Bogotá D.C., 25 de julio de 2023

ADENDA No. 2

Se hace necesario realizar la presente adenda No. 2, al proceso de selección de selección abreviada de menor cuantía No. 177 MDN-COGFM-JEMCO- DIGSA-2023, cuyo objeto es ***ADQUISICIÓN DE SERVICIOS PROFESIONALES PARA LA IMPLEMENTACIÓN DEL MODELO DE SOPORTE NIVEL II, ADMINISTRACIÓN Y GOBIERNO DE LA PLATAFORMA TECNOLÓGICA, CONTINUIDAD DEL NEGOCIO Y PLAN DE TRANSFORMACIÓN DIGITAL DE LA DIRECCIÓN GENERAL DE SANIDAD MILITAR***.", en el sentido de modificar las especificaciones técnicas mínimas requeridas, los cuales quedaran así:

1. **ESPECIFICACIONES TECNICAS MINIMAS REQUERIDAS,**

<table>
<tr><td colspan="2">REQUERIMIENTOS MINIMOS TECNICOS EXCLUYENTES

ADQUISICIÓN DE SERVICIOS PROFESIONALES PARA LA IMPLEMENTACIÓN DEL MODELO DE SOPORTE NIVEL II, ADMINISTRACIÓN Y GOBIERNO DE LA PLATAFORMA TECNOLÓGICA; CONTINUIDAD DEL NEGOCIO Y PLAN DE TRANSFORMACIÓN DIGITAL DE LA DIRECCIÓN GENERAL DE SANIDAD MILITAR.

A continuación, se describen las actividades que el contratista debe realizar para todos los efectos en torno al cumplimiento del objeto contractual a partir de la firma del acta de inicio</td></tr>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th></tr>
<tr><td>1.</td><td>ESPECIFICACIONES GENERALES</td></tr>
<tr><td>1.1</td><td>SITIOS DE PRESTACIÓN DEL SERVICIO
El CONTRATISTA prestará el servicio para la sede en Bogotá D.C. como se detalla a continuación:<table><tr><th>No.</th><th>UBICACIÓN</th></tr><tr><td>SEDE 1</td><td>DIGSA Unidad Principal Dirección: Avenida Calle 26 No. 69-76 Centro Empresarial Elemento, Torre Tierra.</td></tr></table></td></tr>
<tr><td>1.2</td><td>El contratista presentará en un término no mayor a 5 días hábiles luego de firmada el acta de inicio, el cronograma y plan de trabajo detallado en el cual se describan los procesos/actividades inherentes para alcanzar el objeto del contrato; explicando claramente el número de días de la actividad para desarrollar cada actividad relacionada en el cronograma, que incluya, entre otros, actividades, fechas de inicio y terminación, hitos y ruta crítica, firmas. este plan de trabajo será de obligatorio cumplimiento, previa aprobación de los supervisores del contrato.</td></tr>
<tr><td>1.3</td><td>El contratista deberá garantizar el soporte técnico en sitio y remoto si se requiere con personal competente para las actividades programadas y solicitadas por el supervisor del contrato.</td></tr>
<tr><td>1.4</td><td>El contratista debe reportar al supervisor del contrato por cualquier medio de comunicación el ingreso y salida del personal relacionando lo siguiente (nombre, cédula, teléfono y correo electrónico de contacto, datos de contacto familiar, arl.</td></tr>
<tr><td>1.5</td><td>El contratista debe prestar soporte telefónico, presencial o vía e-mail, para lo anterior debe entregar por escrito los nombres, celular y correo electrónico que pone a disposición de la dirección general de sanidad militar para reportar los incidentes presentados, con el fin de brindar soluciones a los requerimientos presentados por el supervisor del contrato.</td></tr>
<tr><td>1.6</td><td>El Contratista entregará en un término no mayor a 5 días hábiles de perfeccionado el contrato los Acuerdos de Nivel de Servicios firmado por las partes y aprobado por la Supervisión del Contrato.</td></tr>
<tr><td>1.7</td><td>El contratista se compromete a no divulgar, trasmitir o compartir la información que reciba, conozca o se genere de la Dirección General de Sanidad Militar durante y después del presente contrato. Por tanto, el CONTRATISTA deberá firmar los Acuerdos de Confidencialidad de toda</td></tr>
</table>

	la información suministrada y generada para el presente proceso y dar cumplimiento a la normatividad vigente de acuerdo con la Directiva del CGFM 154-2014 la cual será socializada por el Supervisor. Este Acuerdo de confidencialidad debe firmarse con el Acta de Inicio del contrato.
1.8	• Será de exclusiva responsabilidad del CONTRATISTA, contratar el personal que requiere para cumplir con el objeto del contrato y asumir por su cuenta y riesgo todas las prestaciones legales a que haya lugar. El Ministerio de Defensa Nacional – Comando General de las Fuerzas Militares – Dirección General de Sanidad Militar - Grupo SISAM Tecnologías de la Información y Comunicaciones aclaran que, aunque ejercerá supervisión no se establecerán vínculos contractuales con estos y la responsabilidad de dichos vínculos será totalmente del contratista adjudicatario. • El contratista efectuará los trámites pertinentes y asumirá los costos a que haya lugar, con respecto a las tarjetas de acceso (ficheros) para el personal solicitado en el presente contrato. • La tarjeta de acceso es de uso personal e intransferible. • Cada funcionario debe portar su tarjeta para ingresar al edificio: las personas de la recepción y de seguridad, no están autorizadas para dar acceso a ningún funcionario que no porte su tarjeta. • Los acompañantes deben registrarse en la recepción antes de ingresar, no pueden hacer uso de la tarjeta del oficial. • Si la tarjeta ha sido extraviada, se debe reportar al supervisor del contrato inmediatamente para realizar trámites administrativos y de cobro por parte del edificio y nueva entrega de este, así como también la inactivación y retirarla del sistema del fichero y actualización de datos del propietario. • El personal como la empresa serán responsables del uso que terceras personas podrían darle, será de carácter informativo no pasar por alto este nivel de seguridad. • El costo estimado por cada fichero es de $31.100 IVA incluido, se Recuerda que solo las firmas autorizadas de cada entidad pueden realizar dicho trámite, este podría variar según cambios del edificio Elemento. • Si no, se cuenta con este documento al momento de ingreso a las instalaciones, el personal contratista debe portar su documento personal que lo identifique Cedula de Ciudadanía, avisar al supervisor encargado para permitir así el acceso. • En caso de cualquier duda o sugerencia se brindará por parte de los supervisores para consultarla e informarla.
1.9	El supervisor podrá exigir el remplazo definitivo del personal que considere no está cumpliendo a satisfacción con las políticas, procedimientos, mecanismos de seguridad y en general por la mala calidad de los servicios prestados, teniendo en cuenta lo pactado en el contrato. El CONTRATISTA contará con un máximo de tres (3) días hábiles, siguientes a la notificación que por escrito que hagan los supervisores, exponiendo las razones del cambio del personal. El CONTRATISTA entregará la nueva hoja de vida del personal propuesto, debiendo éste contar con un perfil académico y de experiencia igual o superior al inicialmente propuesto.
1.10	El contratista se reunirá mensualmente y de común acuerdo con el supervisor del contrato para realizar el seguimiento al cronograma de trabajo que debe ser la ejecución del contrato, entregando informe mensual del avance del plan de trabajo.
2.	**ACTIVIDADES INFRAESTRUCTURA**
2.1	El contratista deberá definir junto con el supervisor, la usabilidad de las Máquinas Virtuales actuales, de acuerdo con el inventario de los servidores existentes, sistema hiperconvergente, y almacenamiento. El contratista debe constituir para la DIGSA, la mejor arquitectura de las aplicaciones que son utilizadas, que se adapten fácilmente a las necesidades de la entidad. Se debe entregar al supervisor del contrato un informe de lo realizado en esta actividad.
2.2	El contratista de acuerdo con el inventario con que cuenta la DIGSA de sus servidores, debe revisar y definir la obsolescencia de cada uno de ellos informando al supervisor la mejor practica que se deba realizar con esta infraestructura.
2.3	EL contratista debe realizar un estudio de las maquinas con sistemas Windows 2008 las cuales no se han podido actualizar ya que están sujetas a aplicativos que maneja la DIGSA. Luego de verificar lo anterior debe entregar al supervisor en documento el estudio realizado con la solución realizada.
2.4	Revisión de las máquinas de SALUD.SIS para realizar la migración a Vmware Tools. estás están Integradas a sistema operacional Linux administradas por soporte y Mantenimiento de SALUD.SIS.

2.5	El contratista debe definir la mejor arquitectura de continuidad del negocio con la infraestructura actual con que cuenta la DIGSA. Debe hacer entrega en un documento donde se especifique la arquitectura implementada y la hoja de ruta.
2.6	El contratista debe definir un plan para la realización de pruebas de conectividad periódicas en la DIGSA. Se realizarán dos (2) pruebas durante la vigencia del presente proceso.
2.7	El contratista debe verificar la actualización de las máquinas virtuales. Se debe detallar en un informe que maquinas fueron actualizadas y cuales no con sus observaciones correspondientes.
2.8	El contratista debe realizar una actualización de afinamiento de la infraestructura tecnológica de la DIGSA.
2.9	El contratista debe verificar junto con el supervisor el control de cambios para aprobación de la actualización de la infraestructura de servidores, almacenamiento, switches, Red LAN, WIFI, FIREWALL. Entre otros.
2.10	El contratista debe realizar una revisión de las autorizaciones de ingresos remotos (donde y quienes tienen los accesos).
2.11	El contratista debe definir en conjunto con el supervisor del contrato los servidores del Directorio Activo principal y de respaldo.
2.12	El contratista debe realizar un afinamiento (limpieza) directorio activo. Entregar informe
	El contratista debe implementar niveles de seguridad para el seguimiento al Directorio Activo. Entregar informe.
2.13	El contratista debe desarrollar un análisis e implementación de políticas de seguridad basado en el Directorio Activo. Entregar informe.
2.14	El contratista debe presentar un informe de modificaciones y/o actualizaciones del Directorio Activo.
2.15	El contratista debe entregar al supervisor del contrato reportes quincenales de acceso al Directorio Activo.
2.16	El contratista debe realizar monitoreo del Directorio Activo y transferencia de conocimiento.
2.17	El contratista realizara transferencia de conocimientos sobre todo lo ejecutado al directorio activo.
2.18	El contratista junto con el supervisor del contrato debe definir el proceso de recuperación ante cualquier desastre DRP para el centro de datos 4º piso DIGSA.
2.19	El contratista debe ejecutar el proceso de DRP y junto con el supervisor diseñar procedimiento.
2.20	El contratista debe realizar una (1) hoja de ruta sobre una prueba del DRP.
2.21	El contratista debe revisar y/o modificar el proceso de IPV6 para el datacenter. Entregar informe del estado actual y su configuración.
2.22	El contratista debe verificar los documentos y los cambios de la consultoría anterior en lo relacionado con IPV4 - IPV6.
2.23	El contratista debe aplicar la configuración IPV6 a las APPS transversales, como DNS, Directorio activo, DHCP.
2.24	El contratista debe aplicar la IPV6 a infraestructura de servidores, almacenamiento, switches LAN, WIFI, FIREWALL. Entre otros.
2.25	El contratista debe resolver los incidentes que no pudieron solucionar los responsables del soporte nivel 1 de acuerdo con los informes entregado en esta etapa.
2.26	Validación y acompañamiento para la solución de incidentes ocasionados por la infraestructura de datacenter aplicaciones y/ o servicios en nube.
2.27	El contratista dará solución de los incidentes presentados en el nivel 2. Documentando cada incidente.
3.	**SOPORTE TÉCNICO**
3.1	Si el soporte implica contacto o manipulación de información el contratista debe informar al supervisor, se debe presentar un plan de backups que respalden la información.
3.2	El contratista informara todos los cambios y actualizaciones realizadas éstos deben ser aprobados por el supervisor del contrato antes de su implementación y deben quedar documentadas conservando la funcionalidad que opera actualmente.
3.3	El contratista debe tener en cuenta los siguientes tiempos de respuesta: Cuando se requiera el servicio solicitando la asistencia, se debe dar respuesta como mínimo entre los siguientes rangos. URGENTE, GRAVE o NO CRITICA: URGENTE - (sistema fuera de servicio) -El Ingeniero asignado deberá llegar al sitio de prestación del servicio dentro de las cuatro (4) horas siguientes a la solicitud de este, para problemas de hardware. O vía remota en un término de 30 minutos siguientes a la solicitud.

	GRAVE - (sistema gravemente debilitado) El Ingeniero asignado deberá llegar al sitio de prestación del servicio dentro del día hábil posterior a la solicitud de este, para problemas de hardware. NO CRÍTICA: El Ingeniero asignado deberá llegar al sitio de prestación del servicio a una hora mutuamente convenida con el supervisor del contrato (posterior al siguiente día hábil) después de la solicitud de servicio, para problemas de hardware.
3.4	El contratista debe realizar la atención y solución de eventos, incidentes y problemas que puedan afectar el funcionamiento del Datacenter mediante mano de obra especializada, que realice las actividades en el momento requerido.
3.5	El contratista debe mantener actualizado el software previa planificación y verificación de compatibilidad de los componentes de la arquitectura implementada frente a las actualizaciones requeridas a nivel de: ○ Herramientas de virtualización ○ Niveles de Firmware ○ Herramientas de monitoreo de los sistemas de almacenamientos, software y agentes de respaldo.
3.6	El contratista debe mantener actualizado a la última versión el software el ambiente virtual con su planificación y verificación de compatibilidad de los componentes de la arquitectura implementada frente a las actualizaciones expedidas por la casa matriz.
3.7	Brindar el soporte a los motores de bases de datos y servidores en caso de cambios o ventanas de mantenimiento que se llegue a necesitar.
3.8	El contratista dispondrá de un Ingeniero en sitio 3 días a la semana con horario de 8 a 12:00 horas.
3.9	El contratista dispondrá de un ingeniero en atención de soporte presencial o remoto para la solución de incidentes críticos o de urgencia.
3.10	El contratista realizara visitas al usuario final si es necesario.
3.11	El contratista brindara soporte y acompañamiento a los técnicos de Nivel 1 y Nivel 3 según sea el caso.
4.	**SEGURIDAD**
4.1	El contratista debe aplicar recomendaciones de seguridad que ofrece cada fabricante en el ambiente virtual VMWARE e infraestructura DELL (limitado a los servicios de hardware y software de la infraestructura que posee específicamente) de la DIGSA y de toda la infraestructura (para los equipos como firewall y router se realizaran recomendaciones, ya que DIGSA ya tiene contrato de soporte) del datacenter.
4.2	El contratista debe desarrollar la mejor estrategia para implementar las acciones que permitan mitigar las vulnerabilidades encontradas en la infraestructura de la DIGSA. Y entregar un informe quincenal sobre las acciones realizadas.
4.3	El contratista debe desarrollar un plan para realizar el seguimiento y hallazgo de nuevas vulnerabilidades.
4.4	El contratista debe implementar un software para realizar las siguientes actividades: ○ Monitoreo. ○ Monitoreo de vulnerabilidades y aplicación de parches.
4.5	El contratista debe entregar a la DIGSA las aplicaciones de la infraestructura tecnológica con el menor número de vulnerabilidades posibles.
4.6	El contratista debe entregar un reporte periódico de nuevas vulnerabilidades encontradas y acciones tomadas para éstas.
4.7	El contratista debe hacer sseguimiento al plan de pruebas de vulnerabilidades internas y externas en modelos de caja blanca y caja negra
4.8	El contratista debe realizar sseguimiento y control a la aplicación de parches y vulnerabilidades.
4.9	El contratista debe realizar junto con el supervisor del contrato un control de cambios para autorizar eliminación de máquinas duplicadas Linux.
4.10	El contratista debe eliminar de máquinas Linux duplicadas.
4.11	El contratista debe entregar un plan de seguridad para accesos remotos.
4.12	El contratista debe verificación la aplicación de los parches de seguridad.
4.13	El contratista debe implementar la mejor estrategia de actualización (parches en seguridad) en las diferentes aplicaciones para hacer el ambiente más seguro.
4.14	El contratista debe realizar el proceso de mejora para el plan de gestión sobre la norma 27000 SGSI que actualmente está en la entidad. Entregar hoja de ruta.

4.15	El contratista debe aplicar los controles de seguridad basado en la norma 27001 para el aseguramiento de la información basado en políticas y procesos del Data Center y entregar hoja de ruta.
5.	**INFORMES Y/O REPORTES**
5.1	El contratista debe entregar un inventario de la Infraestructura obsoleta con la que cuenta la Dirección General de Sanidad Militar.
5.2	El contratista debe entregar el reporte de los servidores que deben ser apagados y los que deben quedar en línea y operando.
5.3	El contratista debe presentar un Informe de la mejor opción costo/beneficio del funcionamiento en producción de cada aplicación de la DIGSA. (en sitio, o Ministerio de Defensa Nacional, o en nube).
5.4	En contratista debe entregar al supervisor un reporte de pruebas realizadas de conectividad en la DIGSA.
5.5	El contratista debe presentar un informe de fortalecimiento a través de la instalación de agentes de seguridad.
5.6	El contratista entregara al supervisor del contrato el reporte de máquinas actualizadas satisfactoriamente.
5.7	El contratista debe entregar el reporte de máquinas que no fueron posible ser actualizadas con posibles causas.
5.8	El contratista debe entregar al contratista un reporte ingresos remotos que se tengan en al DIGSA.
5.9	El contratista debe entregar un reporte al supervisor de lo siguiente: ○ Máquinas duplicadas y borradas. ○ Borrado de máquinas no usadas y borradas. ○ Borrado de snapshot no usables y borrados.
5.10	El contratista entregara a la DIGSA un reporte de licencias que componen el ambiente virtual de la DIGSA incluyendo versiones instaladas.
5.11	El contratista debe entregar al supervisor un reporte de las maquinas que se puedan actualizar.
5.12	El contratista entregara un reporte de las mejores opciones de seguridad implementadas para la infraestructura de la DIGSA.
5.13	El contratista entregara al supervisor reporte y/o documento de fechas de vencimiento, actualización y renovación, de licenciamiento de la Infraestructura tecnológica de la DIGSA.
5.14	El contratista debe entregar al supervisor un reporte, plan de seguimiento y hoja de ruta para la aplicación de la norma ISO 27001, al interior de la entidad.
5.15	El contratista entregara informes de gestión.
5.16	El contratista entregara la documentación de las mejoras a la infraestructura de la DIGSA.
5.17	El contratista entregara un documento de la aplicación de las normas de seguridad SGSI que se realizó a la infraestructura de la DIGSA.
5.18	El contratista entregara un documento de los afinamientos realizados a los servidores y de los equipos de comunicaciones.
5.19	El contratista debe realizar estudio técnico y documentar los servidores que deben ser apagados.
5.20	El contratista debe hacer seguimiento y recomendaciones a la DIGSA sobre los fabricantes para las actualizaciones de BIOS, firmware y parches a los sistemas operativos de la infraestructura tecnológica de la DIGSA.
5.21	El contratista debe entregar el documento actualizado de los procesos de seguridad de la información y el data center.
5.22	El contratista debe entregar a la DIGSA la documentación de relacionada con la configuración IPV6 de lo siguiente: ○ Inventarios. ○ Planes. ○ Configuración aplicada. ○ Pendientes y sus causas.
5.23	El contratista hará transferencia del conocimiento escalamiento, resolución de incidentes y soporte al interior del grupo SISAM.
5.24	El contratista debe entregar informes de la gestión de monitoreo e incidentes nivel 2 realizados, este informe será mensual.
6.	**MONITOREO INFRAESTRUCTURA**
6.1	El contratista debe realizar monitoreo suministrar una herramienta de monitoreo de la infraestructura tecnológica de la DIGSA.

6.2	El contratista debe realizar los ajustes y análisis bajo monitoreo de los servidores para preservar el funcionamiento.
6.3	El contratista debe entregar informes de los cambios y recursos monitoreados
6.4	El contratista hará transferencia de conocimiento en monitoreo de infraestructura al interior del grupo SISAM de la DIGSA.
7.	**GARANTÍA TÉCNICA**
7.1	Los bienes y servicios realizados por el contratista tendrán una garantía de seis (6) meses.
7.2	El contratista garantizará el cumplimiento de los requisitos técnicos exigidos, la correcta funcionabilidad de los servidores.
8.	**MANTENIMIENTO DE LOS SISTEMAS DE ALMACENAMIENTO**
8.1	Se debe realizar una depuración de logs temporales en previa coordinación con los administradores de los sistemas de información, servidores y equipos de almacenamiento de la DIGSA.
8.2	El contratista debe verificar los volúmenes presentados de los diferentes servidores del data-center de la DIGSA.
8.3	El contratista debe verificar físicamente el estado de los sistemas de almacenamiento, servidores con sus respectivos componentes con que cuenta la DIGSA.
9.	**TRANSFORMACIÓN DIGITAL**
9.1	Para la construcción y afinamiento de la hoja de ruta de la implementación de la transformación digital en salud de la DIGSA el contratista debe estudiar y comprender: **1.** Estrategia Nacional MinTIC (Plan de transformación Digital emitido por MinTIC2021) **2.** Estrategia del Ministerio de Defensa (PETI) **3.** Estrategia Institucional (PETI). **4.** Lineamientos y Políticas (Organización Panamericana de Salud y sus lineamientos en Transformación digital en Salud, entre otros).
9.2	Realizar la entrega del plan de transformación digital en Salud, construir junto con el supervisor del contrato los procedimientos impactados, la identificación de los interesados y el plan de comunicaciones y el plan de calidad. Entregar plan de comunicaciones y plan de calidad (La DIGSA debe adoptar actitud de innovación, rendimiento y cambios en sus procesos).
9.3	Realizar la evaluación del estado actual de la DIGSA, realizar el análisis de los procesos, las personas y la tecnología como pilares de la transformación digital. Identificando las brechas a partir del análisis realizado.
9.4	Realizar el estado de madurez de la transformación digital aplicando las herramientas diseñadas por MinTIC.
9.5	Realizar el mapa de calor y procesos claves aplicando la herramienta Digital Shift diseñadas por MinTIC.
9.6	Construir y evaluar junto con el supervisor del contrato el estado actual y medir el índice de madurez digital de la DIGSA.
9.7	Realizar la identificación de brechas, desafíos y oportunidades.
9.8	Elaborar la visión de la transformación digital en Salud de DIGSA, junto con el supervisor del contrato y consolidarla con los interesados.
9.9	Elabora la línea base y destino de la transformación digital DIGSA acorde a la visión y analizando los dominios de arquitectura. Entrega de informe línea base y destino de la transformación digital en salud.
9.10	Diseñar el Plan para la Transformación Digital en Salud de la DIGSA, incluye la estrategia de la transformación digital DIGSA, con su conjunto de proyectos y hoja de ruta de implementación. Entrega de informe detallado con cronograma de ejecución.
9.11	Realizar transferencia de conocimiento de todo lo realizado en transformación Digital en salud.

EQUIPO DE TRABAJO REQUERIDO: El contratista debe proveer en la propuesta las hojas de vida y con las siguientes certificaciones mínimo.

EQUIPO DE TRABAJO REQUERIDO.

El oferente deberá garantizar el personal suficiente, idóneo y necesario para la completa ejecución del objeto del contrato, sin que esto genere costo adicional alguno para la Dirección General de Sanidad Militar.

A. EL PROPONENTE DEBE CONTAR CON TRES (3) INGENIEROS DE SISTEMAS O ELÉCTRICOS O ELECTRÓNICOS O DE TELECOMUNICACIONES, ESPECIALIZADO O MAESTRIA EN SEGURIDAD DE LA INFORMACIÓN Y/O SEGURIDAD INFORMÁTICA Y/O GERENCIA DE PROYECTOS Y/O PROYECTOS INFORMÁTICOS

Todos los perfiles solicitados deberán aportar la siguiente documentación con el fin de acreditar su formación académica:

1. Formato diligenciado de Hoja de vida completo
2. Copia Acta de Grado y/o Diploma Profesional
3. Copia de la tarjeta profesional
4. Certificado de antecedentes disciplinarios expedido por COPNIA (reciente)
5. Certificados de experiencia laboral que acrediten lo solicitado
6. Diploma Especialización en Seguridad de la Información.

Garantizar que el personal solicitado debe contar cada uno con al menos tres (3) de las siguientes certificaciones:

- Symantec - Ultima Versión
- CISSP – Certified Information Systems Security Professional
- ISC2
- 2018 COBIT 5 Fundamentos o COBIT 2019
- ISACA – PeopleCert (ISACA) CISSP – Certified Information Systems Security Professional.
- 2016 ISO/IEC 27001 Foundation
- PECB
- 2016 Network Security Expert - NSE4
- 2015 Red Hat System Administration II - RHEL7 (RH134)
- 2015 Red Hat System Administration - RHEL7 (RH124)
- 2015 Building Security into your PHP Application- Red Hat System Administration II RHEL7 (RH134) BMind Red Hat System Administration - RHEL7 (RH124) BMind
- Zend Technologies- Red Hat System Administration II - RHEL7 (RH134) BMind Red Hat System Administration - RHEL7 (RH124) BMind
- 2014 QualysGuard Certified Specialist
- QualysGuard2014 CEH
- Certified Ethical Hacker EC-Council
- IT Forensic 2011 - Certified Ethical Hacker EC- Council
- Asterisk Training Special Edition Net Security se acepta de los últimos 3 Años
- SharePoint 2019, 2016
- SQL Server 2019, 2016, - Microsoft Certified Tecnology Specialist MCTS SQL 2005 Certificacion Number C427-3942
- Reporting Services, - Microsoft Certified Tecnology Specialist MCTS SQL 2005 Certificacion Number C427-3942
- SQL Server Analytics Services - Business Intelligence - Microsoft Certified Tecnology Specialist MCTS SQL 2005 Certificacion Number C427-3942
- Team Foundation, MSF
- Herramientas de Desarrollo Jscript,
- Windows Server - AZ 900: Microsoft Azure fundamental ,AZ-304: Microsoft Azure architect design
- Core (Active Directory, Dns, Dhcp)
- Windows 10, 8, 7, Vista, XP, 2000 y anteriores
- Linux, RedHat, Suse, Mandrake, Ubuntu, Fedora, CentOS. Red Hat System Administration II - RHEL7 (RH134) BMind Red Hat System Administration - RHEL7 (RH124) BMind –
- Jscript, Java, Visual Studio .net 2018 - Red Hat System Administration II - RHEL7 (RH134) BMind Red Hat System Administration - RHEL7 (RH124) BMind –
- Certificación Ipv6 avanzado LACNIC
- Certificación en red LAN de fabricante con representation en Colombia
- Certificación Vmware VCP
- Certificación Instalación Sistemas hiperconvergentes, debe ser emitida por el fabricante DELL.

B. El proponente debe contar con dos (2) INGENIEROS DE SISTEMAS O ELÉCTRICOS O ELECTRÓNICOS O DE TELECOMUNICACIONES, INDUSTRIAL O MECATRÓNICO.

Experto en Arquitecto Empresarial Líder: Cantidad: Uno (1)

- Posgrado (especialización o maestría) en cualquier especialidad de TI.
- Certificación Togaf Nivel 2.

- 10 años de Experiencia profesional certificada en Tecnología de la Información, o arquitectura empresarial.
- Dos (2) proyectos de arquitectura empresarial usando TOGAF y dos (2) proyectos para la definición o construcción de Planes estratégicos de tecnologías de la información.

Asesor en transformación Digital en Salud: uno (1)

- Especializado o maestría en seguridad de la información y/o seguridad informática
- Mínimo 7 años de experiencia profesional certificada de tecnología de la información o arquitectura empresarial.
- Participación en su rol en dos (2) proyectos de transformación digital, y que uno de ellos esté relacionado con temas de servicios de salud.

LO NO MODIFICADO EN ESTA ADENDA QUEDA INCOLUME

FIRMADO ELECTRONICAMENTE
EN EL SECOP II