



CONVENIO POR EL QUE SE MODIFICA EL PEDIDO DE PRESTACIÓN DE SERVICIOS NO. DAS-TEC-011/19, QUE CON FUNDAMENTO EN LA LEY DE ADQUISICIONES, ARRENDAMIENTO Y SERVICIOS DEL SECTOR PÚBLICO Y SU REGLAMENTO, 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 APODERADO LEGAL, ASISTIDO EN ESTE ACTO POR OSCAR ULISES CONTRERAS LUNA, SUBDIRECTOR TÉCNICO, ADMINISTRADOR DEL PEDIDO Y DEL PRESENTE CONVENIO MODIFICATORIO, ASÍ TAMBIEN COMO POR ROBERTO RAMÍREZ GUZMÁN, JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO Y SERVICIOS, SUPERVISOR DEL PEDIDO Y DEL PRESENTE CONVENIO MODIFICATORIO; POR LA OTRA PARTE "SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V.", REPRESENTADA EN ESTE ACTO 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**

1. Con fecha de 04 de noviembre de 2019, "LAS PARTES" suscribieron el pedido de prestación de servicios no. **DAS-TEC-011/19**, cuyo objeto se cita textualmente: **"EL PROVEEDOR"** se obliga con **"EL INEA"** a prestar la **"Contratación del servicio de infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y extranet (hosting centro de datos externo) para los meses de noviembre y diciembre 2019"**.

2. En la cláusula Segunda referente al Monto, en su primer párrafo, se estableció lo siguiente:

**"Segunda. - Monto.**

**"LAS PARTES"** acuerdan que el monto por la prestación del servicio objeto del presente pedido, es por la cantidad de **\$1,910,350.52 (Un millón novecientos diez mil trescientos cincuenta pesos 52/100 M.N.)**, que incluye el Impuesto al Valor Agregado, que se cubrirá contra la prestación del servicio, como se detalla en el Anexo Único"

3. En la cláusula Octava de **"EL PEDIDO"**, se estableció lo que a la letra dice:

**"Octava. - Vigencia.**

La vigencia del servicio objeto de éste pedido será del 01 de noviembre y hasta el 31 de diciembre del 2019. La vigencia del pedido será a partir de este instrumento jurídico y hasta el 31 de diciembre de 2019."

4. Mediante oficio ST/409/2019 de fecha 12 de diciembre de 2019, el Subdirector Técnico del área requirente, solicita realizar los trámites respectivos para llevar a cabo el convenio modificatorio a **"EL PEDIDO"**, dicha modificación corresponde a la ampliación en monto y vigencia, lo anterior con fundamento en los artículos 25 y 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículos 91 y 92 de su Reglamento, artículo 35 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y 146 de su Reglamento, así como en la cláusula Vigésima séptima del citado instrumento jurídico.

5. Para la formalización del presente convenio modificatorio se cuenta con la justificación de fecha 12 de diciembre de 2019, signada por el Subdirector Técnico del área requirente para la modificación del pedido, lo anterior con el objeto de mantener la continuidad y calidad de la **Contratación del servicio de infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y extranet (hosting centro de datos externo) para los meses de noviembre y diciembre 2019**.

6. Mediante oficio UAF/1220/2019, de fecha 11 de diciembre de 2019, el Titular de la Unidad de Administración y Finanzas de **"EL INEA"**, solicitó a **"EL PROVEEDOR"** informara a este Instituto mediante





escrito, si aceptaba realizar el convenio modificatorio en monto, así como la ampliación en vigencia, bajo las mismas condiciones técnicas y económicas establecidas en **"EL PEDIDO"**, sin rebasar el 20% del instrumento jurídico primigenio.

- 7. En contestación al oficio UAF/1220/2019 del numeral 6 que antecede, **"EL PROVEEDOR"**, mediante escrito de fecha 12 de diciembre de 2019, acepto la petición de **"EL INEA"** manifestando su conformidad para dar continuidad a los servicios relacionados con **"EL PEDIDO"** a fin de ampliar su vigencia del 01 al 12 de enero de 2020, no obstante **"EL PROVEEDOR"** hizo mención que prestará el servicio hasta el día 16 de enero de 2020, y del monto por la cantidad de **\$375,806.64 (trescientos setenta y cinco mil ochocientos seis pesos 64/100 M.N.)**, cantidad que incluye el Impuesto al Valor Agregado, bajo las mismas condiciones técnicas y económicas.
- 8. Mediante oficio UAF/SRF/489/2019 de fecha 23 de diciembre de 2019, la Subdirección de Recursos Financieros en respuesta al oficio UAF/SRMS/1631/2019, informa que, para cubrir las erogaciones derivadas del presente convenio modificatorio en la partida 31602 (Servicios de Telecomunicaciones) no existe inconveniente presupuestario, siempre y cuando se sujeten en todo momento las restricciones presupuestarias establecidas por la Coordinadora de Sector, que no generen presiones de gasto futuras y no afecten en el cumplimiento de los objetivos de **"EL INEA"**, sin que la no realización de la referida condición suspensiva origine responsabilidad alguna para **"LAS PARTES"**. Así también, se cuenta con oficio de autorización presupuestaria número UAYF/1177/2019 emitida por el Titular de la Unidad de Administración y Finanzas; así también, con la Requisición de Bienes y Servicios número ST-002/2020.

**DECLARACIONES**

**Declaran "LAS PARTES" que:**

**Primera.-** Las modificaciones a **"EL PEDIDO"** se ajustan a lo establecido por los artículos 25 y 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, artículos 91 y 92 de su Reglamento, artículo 35 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y 146 de su Reglamento, así como en la cláusula Vigésima séptima del citado instrumento jurídico.

**Segunda.- "LAS PARTES"** se reconocen la personalidad jurídica con la que actúan.

De conformidad con los antecedentes y declaraciones, **"LAS PARTES"** otorgan las siguientes:

**CLÁUSULAS**

**Primera.-** Es objeto del presente instrumento jurídico es la ampliación de vigencia y del monto de **"EL PEDIDO"** hasta máximo el 20% de su monto total en la partida 31602 (Servicios de Telecomunicaciones), al ser un servicio básico e indispensable en términos de lo justificado por el área requirente en el antecedente marcado con el número 5.

**Segunda.-** Se modifica la cláusula *Segunda* en su primer párrafo de **"EL PEDIDO"** para quedar de la siguiente manera:

**"Segunda. - Monto.**

**"LAS PARTES" acuerdan que el monto por la prestación del servicio objeto del presente pedido, es por la cantidad de \$2,286,157.16 (dos millones doscientos ochenta y seis mil ciento cincuenta y siete pesos 16/100 M.N.), que incluye el Impuesto al Valor Agregado, que se cubrirá contra la prestación del servicio, como se detalla en el Anexo único"**

**Tercera.-** Se modifica la cláusula *Octava* de **"EL PEDIDO"** para quedar de la siguiente manera:

**"Octava. - Vigencia.**

**La vigencia del servicio objeto de éste pedido será del 01 de noviembre del 2019 y hasta el 16 de enero de 2020.**





*La vigencia del pedido será a partir de este instrumento jurídico y hasta el 16 de enero de 2020*

**Cuarta.-** La vigencia del presente convenio será del 01 al 16 de enero de 2020.

**Quinta.- "EL PROVEEDOR"** se compromete a entregar a "EL INEA" la modificación de la garantía respectiva, de conformidad con lo establecido en la cláusula Décima séptima de "EL PEDIDO", dentro de los diez días naturales siguientes a la firma del presente instrumento jurídico. Lo anterior en cumplimiento de los artículos 91 y 103 fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

**Sexta.-** A excepción de lo precisado en las cláusulas que anteceden, "LAS PARTES" ratifican en todos y cada uno de sus términos y clausulado de "EL PEDIDO", y de "EL CONVENIO".

Previa lectura y con pleno conocimiento de su contenido y valor legal, "LAS PARTES" suscriben el presente convenio modificatorio firmando por duplicado para constancia y validez, al calce y al margen, constante de tres fojas, en la Ciudad de México, a los 06 de enero de 2020, conservando un ejemplar "EL INEA" y uno "EL PROVEEDOR".

Por "EL INEA"

  
Antonio Quintal Berny  
Apoderado Legal

Por "EL PROVEEDOR"

  
Juan Carlos Martínez Valdés  
Apoderado Legal  
"SIXSIGMA NETWORKS MÉXICO, S.A. DE C.V."

Asistencia

  
Oscar Ulises Contreras Luna  
Subdirector Técnico  
Administrador del Convenio Modificatorio

  
Roberto Ramírez Guzmán  
Jefe de Departamento de Soporte Técnico y Servicios  
Supervisor del Convenio Modificatorio



Las firmas que aparecen en esta hoja, forman parte del Convenio Modificatorio de fecha 06 enero de 2020, por el que se modifica el Pedido de Prestación de Servicios no. DAS-TEC-011/19, celebrado entre el Instituto Nacional para la Educación de los Adultos y "Sixsigma Networks México, S.A. de C.V."



## ANEXO TÉCNICO

**NOMBRE DEL PROYECTO:** Ampliación en vigencia y monto del pedido No. DAS-TEC-011/19 cuyo objeto es la "Contratación del servicio de infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y extranet (hosting centro de datos externo) para los meses de noviembre y diciembre 2019".

### 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 convenio de servicios que provea la infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de internet y extranet de la entidad.

El convenio 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 convenio 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 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 proveedor 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 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) para los meses de noviembre y diciembre de 2019	1	Servicio

### Lugar de prestación de los servicios

El servicio se brindará desde el Centro de Datos externo propuesto por el proveedor 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 Técnica 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.



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

### CARACTERÍSTICAS TÉCNICAS

#### Infraestructura

El centro de datos propuesto por el proveedor, 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 proveedor deberá incluir los documentos que comprueben la certificación ICREA Nivel 4 o TIER III del Uptime Institute. Las instalaciones del proveedor 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 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.
- La superficie o áreas donde se encuentren en operación los equipos de procesamiento y almacenamiento que contengan las aplicaciones e información del CLIENTE, 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 proveedor o el CLIENTE, 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.
- 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 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.
- 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.



Ver 16/01/2019

Indesa, C.P. 06140, Cuauhtémoc, Ciudad de México  
52 54 28 00 www.gob.mx/indesa



- El proveedor incluirá el monitoreo de estos parámetros dentro del sistema de monitoreo integral del centro de datos.
- El proveedor 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.
- Deberá considerar posiciones de trabajo, al menos 4 posiciones de manera eventual, de así requerirlo el CLIENTE, para que servidores públicos puedan acceder a administrar los aplicativos en sitio. Estarán equipadas con mesa, silla, teléfono y acceso a internet, provistos por el proveedor (podrán estar en el centro de datos del proveedor 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 CLIENTE, restringido al acceso lógico asignado.

### **Procesamiento y Virtualización**

El procesamiento propuesto por el proveedor 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 proveedor 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 proveedor 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 convenio, 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 proveedor 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 CLIENTE.

El equipo deberá contar con garantía durante la vigencia del convenio 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.

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.

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 CLIENTE.

### **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 proveedor 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 proveedor considera una red independiente para el monitoreo de los servidores.

Comunicaciones:

Equipamiento de conectividad para la red LAN

El proveedor 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.





**SEP**  
SECRETARÍA  
DE EDUCACIÓN  
PÚBLICA



**INSTITUTO  
NACIONAL PARA  
LA EDUCACIÓN  
DE LOS ADULTOS**

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

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

El proveedor 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 CLIENTE 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 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 proveedor para este servicio deberá ser de 99.80%.

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



La solución propuesta proveerá un ancho de banda garantizado para el CLIENTE 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 proveedor, mismos que se deberán encontrar en diferentes zonas geográficas, por lo cual El proveedor deberá presentar carta bajo protesta de decir verdad que confirme el cumplimiento de este punto.

En todo momento que se requiera el CLIENTE 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 proveedor 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 proveedor 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 proveedor 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 proveedor ofrecerá el servicio de conexión a Internet simétrico con redundancia.

El proveedor 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

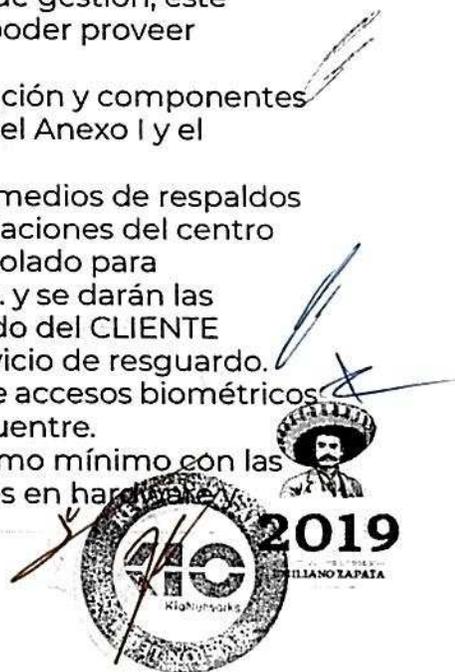
- El proveedor proporcionará al CLIENTE un rango de direcciones IP homologadas para los servidores descritos en el Anexo I, equipos de comunicaciones y seguridad.
- Las direcciones homologadas así como las direcciones IP internas deberán de mantenerse con la misma numeración en cualquier proceso de migración.

#### Servicio DNS

- El proveedor 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 proveedor será responsable de la configuración, administración y dispositivos necesarios para la conexión de los servidores de aplicaciones del instituto al sistema de almacenamiento.
- El proveedor 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 proveedor 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 CLIENTE 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.

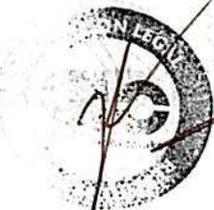
Se deben incluir las siguientes funcionalidades:

*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 proveedor 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 máquinas 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 proveedor 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 proveedor ganador.
- El proveedor será responsable por la correcta instalación y configuración de nuevas aplicaciones que adquiera el instituto durante la vigencia del convenio.
- 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, 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 convenio 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 proveedor y en la red de internet.
- El proveedor 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 proveedor 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 proveedor tendrá capacidad para dirigir el proyecto apegándose a estándares de ITIL, por lo que el proveedor deberá incluir en su propuesta copia de certificado de "ITIL V3 Expert" y Curriculum del contacto encargado.
- Así mismo, el personal de operación del proveedor 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 CLIENTE requiere de un personal especializado en virtualización de la plataforma VMware, para asesoría e implementación de al menos 40 horas, que podrán utilizarse durante la vigencia del convenio.

#### 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 proveedor 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 proveedor estará en la disposición de interactuar con el personal de la Subdirección Técnica del Instituto.
- El proveedor informará inmediatamente sobre problemas detectados en el funcionamiento de servidores y el servicio al personal designado por el CLIENTE 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 proveedor 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 proveedor proporcionará una cuenta de usuario de solo lectura para todos los equipos de comunicaciones y seguridad.
- Como parte de los entregables mensuales, el proveedor entregará el monitoreo de la infraestructura y el estatus de todos los incidentes reportados.
- El proveedor 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 proveedor 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 proveedor 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 proveedor hacia CLIENTE para dar avances en la tarea.
  - Entrega de reporte del proveedor 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

El proveedor ofrecerá 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 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 proveedor 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 (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 proveedor 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 proveedor 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

#### Servicio de Administración de Respaldos

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

- El CLIENTE 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 proveedor notificará al CLIENTE el tiempo esperado para realizar las restauraciones solicitadas y notificará oportunamente al CLIENTE el avance de estas o cualquier imprevisto que se presente durante el proceso
- El proveedor en coordinación con el CLIENTE, realizará de manera aleatoria pruebas de restauración de los servidores en el alcance del convenio. El proveedor presentará al CLIENTE una propuesta de calendario de ejecución de restauraciones el cual deberá considerar escenarios aleatorios.

### Servicio de Administración de Almacenamiento

El proveedor proporcionará el servicio de Almacenamiento dedicado para la atención de CLIENTE

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 CLIENTE. 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 CLIENTE  
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 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.
- El proveedor considera un crecimiento 20% por lo que en caso de que el CLIENTE requiera de este espacio se podrá habilitar de manera inmediata.

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 proveedor deberá estar certificada bajo la norma ISO 20000. Para lo cual el proveedor deberá incluir en su oferta copia de dicha certificación.

## 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 convenio será a partir del 01 al 12 de enero de 2020.

La vigencia total del Pedido mas el convenio será del 01 de noviembre de 2019 al 12 de enero de 2020.

## II. Requerimientos no Funcionales

### Ubicación

El centro de datos propuesto por el proveedor 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 proveedor 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.

### 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 proveedor 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 CLIENTE y en esquema redundante.
- El proveedor 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 proveedor ganador hasta su puesta en marcha.
- La configuración de este sistema de seguridad, deberá ser coordinado en todo momento por personal del proveedor 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 proveedor deberá contar con el personal capacitado y autorizado para efectuar movimientos en las configuraciones de estos equipos cuales quiera que estas sean.
- El proveedor 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 convenio, se deberá acreditar la certificación CISSP.
- El proveedor 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 proveedor 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 proveedor 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 y 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 Scripting 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 proveedor 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 proveedor 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 proveedor deberá identificar y administrar vulnerabilidades de la infraestructura a los que se encuentra expuesto el CLIENTE 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 CLIENTE 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 100 ip´s
- El proveedor 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 proveedor.
  - 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 proveedor ganador llevará a cabo la detección y administración de las vulnerabilidades de la infraestructura del CLIENTE por medio de una solución de escaneo.
- Las actividades que deberá de llevar a cabo el proveedor se mencionan 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 proveedor deberá estar certificada bajo la norma ISO 20000. Para lo cual el proveedor 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 CLIENTE:
  - 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 proveedor 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 proveedor 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 proveedor 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.



- o Contar con un módulo de reporte personalizable. Los reportes deben permitir sacar gráficas y deberán poderse generar en una base de tiempo semanal, mensual o de manera diaria.
- o Cumplimiento de estándares http para prevenir explotaciones del protocolo y técnicas de evasión.
- o Contar con un bypass en caso de un apagado o falla inesperada del o los equipos.
- o Aprender automáticamente las aplicaciones y el comportamiento del usuario sobre estas.
- o Contar con un módulo para la actualización de las firmas de manera automática.
- o Identificar y detener fuentes de ataques conocidos.
- o Mitigar ataques a gran escala integrando direcciones IP de atacantes, BOTS, y servicios anónimos.
- o Realizar la protección de acuerdo a los estándares de seguridad al menos vs OWASP top 10.
- o Soportar alta disponibilidad.
- o Salvaguardar la infraestructura de las aplicaciones incluyendo servidores web, políticas de seguridad de xml y web 2.0.
- o 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.
- o Contar con un módulo de tablero (dashboard) que permita conocer el estatus en tiempo real de las aplicaciones y de los eventos generados.
- o 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.
- o Protección a nivel aplicativo según el top ten del estándar OWASP.
- o Implementación de modo monitoreo.
- o Implementación de modo en línea para bloqueos en tiempo real.
- o Implementación de modo en línea sin bloquear, con el fin de aprender la actividad normal de las aplicaciones, antes de bloquear.
- o El proveedor deberá considerar en su propuesta los siguientes requerimientos mínimos:
  - o Las características de las herramientas para la protección de aplicaciones donde realizará la administración, operación, monitoreo y reportes

- o El monitoreo en tiempo real de las aplicaciones, que permita prevenir incidentes que afecten los niveles de servicio.
- o El monitoreo será con una disponibilidad de 24x7x365
- o 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.
- o Definirá junto con el CLIENTE las aplicaciones y los parámetros y eventos a ser monitoreados por el WAF.
- o Definir procedimientos de notificación y escalación de acuerdo a la estructura organizacional del CLIENTE.
- o Mantenimiento de bitácoras históricas y registro de incidencias (hasta 15 días), desde el inicio del convenio jurídico hasta su conclusión.
- o 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.
- o Monitorear los eventos de seguridad detectados por el WAF en el horario establecido.
- o Analizar eventos de seguridad para identificar y reducir falsos positivos de las alertas generadas.
- o Generar notificaciones por evento de incidencias detectadas (vía correo electrónico o llamada telefónica).
- o Dar recomendaciones generales de seguridad informática relacionada con el WAF y los incidentes detectados.
- o Configurar el WAF para enviar alertas de los eventos de seguridad.
- o Revisar el estado actual del WAF en licencias, actualizaciones, firmas de ataque, hotfix, performance y capacidad de almacenamiento.
- o Dar atención a fallas de los dispositivos WAF en sitio o en forma remota:

#### Soporte primer nivel

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



### Soporte segundo nivel

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

### III. 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 proveedor tendrá que contemplar las configuraciones actuales de los servidores virtuales respetando los sistemas operativos y aplicaciones instaladas.

El proveedor 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 proveedor durante la vigencia del convenio, 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 proveedor provea sea equipo dedicado, vigente y deberá estar en el catálogo del fabricante y con garantía de soporte durante la vigencia del convenio. 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 deberán ser proporcionadas por el proveedor sin costo adicional para el Instituto. En el caso del licenciamiento de Microsoft, se podrá utilizar el convenio 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 proveedor 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 proveedor 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 convenio el proveedor 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:

- Migración Tecnológica de fin de convenio: el proveedor actual deberá coordinar la transferencia tecnológica del servicio objeto de este convenio 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 convenio actual para quedar totalmente concluida al término de convenio actual. El prestador del servicio saliente estará obligado a colaborar y facilitar las labores de transferencia del servicio objeto de este convenio al nuevo prestador del servicio.

Los servidores del Anexo I deberán conservar la virtualización de acuerdo a la arquitectura propuesta por el proveedor 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 Proveedor 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 convenio, 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 convenio y/o pedido antes de i.v.a. no podrá exceder del monto de la garantía de cumplimiento del convenio 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 Unidad 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 "el CLIENTE"

• **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 Unidad 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 "el CLIENTE".

## V. Términos y condiciones de entrega y de aceptación.

### **Plazos, condiciones de entrega y forma de pago:**

Se realizará en un solo pago 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 proveedor 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, todo el año, con un número 01 800. El servicio del proveedor deberá tener las siguientes características distintivas:

- A través del sitio web del proveedor 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.

## VII. Cláusula de Confidencialidad

• El proveedor 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 proveedor 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 proveedor adoptará las precauciones necesarias para proteger la información confidencial o reservada del CLIENTE. Por tal motivo, el proveedor 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 proveedor 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 CLIENTE a través del administrador y supervisor del convenio 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 proveedor ganador, otros elementos que se deberán de tomar en consideración:

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

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
Protección 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: <a href="http://www.inea.gov.mx">www.inea.gov.mx</a> <a href="http://www.conevyt.org.mx">www.conevyt.org.mx</a> <a href="http://www.cursosinea.conevyt.org.mx">www.cursosinea.conevyt.org.mx</a>	
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 proveedor ganador está obligado a presentar los siguientes entregables durante la prestación del servicio.

Reporte
Reporte de operaciones:
Reporte de atención de tickets y CRQ's
Reporte de monitoreo de servidores
Reporte de uso de enlaces de Internet
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.

Se mantendrán las mismas condiciones de calidad y precio estipuladas en el Pedido primigenio.

Monto del convenio: \$375,806.64 (trescientos setenta y cinco mil ochocientos seis pesos 64/100 M.N.)

Monto total del pedido y convenio: \$2,286,157.16 (dos millones doscientos ochenta y seis mil ciento cincuenta y siete pesos 16/100 M.N.)

Atentamente



Oscar Ulises Contreras Luna  
Subdirector Técnico



Condesa, C.P. 06140, Cuauhtémoc, Ciudad de México.  
Tel: 52 55 52 41 79 00 www.gob.mx/inea



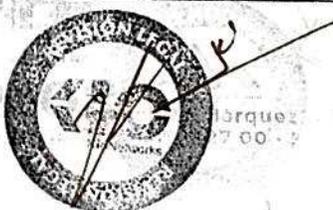
## ANEXO I

### 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	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	BITVRKIOXM01	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	DBPRKIOHAP01	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	1	130	1		2	60 minutos	
7	DBPRKIOXM03	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1487	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
8	DBPRKIOXM04	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	1340	176	SQL Server 2008 R2, SQL Server 2012	1	30 minutos	
9	DBPRKIOXM05	Microsoft Windows Server 2008 R2 (64-bit)	Base de datos	40	620	160	SQL Server 2016 Enterprise Edition	1	30 minutos	
10	DBPRKIOXM06	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 Enterprise Edition	1	30 minutos	
12	FLEXNET	Microsoft Windows Server 2003 (32-bit)	Base de datos	2	240	4	SQL Server 2000 Enterprise	2	60 minutos	
13	FTPLUXKIOXM01	Ubuntu Linux 8.04 Hardy (64-bit)	Web Server	4	135.97	4		2	60 minutos	
14	HQVRKIOXM01	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-cl	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	MINDVRKIOXM01	Microsoft Windows Server 2003 (32-bit)	Base de datos	8	180	32	SQL Server 2005	2	60 minutos	
32	msuxineao1	Linux Red Hat 7.0	Web Server	4	130	8		2	60 minutos	
33	MSUXKIOXPCCONE	Red Hat Enterprise Linux 5.4 Tikanga (64-bit)	Web Server	8	180	32		2	60 minutos	
34	MSUXKIOXPINEA	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	RDBSAELKIOXM	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, BusinessObjects 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, BusinessObjects Enterprise Release 2
39	SIVFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	4	200	24		2	60 minutos	SAP Crystal Reports, BusinessObjects
40	SIVSQL	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	vsalineA-BAAS	Other (32-bit)	Administración	2	158	2		2	60 minutos	
44	WSPDKIOXM02	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	WSPDKIOXM04	Microsoft Windows Server 2003 (32-bit)	Web Server	2	100	32		1	30 minutos	
47	WSPDKIOXM06	Microsoft Windows Server 2003 (32-bit)	Web Server	16	200	32		1	30 minutos	
48	WSPDKIOXM07	Microsoft Windows Server 2003 (32-bit)	Web Server	16	220	32		1	30 minutos	
49	WSPDKIOXM09	Microsoft Windows Server 2003 (32-bit)	Web Server	16	215	32		1	30 minutos	
50	WSSAELKIOXM01	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	ineaycliente	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 Tíkanga (32-bit)	Web Server	2	60 minutos
28	mevvt.ol	Red Hat Enterprise Linux 7 Maipo (64-bit)	Web Server	2	60 minutos
29	mevvtusa	Red Hat Enterprise Linux 5 Tíkanga (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	MSUXKIOMXPONE	Red Hat Enterprise Linux 5.4 Tíkanga (64-bit)	Web Server	2	60 minutos
34	MSUXKIOMXPINEA	Red Hat Enterprise Linux 5.4 Tíkanga (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	SIVFRONT1	Microsoft Windows Server 2008 R2 (64-bit)	Web Server	2	60 minutos
40	SIVSQL	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	vsalNEA-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



## FORMATO DE PROPOSICIÓN ECONÓMICA DE LA EMPRESA:

HOJA \_\_ DE \_\_

**NOMBRE DE LA EMPRESA:** \_\_\_\_\_  
**DOMICILIO FISCAL:** \_\_\_\_\_

**R.F.C.:** \_\_\_\_\_ **TELÉFONO** \_\_\_\_\_

No. de Partida	Descripción	Concepto	Costo por 12 días de enero de 2020
1	Servicio de Infraestructura, Servicios Profesionales y Mantenimiento de Equipos y Aplicaciones de Internet y Extranet (hosting centro de datos externo) para los meses de noviembre y diciembre de 2019	SERVICIO DE MIGRACIÓN DE APLICACIONES Y SERVICIOS	
		SERVICIOS DE HOSPEDAJE	
		INFRAESTRUCTURA Y SERVIDORES	
		SERVICIOS TÉCNICOS PROFESIONALES INTEGRADOS	
		SERVICIOS ADMINISTRADOS	
		LICENCIAMIENTO	
		SERVICIO DE ANÁLISIS DE VULNERABILIDADES	
		SERVICIO DE PROTECCION DE 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 2019





Ciudad de México, 12 de diciembre de 2019.

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

Unidad de Administración y Finanzas

Atención: **Ing. Antonio Quintal Berry**



Estimado Ing. Antonio Quintal,

En respuesta a su oficio UAF/1220/2019 de fecha 11 de diciembre del 2019, mediante el cual solicitan el pronunciamiento sobre la viabilidad de llevar a cabo una ampliación de la infraestructura contratada en el centro de datos externo, al amparo del pedido DAS-TEC-011/19, "Contratación del Servicio de Infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de internet y extranet (hosting centro de datos externo) para los meses de noviembre y diciembre 2019".

De conformidad con lo establecido en el Artículo 25 y 52 de la Ley de Adquisiciones, Arrendamiento y Servicios del Sector Público y el Artículo 91 de su Reglamento, así como la Cláusula Vigésima séptima del pedido referido, le informo que Sixsigma Networks México S.A. de C.V., se encuentra en posibilidades de llevar a cabo la ampliación en monto y vigencia a dicho instrumento legal.

Asimismo, Sixsigma Networks México. S.A. de C.V., manifiesta que su propuesta tiene vigencia por 30 días considerando que conforme al Artículo 54 bis, de la Ley y 102 del Reglamento, se procederá a la terminación anticipada, cuando concurren 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 y/o pedido con motivo de la resolución de una inconformidad emitida por la Secretaría de la Función Pública, o de ser necesario conforme a las disposiciones de contratación de la Cabeza de Sector, Secretaría de Educación Pública o el Instituto Nacional para la Educación de los Adultos.

La propuesta económica contempla la totalidad de los servicios solicitados en el Anexo Técnico firmado en el pedido en comento con una ampliación del 01 de enero al 12 de enero del 2020, sin embargo, todos los servicios considerados en el mismo se continuarán brindando de forma ininterrumpida hasta el 16 de enero del 2020.

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

*Le*

Atentamente,

Juan Carlos Martínez Valdés  
Representante Legal

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**



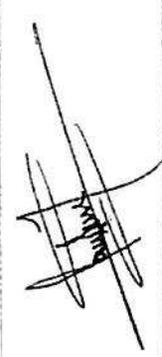
FORMATO DE PROPOSICIÓN ECONÓMICA DE LA EMPRESA

**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.:** SNM010323EBS **TELÉFONO:** (52) 55 85032600 Ext. 3931

No. de Partida	Descripción	Concepto	12 días de servicio
1	Contratación del servicio de Infraestructura, servicios profesionales y mantenimiento de equipos y aplicaciones de Internet y Extranet (Hosting centro de datos externo) para los meses de noviembre y diciembre de 2019	SERVICIO DE MIGRACIÓN DE APLICACIONES Y SERVICIOS	\$ -
		SERVICIOS DE HOSPEDAJE	\$ 13,309.87
		INFRAESTRUCTURA Y SERVIDORES	\$ 133,796.76
		SERVICIO DE TÉCNICOS PROFESIONALES INTEGRADOS	\$ 26,072.26
		SERVICIOS ADMINISTRADOS	\$ 32,833.97
		LICENCIAMIENTO	\$ 36,406.71
		SERVICIO DE ANALISIS DE VULNERABILIDADES	\$ 5,304.38
		SERVICIO DE PROTECCIÓN DE APLICACIONES WEB (WAF)	\$ 42,451.78
		RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	\$ 33,795.51
		<b>SUBTOTAL</b>	<b>\$ 323,971.24</b>
	<b>I.V.A \$ 51,835.40</b>		
	<b>TOTAL INCLUYENDO I.V.A \$ 375,806.64</b>		
<i>Trescientos setenta y cinco mil ochocientos seis mil pesos 64/100 M.N.</i>			

**NOTAS:**

1. LOS IMPORTES ESTAN EXPRESADOS EN MONEDA NACIONAL CON DOS DECIMALES.
2. LA COTIZACIÓN CORRESPONDE A UNA CONTRATACIÓN DE 12 días
3. ES REQUISITO INDISPENSABLE COTIZAR CON LA TOTALIDAD DE LOS CONCEPTOS CONTENIDOS EN LA PARTIDA.
4. LA VIGENCIA DE LA PROPUESTA ECONÓMICA ES DE 30 DÍAS.

  
**Juan Carlos Martínez Valdés**  
 Representante legal

12 de diciembre de 2019

