ADENDA N° 05

REF.: LICITACIÓN PÚBLICA NACIONAL PAC 50/2020 "ADQUISICIÓN DE EQUIPO DE MONITOREO INTEGRAL DE LA RED – AD REFERENDUM – PLURIANUAL – SBE" I.D. N° 387.569.

Por la que se introducen modificaciones o enmiendas a las Bases y Condiciones de la contratación de referencia, en base a las consultas realizadas por potenciales oferentes que se encuentran en el SICP. Los cuales quedan redactados de la siguiente manera:

ESPECIFICACIONES TÉCNICAS Y SUMINISTROS REQUERIDOS

ADQUISICION DE EQUIPO DE MONITOREO INTEGRAL DE LA RED

Objetivo: El objeto de este llamado es cubrir las necesidades de monitoreo del tráfico de la red de datos, de tal manera a tener estadísticas que ayuden a ser proactivos en la resolución de los diversos problemas, mejorando así notablemente la performance de la red de datos y por ende el funcionamiento de todos los sistemas corporativos.

De las especificaciones técnicas obligatorias: El proveedor deberá especificar concretamente en su propuesta para el objeto, equipos que atiendan obligatoriamente, las siguientes especificaciones técnicas.

ESPECIFICACIONES TÉCNICAS.

1. **La solución deberá estar compuesta por.**

   - Solución basada en appliance físico dedicado con módulos de análisis y monitoreo de tráfico en tiempo real, en forma retrospectiva y almacenamiento masivo para estudio histórico. El almacenamiento utilizable es de 15 TB como mínimo y el RAID es optativo.
   - Solución basada en appliance físico rackeable o virtual dedicado con módulos de herramientas de análisis de datos recolectados desde la red. Dicha herramienta realizará el análisis de performance de los parámetros medidos y realizará el armado de las vistas de control.
   - La herramienta contará con licenciamiento perpetuo para el appliance y las funcionalidades de este.
   - La herramienta deberá brindar dentro del soporte del fabricante la posibilidad de actualización de firmware y bases de funcionalidades de 12 meses como mínimo.
   - La herramienta deberá realizar el análisis de los datos recolectados desde 10 puntos de conexión como mínimo en la red

Oscar E. Saldivia P.
JEFE DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2. Características Técnicas.

- Cuatro conectores Gigabit Ethernet, además de una conexión 10/100/1000 separada para la interconexión con su consola y para tareas administrativas, como mínimo.
- Este módulo tendrá una consola para que a nivel operativo y de análisis de fallas se pueda analizar los datos obtenidos.
- Esta consola también podrá procesar archivos capturados previamente y guardados en formato reconocido.
- La consola proveerá para el análisis un selector de tiempo donde visualmente o por medio de un formulario se pueda seleccionar un lapso sobre el cual se desea realizar el análisis.
- Se podrá representar en un gráfico para visualizar el tráfico del lapso seleccionado y en la cual los ejes "X" e "Y" sean modificables en su escala con el fin de obtener mayor detalle en esta visualización y así facilitar el análisis.
- El gráfico podrá ser modificado en sus métricas para que reflejen bits/seg, bytes/seg, paquetes/seg; y podrá ser desplegada en escala lineal o logarítmica.
- Existirán en la consola tablas con diversas características de tráfico tales como VLAN ID, subred, IP origen, IP destino, puerto, protocolo, entre otros.
- Se dispondrá de un gráfico de torta circular donde, según el ordenamiento de las tablas, se dibuje el gráfico para representar las entradas más importantes de acuerdo con dicho ordenamiento.
- El gráfico del punto anterior también estará disponible como gráfico de barras.

2.1. **Las tablas de datos disponibles para cada intervalo seleccionado** deberán tener diversas vistas como:

2.1.1. Un resumen de los paquetes recibidos.
2.1.2. Errores los paquetes recibidos.
2.1.3. Tráfico por dirección IP asociado con puerto, red, dirección MAC, IP destino, VLAN ID, etc.
2.1.4. Tráfico por puerto asociado con el protocolo IP, la dirección MAC, y la tasa de trasmisión en Paquetes/seg y Bytes/seg, etc.
2.1.5. Subredes y su tráfico asociado a las direcciones IP, con datos de bytes y tasa de transmisión.
2.1.6. Direcciones MAC.
2.1.7. Conversaciones entre estaciones con direcciones IP.
2.1.8. Sockets relacionando direcciones IP con puertos lógicos y las tasas de transmisión.
2.1.9. VLAN, mostrando estadísticas por VLAN.

- Las estadísticas en las tablas deben ser seleccionables de modo que el gráfico desplegado se refiera solamente a las instancias de las tablas que se han seleccionado.
- Los datos en las tablas podrán ser ordenados de acuerdo con las columnas que las componen.

Oscar E. Zanabria P.
JEFE DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.2. **La consola de este módulo, además**, permitirá que se seleccionen datos dentro del intervalo de tiempo para ser recuperados y analizados en un sistema experto que permita ver entidades existentes en las diferentes capas o encabezados del tráfico, así como ver los paquetes mismos y sus encapsulamientos. Este sistema experto será de una naturaleza tal que:

2.2.1. Deberá permitir la creación de perfiles de filtros donde puedan crearse diversos filtros con nombres específicos facilitando el trabajo del usuario.

2.2.2. **Deberá soportar DIAGNOSTICOS** en diferentes niveles del modelo OSI. Estas deben incluir:

2.2.2.1. Red

2.2.2.2. Direcciones IP duplicadas

2.2.2.3. Misdirected frame

2.2.2.4. Time-to live expiring

2.2.2.5. Transporte

2.2.2.6. Slow server, Window Size exceeded, Slow File Server

2.2.3. Deberá permitir la captura parcial de paquetes, limitándose a capturar 32, 64, 128,256, 512 o 1024 bytes iniciales, evitando que se capture el resto de las tramas.

- Deberá permitir la interpretación del tráfico clara e inteligible dividida por color conforme a la capa correspondiente.

2.2.4. Deberá desplegar los datos en formato hexadecimal, e interpretando los caracteres en ASCII o EBCDIC

2.2.5. Deberá contar con métodos rápidos que permiten ir a una trama digitando el número de esta.

2.2.6. Deberá desplegar el tiempo relativo entre tramas subsecuentes.

2.2.7. Deberá desplegar el tiempo relativo a una trama específica marcada por el operador.

2.2.8. Deberá desplegar la hora y la fecha absolutas en los que una trama fue capturada.

2.2.9. Deberá permitir la búsqueda por texto a secuencia de caracteres en una captura.

2.2.10. Deberá contar con un filtro rápido que con un solo "clic" se filtren los paquetes que estén relacionados a un diagnostico encontrado.

2.2.11. **Deberá contar con filtros** de pos-captura por:

2.2.11.1. Por dirección IP o MAC

2.2.11.2. Filtros por conversación entre dos estaciones a través de la selección del nombre o la dirección IP

2.2.11.3. Filtro por protocolos

2.2.11.4. Filtro de patrones de datos (Bytes y bits) permitiendo la configuración de patrones dentro de la trama

2.2.11.5. Tamaño de trama

2.2.11.6. Deberá permitir crear combinaciones de criterios.

2.2.12. Deberá poseer los siguientes gráficos estadísticos:

2.2.12.1. Hosts que más utilizan la red (Top 10Hosts) (bytes, paquetes y broadcasts).

2.2.12.2. Conexiones que más utilizan la red.

2.2.12.3. Distribución de la utilización de la red.

2.2.12.4. Utilización, errores, broadcasts vs. Tiempo.

2.2.12.5. Distribución de Protocolos en formato de barras, pie o tabla

Oscar E. Zunabria P.
JEFE - DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.2.13. Deberá desplegar tablas que listan las conexiones entre dispositivos con direcciones IP que muestran las cantidades de Bytes y tramas enviados o recibidos por cada máquina, entre otras informaciones (indicar).

2.2.14. Los siguientes gráficos que estarán disponibles:

2.2.14.1. Paquetes y bytes.
2.2.14.2. Errores por segundo
2.2.14.3. Tamaño de paquetes
2.2.14.4. Top Hosts
2.2.14.5. Top Conversations
2.2.14.6. Top Protocols
2.2.14.7. Tempo de respuesta de aplicaciones

2.2.15. Este sistema experto poseerá vistas en las cuales se podrá ver la descodificación del tráfico analizado, un mapa de tráfico que muestre las relaciones entre estaciones y la distribución de los protocolos en el intervalo.

2.2.16. Además, este experto deberá contar con una tabla que por capas muestre las entidades contenidas en el tráfico y permita seguir filtrando datos hasta llegar al análisis de una sola entidad ya sea esta una IP, red, conexión TCP, flujo de datos UDP o una sola alerta de anomalía.

2.3. **Monitoreo de Aplicaciones.** La solución ofertada deberá contar con la capacidad por medio de una consola adicional de análisis de aplicaciones que sea capaz de auto descubrir aplicaciones corriendo en la red y analizar su tiempo de respuesta y comportamiento.

2.4. Esta solución deberá de desglosar el tiempo de respuesta de aplicaciones en Tiempo en el Servidor y Tiempo de Transferencia de Datos.

2.5. Se necesita que las aplicaciones en este módulo se auto- descubran, y que también puedan ser dadas de alta vía rango de puertos TCP/UDP o sockets.

2.6. Como datos requeridos a las estadísticas brindadas con este módulo de monitoreo LAN se necesita las siguientes estadísticas: consumo de ancho de banda por aplicación, por cliente, por servidor, por VLAN, por QoS y por tiempo de intervalo.

2.7. Se necesita que el módulo solicitado pueda entregar estadísticas presentadas en forma tabular y además en forma gráfica.

2.8. La solución de monitoreo de aplicaciones debe permitir segmentar la vista por VLAN, Tiempo, Clientes, Servidores y Aplicación, QOS, tráfico de VOIP. Las vistas deben estar relacionadas de tal forma que un cambio en una de las vistas afecte a todas las demás.

2.9. La solución deberá ser agnóstica respecto a marcas o modelos de equipos de red o conectados a la red existentes en el ecosistema.

2.10. La solución deberá contar con soporte de protocolos al menos para:

2.10.1. ICMP
2.10.2. IGMP
2.10.3. TCP
2.10.4. EGP
2.10.5. IGP
2.10.6. UDP
2.10.7. GRE
2.10.8. DSR
2.10.9. ESP

Oscar E. Sanabria P.
JEFE - DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.10.10. AH
2.10.11. TLSP
2.10.12. CFTP
2.10.13. DGP
2.10.14. TCF
2.10.15. EIGRP
2.10.16. OSPF
2.10.17. LARP
2.10.18. MTP
2.10.19. VRRP
2.10.20. PGM
2.10.21. L2TP
2.10.22. DDX
2.10.23. IATP
2.10.24. STP

2.11. Los análisis deberán estar soportados al menos para:

2.11.1. Cc: mail
2.11.2. Lotus Notes
2.11.3. HTTP/Web
2.11.4. Oracle
2.11.5. NFS
2.11.6. Internet Mail
2.11.7. MeetingMaker
2.11.8. Entrypoint
2.11.9. DB2
2.11.10. FTP
2.11.11. MS Mail
2.11.12. MS Exchange
2.11.13. Backweb
2.11.14. MS-SQL
2.11.15. TFTP
2.11.16. VINES
2.11.17. MSODBC
2.11.18. Telnet
2.11.19. QuickMail
2.11.20. Java Scripts
2.11.21. Sybase
2.11.22. X-Win
2.11.23. Audio Ingres
2.11.24. SoftPC
2.11.25. Real Audio
2.11.26. Gupta Gopher
2.11.27. AOL UUCP
2.11.28. MS-RPC H.323 Peoplesoft Citrix
2.11.29. MS-Media RTP/RTCP SAP R3 Timbuktu
2.11.30. MS-SNA Server T.120 PCAnywhere
2.11.31. MS-SMS CU-Seeme

Oscar E. Sanabria P.
JEFE - DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.11.32. MS-MQS
2.11.33. MS-Terminal Svr
2.11.34. talkMATIP
2.11.35. Filenet
2.11.36. Quicktime
2.11.37. HTTP
2.11.38. ntalk
2.11.39. VivoActive
2.11.40. SMTP
2.11.41. IRC
2.11.42. Shockwave
2.11.43. NNTP
2.11.44. iChat
2.11.45. VDOLive
2.11.46. FTP
2.11.47. IVisit StreamWorks
2.11.48. Telnet
2.11.49. IMAP
2.11.50. Y protocolos a definir por el usuario

2.12. **Monitoreo de Voz.** Además, la solución deberá ser capaz de analizar el tráfico de sobre VoIP, y que permita decodificar y hacer troubleshooting de protocolos de VoIP como:

2.12.1. H.323 (v4) incluyendo:
2.12.2. H.225 (v4) Call Signaling
2.12.3. H.245 (v8) Media Control
2.12.4. RAS (v4)-Registration, Admission, and Status
2.12.5. H235 (v3)-Security
2.12.6. Faststart
2.12.7. SIP-Session Initialization
2.12.8. SDP-Session Description
2.12.9. SAP-Session Announcement
2.12.10. MGCP-Media Gateway Control
2.12.11. MEGACO / H.248-Media Gateway Control
2.12.12. RTP-Realtime Transport
2.12.13. RTCP-RTP Control
2.12.14. RTSP-Realtime Streaming Protocol
2.12.15. H.261-Video Encoding
2.12.16. H.263-Video Encoding

2.13. La solución de monitoreo de tráfico de voz deberá de dar alarmas de pérdida de paquetes, "jitter" o retardo de las conversaciones.

2.14. **Características del servidor de monitoreo centralizado.** La solución ofertada será tal que pueda ser accedida con la totalidad de las funcionalidades con un browser o por medio de un cliente liviano que se pueda instalar en cualquier computadora personal.

2.15. La solución al recuperar tráfico deberá permitir utilizar filtros de tipo Dirección IP, direcciones MAC y patrones de trama para el periodo de análisis seleccionable por el usuario.

Cesar E. Zavala P.
JEFE DPTO. DE LICITACION
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.16. La solución ofertada podrá brindar estadísticas en tiempo real y almacenará información histórica como reportes hasta por un año.

2.17. El despliegue de la información para su monitoreo ya sea en tiempo real como para el último mes deberá estar basado en tableros configurables que podrán contener diferentes paneles o gráficos de información. Estos tableros deberán ser por usuario. Un usuario podrá compartir estos tableros de forma que puedan ser visualizados por otros usuarios.

2.18. Estos tableros al menos podrán contener información de la siguiente clase:

2.18.1. Uso de los enlaces monitoreados en total y desglosados por

2.18.1.1. Aplicación
2.18.1.2. Hosts
2.18.1.3. Grupos de Aplicaciones
2.18.1.4. Grupos de Hosts
2.18.1.5. Conversaciones entre Hosts

2.18.2. Uso de una aplicación en total y desglosado por

2.18.2.1. Aplicación
2.18.2.2. Hosts
2.18.2.3. Grupos de Aplicaciones
2.18.2.4. Grupos de Hosts
2.18.2.5. Conversaciones entre Hosts

2.19. Los tableros deberán permitir visualizar para un Host.

2.19.1. Su top aplicaciones
2.19.2. Su top conversaciones hacia y desde el Host.

2.20. Los tableros deben permitir ver las aplicaciones para un host.

2.21. Las capturas de paquetes que sean recuperables deberán poder ser exportadas en formatos ya sea .cap o como pcap para su análisis posterior o almacenamiento.

2.22. La solución ofertada deberá permitir que se generen diagramas de las conexiones TCP y como los paquetes se intercambian entre el servidor y el cliente, basado en capturas de tráfico.

2.23. Tendrá capacidad para realizar el inventario de subredes, VLAN y QOS de modo que cada una de ellas sea vista como un enlace separado para permitir el monitoreo del tráfico de cada objeto en forma individual por cada segmento IP.

2.24. La solución podrá calcular y graficar el tiempo de respuesta de aplicaciones mostrándolo como tiempo de red y tiempo de servidor por separado.

2.25. Para VoIP se contará con las siguientes capacidades.

2.25.1. Registro de las llamadas en proceso
2.25.2. MOS de las llamadas
2.25.3. Origen y destino de las llamadas

2.26. La solución será compatible al menos con los protocolos de voz paquetizada.

2.26.1. SIP
2.26.2. H323

2.27. En los gráficos existirán capacidades de acercamiento por despliegue (drill-down), donde basado en una vista se puede ir a otra con más detalle acerca de las estadísticas presentadas en la vista original.

2.28. La solución brindará la capacidad de enviar alertas en casos configurables por las siguientes vías

Oscar E. Sandoval D.
JEFE - DPTO. DE LICITACIÓN
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.28.1. EMAIL
2.28.2. Ejecutando un script
2.28.3. Trap SNMP

2.29. Las estadísticas relativas al tráfico comprenderán al menos
2.29.1. Throughput
2.29.2. Volumen de tráfico
2.29.3. Paquetes

2.30. Respecto al tráfico WEB podrán inventariarse y darse de alta aplicaciones por su URL

2.31. La resolución con que son visualizados los datos más recientes podrá seleccionarse hasta una escala tan granular como milisegundos.

2.32. Los ejes de los gráficos más importantes podrán ser lineales o logarítmicos a elección del usuario para mejor lectura de los datos.

2.33. Existirá la posibilidad de crear tanto grupos de elementos como grupos de usuarios para el monitoreo de las estadísticas de modo que, si un grupo de interfaces tienen relación, puedan agruparse para un análisis más rápido y seguro.

2.34. Cuando los umbrales de las variables a las cuales se configuren alertas sean sobrepasados, además de generar la alerta correspondiente por los medios mencionados antes, se deberá contar con un visor de alarmas que de vista retrospectiva de estas alarmas.

2.35. Los reportes deberán estar disponibles en diferentes formatos que al menos comprenderán:
2.35.1. Reportes inmediatos que se generen a partir de una vista en tiempo real o histórica
2.35.2. Reportes calendarizados que puedan ser generados cada cierto periodo de tiempo y que al menos puedan ser:
2.35.3. Enviados por Email en formato pdf.
2.35.4. Publicados en el servidor central de la solución ofertada para ser accedidos vía Web.

2.36. La solución podrá graficar tráfico en forma cuantitativa (volumetría) así como también gráficos de tiempo de respuesta para las aplicaciones en las cuales se solicite esa información.

2.37. No solo podrá graficar el tiempo de respuesta de una aplicación sino entregar graficas entregando rankings de:
2.37.1. Peores aplicaciones
2.37.2. Peores Servers
2.37.3. Peores Clientes
2.37.4. Para cada una de estas instancias se podrá ver el tiempo de respuesta de la aplicación en cuestión.

2.38. La solución permitirá analizar la cantidad de respuestas que las aplicaciones haya servido y decir cuántas han sido exitosas y cuantas han sido fallidas.

2.39. La solución podrá entregar un reporte diciendo qué cantidad de respuestas han entrado en cada uno de los rangos de tiempos de respuesta que serán configurables.

2.40. Se podrán personalizar aplicaciones por:
2.40.1. Puertos
2.40.2. Direcciones de los servidores combinadas con los puertos
2.40.3. URL

Oscar E. Zavabria P.
JEFE - DPTO. DE LICITACIÓN
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.41. La solución podrá crear roles de usuarios, usuarios y grupos de elementos monitoreados

2.41.1. Se podrá atribuir un grupo de elementos a un usuario para que solo tenga acceso a los elementos monitoreados permitidos.

2.41.2. Cada usuario podrá tener un tamaño de paquete que puede recuperar para observación. El administrador podrá dar visibilidad de paquetes completos a unos usuarios y de paquetes cortados o parciales para otros usuarios.

2.42. Se podrá hacer "drill-down" desde esta interfaz Web hasta una consola de análisis avanzado de aplicaciones que podrá estar como un cliente en el computador de los usuarios.

2.43. En términos de VOIP, la consola WEB podrá entregar reportes de

2.43.1. Volumen de llamadas

2.43.2. Jitter

2.43.3. Packet Loss

2.43.4. MOS Score

2.44. Permitirá usar los paquetes guardados en el almacenamiento de los discos de las sondas para crear "bounce charts" que muestren lo paquetes de una conexión y las latencias de estos. Permitirá de una forma liviana observar los paquetes almacenados sin traerlos a la consola.

2.45. Permitirá que el usuario pida salvar la captura en el disco local de su máquina.

2.46. Permitirá graficar KPis para estadísticas selectas donde se puedan ver errores en esas aplicaciones.

2.47. Permitirá crear reportes comparativos entre las interfaces físicas y las interfaces virtuales (subnets, VLAN, QOS) contenidas en las interfaces físicas.

2.48. Permitirá que los usuarios puedan crear grupos de gráficos que una vez aplicadas a una interfaz, puedan ser recreadas fácilmente en otra interfaz como vistas rápidas

2.49. **Módulo de Análisis de Sesiones Aplicativas**. Además de almacenar paquetes, el módulo de captura de tráfico debe generar registros de sesiones aplicativas de al menos:

2.49.1. Citrix

2.49.2. DNS

2.49.3. SMTP

2.49.4. POP3

2.49.5. FTP

2.49.6. http

2.49.7. LDAP

2.49.8. RADIUS

2.49.9. RTP

2.49.10. SIP

2.49.11. H323

2.49.12. Aplicaciones Web personalizadas por el usuario

Oscar E. Sanabria P
JEFE - DPTO. DE LICITACIÓN
U.O.C. - CORTE SUPREMA DE JUSTICIA

2.50. Estos registros deberán contener la información relevante de las sesiones de dichos aplicativos y una vez que dicho análisis en lazado sobre un espacio de tiempo, los resultados deberán incluir:

2.50.1. Un selector de tiempo para refinar la búsqueda de sesiones y su análisis

2.50.2. Un resumen de Clientes del aplicativo
2.50.3. Un resumen de usuarios del aplicativo
2.50.4. Un resumen de errores descubiertos
2.50.5. En el caso de aplicaciones basadas en http, un resumen de URLS
2.50.6. En el caso de aplicaciones basadas en http, un resumen de tipo de browsers usados.
2.50.7. En el caso de DNS el tipo repetición y el nombre implicado, así como la IP resuelta en el caso de transacciones de tipo exitosas

2.51. Los detalles mencionados anteriormente podrán ser usados para filtrar las sesiones.

2.52. Una vez encontrado el foco del análisis se podrá solicitar un listado de las sesiones de interés de forma rápida e integrada en la pantalla del usuario, que deberá ser accedida vía WEB.

2.53. La presentación de las sesiones de los aplicativos deberá ser tal que muestre una "escalera" que muestre los comandos y respuestas de la sesión en cuestión y que entregue una precisión de milisegundos al colocar los elementos de la escalera.

2.54. Para una sesión específica, será posible ya sea salvar los paquetes en caso de que aun estén almacenados en el buffer del módulo de captura o decodificarlos en el mismo caso, directamente en la pantalla del usuario para permitir un análisis inmediato de la información.

2.55. Deberá permitir mostrar el tiempo de respuesta cuando sea posible por medio de columnas que podrán ser adicionadas a los sumarios como cliente o servidor que se han mencionado.

2.56. Varios análisis de este tipo podrán estar presentes en la pantalla del operador del módulo

IMPLEMENTACIÓN Y TRANSFERENCIA TECNOLÓGICA:

A efecto de garantizar la correcta puesta en marcha de la solución, en forma conjunta entre el Proveedor y el Equipo Técnico de la Dirección de TIC's de la Corte Suprema de Justicia se procederá a la instalación de los componentes que forman parte de la propuesta y su respectiva implementación.

El objetivo principal es transmitir al personal de la institución el conocimiento en el uso de las herramientas tecnológicas para la administración y gestión diaria de la plataforma a implementar. Para ello se propone la modalidad On-Job-Training, este entrenamiento estará a cargo del proveedor y deberá estar dirigido a los técnicos de la TIC.

De esta forma se persigue conformar un equipo de trabajo, con la autonomía suficiente, para operar el servicio en forma integral.

Términos para tener en cuenta

1. Contar como mínimo con 1 técnicos certificados con las certificaciones del producto
2. Contar como mínimo con 2 técnicos con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

3. Soporte técnico 24x7 incluido durante el periodo de 1 año on site y/o remoto.
4. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada 24x7.
5. La convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta.

- Se modifican los siguientes puntos:

• **FECHA LÍMITE DE CONSULTAS**
• **FECHA LÍMITE DE RESPUESTAS**
• **FECHA DE INICIO DE PROPUESTAS**
• **FECHA LÍMITE DE PROPUESTAS**
• **INICIO DE LA ETAPA COMPETITIVA**
• **FECHA DE ENTREGA DE OFERTAS**
• **FECHA DE APERTURA DE OFERTAS**

***Se aclara que las fechas se encuentran en el Sistema de Información de las Contrataciones Públicas.**

OBSERVACIÓN:

- Solo se modifican los puntos citados en la presente Adenda, quedando invariable los demás puntos del Pliego de Bases y Condiciones.

Atentamente,

Oscar E. Sanabria P.
JEFE - DPTO. DE LICITACIÓN
U.O.C. - CORTE SUPREMA DE JUSTICIA