TÉRMINO DE REFERENCIA

Objeto de Contratación: Contratación de servicio de Cloud C3-RRAA

Código del proceso: EC-INEC-410594-NC-RFB

Fecha: 5-11-2024

A. DATOS GENERALES

1. Plazo de Ejecución:

Ejecución del Contrato inicia: A partir del día siguiente a la suscripción del contrato distribuido de la siguiente manera:

- Hasta 15 días calendario plazo para la configuración
- 593 días calendario plazo a partir de la aceptación de la entrega de la configuración del servicio

2. Vigencia de la Oferta: 90 días calendario

3. Forma y cronograma de entregas:

ENTREGA	PLAZO DE EJECUCIÓN	DESCRIPCIÓN	FORMA DE ENTREGA	PRESUPUESTO
TOTAL	15 días calendario plazo a partir del siguiente día de la suscripción del contrato.	Configuración.	Única, conforme plazo de ejecución	Inversión
PARCIAL	593 días calendario plazo a partir de la aceptación de la entrega de la configuración del servicio	Servicio de Cloud	Mensual	Inversión

4. Presupuesto Referencial y formas de Pago

4.1 Formas de Pago

4.2 Pago contra entrega recepción: CONFIGURACIÓN.

El Instituto Nacional de Estadística y Censos se compromete a pagar el 100% del valor total de los servicios de configuración, previa suscripción del Acta Entrega recepción del SERVICIO DE CONFIGURACIÓN, informe de aceptación y presentación de la factura correspondiente.

4. 3Pagos mensuales:

El Instituto Nacional de Estadística y Censos se compromete a pagar el SERVICIO DE CLOUD, mensualmente a la entrega recepción del servicio efectivamente recibido, previo informe pertinente del administrador del contrato, acta entrega recepción parcial y para el pago final obligatoriamente el acta entrega recepción definitiva, presentando para cada pago la factura correspondiente.

Los servicios se habilitarán en función de las necesidades del INEC, en base a lo cual se procederá a emitir la factura, para el pago correspondiente.

5. Tipo de presupuesto:

Inversión para (configuración, servicios)

- ✓ **Nombre del proyecto:** "Robustecimiento de la Producción Estadística del Ecuador" CUP No. 31210000.0000.388017– Componente 3

B. REQUERIMIENTO DE LA CONTRATACIÓN:

1. Antecedentes:

La producción estadística nacional, constituye la función principal del INEC y, como organismo rector del Sistema Estadístico Nacional (SEN), tiene por labor establecer las directrices, adquirir la infraestructura y las capacidades humanas, logísticas necesarias y acordes a las mejores prácticas para institucionalizar, priorizar y fortalecer esta responsabilidad. Al mismo tiempo, esta responsabilidad, se encuentra alineada al Plan Nacional de Desarrollo El Nuevo Ecuador, del país. De ahí, que el desarrollo e implementación de esta premisa, que fundamenta los objetivos estratégicos del INEC, requiere de una infraestructura tecnológica escalable, estandarizada, robusta, capaz de responder a los diferentes lineamientos de cada proyecto de investigación estadística (nacional, sectorial y espacial mediante cartografías), de estudio analítico y de mejoramiento institucional. El INEC tiene entre sus responsabilidades la de "Coordinar el levantamiento en campo y procesamiento de censos y encuestas dentro de todo el territorio nacional".

El 20 de diciembre del 2021, mediante el Programa Nacional de Estadística aprobado por el Consejo Nacional de Estadística y Censos -CONEC-, se dispone como un objetivo estratégico

"Ser eficientes, asegurando la pertinencia, comparabilidad y continuidad de la información estadística, a partir del fortalecimiento de la infraestructura técnica y tecnológica para atender las necesidades de la planificación del desarrollo."

Con documento 102-2022-BM-LC6-EC de fecha 1 de julio de 2022, se notifica al Ministerio de Economía y Finanzas que el Directorio Ejecutivo del Banco Internacional de Reconstrucción y Fomento (BIRF) ha aprobado un Préstamo a la República del Ecuador para el Proyecto "Fortalecimiento del Sistema Estadístico del Ecuador" por un monto de US$80,0 millones, el 30 de junio de 2022, el cual será efectivo mediante la firma de un acuerdo de préstamo entre el INEC y Banco Mundial para lo cual el INEC debe cumplir con las condiciones de firma y efectividad.

Mediante Oficio Nro. SNP-SNP-SGP-2022-0111-O, de fecha 14 de septiembre de 2022 la Secretaría Nacional de Planificación emite el dictamen de prioridad al Proyecto: "Robustecimiento de la Producción Estadística del Ecuador", con CUP: 31210000.0000.388017, por el Período Agosto 2022 – Septiembre 2026.
Con oficio MEF-SP-2022-0982, la Subsecretaría de Presupuesto del Ministerio de Economía y Finanzas comunica al INEC que el Comité de Deuda y Financiamiento a través de RESOLUCIÓN CDF-RES-2022-011 del 7 de octubre de 2022, resolvió autorizar al Ministerio de Economía y Finanzas la contratación de endeudamiento a través del

Contrato de Préstamo que otorgaría el Banco Internacional de Reconstrucción y Fomento (BIRF) a la República del Ecuador, representada por el Ministerio de Economía y Finanzas, por hasta USD 80.000.000,00 para el financiamiento de proyectos de inversión en el marco del "Strengthening the National Statistical System in Ecuador Project" (Préstamo 9241-EC), contrato que se suscribe el 26 de octubre de 2022.

Mediante memorando Nro. INEC-INEC-2023-1057-M de 28 de diciembre de 2023, a través del cual se indica "(…) procede a aprobar el Plan de Dirección de Proyecto " C6 - Aprovechamiento de Registros Administrativos para la Producción Estadística" 2024; en el marco de lo que dispone la Resolución No. 021-DIREJ-DIJU NI-2017 de 19 de mayo de 2017 y su reforma emitida en Resolución No. 024-DIREJ DIJU-NI-2023 de 06 de junio de 2023, a fin de que prosigan con el trámite respectivo, en el ámbito de sus competencias de acuerdo a la normativa y más disposiciones emitidas para el efecto (…)".

Mediante correo electrónico de fecha 4 de mayo de 2024, Alejandro Medina Giopp, indica al señor José Pinto, Coordinador del Proyecto PMU, lo siguiente: *(…) Hemos recibido el borrador del Plan de Adquisiciones (PA) del proyecto anteriormente mencionado, enviado al Banco el 2024/05/02. Sobre la base de la información proporcionada, el Banco no tiene objeción a las actividades marcadas como "Aprobada" en el Plan de Adquisiciones (…)*

Con memorando Nro. INEC-DIPLA-2024-0509-M con fecha 28 de junio de 2024, la Dirección de Planificación y Gestión Estratégica, socializa la Programación Anual de la Planificación al 28 de junio de 2024", en la que consta la presente contratación.
Con memorando INEC-DITIC-2024-0279-M, de fecha 17 de mayo de 2024, la Dirección de Tecnologías de la Información y Comunicación solicita a la Dirección Ejecutiva la aprobación del Plan Estratégico de Tecnologías de la Información –PETI.

Con memorando Nro. INEC-INEC-2024-0226-M de fecha 20 de mayo de 2024 la Dirección Ejecutiva aprueba el Plan Estratégico de Tecnologías de la Información –PETI, donde consta la presente contratación.

2. OBJETO DE LA CONTRATACIÓN

2.1 Objetivo General

Robustecer la infraestructura tecnológica y la capacidad estadística del INEC en la producción, difusión de estadísticas económicas, sociodemográficas, ambientales y de registros administrativos oportunas y de alta calidad para la formulación de políticas públicas basadas en evidencia.

2.2 Objetivo Especifico

Contratar el Servicio de Cloud C3-RRAA que permita contar con infraestructura para almacenamiento y memoria en un Centro de Datos en la nube garantizando la disponibilidad de los servicios que ofrece el INEC, cumpliendo con normativa vigente y permitiendo disponer de recursos de forma flexible y dinámica para migrar y alojar aplicativos nuevos y actualizaciones, el portal web institucional, además del IDE – Geoportal Estadístico; servicios que brinda la institución.

3. ALCANCE

Disponer de los servicios de nube con un pool de recursos técnicos necesarios para los servidores virtuales y almacenamiento en nube para los aplicativos del INEC, en las que puedan ser administradas, con el fin de garantizar la disponibilidad de los servicios implementados y soporte el número de accesos concurrentes al producto de Software sin afectar el rendimiento y funcionabilidad del mismo.

4. INFORMACIÓN QUE DISPONE LA ENTIDAD

No aplica

5. SERVICIO ESPERADO

Los servicios **deben** cumplir con lo requerido en las siguientes características técnicas:

1	CONDICIONES GENERALES
1.1	El proveedor debe ser distribuidor autorizado de los servicios ofertados. El oferente deberá presentar certificado emitido por el fabricante.
1.2	El oferente deberá tener la especialización de implementación y migración en el servicio de nube pública ofertado.
1.3	El servicio de respaldo y recuperación ante desastres deberá alojarse en una nube pública que cuente con al menos con las certificaciones: CSA STAR de nivel 2, ISO 9001:2015, 27001, 27017, 27018, 27701 y SOC 1,2,3.
1.4	El proveedor deberá entregar un Data Center Virtual (DCV) o servicio de nube pública bajo la modalidad de Infraestructura como Servicio (IaaS) y/o Plataforma como Servicio (PaaS) y/o software como servicio.
1.5	El Data Center Virtual (DCV) o servicio de nube pública deberá contar un pool o plantillas de recursos (memoria, procesamiento, almacenamiento), cuya configuración y administración esté bajo responsabilidad del INEC con los accesos respectivos y previa comunicación al proveedor.
1.6	Los recursos contratados en el Data Center Virtual (DCV) o servicio de nube pública deberán ser entregados por el Proveedor según requerimientos del INEC.
1.7	El Data Center Virtual (DCV) o servicio de nube pública deberá incorporar un nivel básico de seguridad que permita bloqueo de puerto según necesidad del INEC.
1.8	El proveedor deberá ofrecer los servicios de IaaS y PaaS en modalidad pago por uso por medio de internet, con la finalidad que el INEC pueda contratar en función de su necesidad, previo acuerdo técnico y comercial entre las partes.
1.9	El proveedor deberá desplegar los servicios contratados con el fin de estar disponibles y listos para las configuraciones de los respectivos aplicativos, firewall, bases de datos y sistemas web en base a la arquitectura indicada por el INEC.
2	**CARACTERÍSTICAS DEL SERVICIO DE SEGURIDAD PERIMETRAL**
2.1	El servicio de seguridad perimetral debe realizarse con un Firewall de siguiente generación (NGFW), en modalidad Virtual.
2.2	El proveedor deberá incluir en su oferta las siguientes capacidades de cómputo para un Security Network Virtual Appliance: vCPU: 4 RAM: 16 GB

	Storage: 60 GB de almacenamiento SSD
2.3	La administración del servicio de seguridad perimetral debe ser desde una consola web centralizada, donde podrá realizarse todas las configuraciones necesarias.
2.4	El Equipo virtual de seguridad perimetral debe contar con al menos las siguientes características: **Acceso Remoto:** Soporte para la creación de VPNs tipo IPSec y client to site. Estas VPNs deberán ser soportadas nativamente, de forma que no limiten a la institución su creación y no dependan de un licenciamiento activo. **Registro de navegación:** Registro completo y reportes de seguridad de la red. **Network Address Traslation (NATs):** Deberá tener la capacidad de realizar NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla. **Calidad de Servicio:** Deberá realizar QoS (calidad de servicio) en páginas web, reglas de firewall y aplicaciones. **Filtrado de direcciones URL:** Filtrar en base a direcciones configurables por categorías y manejo de reputación. **Registro de navegación:** Registro completo y reportes de seguridad de la red. **Filtrado de URL:** - Deberá precisar las categorías y clasificaciones de riesgo. - Analizará el contenido URL, mediante el aprendizaje automático con análisis estático y dinámico. - Clasificará las direcciones URL en categorías benignas y malintencionadas para el control total del tráfico web. - Deberá detectar direcciones URL malintencionadas recién categorizadas para bloquearlas inmediatamente sin necesidad de intervención de los administradores. **Carga y Descarga de archivos:** Deberá realizar el control de archivos con base a su tipo de extensión. **Filtrado P2P:** Al menos las siguientes aplicaciones: Ares, BitTorrent, Direct Connect, Gnutella, WinMX. **Antivirus y Malware:** Deberá contar con este servicio y adicionalmente permitir el acceso a la muestra del malware original mediante la descarga de dicho malware o a través de paquetes capturados (PCAP) para su análisis. **Anti-phishing:** La solución ofertada debe incluir protección contra ataques de Phishing.

	Servicio de anti-bot: Deberá proveer una herramienta que haga descubrimiento de bots dentro de la red institucional. Esta herramienta deberá bloquear la comunicación que intenten establecer los bots con los atacantes. **Análisis de enlaces:** Deberá analizar HTTP/HTTPS contenidos en mensajes de correos electrónicos de tipo SMTP y POP3. **Creación de reglas de acceso:** Reglas basadas en usuarios, grupos y horarios. **Control de aplicaciones:** Reconocimiento y control de tráfico en capa 7 de forma nativa, es decir que no dependa de un licenciamiento activo. **Protección en la nube:** Deberá contar con el servicio de Sandboxing. **Firmas de seguridad:** Deberá contar con firmas que bloquee vulnerabilidades conocidas como malware , comandos y controles. **Inspección de tráfico:** - Deberá inspeccionar todo tipo de tráfico en busca de amenazas independiente del puerto, protocolo o cifrado. - Deberá incluir la capacidad de CDR (Content Disarm and Reconstruction) u otras tecnologías de detección de amenazas como Dynamic unpacking, Machine learning, URL crawling, que le permitan ser eficiente en el control de amenazas desconocidas. - Deberá permitir que, como resultado de la emulación, se entregue un reporte (online o en video o mediante un PDF o a través de la misma plataforma de administración) con los hallazgos explotados. **Reportería:** Reportes para visualizar la cantidad de amenazas detectadas y mitigadas de los dispositivos comprometidos en la red de datos institucional. **Protección IPS:** Deberá detectar, bloquear ataques de red y de aplicaciones, protegiendo al menos los siguientes servicios DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP. **Actualización de firmas:** La actualización debe realizarse de forma automática. **Protección de ataques:** Detección de DOS, DDOS, Portscan, Gusanos y Flood. **Seguridad para VOZ IP:** Debe incluir seguridad para VOZ IP. **SDWAN:** Debe contar con este servicio. **DLP:** Debe contar con este servicio.
2.5	El soporte del PROVEEDOR para el servicio de seguridad perimetral ofertado deberá ser soporte especializado en modalidad 8x5 para la atención de requerimientos e incidentes de acuerdo al SLA establecido el cual deberá ajustarse a la zona horaria del país (Ecuador Continental), en idioma español.

<table>
<tr><td>2.6</td><td>El PROVEEDOR debe notificar quién será la persona asignada para la atención del requerimiento abierto por INEC.</td></tr>
<tr><td>2.7</td><td>La asistencia para atención a los casos, y soporte se estipula de acuerdo al siguiente horario:

Lunes a viernes, las 8 horas del día (horario 8 x 5), incluyendo los días feriados.

<table>
<tr><th>Categoría</th><th>Severidad</th><th>Tiempo Max. respuesta telefónica o correo electrónico</th><th>Tiempo Max. Asistencia diagnóstico y neutralización</th></tr>
<tr><td>1</td><td>ALTA</td><td>1 hora.</td><td>4 horas</td></tr>
<tr><td>2</td><td>MEDIA</td><td>2 horas</td><td>8 horas</td></tr>
<tr><td>3</td><td>BAJA</td><td>72 horas</td><td>N/A</td></tr>
</table>

ALTA: Pérdida Total de los servicios

MEDIA: Pérdida parcial de los servicios

BAJA: Consultas y solicitudes de configuración</td></tr>
<tr><td>3</td><td>CARACTERÍSTICAS DEL SERVICIO DE NUBE PÚBLICA O DATA CENTER VIRTUAL</td></tr>
<tr><td></td><td>El proveedor deberá incluir en su oferta las siguientes capacidades de cómputo:

<table>
<tr><th rowspan="2">REQUERIMIENTO</th><th colspan="2">VCPU</th><th rowspan="2">RAM GB</th><th rowspan="2">ALMACENAMIENTO GB</th></tr>
<tr><th>LINUX</th><th>WINDOWS</th></tr>
<tr><td>DESARROLLO</td><td>112</td><td></td><td>155</td><td>809</td></tr>
<tr><td>PORTAL WEB + SEGURIDAD</td><td>110</td><td>42</td><td>242</td><td>6947</td></tr>
<tr><td>IDE CARTOGRAFICO</td><td>36</td><td></td><td>122</td><td>1670</td></tr>
<tr><td>SUBTOTAL</td><td>258</td><td>42</td><td>519</td><td>9426</td></tr>
<tr><td>CRECIMIENTO 10% ANUAL</td><td>26</td><td>4</td><td>52</td><td>943</td></tr>
<tr><td>TOTAL</td><td>284</td><td>46</td><td>571</td><td>10369</td></tr>
</table></td></tr>
<tr><td>3.2</td><td>El proveedor deberá incluir en su oferta un servicio administrado de copia de seguridad (respaldo) y recuperación ante desastre del ambiente Portal Web con una capacidad de almacenamiento de 5,729 GB con crecimiento anual del 10 %</td></tr>
<tr><td>3.3</td><td>El proveedor deberá incluir en su oferta un servicio administrado de balanceador de carga definido por software con las siguientes capacidades: 30 reglas de redireccionamiento, 1,204 GB de datos procesados de entrada y salida mensual.</td></tr>
</table>

<table>
<tr><td>3.4</td><td>El proveedor deberá incluir en su oferta un servicio administrado de firewall de aplicaciones con las siguientes capacidades: 2 políticas, 12 reglas y 1,000,000 de solicitudes entrantes HTTP procesadas mensualmente.</td></tr>
<tr><td>3.5</td><td>El proveedor deberá incluir en su oferta un servicio administrado de VPN con 2 túneles</td></tr>
<tr><td>3.6</td><td>El proveedor deberá incluir en su oferta un tráfico de salida (internet egress) de 1,024 GB mensual.</td></tr>
<tr><td>3.7</td><td>El proveedor deberá incluir en su oferta soporte del fabricante de la nube pública ofertada en horario de 8 horas al día, 5 días a la semana para el servicio administrado de infraestructura de los servicios nativos de nube pública.</td></tr>
<tr><td>3.8</td><td>El proveedor deberá incluir en su oferta soporte bajo demanda. El servicio se deberá brindar 8 horas al día, 5 días a la semana en español con el siguiente acuerdo de nivel de servicio (SLA):</td></tr>
<tr><td>3.9</td><td>
<table>
<tr><th>Prioridad</th><th>Descripción</th><th>8X5</th></tr>
<tr><td>Critica</td><td>Casos que impiden el normal funcionamiento de la aplicación en forma total o parcial y que impliquen la imposibilidad de acceder a los servicios</td><td>Primera respuesta: 1 hora</td></tr>
<tr><td>Alta</td><td>Casos que impiden el normal funcionamiento de la infraestructura que impacte directamente sobre actividades core de la operación</td><td>Primera respuesta: 2 hora</td></tr>
<tr><td>Media</td><td>Casos que impiden el normal funcionamiento de la infraestructura que impacte sobre actividades consideradas no criticas</td><td>Primera respuesta: 3 hora</td></tr>
<tr><td>Baja</td><td>Casos que impiden el normal funcionamiento de opciones de generación de reportes o consultas que impacten sobre actividades consideradas no criticas tales como consultas o reportes de movimientos contable o presupuestos.</td><td>Primera respuesta: 4 hora</td></tr>
</table>
</td></tr>
<tr><td>3.10</td><td>El proveedor deberá incluir en su oferta una inducción para hasta 5 personas. Incluir el temario y duración de la inducción</td></tr>
<tr><td>3.11</td><td>El proveedor deberá ofrecer el servicio de cómputo (máquinas virtuales) en modalidad Infraestructura como Servicio (IaaS)</td></tr>
<tr><td></td><td>El servicio de cómputo deberá ofrecer imágenes preconfiguradas con sistemas operativos Linux sin necesidad de un marketplace.</td></tr>
<tr><td></td><td>“El servicio de cómputo deberá ajustarse a las cargas de trabajo que el INEC requiera desplegar.</td></tr>
</table>

	El proveedor deberá garantizar que durante un evento de mantenimiento planificado en el hardware de una instancia de máquina virtual se realice una migración en vivo de la VM a otro host sin interrumpir la carga de trabajo, reiniciar la VM ni modificar ninguna de sus propiedades.
3.12	El servicio de cómputo debe permitir el cifrado en reposo, en tránsito y en uso de los datos.
3.13	El servicio de cómputo debe supervisar el uso de CPU y memoria de las máquinas virtuales en ejecución y hacer recomendaciones de optimización de uso de recursos.
3.14	El servicio de cómputo deberá permitir iniciar y detener las máquinas virtuales de manera automática y programada.
3.15	Las máquinas virtuales del servicio de cómputo deben soportar almacenamiento en bloque con discos en formato HDD y SSD
3.16	El servicio de copias de seguridad (respaldo) y recuperación ante desastres deberá soportar utilizar instantáneas para realizar copias de seguridad incrementales de los datos de los discos persistentes a nivel de instancia de máquina virtual.
3.17	El servicio de copias de seguridad (respaldo) y recuperación ante desastres deberá soportar montar el respaldo en una instancia existente, crear una nueva instancia o restaurar los discos de la instancia.
3.18	El servicio de balanceo de carga deberá ser completamente distribuido, definido por software y administrado.
3.19	El servicio de balanceo de carga deberá escalar a medida que aumentan la cantidad de usuarios y el tráfico además el ajuste de escala automático no debe requerir preparación previa.
3.30	El servicio de balanceo de carga deberá ser basado en la capa 7 para agregar decisiones de enrutamiento de solicitudes en función de atributos, como el encabezado HTTP y el identificador uniforme de recursos.
3.21	El servicio administrado de firewall de aplicaciones deberá proteger contra varios tipos de amenazas, incluidos los ataques de denegación de servicio distribuido (DSD) y los ataques de aplicaciones, como las secuencias de comandos entre sitios (XSS) y la inserción de SQL (SQLi).
3.22	El servicio administrado de firewall de aplicaciones deberá permitir configurar políticas de seguridad de forma manual, con acciones y condiciones de coincidencia.
3.23	El servicio administrado de firewall de aplicaciones deberá incluir reglas preconfiguradas con decenas de firmas que se compilan a partir de estándares de la industria de código abierto para ayudar a mitigar los 10 riesgos principales de OWASP.

3.24	El proveedor deberá incluir el servicio de Virtual Private Network (VPN) gestionado mediante una conexión IPsec entre el entorno local y la nube pública.
3.25	El servicio gestionado de VPN deberá permitir una disponibilidad o uptime mensual mayor o igual a 99,9%.
	El proveedor deberá proporcionar un servicio de Virtual Network que abarcan varias zonas de disponibilidad.
	El proveedor deberá permitir el acceso a las máquinas virtuales a través de un mecanismo seguro mediante HTTPS"
3.26	El servicio de nube deberá permitir la gestión de identidades y accesos para adoptar el principio de seguridad de privilegio mínimo.
3.27	El proveedor deberá ofrecer un servicio de gestión de acceso e identidades que permita otorgar accesos detallados a recursos específicos.
3.28	El servicio de gestión de acceso e identidades deberá soportar la configuración de roles predefinidos y personalizados
3.29	El servicio de gestión de acceso e identidades deberá permitir registros de auditoría de la actividad del administrador y de acceso a los datos

C. CRITERIOS DE CALIFICACION

1. Evaluación de criterios mínimos pasa/no pasa

PARÁMETRO	PASA	NO PASA
Presentación de Formularios		
Especificaciones Técnicas		
Capacidad Financiera		
Experiencia y Capacidad Técnica		
Experiencia especifica del proveedor		
Requisitos Adicionales		
Precio más bajo		

D. INFORMACION PARA LA CALIFICACIÓN

La Oferta deberá contener los Formularios que se especifican en el Pliego SDO.

Asimismo, deberán presentar fotocopias simples de los siguientes documentos:

- Nombramiento del Representante Legal de la empresa licitante, con facultades para presentar ofertas y suscribir contratos, registrado en la Superintendicia de Compañias.
- Cédula de identidad del Representante Legal.

Capacidad financiera:

Los Licitantes, mediante la presentación de estados financieros correspondientes a los últimos tres (3) años debidamente registrados en la Superintendencia de Compañías.

Experiencia Específica y capacidad técnica:

El Licitante deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de experiencia y capacidad técnica por el Total de la oferta:

- Demostrar mediante copias de contratos, facturas y/o otros documentos legales, haber realizado servicios del mismo tipo y alcance en los últimos ocho años y detalles de los servicios que está prestando actualmente, señalando nombres y direcciones de clientes que puedan contactarse para obtener más información sobre esos contratos.
- Haber ejecutado al menos dos contratos de características similares al objeto de la contratación durante los últimos 5 años suscrito y que sea de mínimo $ 163.500,00 (Ciento sesenta y tres mil quinientos 00/100 dólares americanos) valor que no incluye IVA.

1.1. Cumplimiento de Términos de Referencia

Los oferentes deberá presentar su oferta con todas las características técnicas detallado en las especificaciones técnicas. Para cada ítem o característica solicitada, el proveedor deberá: Adjuntar e indicar y subrayar la página y texto del servicio, donde se pueda verificar lo solicitado, y/o en su defecto adjuntar documentación de respaldo, según corresponda. En idioma español.

1.2. Personal Técnico Clave mínimo

Personal Técnico:

Datos necesarios para el registro del Personal Técnico Mínimo:

- ✓ Función de la Persona: Gerente de Proyecto
  - Nivel de Estudio: Tercer Nivel con título
  - Titulación académica: Ingeniero o Tecnólogo en informática, electrónica, redes y telecomunicaciones Sistemas, Electrónica y Control, Electrónica, Mecánico, Telecomunicaciones, Eléctrico, Sistemas, Redes, Electrónica automatización y Control, Electrónica y Telecomunicaciones, Tecnología de la Información
  - Cantidad: 1
  - Certificado: Deberá presentar un certificado vigente PMP y/o ITIL

- ✓ Función de la Persona: Técnico arquitecto de Nube

- Nivel de Estudio: Tercer Nivel con título
- Titulación académica: Ingeniero o Tecnólogo en informática, electrónica, redes y telecomunicaciones, Electrónica y Control, Electrónica, Mecánico, Telecomunicaciones, Eléctrico, Sistemas, Redes, Electrónica automatización y Control, Electrónica y Telecomunicaciones, Tecnología de la Información
- Cantidad: 1
- Certificado: Deberá presentar una certificación de arquitecto de nube de la marca ofertada

✓ Función de la Persona: Técnico de seguridad de Nube

- Nivel de Estudio: Tercer Nivel con título
- Titulación académica: Ingeniero o Tecnólogo en informática, electrónica, redes y telecomunicaciones, Electrónica y Control, Electrónica, Mecánico, Telecomunicaciones, Eléctrico, Sistemas, Redes, Electrónica automatización y Control, Electrónica y Telecomunicaciones, Tecnología de la Información
- Cantidad: 1
- Certificado: Deberá presentar una certificación de seguridad en nube de la marca ofertada

El nivel de estudios del personal técnico se validará con la presentación de la impresión del documento emitido por la Senescyt o copia del Título.

En el caso de que el personal técnico sea extranjero, se requerirá que el titulo sea apostillado, para la firma del contrato.

1.3 Experiencia Mínima del Personal Técnico:

✓ **Gerente de Proyecto:** Dentro de los últimos 5 años deberá haber participado en dos proyectos tecnológicos, como Gerente de Proyecto, relacionados con el servicio de nube, para lo cual deberá presentar mínimo dos certificados u otros documentos que acredite la experiencia requerida en el cargo.

✓ **Técnico arquitecto de nube:** Dentro de los últimos 5 años deberá haber participado en dos proyectos que acredite experiencia y participación en proyectos relacionados con la arquitectura y/o configuración y/o implementación de soluciones nube de la marca ofertada, para lo cual deberá presentar al menos un certificado laboral que acredite la experiencia requerida.

✓ **Técnico de seguridad de nube:** Dentro de los últimos 5 años deberá haber participado en dos proyectos en donde acredite la experiencia y participación en proyectos relacionados con la configuración y/o implementación de soluciones de seguridad en nube de la marca ofertada, para lo cual deberá presentar al menos un certificado laboral que acredite la experiencia requerida.

1.4 **Otros requisitos**

- ✓ **Certificado de Distribuidor Autorizado, representante o vendedor autorizado:** El proveedor deberá entregar adjunto a la oferta el Certificado de ser un Distribuidor Autorizado o representante o vendedor autorizado para el Ecuador, el cual deberá ser emitido directamente por la marca de la nube ofertada.

2. GARANTIAS

En el caso de resultar ganador deberá presentar una Póliza de fiel cumplimento emitida por una compañía de seguros debidamente registrada en el país a favor del INEC de cobro inmediato o garantía bancaria por el valor del 5% del valor del contrato.

	Nombre:	**Cargo:**	**Firma:**
Elaborado por:	Luis Ávila Vaca	Responsable Gestión de Infraestructura de TI	Firmado electrónicamente por: LUIS EDUARDO AVILA VACA
Aprobado y Revisado por:	Carlos Rivas Recalde	Director de Tecnologías de la Información y Comunicación	Firmado electrónicamente por: CARLOS HUGO RIVAS RECALDE