Gobernación del CAUCA | Secretaría General

CARTA DE ACEPTACIÓN DE OFERTA No. 2373-2026

Señores:
MIHOSTING S.A.S.
Nit. 900724548-6
Representante Legal actual: **JORGE LUIS VILLEGAS MAGUIÑA**
C.C. 2.000.029.772 de Pasto Nariño
Tel: 300-203-0723
Dirección: Calle 20 31 B-40 OF 305 EDIFICIO OFFICE CENTER
Correo: gerencia@esmihosting.co
Pasto, Nariño

ASUNTO: Carta de aceptación del proceso de Mínima Cuantía No. **DC-SG-MC-007-2026**

El DEPARTAMENTO DEL CAUCA – SECRETARÍA GENERAL, se permite comunicarle que su propuesta ha sido aceptada expresa e incondicionalmente, de conformidad con lo dispuesto en el art. 94 de la ley 1474 de 2011 y 2.2.1.2.1.5.2. Del Decreto 1082 de 2015. Por lo anterior, para todos los efectos jurídicos la presente aceptación junto con la oferta por usted presentada constituye el contrato, que se regirá entre otras por las siguientes cláusulas:

1. **OBJETO:**

   CONTRATAR SERVIDOR CLOUD PRIVADO VIRTUAL (VPS) ADMINISTRADO Y SUS SERVICIOS ESPECIALIZADOS DE AUDITORÍA, ACTUALIZACIÓN, SOPORTE Y ADMINISTRACIÓN PARA ALOJAR LOS DIFERENTES SITIOS WEB DE LA GOBERNACIÓN DEL CAUCA.

2. **PLAZO:** El plazo de ejecución del contrato será hasta el 31 de diciembre de 2026, contados a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución. La prestación del servicio debe garantizarse por un (1) año.

3. **VALOR:** El valor total del contrato es de hasta **CINCUENTA Y SEIS MILLONES SEISCIENTOS MIL PESOS M/CTE. ($56.600.000) IVA INCLUIDO** y todos los demás costos directos e indirectos, teniendo en cuenta que es el presupuesto designado para la presente vigencia, de conformidad a la necesidad presentada.

   El presente proceso se encuentra amparado por los siguientes Certificados de Disponibilidad Presupuestal**: No. 3103 del 29 de mayo de 2026.**

   Teniendo en cuenta así el valor unitario ofertado por el proponente discriminado así de la siguiente manera:

Nro.	Descripción	Cantidad	Valor Unitario
1	SERVIDORES CLOUD PRIVADO VIRTUAL (VPS) ADMINISTRADO	10	24.500.000,00
2	SERVIDOR NAS PARA EL ALMACENAMIENTO DE LAS COPIAS DE SEGURIDAD DE LAS VPS	1	5.800.000,00

3	SOPORTE, AUDITORÍA Y MANTENIMIENTO ESPECIALIZADO	1	8.600.000,00
4	CERTIFICADOS	20	5.800.000,00
5	ASESORÍA Y CONSULTORÍA ESPECIALIZADA	1	11.900.000,00

4. ESPECIFICACIONES TÉCNICAS

Para la correcta ejecución del objeto contractual, el futuro contratista debe tener en cuenta los siguientes aspectos y/o especificaciones técnicas:

DESCRIPCIÓN	REQUERIMIENTOS TÉCNICOS MÍNIMOS	CANTIDAD
10 SERVIDORES CLOUD PRIVADO VIRTUAL (VPS) ADMINISTRADO	CAPACIDAD DE CÓMPUTO FRAGMENTABLE CLOUD PRIVADO PARA 10 SERVIDORES CLOUD VPS TOTALMENTE ADMINISTRADOS: CAPACIDAD DE COMPUTO, ALMACENAMIENTO SSD NVME Y RAM: Capacidad de cómputo basado en Procesadores de uso intensivo tipo Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 134 Cores dedicados verificable, distribuidos de acuerdo con las necesidades DISTRIBUIDAS en las 10 máquinas virtuales. - Uso actual: 8 VPS (2 vps con Cpanel y 6 sin panel basados en Linux con múltiples configuraciones y aplicaciones. - 256 GB de RAM(Verificable), distribuidas de acuerdo a las necesidades entre las 10 VPS. - 10 TB de disco duro SSD NVME(velocidad Verificable por prueba de escritura). - GESTIÓN Y ADMINISTRACIÓN DEL NIVEL DE HIPERVISOR (PANEL CLOUD) El contratista será responsable de la administración integral del servidor desde la plataforma de virtualización (Hypervisor/Panel Cloud), garantizando la disponibilidad del hardware virtual y la gestión de recursos críticos. Para ello, la entidad (o el proveedor) suministrará las credenciales de acceso con privilegios administrativos totales root para las siguientes funciones de monitoreo y verificación por la entidad: • Operaciones de Control de Instancia (Power Management): Capacidad de ejecutar acciones de Inicio (Start), Detención (Stop), Reinicio Forzado (Hard Reboot) y Suspensión del servidor en caso de fallos críticos del Kernel o bloqueos por ataques de denegación de servicio (DoS) que impidan el acceso vía SSH. • Monitoreo de Recursos de Hardware Virtual: Seguimiento en tiempo real e histórico de métricas de rendimiento: Uso de CPU y Memoria RAM. • Operaciones de lectura/escritura en disco (I/O Wait). • Ancho de banda de red (Entrante/Saliente) para detectar patrones de tráfico anómalos o ataques de inundación (Flooding).	1

- Diagnóstico mediante Consola KVM / VNC: Acceso directo a la terminal del servidor (Consola de Emergencia) para la resolución de problemas cuando la pila de red esté caída o el firewall local (CSF) bloquee por error las IPs administrativas.

- Revisión de Logs de Arranque y Mensajes del Sistema (dmesg) a nivel de Hipervisor.

- Implementación de Firewall Perimetral (Edge Firewall): Configuración y mantenimiento de un Firewall de Red (Capa 3 y 4) externo al servidor, que actúe como primera línea de defensa antes de que el tráfico llegue al sistema operativo.

- Definición de políticas de "Lista Blanca" (Whitelist) para acceso administrativo y bloqueo de puertos críticos no utilizados (ej. bloquear puerto 445/SMB, puerto 22 para IPs no autorizadas).

- Gestión de Instantáneas (Snapshots) y Backups: Programación y ejecución de Snapshots antes de cambios críticos en la configuración del servidor, permitiendo un "Rollback" (retorno a un estado funcional anterior) inmediato en caso de desastre o infección masiva.

- Redimensionamiento Recursos: Se debe poder asignar y reasignar más recursos en tiempo real y sin Down times de los servidores VPS desde el panel del Cloud hasta agotar los recursos de procesador, RAM y Disco contratados. (verificación que se realizará por el supervisor del contrato durante toda la ejecución de este)
- 100 TB de ancho de banda mensual
- Hasta 10 IPs dedicadas versión IPV4 e IPV6(DualStack Habilitado), según necesidad
- Velocidad de conexión de al menos de 3 GB/S.
- Sistemas operativos soportados: Oracle Linux, Alma Linux, Roky Linux, Cloud Linux, Ubuntu y otras Distribuciones Enterprise-Grade y compatibles con RHEL.
- Uptime 99.999%. Seguridad Anti DDoS.
- Parqueos de Dominios y subdominios ilimitados.
- Cuentas de FTP ilimitada.
- Acceso Root vía SSH(Obligatorio durante toda la ejecución del contrato).
- CPanel /whm para la administración EN 2 vps LICENCIAS 200 y 100 dominios con características de: Encriptación SSL para todos los dominios y subdominios. Licencia y Acceso WHM con usuario root - verificación de licencia válida Licencia Cpanel /WHM para mínimo 300 cuentas independientes Cpanel asignada, configurada e instalada en dos de las VPS(200 y 100).
- Creación de Nuevas cuentas de Cpanel siempre que se requieran para el alojamiento de nuevos sitios y/o aplicaciones web.
- Sistema de Copias de seguridad Licenciado Comercial de todas las VPS para realizar copias completas mensuales, semanales y diarias de seguridad de los datos en una NAS especializada, con copias dispuestas en el momento que requiera la entidad, con la posibilidad de restaurar de forma individual e independiente archivos, bases de datos, con una retención de hasta 30 días de forma individual o fullbackup.

	- DATACENTER DE LOS SERVIDORES CLOUD VPS: DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar en su oferta técnica a el Datacenter en el cual se alojará el servicio mediante una certificación firmada por el representante legal, además de entregar evidencias de un vínculo con el datacenter (Certificado Partner o Facturas pago último mes) El proponente deberá aportar, junto con la Certificación del Datacenter, las siguientes certificaciones que el Datacenter debe cumplir como mínimo, sin excepción, acompañadas de un enlace a la URL oficial y vigente del sitio web del Datacenter: 1. ISO_IEC_27001ISO 27001, 27017 y 27018 2. ISO 27701 3. RGPD 4. SOC 1, 2 y 3 5. CSA STAR 6. HIPAA e HITECH 7. PCI-DSS 8. SWIPO 9. ISO 14001 10. ISO 50001 11. Política de Seguridad del datacenter SEGMENTO DE IP ACTUALES CONTRATADAS CON EL DATACENTER DONDE SE ALOJARÁ EL SERVICIO: El proponente deberá indicar en su oferta técnica el segmento de direcciones IP (o, en su defecto, el número de sistema autónomo – ASN) en el cual se alojará el servicio. Dicho segmento deberá coincidir con el registro público de proveedores de infraestructura (LACNIC/ARIN) a nombre del Datacenter y el Proponente. En caso de adjudicación del proceso, el proponente no podrá, bajo ninguna circunstancia, alojar el servidor en centros de cableado o cuartos de TI que no cumplan con los requisitos establecidos en el presente documento. Todo cambio o traslado del servidor durante la vigencia del contrato deberá ser informado oportunamente al supervisor para su autorización. El supervisor validará las direcciones IP asignadas durante toda la ejecución contractual. - SISTEMAS OPERATIVOS 10 VPS serán basados en Linux en diferentes versiones como Oracle Linux, debian, Ubuntu, Alma Linux, Rocky Linux, debidamente asegurados y configurados por el especialista en seguridad informática. Gratuitas.	
SERVIDOR NAS PARA EL ALMACENAMIENTO DE LAS COPIAS DE SEGURIDAD DE LAS VPS	- Suministro, configuración e implementación de un sistema de almacenamiento en red (NAS) de alto rendimiento, destinado al respaldo de hasta 10 servidores virtuales (VPS). El sistema debe garantizar una capacidad de almacenamiento neto usable de 10 TB bajo un esquema de redundancia que permita la falla de hasta dos unidades de disco sin pérdida de datos (RAIDZ2 o equivalente)." - Conectividad y Seguridad: - El contratista debe garantizar la integración del NAS en un Datacenter geográficamente distinto al de los servidores de origen.	1

	- La comunicación se realizará mediante una VLAN privada y vRack virtual independiente, asegurando aislamiento total de la red pública y garantizando latencias mínimas para el tráfico de backup. - Configuración Lógica (NAS/ZFS): - Estructura de Datos: Se deberán configurar Datasets independientes para cada una de las 10 VPS, aplicando cuotas de disco si la supervisión lo requiere. - Optimización: Se debe habilitar compresión (LZ4) y deduplicación para optimizar el uso de los recursos. - Entregables y Acceso: - Entrega de credenciales de administración total al supervisor del contrato. - Configuración de accesos granulares (usuarios/passwords o llaves SSH) independientes para que cada VPS solo tenga visibilidad de su propio Dataset asignado. - Especificaciones Técnicas mínimas NAS: Procesador: Mínimo 16 Cores físicos (o combinación de núcleos/hilos que sumen 16 hilos de procesamiento de alto rendimiento). Memoria RAM: Mínimo 16-32 GB RAM DDR4/DDR5 con corrección de errores (ECC) indispensable para la integridad de datos en sistemas tipo NAS Almacenamiento de Sistema: 2 unidades SSD NVME (mínimo 240 GB) configuradas en Mirror (Espejo) para el sistema operativo del servidor NAS Configuración de Discos y Rendimiento 1. (Pool de Datos): Garantizar 20 TB usables con protección y las unidades de aceleración solicitadas, el proponente debe cumplir con: Almacenamiento Masivo Ejemplo: Mínimo de discos tipo SAS de 10Gb/s (7.2K RPM o superior). Recomendación de RAID: Para obtener 20 TB usables con protección, se sugiere una configuración RAIDZ2 (equivalente a RAID 6). Esto requiere al menos 4 discos de 8 TB o 6 discos de 6 TB. 2. Unidad de Caché (L2ARC): 1 unidad SSD NVMe de 500 GB dedicada para aceleración de lectura. 3. Unidad de Log (SLOG): 1 unidad SSD NVMe de 20 GB (o superior) de alta resistencia (High Endurance) para acelerar las escrituras sincrónicas y proteger el log de transacciones.	
SOPORTE, AUDITORÍA Y MANTENIMIENTO ESPECIALIZADO	Para el Soporte especializado se requiere que el proponente presente como requisito habilitante la hoja de vida de Un ingeniero de Sistemas Especialista en Seguridad informática, certificado como Auditor Líder ISO 27001 versión 2022 vigente(verificable vía web) con amplia experiencia en administración de servidores Linux, implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas en los 2 últimos años, quien debe debe firmar carta de compromiso y presentar dicha carta como anexo a su propuesta y con una vinculación durante toda la ejecución del proyecto, dado que será el responsable de la seguridad de los servidores y de garantizar la protección de la información de la entidad, desempeñando y velando mínimo las siguientes actividades: - Migración y Soporte permanente por el especialista en seguridad informática de todos servidores y sitios web, que son actualmente 8 VPS. Además dicho profesional será el encargado de realizar la migración completa de 2 servidor Cloud VPS con Cpanel/WHM y 6 VPS sin panel de control, y los que se creen durante la ejecución del contrato (hasta 10) las cuales tienen diferentes configuraciones	1

basadas en linux), realizar la configuración además revisión de todos los sitios web con sus respectivas cuentas de CPanel, en la infraestructura adquirida, inclusive subdominios. Soporte Técnico 24/7 y asesoría por doce (12) meses.

Servidores actuales:
1. servidor1.cauca.gov.co (Cpanel)
2. servidor2.cauca.gov.co (Cpanel)
3. tics.sedcauca.gov.co (Linux)
4. oracle.cauca.gov.co (Linux)
5. sgsri.sedcauca.gov.co (Linux)
6. riesgos.sedcauca.gov.co (Linux)
7. siscpd.cauca.gov.co (Linux)
8. oagrd.cauca.gov.co (Linux)

- Auditoría y asesoría permanente, frente a cualquier situación relacionada con incidentes y vulnerabilidades, y defensa proactiva ante ataques informáticos durante toda la ejecución del contrato de todos los sitios alojados en el servidor en actividades mínimas como:

- Mitigación de ataques de Denegación de Servicio (DDoS/Flood): Capacidad para identificar y filtrar ataques de inundación SYN (Layer 4) y ataques de aplicación (Layer 7) mediante el uso coordinado de Firewalls perimetrales y WAF.
- Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge.
- Hardening de Servidores Web (CPanel/WHM): Implementación de políticas de aislamiento de cuentas, saneamiento de versiones de PHP obsoletas y restricción de tráfico saliente para evitar que el servidor sea usado como nodo de ataque.

- Forense y Limpieza de Malware en CMS: Identificación de vectores de entrada (exploits en plugins), eliminación de backdoors complejos, purga de inyecciones de spam SEO en bases de datos y restauración de integridad de archivos.

- Administración Avanzada de Firewall Local (CSF/LFD): Configuración de listas de bloqueo dinámicas (como la red TOR), control de tasas de conexión (CT_LIMIT) y protección contra escaneos de puertos.
- Entregar un reporte de versiones y componentes vulnerables, identificados mediante el software licenciado parchado con análisis de vulnerabilidades en los CMS más populares (Joomla, Wordpress, Drupal), una vez identificada la vulnerabilidad, el sistema debe permitir 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.

- En caso de incidentes y ataques El especialista será responsable de liderar el ciclo completo de respuesta ante incidentes (IR), que incluye la detección, contención, erradicación y, fundamentalmente, la elaboración de un Informe Técnico Forense y de Remediación. Este documento debe consolidar todas las evidencias recolectadas durante el ataque y las acciones correctivas aplicadas. El informe debe contener como mínimo:

	• Resumen Ejecutivo: Descripción no técnica del impacto del ataque en los servicios institucionales y el estado final de la seguridad. • Línea de Tiempo del Incidente (Timeline): Detalle cronológico desde la detección de los primeros síntomas (ej. lentitud por tráfico de IPs de Indonesia/red TOR) hasta la resolución total. • Identificación de Vectores de Entrada: Análisis de cómo el atacante logró vulnerar el sistema (ej. vulnerabilidad en el plugin Anywhere Elementor, archivos de verificación de Google inyectados o backdoors ocultos). • Evidencia Técnica y Logs: Consolidación de capturas de logs de Apache, reportes de Imunify360, procesos sospechosos en WHM y listado de direcciones IP bloqueadas. • Acciones de Contención y Limpieza: Detalle de las medidas tomadas: • Configuración del Firewall Edge y Cloudflare. • Limpieza manual de inyecciones de código en la base de datos (spam SEO). • Saneamiento de archivos del núcleo de WordPress. • Ajustes en los límites de procesos PHP-FPM y CURL. • Plan de Remediación y Mejora Continua: Recomendaciones de seguridad a corto y largo plazo (ej. política de contraseñas, actualización obligatoria de plugins, auditoría de red interna para detectar saltos laterales). Verificar el estado del servidor y realizar actualizaciones del software del servidor y las herramientas de Cpanel. Soporte técnico permanente vía web, correo electrónico, teléfono, chat, en caso de requerirse del ingeniero especialista en seguridad informática 24/7, tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. Aspectos que garanticen la seguridad del servidor. Para 2 servidores cpanel: Software licenciado Parcheo Automático como Patchaman u otros similares comerciales 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. Para 2 servidores cpanel: 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. Para 2 servidores cpanel: Sistema de detección de virus y malware basado en inteligencia artificial licenciado para 300 dominios tipo Imunify360 u otros con licencias comercial que cumplan con lo solicitado, no se aceptan versiones inferiores a 360.	

	Server side que identifique y elimine amenazas de su servidor. Actualizaciones diarias del software del servidor y las herramientas. Para 2 servidores cpanel: Suministro de un software comercial licenciado para 300(200 vps 1 y 100 vps2) dominios, para la protección avanzada de firewall que utiliza heurística en la nube e inteligencia artificial para detectar nuevas amenazas y proteger todos los servidores que ejecutan el software. El firewall es capaz de defenderse contra ataques de fuerza bruta, ataques DoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios (hasta 300). tipo Imunify360 u otros con licencias comercial que cumplan con lo solicitado, no se aceptan versiones inferiores a 360 Soporte técnico permanente vía web, correo electrónico, teléfono, chat, o presencial en caso de requerirse del ingeniero especialista en seguridad informática. Tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. Copias de seguridad permanente de todo el contenido del servidor hasta de un mes atrás. 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.	
CERTIFICADO	- Certificado SSL WILDCARD Cifrado SHA-2 Y DE 2048 bits reforzado o superior para el dominio principal y subdominios Certificado SSL POSITIVO O COMODO Cifrado SHA-2 y de 2048 bits reforzado, para los demás sitios web a hospedar. El certificado SSL es un componente software que permite una comunicación cifrada entre el navegador y el servidor que aloja el sitio web. El certificado incrementa la seguridad en la información procesada en el sitio web y brinda mayor confianza al usuario que accede al mismo, debe ser verificable permitiendo visualizar el sitio web con la extensión segura del protocolo https:// también se debe visualizar el candado (o icono equivalente) a la izquierda de la URL.	20 certificados Wildcard
ASESORÍA Y CONSULTORÍA ESPECIALIZADA	Servicios de asesoría, consultoría y/o capacitación especializada en informática para mejorar las competencias de los servidores públicos en seguridad informática, tecnologías web, cloud computing, optimización de plataformas software, desarrollo de aplicaciones web y móviles, a cargo del especialista en seguridad informática y adicionalmente de un un Ingeniero con título de Maestría en Seguridad Informática certificado en ciberseguridad, Web Application Penetration Tester, AppSec, INE Certified Cloud Associate, como mínimo). El proponente deberá aportar el perfil del un Ingeniero con título de Maestría en Seguridad Informática como requisito habilitante obligatorio del presente proceso.	Mínimo 30 horas

PARÁGRAFO: Independientemente del plazo de ejecución del contrato, la vigencia del servicio de hosting será por doce (12) meses.

- **EQUIPO DE TRABAJO**

Para la ejecución del objeto contractual, el proponente deberá ofertar y mantener durante toda la ejecución del contrato, como mínimo el siguiente equipo de trabajo:

PERFIL	REQUISITOS
Ingeniero Especialista o áreas afines	Hoja de vida con soporte de: • Ingeniero de Sistemas Especialista en Seguridad Informática o áreas afines. • Certificación vigente como Auditor Líder ISO 27001 versión 2022 (verificable en web). • Experiencia de 2 años en administración Linux e implementación de ISO 27001. • Carta de compromiso firmada y anexada a la propuesta.
Ingeniero con maestría en Seguridad Informática	Hoja de vida de Ingeniero con título de Maestría en Seguridad Informática certificado en ciberseguridad, Web Application Penetration Tester, AppSec, o INE Certified Cloud Associate (Mínimo para dictar 30 horas de asesoría).

5. FORMA DE PAGO: EL DEPARTAMENTO DEL CAUCA pagará al CONTRATISTA el valor del contrato mediante actas parciales, conforme a las actividades realizadas e insumos suministrados, previa presentación de la cuenta de cobro y/o factura y de la constancia de recibo a satisfacción suscrita por el supervisor del contrato.

Para efectos de realizarse los pagos, EL CONTRATISTA debe acreditar que se encuentra el día en el pago de aportes a seguridad social (salud, pensión y riesgos) y parafiscales (SENA, ICBF Y CAJAS DE COMPENSACIÓN FAMILIAR).

6. OBLIGACIONES GENERALES DEL CONTRATISTA

A. Cumplir a cabalidad con el cronograma de fechas establecidas para las entregas correspondientes de bienes y servicios contratados. Si por justificación alguna se puede llegar a incumplir el mismo, notificar al supervisor con tres (3) días de antelación.
B. Presentar la respectiva factura acorde con la propuesta económica presentada en la invitación pública e informe de ejecución del contrato.
C. Cumplir las normas legales vigentes, en especial lo dispuesto en las leyes 789 de 2002, 797 de 2003, 1122 de 2007 y 1150 de 2007 en lo referente al pago de aportes al Sistema de Seguridad Social Integral (salud-pensión - riesgos laborales – Sena – Instituto Colombiano de Bienestar Familiar – Caja de Compensación Familiar) y en especial el decreto 723 de 2013 que regula la afiliación al Sistema General de Riesgos Laborales de las personas vinculadas a través de un contrato de prestación de servicios con entidades públicas.
D. El contratista deberá constituir a favor de la Gobernación del Departamento del Cauca las garantías pactadas en el contrato.
E. Garantizar la adecuada planeación y ejecución del contrato.
F. Cumplir con el objeto contractual durante el plazo de ejecución del contrato, en la forma establecida en las cláusulas del contrato que se suscribió.

G. Atender todas y cada una de las sugerencias y recomendaciones que haga la supervisión

del contrato para el buen cumplimiento del objetivo contractual.

H. Mantener absoluta reserva de la información que conozca por causa y por ocasión del contrato.
I. Informar oportunamente al supervisor del contrato, de cualquier situación que pueda afectar la correcta ejecución de este.

7. OBLIGACIONES ESPECIALES DEL CONTRATISTA

A. Migrar (si se requiere) los (16) Dieciséis sitios web al hosting adquirido conservando la integridad de los datos.
B. El contratista se obliga a entregar en medio físico una copia de seguridad de los datos migrados de cada uno de los (16) Dieciséis sitios. Configurar el servidor y dejarlo totalmente funcional.
C. 3. Brindar el servicio por mínimo doce meses a partir de la suscripción del acta de inicio.
D. Configurar el registro SPF e interactuar con el proveedor para garantizar la publicación (Un registro SPF es un tipo de registro de Servicio de nombre de dominio que identifica los servidores de correo que pueden enviar mensajes en nombre del dominio institucional (G Suite).
E. Capacitar en el uso de las herramientas básicas de administración para los funcionarios que darán soporte de primer nivel.
F. Habilitar el servicio FTP.
G. Brindar soporte técnico durante el término del contrato.
H. Reconfigurar de ser necesario los DNS primarios y secundarios para estabilizar los servicios y garantizar su correcta propagación.
I. Crear nuevas cuentas de CPANEL para nuevos planes de alojamiento cuando la administración departamental lo requiera para alojar nuevos sitios y/o aplicaciones.
J. Brindar soporte, seguridad y administración del Servidor.
K. 11. Administrar, configurar y mantener todos los componentes instalados en el sistema y en cada servidor cloud, siendo los de carácter crítico el software del servidor web y los sistemas gestores de bases de datos, que ofrecen la disponibilidad de los sitios web alojados en el servidor.
L. Actualizar constantemente los parches de software y seguridad de todos los componentes instalados en el sistema, como pueden ser la actualización del Kernel del SO, httpd, bind, Mysql, PHP, WHM, CPANEL, etc.
M. Administrar y configurar IPTABLES en el servidor, con reglas que permitan proteger el servidor de ataques externos.
N. Asegurar el servidor, instalando, configurando y administrando APF, CSF, Etc. y el software necesario para la protección y prevención de ataques al servidor.
O. Monitorear el servidor 24/7/365 días.
P. Monitorear la capacidad y los indicadores de Almacenamiento en Disco del servidor alertando al supervisor del contrato las novedades y estadísticas de uso.
Q. Asegurar el directorio /tmp en el servidor.
R. Instalar, configurar y administrar el software de seguridad del servidor.
S. Monitorear permanentemente los recursos como son uso de RAM y CPU en el servidor.
T. Generar las copias de seguridad (Backup) completas del servidor todas las noches usando Snap Shots con retención de 30 días.
U. Crear dominios y subdominios a solicitud dentro del servidor.
V. Configurar Bind y DNS en el servidor.
W. Presentar reportes de estadísticas con webalizer o Awstats además de reporte de amenazas y seguridad de los sitios WEB mensualmente al correo del supervisor que designe la entidad.

X. Generar reportes del sistema gestores de bases de datos y carga general del servidor.
Y. Verificar el estado de Backups válido en todas las máquinas virtuales.
Z. Realizar migración (de ser necesario) de nuevos sitios web y/o aplicaciones al VPS siempre y cuando el servidor cuente con el espacio necesario para tal fin.
AA. Proveer de una licencia software que cumpla con lo siguiente: Aplicación software para el análisis, detección y corrección de vulnerabilidades web. Software que integre un WAF (Web Application Firewall) que filtre las conexiones a su sitio o aplicación web y detenga automáticamente los ataques más comunes. (XSS, CSRF, SQL Injection). Software que realice 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. Software que realice un sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones correctivas antes de que el ataque suceda. Software que implemente un sistema de detección de virus y malware server side que identifique y elimine amenazas de su servidor.
BB. Finalizado el plazo de ejecución del contrato, entregar al supervisor las respectivas copias de seguridad completas de las cuentas CPANEL de alojamiento de los sitios web, también incluye la imagen de servidor y entornos de ejecución configurados.
CC. Brindar asesoría especializada por un Ingeniero con título de Maestría en Seguridad Informática en temas de seguridad digital, tecnologías web, cloud computing, optimización de plataformas software, desarrollo de aplicaciones web y móviles.

8. OBLIGACIONES DEL DEPARTAMENTO DEL CAUCA

A. Pagar el servicio efectivamente prestado
B. Ejercer la supervisión del contrato.

9. IMPUTACIÓN PRESUPUESTAL: El anterior valor, se encuentra respaldado presupuestalmente con los Certificados de Disponibilidad Presupuestal No. **3103** del 29 de mayo de 2026 de gastos de funcionamiento.

10. SUPERVISOR: EL DEPARTAMENTO DEL CAUCA supervisará el cumplimiento del presente contrato a través del líder la oficina de Gestión Tecnológica del Departamento o quien haga sus veces. Las partes acuerdan que **EL DEPARTAMENTO DEL CAUCA** podrá modificar unilateralmente la designación del supervisor para lo cual bastará comunicación escrita en tal sentido. **NOTA:** La supervisión tendrá las facultades establecidas en los artículos 83 y 84 de la Ley 1474 de 2011.

11. LUGAR DE EJECUCIÓN Y DOMICILIO CONTRACTUAL

La ejecución del contrato se adelantará en el municipio de Popayán y El domicilio contractual se establece en el Municipio de Popayán, sede de la Gobernación del Cauca calle 4 con carrera 7.

12. GARANTÍAS: El contratista deberá constituir a su costa y a favor de la entidad, ante una compañía de seguros o una institución bancaria legalmente establecida en el país que cubra los siguientes riesgos y por los valores, plazos y condiciones que a continuación se precisan:

a. **CUMPLIMIENTO DEL CONTRATO**, pago de multas, cláusula penal pecuniaria, equivalente al 10% del valor del contrato, con una vigencia igual a la duración del contrato y cuatro
(4) meses más;
b. **CALIDAD DE LOS BIENES Y SERVICIOS** equivalente al 10% del valor del contrato, con una vigencia igual a la del contrato y cuatro (4) meses más.
c. **CALIDAD DEL SERVICIO** equivalente al 10% del valor del contrato, con una vigencia igual a la del contrato y cuatro (4) meses más.
d. **PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES**, por una Cuantía equivalente al cinco por ciento (5%) del valor del contrato y una vigencia igual a la duración del mismo y tres (3) años más

Si se adiciona el valor del contrato, o se prorroga el plazo de ejecución o si es objeto de suspensión, el contratista deberá ajustar las pólizas de manera proporcional, de conformidad con lo dispuesto en el artículo 2.2.1.2.3.1.18. del Decreto 1082 de 2015.

El hecho de la constitución de los amparos de que trata esta estipulación no exonera al CONTRATISTA de las responsabilidades en relación con los riesgos asegurados.

Será de cargo del CONTRATISTA el pago oportuno de todas las primas y erogaciones de constitución y mantenimiento de las garantías. En caso de demora en pagar oportunamente tales gastos, EL DEPARTAMENTO podrá hacerlo y descontará su valor de la primera factura o facturas que debe pagar al CONTRATISTA. Igualmente deberá reponer las garantías cuando el valor de las mismas se vea afectado por razón de siniestros.

No obstante, la constitución de las pólizas podrá ser modificada de común acuerdo durante la ejecución del contrato. Una vez iniciada la ejecución del contrato, en caso de incumplimiento del contratista de la obligación de obtener la ampliación de la garantía o de la obligación de obtener su renovación o de la obligación de restablecer su valor o de aquella de otorgar una nueva garantía que ampare el cumplimiento de las obligaciones que surjan por razón de la celebración, ejecución y liquidación del contrato, la entidad contratante podrá declarar la caducidad del mismo.

13. **CLAUSULA PENAL:** En caso de declaratoria de incumplimiento, **EL DEPARTAMENTO DEL CAUCA – SECRETARIA GENERAL.,** hará efectiva una sanción penal pecuniaria, la cual tendrá un monto del veinte por ciento (20%) del valor del contrato, pena que se pacta por el mero retardo y sin perjuicio del cumplimiento de la obligación principal. Para efectos de cobrar la cláusula penal se podrá hacer uso de la compensación de sumas o jurisdicción coactiva.

El contratista renuncia a ser requerido para efectos de constitución en mora y a la tasación proporcional de la pena.

14. **EJECUCIÓN Y LEGALIZACIÓN DEL CONTRATO POR PARTE DEL OFERENTE SELECCIONADO**.

Las partes acuerdan un plazo máximo de 2 días hábiles para que se proceda al cumplimiento de requisitos para la ejecución del contrato. Vencido el término sin que el CONTRATISTA haya cumplido los requisitos de ejecución se entiende que el CONTRATISTA renuncia al contrato.

15. **PERFECCIONAMIENTO Y EJECUCIÓN:** la presente carta de aceptación se entenderá perfeccionada con la firma electrónica de las partes dentro de la plataforma SECOP II y para su ejecución se requiere el correspondiente registro presupuestal y la aprobación de garantías.

16. **INTERPRETACIÓN UNILATERAL**. Si durante la ejecución del presente contrato llegasen a surgir discrepancias entre las partes sobre la interpretación de algunas de sus estipulaciones que puedan conducir a la paralización o a la afectación grave del servicio público que se pretende satisfacer con el objeto contratado, la entidad estatal, si no se logra acuerdo, interpretará en acto administrativo debidamente motivado, las estipulaciones o cláusulas objeto de la diferencia.

17. **MODIFICACIÓN UNILATERAL**. Si durante la ejecución del contrato y para evitar la paralización o la afectación grave del servicio público que se deba satisfacer con él, si fuere necesario introducir variaciones en el contrato y previamente las partes no llegan al acuerdo respectivo, la entidad por medio de acto administrativo debidamente motivado, lo modificará mediante la supresión o adición de obras, trabajos, suministros o servicios. Si las modificaciones alteran el valor del contrato en veinte por ciento (20%) o más del valor inicial, el contratista podrá renunciar a la continuación de la ejecución. En este evento, se ordenará la liquidación del contrato y la entidad adoptará de manera inmediata las medidas que fueren necesarias para garantizar la terminación del objeto del mismo.

18. **TERMINACIÓN UNILATERAL.** La entidad en acto administrativo debidamente motivado dispondrá la terminación anticipada del contrato en los siguientes eventos:

A.) Cuando las exigencias del servicio público lo requieran o la situación de orden público lo imponga.

B.) Por muerte o incapacidad física permanente del contratista, si es persona natural, o por disolución de la persona jurídica del contratista.

C.) Por interdicción judicial o declaración de quiebra del contratista.

D.) Por cesación de pagos, concurso de acreedores o embargos judiciales del contratista que afecten de manera grave el cumplimiento del contrato.

E.) La iniciación de trámite concordatario no dará lugar a la declaratoria de terminación unilateral. En tal evento la ejecución se hará con sujeción a las normas sobre administración de negocios del deudor en concordato. La entidad dispondrá las medidas de inspección, control y vigilancia necesarias para asegurar el cumplimiento del objeto contractual e impedir la paralización del servicio.

19. **LIQUIDACIÓN**. Al producirse una causa de terminación del contrato, se procederá a su liquidación, la cual se realizará en un plazo de cuatro (4) meses contados a partir de la fecha de terminación. La liquidación se hará mediante acta firmada por las partes, en la cual constarán los ajustes, revisiones y reconocimientos a que haya lugar, los acuerdos, conciliaciones y transacciones a que llegasen las partes para poner fin a las divergencias presentadas y poder declararse a paz y salvo.

20. **INTEGRALIDAD.** El presente documento hace parte integral del expediente electrónico del proceso y se da por entendido, fechado y firmado una vez se apruebe electrónicamente por las partes a través del Sistema Electrónico para la Contratación Pública –SECOP II Parágrafo: El contrato se regirá por lo dispuesto en la invitación referida, los estudios previos, la propuesta y junto con las disposiciones legales vigente.