San Juan de Pasto, 03 de Julio de 2025

Señores:
INSTITUTO DEPARTAMENTAL DE BELLAS ARTES
Avenida 2N #7N-66
Cali- valle

Asunto: **Renovación Alquiler Servidores Hosting**

Cordial Saludo,

De acuerdo a su solicitud me permito hacer llegar una propuesta para la renovación del servicio de Alquiler de servidores Hosting para su importante entidad, que tiene como objeto "**Se requiere el contratar un servicio de Hosting con 3 servidores en la nube para los servicios DNS y sitios WEB y aplicaciones institucionales en un modelo que funcione bajo estándares de virtualización compatibles con IPV4 e IPv6**":

FICHA TECNICA: ALQUILER HOSTING EN LA NUBE CON COMPATIBILIDAD IPV4 E IPV6	
SERVIDOR 1 LINUX (CPANEL+CLOUD LINUX OS + LITESPPED+IMUNIFY 360 + JETBACKUPS)	
ITEMS	DESCRIPCIÓN
TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	24 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	1000 GB SSD NVME(VERIFICABLE)
RAM	64 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	CloudLinuxOS (VERIFICABLE)
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD

ACCESO CONSOLA HOSTING	LICENCIA CPANEL(VERIFICABLE)
DISPONIBILIDAD	99.96 %
SERVIDOR WEB	LITESPEED / LS CACHE INCLUIDO(VERIFICABLE)
FTP	SI
FIREWALL Y DETECCIÓN DE PREVENCIÓN DE INTRUSOS BASADO EN INTELIGENCIA ARTIFICIAL	SI – EJEMPLO: IMUNIFY 360
FULL BACKUP	DIARIO, EXTERNO, CON RETENCION DE 15 DÍAS MÍNIMO EJEMPLO: JETBACKUP
CALIDAD DEL SERVICIO	Contamos con la tecnología e infraestructura necesaria, administrada por nosotros que permite brindarle niveles muy altos en la calidad del servicio,
SEGURIDAD Y SOPORTE ESPECIALIZADO	Se requiere como mínimo las siguientes actividades durante toda la ejecución del contrato, realizadas directamente por un Ingeniero de Sistemas Especialista en Seguridad Informática, certificado en Ciberseguridad o Auditor Líder, vinculado al proyecto, el cual no puede cambiarse durante toda la ejecución del contrato: - Migración, configuración, revisión de seguridad continua de la infraestructura adquirida, inclusive subdominios. Soporte Técnico 24/7 y asesoría por doce (12) meses. - Auditoría permanente, vulnerabilidades y defensa proactiva ante ataques informáticos durante doce meses de todos los sitios alojados en el servidor, para esto se debe de proveer de software especializado comercial que permita de manera automática, permanente y autónoma lo siguiente: Análisis, detección y corrección de vulnerabilidades web. Firewall WEB (Web Application Firewall) que filtra las conexiones a los sitios o aplicación web y detenga automáticamente los ataques más comunes (XSS, CSRF, SQL Injection). - Monitoreo del Software licenciado que permita el parcheo Automático con análisis de vulnerabilidades en los CMS más populares (Joomla, Wordpress, Drupal) en busca de versiones y componentes vulnerables, una vez identificada la vulnerabilidad, el sistema permite las actualizaciones pertinentes y las correcciones de seguridad. - Sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones proactivas y correctivas antes de que el ataque suceda.

	- Monitoreo del sistema de detección de virus y malware comercial basado en inteligencia artificial licenciado entregado por el contratista (Antivirus EDR comercial) - Actualizaciones del software del servidor y todas las herramientas. - El proveedor deberá suministrar la configuración establecida para el Firewall WEB, Antivirus EDR la cual será revisada por el personal responsable de oficina de las Tics. - Monitoreo del software comercial licenciado, para la protección avanzada de firewall que utiliza heurística en la nube e inteligencia artificial para detectar nuevas amenazas (Dia cero) y proteger todos los servidores que ejecutan el software. El firewall WEB deberá ser capaz de defenderse contra ataques de fuerza bruta, ataques DoS y escaneos de puertos, con licencia comercial (No se admite gratuitos) en caso de ataque el contratista deberá informar a la persona que delegue el supervisor del contrato. Así mismo, la plataforma deberá informar automáticamente a la entidad el posible ataque al que a sido expuesta por medio de correo electrónico. - Soporte técnico permanente vía web, correo electrónico, teléfono, chat y personalizado del ingeniero especialista en seguridad. - Tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. - Velar y asegurar las copias de seguridad permanente de todo el contenido del servidor en el espacio externo suministrado por contratista(Software de backups comercial) - Actualizaciones del sistema operativo del servidor, Sistema de análisis y prevención de ransomware, Monitoreo proactivo del servidor para verificar su disponibilidad Configurar el servicio de monitoreo “uptime” que notifique mediante alertas el estado de inactividad y rendimiento de los sitios web por separado

FICHA TECNICA: ALQUILER HOSTING EN LA NUBE CON COMPATIBILIDAD IPV4 E IPV6	
SERVIDOR 2 **LINUX (CPANEL+CLOUD LINUX OS + LITESPPED+IMUNIFY 360 + JETBACKUPS)**	
ITEMS	**DESCRIPCIÓN**
TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	24 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	500 GB SSD NVME(VERIFICABLE)
RAM	32 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	CloudLinuxOS (VERIFICABLE)
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD
ACCESO CONSOLA HOSTING	LICENCIA CPANEL(VERIFICABLE)
DISPONIBILIDAD	99.96 %
SERVIDOR WEB	LITESPEED / LS CACHE INCLUIDO(VERIFICABLE)
FTP	SI
FIREWALL Y DETECCIÓN DE PREVENCIÓN DE INTRUSOS BASADO EN INTELIGENCIA ARTIFICIAL	SI – EJEMPLO: IMUNIFY 360
FULL BACKUP	DIARIO, EXTERNO, CON RETENCION DE 15 DÍAS MÍNIMO EJEMPLO: JETBACKUP
CALIDAD DEL SERVICIO	Contamos con la tecnología e infraestructura necesaria, administrada por nosotros que permite brindarle niveles muy altos en la calidad del servicio,
SEGURIDAD Y SOPORTE ESPECIALIZADO	Se requiere como mínimo las siguientes actividades durante toda la ejecución del contrato, realizadas directamente por un Ingeniero de Sistemas Especialista en Seguridad Informática, certificado en Ciberseguridad o Auditor Líder, vinculado al proyecto, el cual no puede cambiarse durante toda la ejecución del contrato:

	- Migración, configuración, revisión de seguridad continua de la infraestructura adquirida, inclusive subdominios. Soporte Técnico 24/7 y asesoría por doce (12) meses. - Auditoría permanente, vulnerabilidades y defensa proactiva ante ataques informáticos durante doce meses de todos los sitios alojados en el servidor, para esto se debe de proveer de software especializado comercial que permita de manera automática, permanente y autónoma lo siguiente: Análisis, detección y corrección de vulnerabilidades web. Firewall WEB (Web Application Firewall) que filtra las conexiones a los sitios o aplicación web y detenga automáticamente los ataques más comunes (XSS, CSRF, SQL Injection). - Monitoreo del Software licenciado que permita el parcheo Automático con análisis de vulnerabilidades en los CMS más populares (Joomla, Wordpress, Drupal) en busca de versiones y componentes vulnerables, una vez identificada la vulnerabilidad, el sistema permite las actualizaciones pertinentes y las correcciones de seguridad. - Sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones proactivas y correctivas antes de que el ataque suceda. - Monitoreo del sistema de detección de virus y malware comercial basado en inteligencia artificial licenciado entregado por el contratista (Antivirus EDR comercial) - Actualizaciones del software del servidor y todas las herramientas. - El proveedor deberá suministrar la configuración establecida para el Firewall WEB, Antivirus EDR la cual será revisada por el personal responsable de oficina de las Tics. - Monitoreo del software comercial licenciado, para la protección avanzada de firewall que utiliza heurística en la nube e inteligencia artificial para detectar nuevas amenazas (Dia cero) y proteger todos los servidores que ejecutan el software. El firewall WEB deberá ser capaz de defenderse contra ataques de fuerza bruta, ataques DoS y escaneos de puertos, con licencia comercial (No se admite gratuitos) en caso de ataque el contratista deberá informar a la persona que delegue el supervisor del contrato. Así mismo, la plataforma deberá informar automáticamente a la entidad el posible ataque al que a sido expuesta por medio de correo electrónico.

	- Soporte técnico permanente vía web, correo electrónico, teléfono, chat y personalizado del ingeniero especialista en seguridad. - Tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. - Velar y asegurar las copias de seguridad permanente de todo el contenido del servidor en el espacio externo suministrado por contratista(Software de backups comercial) - Actualizaciones del sistema operativo del servidor, Sistema de análisis y prevención de ransomware, Monitoreo proactivo del servidor para verificar su disponibilidad Configurar el servicio de monitoreo "uptime" que notifique mediante alertas el estado de inactividad y rendimiento de los sitios web por separado

FICHA TECNICA: ALQUILER HOSTING EN LA NUBE CON COMPATIBILIDAD IPV4 E IPV6	
SERVIDOR 3 **LINUX (CPANEL+CLOUD LINUX OS + LITESPPED+IMUNIFY 360 + JETBACKUPS)**	
ITEMS	**DESCRIPCIÓN**
TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	24 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	500 GB SSD NVME(VERIFICABLE)
RAM	32 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	CloudLinuxOS (VERIFICABLE)
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD
ACCESO CONSOLA HOSTING	LICENCIA CPANEL(VERIFICABLE)
DISPONIBILIDAD	99.96 %
SERVIDOR WEB	LITESPEED / LS CACHE INCLUIDO(VERIFICABLE)

FTP	SI
FIREWALL Y DETECCIÓN DE PREVENCIÓN DE INTRUSOS BASADO EN INTELIGENCIA ARTIFICIAL	SI – EJEMPLO: IMUNIFY 360
FULL BACKUP	DIARIO, EXTERNO, CON RETENCION DE 15 DÍAS MÍNIMO EJEMPLO: JETBACKUP
CALIDAD DEL SERVICIO	Contamos con la tecnología e infraestructura necesaria, administrada por nosotros que permite brindarle niveles muy altos en la calidad del servicio,
SEGURIDAD Y SOPORTE ESPECIALIZADO	Se requiere como mínimo las siguientes actividades durante toda la ejecución del contrato, realizadas directamente por un Ingeniero de Sistemas Especialista en Seguridad Informática, certificado en Ciberseguridad o Auditor Líder, vinculado al proyecto, el cual no puede cambiarse durante toda la ejecución del contrato: - Migración, configuración, revisión de seguridad continua de la infraestructura adquirida, inclusive subdominios. Soporte Técnico 24/7 y asesoría por doce (12) meses. - Auditoría permanente, vulnerabilidades y defensa proactiva ante ataques informáticos durante doce meses de todos los sitios alojados en el servidor, para esto se debe de proveer de software especializado comercial que permita de manera automática, permanente y autónoma lo siguiente: Análisis, detección y corrección de vulnerabilidades web. Firewall WEB (Web Application Firewall) que filtra las conexiones a los sitios o aplicación web y detenga automáticamente los ataques más comunes (XSS, CSRF, SQL Injection). - Monitoreo del Software licenciado que permita el parcheo Automático con análisis de vulnerabilidades en los CMS más populares (Joomla, Wordpress, Drupal) en busca de versiones y componentes vulnerables, una vez identificada la vulnerabilidad, el sistema permite las actualizaciones pertinentes y las correcciones de seguridad. - Sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones proactivas y correctivas antes de que el ataque suceda. - Monitoreo del sistema de detección de virus y malware comercial basado en inteligencia artificial licenciado entregado por el contratista (Antivirus EDR comercial) - Actualizaciones del software del servidor y todas las herramientas.

	- El proveedor deberá suministrar la configuración establecida para el Firewall WEB, Antivirus EDR la cual será revisada por el personal responsable de oficina de las Tics. - Monitoreo del software comercial licenciado, para la protección avanzada de firewall que utiliza heurística en la nube e inteligencia artificial para detectar nuevas amenazas (Dia cero) y proteger todos los servidores que ejecutan el software. El firewall WEB deberá ser capaz de defenderse contra ataques de fuerza bruta, ataques DoS y escaneos de puertos, con licencia comercial (No se admite gratuitos) en caso de ataque el contratista deberá informar a la persona que delegue el supervisor del contrato. Así mismo, la plataforma deberá informar automáticamente a la entidad el posible ataque al que a sido expuesta por medio de correo electrónico. - Soporte técnico permanente vía web, correo electrónico, teléfono, chat y personalizado del ingeniero especialista en seguridad. - Tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. - Velar y asegurar las copias de seguridad permanente de todo el contenido del servidor en el espacio externo suministrado por contratista(Software de backups comercial) - Actualizaciones del sistema operativo del servidor, Sistema de análisis y prevención de ransomware, Monitoreo proactivo del servidor para verificar su disponibilidad Configurar el servicio de monitoreo “uptime” que notifique mediante alertas el estado de inactividad y rendimiento de los sitios web por separado

COSTO ANUAL:

El costo por la renovación del servidor durante un año es de VEINTISIETE MILLONES DE PESOS MCTE (27.000.000)

Atentamente,

Firma _____