CUADRO 001
DE ANÁLIS DE OFERTA
EC-INEC-410594-NC-RFB
CONTRATACIÓN DE SERVCIO DE CLOUD C3-RRAA

REQUISITOS MÍNIMOS		OFERTA No. 00
		WURSTA TECHNOLOGY ECUADOR S.A.
		RUC: 1793195642001
1. **INTEGRIDAD DE LA OFERTA**		PRESENTA/ NO PRESENTA/ACLARAR
FORMULARIOS SOLICITADOS	**FORMULARIO PRESENTADOS**	
1.1 Formulario Carta de la oferta	1.1 Formulario Carta de la oferta	PRESENTA
1.2 Formulario de información sobre el Licitante	1.2 Formulario de información sobre el Licitante	PRESENTA
1.3 Formulario de información para la Calificación	1.3 El formulario de información para la Calificación	PRESENTA
1.4 Información de los Servicios	1.4 Información de los Servicios	PRESENTA
1.5 Formulario Lista de Actividades con Precios	1.5 Formulario Lista de Actividades con Precios	PRESENTA
1.6 Declaración de Mantenimiento de Oferta	1.6 Declaración de Mantenimiento de Oferta Documento sin firma No se solicita aclaración puesto que presento estados financieros de 2 años y mínimo se requirió 3 años.	NO PRESENTA
Solicitado	***Ofertado***	
2. **SERVICIO REQUERIDO**	**SERVICIO OFERTADO**	PRESENTA

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, lo cual se validará con lo solicitado en la experiencia específica y capacidad técnica.
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	CONDICIONES GENERALES
1.1	El proveedor debe ser distribuidor autorizado de los servicios ofertados. El oferente deberá presentar certificado emitido por el fabricante. Se adjunta certificado emitido por el fabricante de ser distribuidor del servicio.
1.2	El oferente deberá tener la especialización de implementación y migración en el servicio de nube pública ofertado, lo cual se validará con lo solicitado en la experiencia específica y capacidad técnica. Se adjunta experiencias, así como el certificado de Premium Partner de Google Cloud.
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. Se adjuntan listado de certificaciones que cuenta la nube pública y link para verificación: https://cloud.google.com/security/compliance/offerings?hl=es-419
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.

1.8	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.		El servicio prestado será Google Cloud Platform que consiste en un conjunto de recursos de computación bajo demanda tales como infraestructura como servicio. (IaaS). Como se detalla en el documento Descripción General de Google Cloud – Acceder a los recursos a través de los servicios, pág 1.
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.	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. Se detalla en el documento Descripción General de Google Cloud en la parte Proyectos, pag 2.
2	**CARACTERÍSTICAS DEL SERVICIO DE SEGURIDAD PERIMETRAL**	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. Se entregará los recursos acorde a los requerimientos del INEC.
2.1	El servicio de seguridad perimetral debe realizarse con un Firewall de siguiente generación (NGFW), en modalidad Virtual.	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. Se adjunta documento Descripción General de Seguridad
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	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. El servicio que se propone es un servicio IaaS y PasS bajo demanda.
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.		

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. Se cumplirá con lo solicitado 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. Google Cloud ofrece un sólido servicio de firewall de siguiente generación (NGFW) que se integra de forma nativa con su infraestructura. Este servicio, conocido como Cloud NGFW, proporciona una capa de seguridad avanzada para proteger tus cargas de trabajo en la nube.
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 La nube de Google cuenta con infraestructura confiable y de alto rendimiento, se puede realizar la configuración a 4 vCPU, 16 GB de RAM y 60 GB de SSD, este SNVA es capaz de ofrecer un alto nivel de seguridad de red. Como se indica en el documento Maquinas virtuales para todo tipo de trabajo.

	- 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.		2.3	La administración del servicio de seguridad perimetral debe ser desde una consola web centralizada, donde podrá realizarse todas las configuraciones necesarias. Se indica en el documento Why Google página 22.		
			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.		

	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.		- 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.		

<table>
<tr><td></td><td>SDWAN: Debe contar con este servicio.

DLP: Debe contar con este servicio.</td></tr>
<tr><td>2.5</td><td>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.</td></tr>
<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>Tien diagnó</th></tr>
<tr><td>1</td><td>ALTA</td><td>1 hora.</td><td></td></tr>
<tr><td>2</td><td>MEDIA</td><td>2 horas</td><td></td></tr>
<tr><td>3</td><td>BAJA</td><td>72 horas</td><td></td></tr>
</table>
ALTA: Pérdida Total de los servicios

MEDIA: Pérdida parcial de los servicios</td></tr>
</table>

<table>
<tr><td></td><td>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.</td></tr>
</table>

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

REQUERIMIENTO	VCPU		RAM GB	ALMACENAMIENTO GB
	LINUX	WINDOWS		
DESARROLLO	112		155	809
PORTAL WEB + SEGURIDAD	110	42	242	6947
IDE CARTOGRAFICO	36		122	1670
SUBTOTAL	**258**	**42**	**519**	**9426**
CRECIMIENTO 10% ANUAL	26	4	52	943
TOTAL	**284**	**46**	**571**	**10369**

3.2	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 %	
	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. El servicio planteado cumple con los requisitos que se han planteado entregando un equipo virtual de seguridad perimetral altamente sofisticado, capaz de proteger una red corporativa de una amplia gama de amenazas. Las características puedes ser revisadas en el documento Google Cloud Armor descripción.	
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. Se entregará un soporte premium que es 24/7, acorde al Instructivo de portal que se adjunta.	

3.3	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.
3.4	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.
3.5	El proveedor deberá incluir en su oferta un servicio administrado de VPN con 2 túneles
3.6	El proveedor deberá incluir en su oferta un tráfico de salida (internet egress) de 1,024 GB mensual.
3.7	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.
3.8	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):

3.9	Prioridad	Descripción	8X5
	Critica	Casos que impiden el normal funcionamiento de la aplicación en forma total o parcial y que impliquen la imposibilidad de acceder a los servicios	Primera respuesta: 1 hora

2.6	El PROVEEDOR debe notificar quién será la persona asignada para la atención del requerimiento abierto por INEC. La persona asignada para la atención del requerimiento será: Ing. Jose Michael Aviles Ramia, correo electrónico michael.aviles@wursta.com , teléfono: 0996018530. De igual manera en el Instructivo de portal se detalla cada uno de las personas que podrán dar asistencia técnica en cada etapa.
2.7	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.

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

ALTA: Pérdida Total de los servicios

MEDIA: Pérdida parcial de los servicios

BAJA: Consultas y solicitudes de configuración

	Alta	Casos que impiden el normal funcionamiento de la infraestructura que impacte directamente sobre actividades core de la operación	Primera respuesta: 2 hora
	Media	Casos que impiden el normal funcionamiento de la infraestructura que impacte sobre actividades consideradas no criticas	Primera respuesta: 3 hora
	Baja	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.	Primera respuesta: 4 hora
3.10	El proveedor deberá incluir en su oferta una inducción para hasta 5 personas. Incluir el temario y duración de la inducción		
3.11	El proveedor deberá ofrecer el servicio de cómputo (máquinas virtuales) en modalidad Infraestructura como Servicio (IaaS)		
	El servicio de cómputo deberá ofrecer imágenes preconfiguradas con sistemas operativos Linux sin necesidad de un marketplace.		
	"El servicio de cómputo deberá ajustarse a las cargas de trabajo que el INEC requiera desplegar.		
	El proveedor deberá garantizar que durante un evento de mantenimiento planificado en el hardware de una instancia de máquina virtual se realice		

Se detalla en el Instructivo de portal página 9.

3 CARACTERÍSTICAS DEL SERVICIO DE NUBE PÚBLICA O DATA CENTER VIRTUAL

El proveedor deberá incluir en su oferta las siguientes capacidades de cómputo:

REQUERIMIENTO	VCPU		RAM GB	ALMACENAMIENTO GB
	LINUX	WINDOWS		
DESARROLLO	112		155	809
PORTAL WEB + SEGURIDAD	110	42	242	6947
IDE CARTOGRAFICO	36		122	1670
SUBTOTAL	**258**	**42**	**519**	**9426**
CRECIMIENTO 10% ANUAL	26	4	52	943
TOTAL	**284**	**46**	**571**	**10369**

3.2 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 %

Se cumple con el requerimiento con el servicio administrado de copia de seguridad (respaldo) y recuperación ante desastre del

	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.

	ambiente Portal Web con una capacidad de almacenamiento de 5,729 GB con crecimiento anual del 10 %.
3.3	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. Google Cloud Platform (GCP) ofrece un servicio de balanceo de carga administrado llamado Cloud Load Balancing. Este servicio es altamente configurable y escalable, y puede adaptarse a una amplia variedad de cargas de trabajo. En el documento descripción carga de la nube puede evidenciar.
3.4	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. Se cumple con el requerimiento, Google Cloud Platform (GCP), es altamente configurables y escalables. Esto significa que los límites y capacidades exactas pueden variar según la configuración que se requiera.
3.5	El proveedor deberá incluir en su oferta un servicio administrado de VPN con 2 túneles Se cumple con el requerimiento, Google Cloud Platform (GCP) ofrece un servicio administrado de VPN con alta disponibilidad (HA) que te permite establecer conexiones seguras y redundantes entre tu red en la nube y otras redes.

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"

	Dos túneles: Cuando configuras una puerta de enlace de VPN con alta disponibilidad en GCP, se crean automáticamente dos túneles IPsec. Estos túneles proporcionan redundancia, lo que significa que si uno de los túneles falla, el tráfico se redirige automáticamente al otro túnel, asegurando la continuidad de tu conexión
3.6	El proveedor deberá incluir en su oferta un tráfico de salida (internet egress) de 1,024 GB mensual. Se contemplo para la presentación de los precios el tráfico de salida de 1,024 GB mensual.
3.7	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. Google Cloud Platform (GCP) proporciona soporte técnico para su infraestructura administrada en la nube 24/7.
3.8	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): Se cumple con el requerimiento de acuerdo de nivel de servicio (SLA): Conforme el siguiente link https://cloud.google.com/support?hl=es

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

3.9	**Prioridad**	**Descripción**	**8X5**
	Critica	Casos que impiden el normal funcionamiento de la aplicación en forma total o parcial y que impliquen la imposibilidad de acceder a los servicios	Primera respuesta: 1 hora
	Alta	Casos que impiden el normal funcionamiento de la infraestructura que impacte directamente sobre actividades core de la operación	Primera respuesta: 2 hora
	Media	Casos que impiden el normal funcionamiento de la infraestructura que impacte sobre actividades consideradas no criticas	Primera respuesta: 3 hora
	Baja	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.	Primera respuesta: 4 hora En el documento Customer Care _ Google Cloud se puede evidenciar los niveles de plazos de respuesta, para este caso se brindará la asistencia premium.
3.10	El proveedor deberá incluir en su oferta una inducción para hasta 5 personas. Incluir el temario y duración de la inducción		

		Nos compromentemos a dar una inducción hasta 5 personas, se incluye el temario y duración de la inducción en el documento Temario Inducción.		
	3.11	El proveedor deberá ofrecer el servicio de cómputo (máquinas virtuales) en modalidad Infraestructura como Servicio (IaaS) Nos compromentemos a dar una inducción hasta 5 personas, se incluye el temario y duración de la inducción en el documento Temario Inducción.		
		El servicio de cómputo deberá ofrecer imágenes preconfiguradas con sistemas operativos Linux sin necesidad de un marketplace. Se cumple con el requerimiento, acorde a la configuración premium que se entregara como servicio.		
		"El servicio de cómputo deberá ajustarse a las cargas de trabajo que el INEC requiera desplegar. Nos ajustaremos a las cargas de trabajo que el INEC requiera.		
		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.		

		Se garantizará la 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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	3.14	El servicio de cómputo deberá permitir iniciar y detener las máquinas virtuales de manera automática y programada. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	3.15	Las máquinas virtuales del servicio de cómputo deben soportar almacenamiento en bloque con discos en formato HDD y SSD Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		

	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	3.18	El servicio de balanceo de carga deberá ser completamente distribuido, definido por software y administrado. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		

	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	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). Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		
	3.22	El servicio administrado de firewall de aplicaciones deberá permitir configurar políticas de seguridad de forma manual, con acciones y condiciones de coincidencia. Se cumple con el requerimiento, en el documento Descripción General de Google.		
	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.		

	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. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.
	3.25	El servicio gestionado de VPN deberá permitir una disponibilidad o uptime mensual mayor o igual a 99,9%. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.
		El proveedor deberá proporcionar un servicio de Virtual Network que abarcan varias zonas de disponibilidad. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.
		El proveedor deberá permitir el acceso a las máquinas virtuales a través de un mecanismo seguro mediante HTTPS" Se cumple con el requerimiento, en el documento Descripción General de Google.

	3.26	El servicio de nube deberá permitir la gestión de identidades y accesos para adoptar el principio de seguridad de privilegio mínimo. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.
	3.27	El proveedor deberá ofrecer un servicio de gestión de acceso e identidades que permita otorgar accesos detallados a recursos específicos. Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.
	3.28	El servicio de gestión de acceso e identidades deberá soportar la configuración de roles predefinidos y personalizados Se cumple con el requerimiento, en el documento Descripción General de Google.
	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 Se cumple con el requerimiento, en el documento Descripción General de Google Cloud.

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.	**Cumplimiento de Términos de Referencia** Presenta la oferta con el detalle de las características técnicas solicitadas.	PRESENTA
3. **INFORMACIÓN ADICIONAL**		
La Oferta deberá contener los Formularios que se especifican en el Pliego SDO. • Nombramiento del Representante Legal de la empresa licitante, con facultades para presentar ofertas y suscribir contratos, registrado en la Superintendencia de Compañías.	Presenta el nombramiento del representante legal	PRESENTA
• Cédula de identidad del Representante Legal.	Presenta cédula de identidad del representante legal	PRESENTA
Capacidad financiera: Los Licitantes, mediante la presentación de estados financieros correspondientes a los últimos tres (3) años debidamente registrados en la Superintendencia de Compañías.	Presenta estados financieros de 2 años y mínimo se requirió 3 años. Se verificó que la empresa inicia sus actividades en abril de 2022.	NO PRESENTA
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: • Haber ejecutado al menos un contrato de características similares al objeto de la contratación durante los últimos 8 años y que sea de mínimo $ 163.500,00 (Ciento sesenta y tres mil	El oferente presenta un acta entrega recepción de la orden de servicio 001 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 48.630,88. Con el objeto de contratación "Implementación de Servicio google workspace y Cloud Plataform para el cliente ARCA.	NO PRESENTA

quinientos 00/100 dólares americanos) valor que no incluye IVA o varios verificables que sumados den el monto antes indicado. Para validar lo antes indicado deberá presentar copias de contratos, facturas y/o otros documentos legales, señalando nombres y direcciones de clientes que puedan contactarse para obtener más información sobre esos contratos.	El oferente presenta un acta entrega recepción de la orden de servicio 002 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 18.427,92. Con el objeto de contratación "Implementación de Servicio google Cloud Plataform para el cliente MTOP. El oferente presenta un acta entrega recepción de la orden de servicio 003 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $636,00. Con el objeto de contratación "Licenciamiento de google workspace y Cloud Plataform para el cliente ARCA. Sin embargo el objeto de la orden no corresponde a lo solicitado. El oferente presenta un acta entrega recepción de la orden de servicio 004 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 612,00. Con el objeto de contratación "Licenciamiento de google workspace para el cliente ARCA. Sin embargo el objeto de la orden no corresponde a lo solicitado. El oferente presenta un acta entrega recepción de la orden de servicio 005 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 60.000,00. Con el objeto de contratación "Licenciamiento de google workspace para el cliente Universidad de Cuenca. Sin embargo el objeto de la orden no corresponde a lo solicitado. El oferente presenta un acta entrega recepción de la orden de servicio 006 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 360,00. Con el objeto de contratación "Licenciamiento de google workspace para suscripción para el Ministerio de Educación. Sin embargo el objeto de la orden no corresponde a lo solicitado El oferente presenta un acta entrega recepción de la orden de servicio 007 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 56.744,04. Con el objeto de contratación "Implementación de Servicio cloud Plataform para el cliente GAD Manta" El oferente presenta un acta entrega recepción de la orden de servicio 009 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 432,00. Con el	

	objeto de contratación "Google Workspace, Licenciamiento Bussines Plus". Sin embargo el objeto de la orden no corresponde a lo solicitado. El oferente presenta un acta entrega recepción de la orden de servicio 011 con la Corporación Nacional de Telecomunicaciones CNT E.P, por un monto de $ 5.564,20. Con el objeto de contratación "Google Cloud Plataform". El oferente presenta un contrato con Farmaenlace, por un monto de $135.1913, 94. Con el objeto de contratación "Contrato para la prestación de Servicios Tecnológicos". Sin embargo el contrato se encuentra en ejecución y se solicitó contratos ejecutados. Los documentos de la experiencia acorde al objeto de contratación ascienden a: $ 129.367,04 y lo solicitado fue por $163.500,00 No se solicita aclaración puesto que presento estados financieros de 2 años y mínimo se requirió 3 años.	
Personal Técnico Clave mínimo		
Datos necesarios para el registro del Personal Técnico Mínimo: 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. <u>Función de la Persona: Gerente de Proyecto</u> • Nivel de Estudio: Tercer Nivel con título	Presenta al Ing. Ronny Barba Gomezcoello, con el título de Ing. En Electrónica y Telecomunicaciones, adjunta certificado de SENESCYT y certificaciones de PMP	PRESENTA

• 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		
Datos necesarios para el registro del Personal Técnico Mínimo: 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. <u>Función de la Persona: Técnico arquitecto de Nube</u> • 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	Presenta a la Ing. Michelle Nathaly Morillo Celli, con el título de Ing. En Electrónica y Redes de Información, adjunta certificado de SENESCYT y certificaciones de Arquitecto de solución de la marca ofertada Google.	PRESENTA
Datos necesarios para el registro del Personal Técnico Mínimo: 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.	Presenta al Ing. Fausto Andres Velasquez, con el título de Ing. En Electrónica y Redes de Información adjunta certificado de SENESCYT y falta la certificación de seguridad en nube de la marca ofertada	NO PRESENTA

En el caso de que el personal técnico sea extranjero, se requerirá que el título sea apostillado, para la firma del contrato. Función de la Persona: Técnico de seguridad de Nube • Nivel de Estudio: Tercer Nivel con título • Titulación académica: Ingeniero o Tecnólogo en informática, electrónica, red es 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	No se solicita aclaración puesto que presento estados financieros de 2 años y mínimo se requirió 3 años.	
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.	Presenta al Ing. Ronny Barba Gomezcoello, adjunta certificado de experiencia por la empresa WURSTA y detalla los proyectos en los que participo, así como su función. Sin embargo se solicitó mínimo 2 certificados u otros documentos que acredite la experiencia requerida en el cargo. Adicional presenta una carta de referencia y un certificado de Telefónica que no está dentro de los últimos 5 años. No se solicita aclaración puesto que presento estados financieros de 2 años y mínimo se requirió 3 años.	NO PRESENTA
✓ **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	Presenta a la Ing. Michelle Nathaly Morillo Celli, adjunta certificado de experiencia por la empresa WURSTA y detalla los proyectos en los que participo, así como su función.	PRESENTA

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.	Presenta al Ing. Fausto Andres Velasquez, adjunta certificado de experiencia por la empresa WURSTA y detalla los proyectos en los que participo, así como su función. Sin embargo no acredita la experiencia en seguridad de nube. No se solicita aclaración puesto que presento estados financieros de 2 años y mínimo se requirió 3 años.	NO PRESENTA
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.	Presenta el certificado de ser distribuidor autorizado de google	PRESENTA
Bases de la licitación numeral 19.4 ✓ El licitante deberá presentar de forma física: En la dirección indicada en la cláusula 20.1. En el caso de que presente algún documento con firma electrónica debe enviar en su oferta el medio magnético para poder validar la firma.	El licitante presentó de forma física su oferta la cual contiene firmas digitales y envío el medio magnético; sin embargo, los documentos firmados digitalmente no se pueden validar debido a que encuentran consolidados.	NO PRESENTA

Fuente: Oferta Técnica

REPÚBLICA
DEL ECUADOR

Instituto Nacional
de Estadística y Censos

Luis Avila
0400873428
Delegado de la Máxima Autoridad

Jeaneth Zarsosa
1710292432
Delegado de la unidad requirente

Jimmy Tobar
1712250669
Profesional a fin al objeto de contratación

Ximena Gonzalez
1713940730
Secretaria