Gobernación del CAUCA

FICHA TECNICA
PROCESO DC-SG-MC-007-2026

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 La no entrega de estos requisitos técnicos dará como resultado el rechazo de la propuesta, ya que es requisito técnico habilitante. 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. - La comunicación se realizará mediante una VLAN privada y vRack virtual independiente,	1

	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	1

	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 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.	

FICHA TECNICA
PROCESO DC-SG-MC-007-2026

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

Proponente:	
Representante Legal del proponente (Si aplica):	
Dirección:	Teléfono:
Documento de identificación:	
Firma del Representante Legal (persona natural o jurídica):	