servicios y asesoría técnica.

- Asegurar un tiempo de respuesta a falla de máximo 30 minutos.

Cláusula de Confidencialidad

KIO Networks en caso de resultar adjudicado se obliga a que toda la información suministrada por el INEA o a la que tenga acceso, sea o no confidencial o reservada, es propiedad del INEA; por consiguiente, está expresamente prohibido transmitir, divulgar o comercializar total o parcialmente dicha información, y esta será manejada con carácter estrictamente confidencial o reservada.

KIO Networks guardará absoluta confidencialidad respecto del contenido de la documentación y/o información a la que tenga acceso, en el supuesto de que se incumpla con esta obligación, se deberá pagar al INEA los daños y perjuicios que se le ocasione.

KIO Networks adoptará las precauciones necesarias para proteger la información confidencial o reservada del INEA. Por tal motivo, KIO Networks asume expresamente cualquier responsabilidad que se derive del incumplimiento por parte de sus respectivos empleados a las obligaciones de confidencialidad descritas en el presente documento. Cuando la información confidencial o reservada ya no sea necesaria, se devolverá al INEA o se destruirá si esta así lo solicita.

El licitante notificará inmediatamente al INEA en caso de descubrir un uso, revelación o divulgación no autorizados de información confidencial o reservada, y cooperará con el INEA para ayudarla a retomar posesión e impedir usos no autorizados adicionales de su información confidencial o reservada.

Supervisión del servicio contratado.

Administración, supervisión y vigilancia.

El administrador del instrumento jurídico será el Titular de la Subdirección Técnica y el Supervisor será el Titular del Departamento de Soporte Técnico y Servicios.

Funciones del administrador: responsable de interactuar con el supervisor para dar seguimiento y verificar que el servicio cuente con las especificaciones y actividades solicitadas.

Funciones del supervisor: responsable de interactuar con el administrador y el proveedor, para dar seguimiento y verificar que el servicio cumpla con las especificaciones, actividades y entregas puntuales del servicio.

El INEA a través del administrador y supervisor del contrato realizarán la comprobación y verificación en cualquier tiempo y lugar del desarrollo de los servicios y el cumplimiento en tiempo y forma de la presentación de los entregables por parte de KIO Networks en caso de resultar adjudicados, otros elementos que se deberán de tomar en consideración:

- Monitoreo cotidiano del servicio.
- Seguimiento a tickets:
  - Levantados.
  - Resueltos.
  - En proceso.
- Revisión del entregable mensual.

TABLA DE SUPERVISIÓN

Elemento a supervisar	Descripción	Documento de supervisión	Comentarios
Servidores	Que los servidores estén disponibles y operables con respecto a procesamiento, memoria y almacenamiento	Gráficas mensuales de uso de procesador, memoria y disco	En caso de incumplimiento o cumplimiento parcial por parte del proveedor de servicio se aplicará la pena convencional o deductiva correspondiente
Proteccion de aplicaciones Web	Que los sitios web estén protegidos de posibles ataques de seguridad.	Reporte mensual de intentos de ataque de los siguientes sitios web: www.inea.gob.mx www.conevyt.org.mx www.cursosinea.conevyt.org.mx	
Registro y seguimiento de incidentes	Que la mesa de servicio proporcione el seguimiento de los incidentes presentados	Reporte mensual de incidentes y cambios solicitados.	
Enlaces de internet	Que se tenga disponible el ancho de banda solicitado	Gráfica mensual de uso de enlaces	

Entregables.

KIO Networks en caso de resultar adjudicado está obligado a presentar los siguientes entregables durante la prestación del servicio.

Reporte	Fecha	Observaciones
Reportes sobre el inicio y fin de la migración de aplicaciones	Primera semana de iniciada la migración y hasta concluir la actividad satisfactoriamente	
Reporte mensual de operaciones: Reporte de atención de tickets y CRQ´s Reporte de monitoreo de servidores Reporte de uso de enlaces de Internet	Los primeros 5 días del mes siguiente	
Reporte mensual	Los primeros 5 días del mes	Reporte WAF

Otros resultados, aportaciones y compromisos.

KIO Networks en caso de resultar adjudicado acudirá a las reuniones que se le soliciten vía correo electrónico, por parte del personal adscrito a la Subdirección Técnica del INEA, ubicada en la Calle Francisco Márquez # 160, Colonia Condesa, C.P.06140, Cuauhtémoc, Ciudad de México; con la finalidad de validar los avances del proyecto.

Anexo
TABLA DE SERVIDORES

KIO Networks considera como parte de su propuesta el hardware que contará con las capacidades de procesamiento, memoria RAM y almacenamiento suficientes para hospedar los siguientes servidores.

	Name	Plataforma	Tipo de servicio	Procesadores	HD (GB)	RAM (GB)	Motor de BD	Nivel de criticidad	Minutos máximos de indisponibilidad en el mes	Observaciones
1	App_Mevyt	Red Hat Enterprise Linux 6.4 Santiago(64-bit)	Web Server	8	150	32		2	60 minutos	
2	app-mevyt	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	4	100	16		2	60 minutos	
3	APPRKIOCFE01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	90	2		2	60 minutos	
4	BITVRKIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	8	558	32	SQL Server 2005	1	30 minutos	
5	CURSOS_INEA	Red Hat Enterprise Linux 6.6 Santiago (64-bit)	Web Server	4	170	16		2	60 minutos	
6	DBPRKIOINAP01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	130	1		2	60 minutos	
7	DBPRKIOMX03	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1487	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
8	DBPRKIOMX04	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1340	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
9	DBPRKIOMX05	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	620	160	SQL Server 2016	1	30 minutos	
10	DBPRKIOMX06	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	478	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
11	dbprkiosasa	Microsoft Windows Server 2012 (64-bit)	Base de datos	8	230	8	SQL Server 2016	1	30 minutos	
12	FLEXNET	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	240	4	SQL Server 2000	2	60 minutos	
13	FTPUXKIOMX01	Ubuntu Linux 8.04 Hardy (64-bit)	Web Server	4	135.97	4		2	60 minutos	
14	HDVRKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	8	245	16	SQL Server 2008 R2	1	30 minutos	
15	ineavcliente	Microsoft Windows 8 (64-bit)	Web Server	4	54	4		2	60 minutos	
16	INEA-W16	Microsoft Windows Server 2003 Standard (32-bit)	Web Server	4	78	4		1	30 minutos	
17	ineawad01	Microsoft Windows Server 2008 R2 (64-bit)	Administración	4	100	4		1	30 minutos	
18	ineawad02	Microsoft Windows Server 2003	Administración	8	100	8		1	30 minutos	
19	ineawbd01	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	50	4	SQL Server 2014	2	60 minutos	
20	ineawbd02	Microsoft Windows Server 2012 (64-bit)	Base de datos	32	642	128	SQL Server 2008 R2, SQL Server 2012, SQL Server 2014	1	30 minutos	
21	ineawbd03	Microsoft Windows Server 2012 (64-bit)	Base de datos	4	442	4	SQL Server 2008 R2, SQL Server 2012, SQL Server 2014	2	60 minutos	
22	ineawws01	Microsoft Windows Server 2012 (64-bit)	Web Server	4	150	32		2	60 minutos	
23	ineawws02	Microsoft Windows Server 2003 Enterprise x64 SP2	Web Server	2	50	4		2	60 minutos	
24	ineawws03	Microsoft Windows Server 2012 (64-bit)	Web Server	32	1155	32		1	30 minutos	
25	ineawws04	Microsoft Windows Server 2012 (64-bit)	Web Server	4	405	4		2	60 minutos	
26	ineawws05	Microsoft Windows Server 2012 R2(64-bit)	Web Server	16	150	4		1	30 minutos	
27	MEVYTMX	Red Hat Enterprise Linux 5.4 Tikanga (32-bit)	Web Server	2	118	4		2	60 minutos	
28	mevyt-ol	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	4	100	8		2	60 minutos	
29	mevytusa	Red Hat Enterprise Linux 5 Tikanga (64-bit)	Web Server	16	207	32		2	60 minutos	
30	MICROINEA	Red Hat Enterprise Linux 6.1 - Santiago (64-bit)	Web Server	1	136	1		2	60 minutos	
31	MINDVRKIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	8	180	32	SQL Server 2005	2	60 minutos	
32	msuxinea01	Linux Red Hat 7.0	Web Server	4	130	8		2	60 minutos	
33	MSUXKIOMXPCONE	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	8	180	32		2	60 minutos	
34	MSUXKIOMXPINEA	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	8	119	32		2	60 minutos	
35	POWERBI	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	100	4	SQL Server 2008 R2, SQL Server 2014	2	60 minutos	
36	RDBSAELKIOMX	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	64	130	128	SQL Server 2008 R2	1	30 minutos	
37	rppdkiomx02	Microsoft Windows Server 2003 (32-bit)	Base de datos	4	250	32	SQL Server 2000	1	30 minutos	Se requiere licencia para Crystal Reports XI Release 1, BussinesObjects Enterprise Release 2
38	rppdkiomx03	Microsoft Windows Server 2003 (32-bit)	Base de datos	4	230	32	SQL Server 2000	1	30 minutos	Se requiere licencia para Crystal Reports XI Release 1, BussinesObjects Enterprise Release 2
39	SIVEFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	4	200	24		2	60 minutos	SAP Crystal Reports, BusinessObjects
40	SIVESQL	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	4	300	16	SQL Server 2008 R2	2	60 minutos	
41	SPLAZAS	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	8	456	16	SQL Server 2008 R2	2	60 minutos	
42	VCSRV-INEA01	Microsoft Windows Server 2012 (64-bit)	Administración	8	228	8		2	60 minutos	
43	vsaINEA-BAAS	Other (32-bit)	Administración	2	158	2		2	60 minutos	
44	WSPDKIOMX02	Microsoft Windows Server 2003 (32-bit)	Web Server	16	200	32		1	30 minutos	
45	wspdkiomx03	Microsoft Windows Server 2003 (32-bit)	Web Server	32	290	32		1	30 minutos	
46	WSPDKIOMX04	Microsoft Windows Server 2003 (32-bit)	Web Server	2	100	32		1	30 minutos	
47	WSPDKIOMX06	Microsoft Windows Server 2003 (32-bit)	Web Server	16	200	32		1	30 minutos	
48	WSPDKIOMX07	Microsoft Windows Server 2003 (32-bit)	Web Server	16	220	32		1	30 minutos	
49	WSPDKIOMX09	Microsoft Windows Server 2003 (32-bit)	Web Server	16	215	32		1	30 minutos	
50	WSSAELKIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	32	200	64		1	30 minutos	

ANEXO
NIVELES DE SERVICIO

No	Nombre	Plataforma	Tipo de servicio	Nivel de criticidad	Minutos máximos de indisponibilidad en el mes
1	App_Mevot	Red Hat Enterprise Linux 6.4 Santiago(64-bit)	Web Server	2	60 minutos
2	app-mevot	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	2	60 minutos
3	APPRIOCEF01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	60 minutos
4	BITVRIOMX01	Microsoft Windows Server 2008 (32-bit)	Base de datos	1	30 minutos
5	CURSOS_INEA	Red Hat Enterprise Linux 6.6 Santiago (64-bit)	Web Server	2	60 minutos
6	DBPRIOINAP01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
7	DBPRIOMX03	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
8	DBPRIOMX04	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
9	DBPRIOMX05	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
10	DBPRIOMX06	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
11	dbprldosasa	Microsoft Windows Server 2012 (64-bit)	Base de datos	1	30 minutos
12	FLEXNET	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	60 minutos
13	FTPUXIOMX01	Ubuntu Linux 8.04 Hardy (64-bit)	Web Server	2	60 minutos
14	HDVRIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
15	ineavcliente	Microsoft Windows 8 (64-bit)	Web Server	2	60 minutos
16	INEA-W16	Microsoft Windows Server 2008 Standard (32-bit)	Web Server	1	30 minutos
17	ineawad01	Microsoft Windows Server 2008 R2 (64-bit)	Administración	1	30 minutos
18	ineawad02	Microsoft Windows Server 2008	Administración	1	30 minutos
19	ineawbd01	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
20	ineawbd02	Microsoft Windows Server 2012 (64-bit)	Base de datos	1	30 minutos
21	ineawbd03	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
22	ineawws01	Microsoft Windows Server 2012 (64-bit)	Web Server	2	60 minutos
23	ineawws02	Microsoft Windows Server 2003 Enterprise x64 SP2	Web Server	2	60 minutos
24	ineawws03	Microsoft Windows Server 2012 (64-bit)	Web Server	1	30 minutos
25	ineawws04	Microsoft Windows Server 2012 (64-bit)	Web Server	2	60 minutos
26	ineawws05	Microsoft Windows Server 2012 R2(64-bit)	Web Server	1	30 minutos
27	MEVOTMX	Red Hat Enterprise Linux 5.4 Tikanga (32-bit)	Web Server	2	60 minutos
28	mevot-ol	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	2	60 minutos
29	mevotusa	Red Hat Enterprise Linux 5 Tikanga (64-bit)	Web Server	2	60 minutos
30	MICRONEA	Red Hat Enterprise Linux 6.1 - Santiago (64-bit)	Web Server	2	60 minutos
31	MINDVRIOMX01	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	60 minutos
32	msusinea01	Linux Red Hat 7.0	Web Server	2	60 minutos
33	MSUSRIOMXPCONE	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	2	60 minutos
34	MSUSRIOMXPINEA	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	2	60 minutos
35	POWERBI	Microsoft Windows Server 2012 (64-bit)	Base de datos	2	60 minutos
36	RDBSAEUXIOMX	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	30 minutos
37	rpodldomx02	Microsoft Windows Server 2003 (32-bit)	Base de datos	1	30 minutos
38	rpodldomx03	Microsoft Windows Server 2003 (32-bit)	Base de datos	1	30 minutos
39	SIVEFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	60 minutos
40	SIVESQL	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
41	SPLAZAS	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	2	60 minutos
42	VCSRV-INEA01	Microsoft Windows Server 2012 (64-bit)	Administración	2	60 minutos
43	vsaINEA-BAAS	Other (32-bit)	Administración	2	60 minutos
44	WSPDIOMX02	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
45	wspdiomx03	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
46	WSPDIOMX04	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
47	WSPDIOMX06	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
48	WSPDIOMX07	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
49	WSPDIOMX09	Microsoft Windows Server 2003 (32-bit)	Web Server	1	30 minutos
50	WSSAEUXIOMX01	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	1	30 minutos

Juan Carlos Martínez Valdés
Representante Legal

SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.
Prol. Paseo de la Reforma No. 5287
Col. Cuajimalpa, Ciudad de México, C.P. 05000
SNM010323 EB5