Gobernación de Boyacá | TIC

Tunja, 6 de abril de 2026

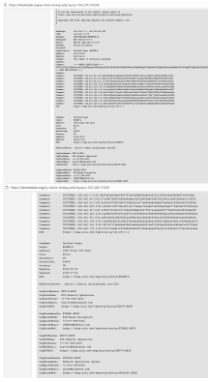
Doctor
JORGE MARIO IBAÑEZ ARANGO
Secretario de Contratación
Gobernación de Boyacá

Asunto: INFORME DE EVALUACIÓN COMPONENTE TÉCNICO DEL PROCESO SMC-GB-023-2026

Respetado, Dr Ibañez:

La Secretaría de TIC y Gobierno Abierto a través de la Dirección de Sistemas de Información, se permite dar evaluación a las ofertas presentadas según el orden del factor económico, en el proceso N° **SMC-GB-023-2026** cuyo objeto es: "*GC1 - PRESTACION DEL SERVICIO DE HOSTING EN SERVIDOR CLOUD DEDICADO PARA EL SITIO WEB, SUBSITIOS Y SEDES ELECTRONICAS CON DOMINIO BOYACA.GOV.CO, ASI COMO SERVICIOS DE EMAIL MARKETING PARA LA GOBERNACION DE BOYACA"* por la vigencia de 3 años y soporte.

1. OFERTA PRESENTADA GRUPO VECTOR SAS POR VALOR DE $65.730.000,00

ESPECIFICACIONES TÉCNICAS REQUERIDAS Propuesta Técnica Anexo 05.					
ITEM	**DESCRIPCIÓN**	**CUMPLE /NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**ESPECIFICACIONES TÉCNICAS MÍNIMA DEL HOSTING** SERVIDOR: Cloud Privado Dedicado DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar 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). CERTIFICACIONES DATACENTER: 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_27001 ISO 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**. 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 certificado.	**NO CUMPLE**	15. propuesta tecnica.pdf Certificaciones Servidor.pdf	1-4 1-73	Se validan las IPS aportadas, las cuales no dan certeza que estén registradas a nombre de Grupo Vector SAS.  Las certificaciones del Datacenter aportadas no vienen acompañadas de un enlace URL oficial del sitio web del Datacenter. No figura el Datacenter propuesto en la declaración de SWIPO.

	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. MANEJO/ADMINISTRACIÓN: Servidor administrado 100% contratista NAVEGACIÓN: 7*24*365 días del año, del 99.6% mensual de alta disponibilidad. COPIAS DE RESPALDO: Incluido. Opción de restaurar en el Cpanel con soporte técnico 7x24. Suministro de un software o sistema comercial para realizar copias de respaldo de los sitios web, bases de datos y todos los archivos alojados en el servidor. El software debe permitir restaurar de forma individual las copias de seguridad de bases de datos, emails, DNS, o full backup de los sitios desde el cpanel/WHM con soporte técnico 7x24 a solicitud de la entidad. Copias completas mensuales, semanales y diarias de seguridad de los datos en servidores externos, 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 Validar y verificar las copias de seguridad permanente de todo el contenido del servidor hasta de 15 días atrás. MIGRACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. INSTALACIÓN Y CONFIGURACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. SOPORTE TÉCNICO ESPECIALIZADO, AUDITORÍA Y MANTENIMIENTO: 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 Business. • 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. SEGURIDAD Y CAPA DE BORDE (CLOUDFLARE BUSINESS): El contratista deberá proveer e implementar una capa de seguridad basada en Cloudflare Business Plan, que cumpla estrictamente con las siguientes funcionalidades: • Redireccionamiento por IP y CNAME (CNAME Flattening): Capacidad de resolución de registros CNAME en el ápice del dominio (dominio raíz) para permitir la redirección de tráfico y gestión de IP de destino sin necesidad de modificar los servidores DNS autoritativos de la entidad, garantizando flexibilidad en la infraestructura. • WAF (Web Application Firewall): Protección activa contra el Top 10 de OWASP, incluyendo bloqueos automáticos para Inyecciones SQL, Cross-Site Scripting (XSS) y mitigación de vulnerabilidades de "Día Cero" mediante reglas administradas. • Mitigación Anti-DDoS Avanzada: Protección ilimitada contra ataques de denegación de servicio en las capas 3, 4 y 7 (volumétricos y de aplicación) con prioridad en la red global de Cloudflare. • Ocultación de IP (Proxy Inverso): Enmascaramiento total de la dirección IP real del servidor de origen para prevenir ataques directos a la infraestructura física.				

	• Certificación SSL/TLS: Implementación de cifrado de extremo a extremo con soporte para TLS 1.3 y gestión automática de certificados. Reglas de Filtrado Dinámico (WAF Custom Rules): Capacidad de crear reglas de firewall personalizadas basadas en geolocalización (IP Colombia), comportamiento de usuario y reputación de IP.				
2	**ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR CLOUD DEDICADO** **HARDWARE MÍNIMO Y ESCALABLE** PROCESADOR: Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 36 cores, verificables durante toda la vigencia por supervisor, auto escalable a mayor potencia en caso de altos niveles de tráfico. MEMORIA RAM: 256 GB DDR5 4800 Mhz auto escalable a más memoria RAM en caso de altos niveles de tráfico. DISCO DURO: 4 discos de 2TB C/U en estado sólido con tecnología NVME Auto escalable en tamaño caso de alcanzar tope de consumo, configurado RAID 10. Verificable desde el Panel. ESPACIO PARA BACKUP REMOTO: 5 TB externo con acceso usuario y clave mediante SSH para transferencia las copias de seguridad desde el servidor cpanel. Cloud. Verificable desde el Panel Cloud. Las credenciales de acceso se deben entregar al supervisor para descargar de backups mensuales durante toda la vigencia del contrato RED HACIA Y DESDE INTERNET: 1 tarjeta de red de 1Gb garantizado ANCHO DE BANDA: Ilimitado **CARACTERISTICAS** PANEL DE CONTROL CPANEL: El contratista realizará la entrega formal del servidor licenciado con panel de control Cpanel /WHM para 200 usuarios, mediante un entorno "Ready-to-Host", cumpliendo con los siguientes hitos de configuración y transferencia de conocimiento: 1. Consolidado de Credenciales y Accesos Matriz de Acceso Seguro: Entrega de llaves SSH, credenciales de usuario root y accesos administrativos al WHM/cPanel bajo protocolos de cifrado. 2. Configuración de Software Entorno de Ejecución: Verificación de la instalación de CloudLinux y cPanel/WHM en sus versiones estables más recientes, incluyendo la configuración de perfiles MultiPHP (desde versiones legacy como 5.3 hasta actuales)., entre otros. 3. Verificación de la Licencia: La licencia se podrá verificar en https://verify.cpanel.net/app/verify con la IP principal asignada al servidor. MANEJO/ADMINISTRACIÓN: Administración Integral de Servidor: Administración Proactiva y Gestión Full-Managed: El contratista asumirá la administración total (100%) del ecosistema de servidor, garantizando la operatividad, seguridad y rendimiento óptimo mediante las siguientes facultades y responsabilidades: 1. Gestión de Infraestructura y Sistema Operativo Aprovisionamiento y Despliegue: Instalación, configuración inicial y despliegue de instancias basadas en AlmaLinux/CloudLinux bajo estándares de industria. Ciclo de Vida del Software: Gestión completa de actualizaciones de Kernel (mediante KernelCare si aplica), parches de seguridad críticos y actualizaciones de sistema operativo sin interrupción de servicio. Hardening (Endurecimiento): Implementación de políticas de seguridad a nivel de OS, cierre de puertos no esenciales, configuración de firewalls proactivos e Imunify360 para mitigación de ataques en tiempo real. 2. Administración del Stack de Aplicaciones (Middleware)	CUMPLE	15. propuesta tecnica.pdf	4-8	

	Optimización de Web Server & PHP: Configuración y tunning de Apache/Nginx/Litespeed y manejadores PHP (FPM/Isapi) según los requerimientos de carga de la entidad. Gestión de Bases de Datos: Administración avanzada de MySQL/MariaDB, incluyendo optimización de variables de entorno, limpieza de logs y monitoreo de consultas lentas (Slow Queries). Ecosistema cPanel/WHM: Administración total del panel, gestión de cuentas, configuración de respaldos (locales y remotos) y monitoreo de integridad de servicios. 3. Conectividad y Servicios de Red Arquitectura de DNS Redundante: Configuración y mantenimiento de clústeres DNS para garantizar la resolución de nombres con tolerancia a fallos. Gestión de Correo y Transferencia: Administración y parcheo de Exim (SMTP), Dovecot (IMAP/POP3) y servicios de FTP, asegurando la correcta entregabilidad de correos y seguridad en transferencias. Seguridad Perimetral y CDN: Integración y gestión de capas de protección externa como Cloudflare, incluyendo reglas de firewall, optimización de caché y gestión de certificados SSL/TLS. 4. Monitoreo y Soporte Continuo Monitoreo 24/7: Supervisión constante de métricas críticas (CPU, RAM, I/O de disco y carga de red) para la resolución preventiva de incidentes. Soporte On-Demand: Capacidad de respuesta inmediata para cualquier requerimiento técnico o aplicación adicional que la entidad solicite para garantizar la continuidad del negocio. SISTEMA OPERATIVO: El servidor debe ser suministrado con el Sistema Operativo CloudLinux OS Shared Pro (o versión superior vigente), configurado y optimizado para entornos de alta criticidad, cumpliendo con las siguientes especificaciones técnicas: • Aislamiento de Recursos (LVE): Implementación de la tecnología Lightweight Virtualized Environment para encapsular cada cuenta de usuario, garantizando que picos de consumo de CPU, RAM o procesos (como los observados en el pool de PHP-FPM) no afecten la disponibilidad de los demás servicios del servidor. • Aislamiento del Sistema de Archivos (CageFS): Activación obligatoria de CageFS para evitar que un usuario pueda ver o acceder a archivos, procesos o información de configuración de otros usuarios o del sistema raíz, mitigando ataques de escalada de privilegios o infecciones cruzadas entre cuentas. • Selector de PHP Hardened: Disponibilidad de múltiples versiones de PHP con parches de seguridad para versiones antiguas (vía HardenedPHP), permitiendo la ejecución segura de aplicaciones que aún no han sido migradas a versiones 8.x. • Monitoreo de Rendimiento en Tiempo Real: Configuración de herramientas de análisis para identificar de forma inmediata qué usuario o script está generando una carga anómala o sufriendo un ataque de denegación de servicio (DoS). • MySQL Governor: Implementación de límites de uso de la base de datos por usuario para evitar que consultas lentas o ataques de inyección saturen el servicio MariaDB/MySQL. SOPORTE PARA DOMINIOS INDEPENDIENTES: Licencia para mínimo 200 dominios con Cpanel independientes. CERTIFICADO SSL: Wildcard, con cifrado SHA-2 y mínimo de 2048 bits y encriptación 128 Mb. Incluye instalación y configuración para el dominio boyaca.gov.co y los subdominios alojados en el servidor. Se debe suministrar reemisiones del certificado ilimitados cada vez que se requiera la instalación en servidores locales de la entidad para servidores Windows y Linux con soporte 24/7 incluido				

	SERVICIOS PARA ADMINISTRACIÓN: Acceso root SSH al servidor Cloud, FTP, VNC, DNS, acceso al servidor mediante sistema de rescate. ACTIVIDAD ESPECIALIZADA: 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). • 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. LICENCIA ANTIVIRUS: Sistema de análisis, detección y prevención de spam, malware, ramsomware y virus en tiempo real. Instalado, configurado y en ejecución para mínimo 100 dominios. Antivirus basado en inteligencia artificial con Cortafuegos avanzado, IDS / IPS, Detección de malware, Defensa proactiva, Manejo de reputación, entre otros con licencia comercial para todos los dominios. LICENCIA SOFTWARE COMERCIAL PARA PARCHADO AUTOMÁTICO DE SCRIPTS Y VULNERABILIDADES: Software de seguridad para realizar el parchado automático de scripts y páginas de todos los sitios del servidor en tiempo real. FIREWALL: Red/Servidor. Firewall Instalado, configurado y en ejecución. 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 DDoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios. IP DEDICADAS: • 4 IPs dedicadas IPV4. • 10 IP dedicadas IPV6 (Se debe incluir suministro, instalación, configuración y soporte 24/7). • Servidor configurado en DualStack con soporte para IPV4 e IPV6. • Suministro del servicio Cloud DNS con soporte Dual Stack, que permita al servidor DNS contar con IPV4 e IPV6.				

	• Se verificará el estado del Dual Stack en https://ready.chair6.net/, tanto para la IPV4/IPV6 como para los dominios como para los servidores DNS PROTECCIÓN ATAQUE DDOS A NIVEL DE DATACENTER Y FIREWALL COMERCIAL: Sí. Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge a nivel de RED en el DATACENTER. BASE DE DATOS: MySQL, PostgreSQL y demás sujetas a necesidad de la entidad con réplicas automáticas para respaldo, recuperación y failover. LENGUAJES DE PROGRAMACIÓN: Javascript/Java/PHP/Perl/Phyton y demás sujetos a necesidad de la entidad. SOFTWARE: Apache/PhpMyAdmin/Tomcat/Joomla/Wordpress/Dupral sujeto a versiones requeridas por la entidad. REPORTES: Dentro del panel deberá disponer de un informe mensual de transferencia (tráfico) web y de los intentos de intrusión. Acceso a estadísticas completas.				
3	**ESPECIFICACIONES TÉCNICAS EMAIL MARKETING** GESTOR DE PLANTILLAS: Disponer de un editor dinámico de textos y contenidos, en el cual se puedan insertar imágenes y audios en los diseños. MULTIUSUARIO Y CREACIÓN DE ROLES: El sistema debe permitir la creación de usuario y roles de acuerdo a la necesidad de la entidad sin restricción. ENVÍOS DESDE DIFERENTES CORREOS AUTORIZADOS DE LA ENTIDAD: La plataforma debe permitir el envío desde diferentes y múltiples correos de remitentes de la entidad sin restricción y con cuentas de usuarios al panel de email marketing diferentes. Ejemplos remitentes: prensa@boyaca.gov.co, boletin@boyaca.gov.co, etc PLANTILLAS PROFESIONALES PREDISEÑADAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML. DISEÑOS Y PLANTILLAS RESPONSIVAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML GESTIÓN DE CONTACTOS Y SUSCRIPTORES: Permitir crear listas de contactos y suscriptores teniendo la opción de organizarlos y clasificarlos de acuerdo con filtros como por ejemplo ciudad, rango de edad, género, etc. Cada suscriptor debe ser único y poder pertenecer a múltiples segmentos y listas de distribución. IMPORTAR/EXPORTAR CONTACTOS: Opción de cargar y exportar en forma masiva desde un archivo Excel o .CSV (esta actividad estará a cargo del contratista y será realizada en caso de migración o a solicitud de la entidad) NÚMERO DE SUSCRIPTORES: Ilimitados sin restricción CREACIÓN Y ENVÍO DE CAMPAÑAS: Cuando se cree un boletín el envío se puede realizar de inmediato o pueda ser programado para ser envío en una fecha y hora específica. NÚMERO DE ENVÍOS EN EL MES: Ilimitados FORMULARIOS: Permitir crear formularios de la suscripción a su lista de correos para insertar en su página Web REPORTES: Generar reportes en tiempo real a la información detallada de correos recibidos, abiertos, rebotados y visitas a enlaces incluidos en su mensaje. SISTEMA ANTI SPAM: Sí. Los correos enviados cumplen con leyes anti- spam, incluida la Ley CAN-SPAM de los Estados Unidos. CANCELACIÓN DE SUSCRIPCIÓN: Sí. Incluir el enlace de cancelación de suscripción en las campañas de correo electrónico. SEGURIDAD SSL: Sí. REDES SOCIALES: Permitir integrar enlaces a los perfiles sociales de la entidad. GOOGLE ANALYTICS: Permitir Integración con Google Analytics SEGUIMIENTO ANÓNIMO Y "FINGERPRINTING": Sí AUTOMATIZACIÓN MULTICANAL NATIVA: Flujos de trabajo Notificaciones Web Push: Enviar un mensaje al navegador del usuario., mensajes de Foco: Mostrar pop-ups o barras personalizadas en tu web basadas en el segmento del usuario (ej: mostrar un cupón solo a quien ya ha comprado antes). FILTROS Y SEGMENTACIÓN: Etiquetas, clics, visitas a URLs específicas, valor de campos personalizados, puntos de lead scoring e incluso la tecnología que usa el usuario.	**CUMPLE**	15. propuesta tecnica.pdf	8-9	

	SEGMENTOS TRANSVERSALES: Posibilidad de mover contactos entre listas automáticamente, contactos disponibles en múltiples listas. SUSCRIPCIÓN A SOUNCLOUD PARA CARGA DE AUDIOS: Plan con la capacidad de subida Ilimitado, que soporte formatos mp3, wav, flac, etc. Con posibilidad de publicar en otras plataformas. El proveedor entregará las credenciales de acceso a la plataforma https://soundcloud.com/ por el término de la vigencia del contrato.				

PERSONAL MÍNIMO REQUERIDO	
El proponente deberá acreditar que cuenta con el personal mínimo requerido para ejecutar el presente contrato, mediante certificaciones suscrita por el Representante Legal en la que manifieste que dispone de los perfiles acordes al objeto del contrato y determinar su disponibilidad de tiempo, actividades a desarrollar y experiencia	CUMPLE

ITEM	DESCRIPCIÓN	CUMPLE/ NO CUMPLE	ARCHIVO	No. FOLIOS	OBSERVACIÓN
1	**PERFIL** Un ingeniero de sistemas o electrónico con especialización en seguridad informática. **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico Especialización en Seguridad Informática Certificado ISO 27001/2022 vigente **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. Acreditar en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso. • Copia diploma Especialista en Seguridad informática. • Certificado internacional Auditor líder ISO 27001/2022 verificable online vigente. No se admiten cursos, se debe contar con certificado internacional vigente.	**NO CUMPLE**	15. personal.pdf	2-22 22-34	Se aporta título de un ingeniero de sistemas, especializado en Construcción de Software y NO con especialización en Seguridad Informática. Se aporta título de un ingeniero de sistemas, especializado en Seguridad Informática, pero no cuenta con el Certificado Internacional Auditor Líder ISO 27001/2022 Las certificaciones de experiencia acreditada en implementación de sistemas de Seguridad de la Información ISO 27001 NO son de entidades públicas.
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así:	**NO CUMPLE**	15. personal.pdf	22-34	Se aporta título de un ingeniero de sistemas, especializado en Seguridad Informática, pero no se evidencia en uno de los certificados la experiencia en los 2 últimos años.

	• Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.				
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**NO CUMPLE**	15. personal.pdf	35-42	Se aporta título de un ingeniero de sistemas, con UN (1) solo certificado que acredita experiencia profesional en implementación y configuración de servicios hosting, firewall, base de datos y administración de servidores Linux, pero no se evidencia que sea en los 2 últimos años. Se aporta otro certificado que no es acorde a la experiencia solicitada para este perfil.

EXPERIENCIA MÍNIMA REQUERIDA					
ITEM	**DESCRIPCIÓN**	**CUMPLE/ NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	El proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas cuyo objeto sea igual o similar al presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera: De conformidad a la Circular Conjunta de fecha junio de 2019 de Despacho del Gobernador y Secretaría de Contratación, el proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas, cuyo objeto sea igual o similar al del presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera. **Número de contratos con los cuales el proponente cumple la experiencia acreditada** / **Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)** De 1 hasta 2 — 75% De 3 hasta 4 — 120% De 5 hasta 6 — 150%	**NO CUMPLE**	10. WEB ESDEGUE 2012.pdf 153 Cesof_70.jpg filarmonica13.pdf pezca 16.pdf	1-3 1 1-2 1-4	El objeto contractual no cumple, en el entendido que su objeto no es igual o similar al presente proceso. No se aporta experiencia en el servicio de Email Marketing, por lo tanto no se tiene en cuenta los contratos con las entidades Escuela Superior de Guerra, Filamónica de Bogotá y AUNAP.

2. OFERTA PRESENTADA POR ROYAL TECH GROUP POR VALOR DE $105.000.000,00

ESPECIFICACIONES TÉCNICAS REQUERIDAS Propuesta Técnica Anexo 05.					
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**ESPECIFICACIONES TÉCNICAS MÍNIMA DEL HOSTING** SERVIDOR: Cloud Privado Dedicado DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar el Datacenter en el cual se alojará el servicio mediante una certificación firmada por el representante legal,	**NO CUMPLE**	2. Cumplimiento Especificaciones Tecnicas.pdf	1-7	No aporta certificación firmada por el representante legal ni evidencias, ni certificado partner o facturas. No se aportan certificaciones del Datacenter.

	además de entregar evidencias de un vínculo con el datacenter (Certificado Partner o Facturas pago último mes). CERTIFICACIONES DATACENTER: 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: 12. ISO_IEC_27001ISO 27001, 27017 y 27018 13. ISO 27701 14. RGPD 15. SOC 1, 2 y 3 16. CSA STAR 17. HIPAA e HITECH 18. PCI-DSS 19. SWIPO 20. ISO 14001 21. ISO 50001 22. Política de Seguridad del datacenter **La no entrega de estos requisitos técnicos dará como resultado el rechazo de la propuesta**. 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 certificado. 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. MANEJO/ADMINISTRACIÓN: Servidor administrado 100% contratista NAVEGACIÓN: 7*24*365 días del año, del 99.6% mensual de alta disponibilidad. COPIAS DE RESPALDO: Incluido. Opción de restaurar en el Cpanel con soporte técnico 7x24. Suministro de un software o sistema comercial para realizar copias de respaldo de los sitios web, bases de datos y todos los archivos alojados en el servidor. El software debe permitir restaurar de forma individual las copias de seguridad de bases de datos, emails, DNS, o full backup de los sitios desde el cpanel/WHM con soporte técnico 7x24 a solicitud de la entidad. Copias completas mensuales, semanales y diarias de seguridad de los datos en servidores externos, 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 Validar y verificar las copias de seguridad permanente de todo el contenido del servidor hasta de 15 días atrás. MIGRACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. INSTALACIÓN Y CONFIGURACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. SOPORTE TÉCNICO ESPECIALIZADO, AUDITORÍA Y MANTENIMIENTO: 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 Business. • 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. SEGURIDAD Y CAPA DE BORDE (CLOUDFLARE BUSINESS): El contratista deberá proveer e implementar una capa de seguridad basada en Cloudflare Business Plan, que cumpla estrictamente con las siguientes funcionalidades: • Redireccionamiento por IP y CNAME (CNAME Flattening): Capacidad de resolución de registros CNAME en el ápice del dominio (dominio raíz) para permitir la redirección de tráfico y gestión de IP de destino sin necesidad de modificar los servidores DNS autoritativos de la entidad, garantizando flexibilidad en la infraestructura. • WAF (Web Application Firewall): Protección activa contra el Top 10 de OWASP, incluyendo bloqueos automáticos para Inyecciones SQL, Cross-Site Scripting (XSS) y mitigación de vulnerabilidades de "Día Cero" mediante reglas administradas. • Mitigación Anti-DDoS Avanzada: Protección ilimitada contra ataques de denegación de servicio en las capas 3, 4 y 7 (volumétricos y de aplicación) con prioridad en la red global de Cloudflare. • Ocultación de IP (Proxy Inverso): Enmascaramiento total de la dirección IP real del servidor de origen para prevenir ataques directos a la infraestructura física. • Certificación SSL/TLS: Implementación de cifrado de extremo a extremo con soporte para TLS 1.3 y gestión automática de certificados. Reglas de Filtrado Dinámico (WAF Custom Rules): Capacidad de crear reglas de firewall personalizadas basadas en geolocalización (IP Colombia), comportamiento de usuario y reputación de IP.				
2	**ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR CLOUD DEDICADO** **HARDWARE MÍNIMO Y ESCALABLE** PROCESADOR: Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 36 cores, verificables durante toda la vigencia por supervisor, auto escalable a mayor potencia en caso de altos niveles de tráfico. MEMORIA RAM: 256 GB DDR5 4800 Mhz auto escalable a más memoria RAM en caso de altos niveles de tráfico. DISCO DURO: 4 discos de 2TB C/U en estado sólido con tecnología NVME Auto escalable en tamaño caso de alcanzar tope de consumo, configurado RAID 10. Verificable desde el Panel. ESPACIO PARA BACKUP REMOTO: 5 TB externo con acceso usuario y clave mediante SSH para transferencia las copias de seguridad desde el servidor cpanel. Cloud. Verificable desde el Panel Cloud. Las credenciales de acceso se deben entregar al supervisor para descargar de backups mensuales durante toda la vigencia del contrato RED HACIA Y DESDE INTERNET: 1 tarjeta de red de 1Gb garantizado ANCHO DE BANDA: Ilimitado **CARACTERISTICAS** PANEL DE CONTROL CPANEL: El contratista realizará la entrega formal del servidor licenciado con panel de control Cpanel /WHM para 200 usuarios, mediante un entorno "Ready-to-Host", cumpliendo con los siguientes hitos de configuración y transferencia de conocimiento: 1. Consolidado de Credenciales y Accesos	CUMPLE	2. Cumplimiento Especificaciones Tecnicas.pdf	7-15	

	Matriz de Acceso Seguro: Entrega de llaves SSH, credenciales de usuario root y accesos administrativos al WHM/cPanel bajo protocolos de cifrado. 2. Configuración de Software Entorno de Ejecución: Verificación de la instalación de CloudLinux y cPanel/WHM en sus versiones estables más recientes, incluyendo la configuración de perfiles MultiPHP (desde versiones legacy como 5.3 hasta actuales)., entre otros. 3. Verificación de la Licencia: La licencia se podrá verificar en https://verify.cpanel.net/app/verify con la IP principal asignada al servidor. MANEJO/ADMINISTRACIÓN: Administración Integral de Servidor: Administración Proactiva y Gestión Full-Managed: El contratista asumirá la administración total (100%) del ecosistema de servidor, garantizando la operatividad, seguridad y rendimiento óptimo mediante las siguientes facultades y responsabilidades: 1. Gestión de Infraestructura y Sistema Operativo Aprovisionamiento y Despliegue: Instalación, configuración inicial y despliegue de instancias basadas en AlmaLinux/CloudLinux bajo estándares de industria. Ciclo de Vida del Software: Gestión completa de actualizaciones de Kernel (mediante KernelCare si aplica), parches de seguridad críticos y actualizaciones de sistema operativo sin interrupción de servicio. Hardening (Endurecimiento): Implementación de políticas de seguridad a nivel de OS, cierre de puertos no esenciales, configuración de firewalls proactivos e Imunify360 para mitigación de ataques en tiempo real. 2. Administración del Stack de Aplicaciones (Middleware) Optimización de Web Server & PHP: Configuración y tunning de Apache/Nginx/Litespeed y manejadores PHP (FPM/lsapi) según los requerimientos de carga de la entidad. Gestión de Bases de Datos: Administración avanzada de MySQL/MariaDB, incluyendo optimización de variables de entorno, limpieza de logs y monitoreo de consultas lentas (Slow Queries). Ecosistema cPanel/WHM: Administración total del panel, gestión de cuentas, configuración de respaldos (locales y remotos) y monitoreo de integridad de servicios. 3. Conectividad y Servicios de Red Arquitectura de DNS Redundante: Configuración y mantenimiento de clústeres DNS para garantizar la resolución de nombres con tolerancia a fallos. Gestión de Correo y Transferencia: Administración y parcheo de Exim (SMTP), Dovecot (IMAP/POP3) y servicios de FTP, asegurando la correcta entregabilidad de correos y seguridad en transferencias. Seguridad Perimetral y CDN: Integración y gestión de capas de protección externa como Cloudflare, incluyendo reglas de firewall, optimización de caché y gestión de certificados SSL/TLS. 4. Monitoreo y Soporte Continuo Monitoreo 24/7: Supervisión constante de métricas críticas (CPU, RAM, I/O de disco y carga de red) para la resolución preventiva de incidentes. Soporte On-Demand: Capacidad de respuesta inmediata para cualquier requerimiento técnico o aplicación adicional que la entidad solicite para garantizar la continuidad del negocio. SISTEMA OPERATIVO: El servidor debe ser suministrado con el Sistema Operativo CloudLinux OS Shared Pro (o versión				

	superior vigente), configurado y optimizado para entornos de alta criticidad, cumpliendo con las siguientes especificaciones técnicas: • Aislamiento de Recursos (LVE): Implementación de la tecnología Lightweight Virtualized Environment para encapsular cada cuenta de usuario, garantizando que picos de consumo de CPU, RAM o procesos (como los observados en el pool de PHP-FPM) no afecten la disponibilidad de los demás servicios del servidor. • Aislamiento del Sistema de Archivos (CageFS): Activación obligatoria de CageFS para evitar que un usuario pueda ver o acceder a archivos, procesos o información de configuración de otros usuarios o del sistema raíz, mitigando ataques de escalada de privilegios o infecciones cruzadas entre cuentas. • Selector de PHP Hardened: Disponibilidad de múltiples versiones de PHP con parches de seguridad para versiones antiguas (vía HardenedPHP), permitiendo la ejecución segura de aplicaciones que aún no han sido migradas a versiones 8.x. • Monitoreo de Rendimiento en Tiempo Real: Configuración de herramientas de análisis para identificar de forma inmediata qué usuario o script está generando una carga anómala o sufriendo un ataque de denegación de servicio (DoS). • MySQL Governor: Implementación de límites de uso de la base de datos por usuario para evitar que consultas lentas o ataques de inyección saturen el servicio MariaDB/MySQL. SOPORTE PARA DOMINIOS INDEPENDIENTES: Licencia para mínimo 200 dominios con Cpanel independientes. CERTIFICADO SSL: Wildcard, con cifrado SHA-2 y mínimo de 2048 bits y encriptación 128 Mb. Incluye instalación y configuración para el dominio boyaca.gov.co y los subdominios alojados en el servidor. Se debe suministrar reemisiones del certificado ilimitados cada vez que se requiera la instalación en servidores locales de la entidad para servidores Windows y Linux con soporte 24/7 incluido SERVICIOS PARA ADMINISTRACIÓN: Acceso root SSH al servidor Cloud, FTP, VNC, DNS, acceso al servidor mediante sistema de rescate. ACTIVIDAD ESPECIALIZADA: 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). • 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. LICENCIA ANTIVIRUS: Sistema de análisis, detección y prevención de spam, malware, ramsomware y virus en tiempo real. Instalado, configurado y en ejecución para mínimo 100 dominios. Antivirus basado en inteligencia artificial con Cortafuegos avanzado, IDS / IPS, Detección de malware, Defensa proactiva, Manejo de reputación, entre otros con licencia comercial para todos los dominios. LICENCIA SOFTWARE COMERCIAL PARA PARCHADO AUTOMÁTICO DE SCRIPTS Y VULNERABILIDADES: Software de seguridad para realizar el parchado automático de scripts y páginas de todos los sitios del servidor en tiempo real. FIREWALL: Red/Servidor. Firewall Instalado, configurado y en ejecución. 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 DDoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios. IP DEDICADAS: • 4 IPs dedicadas IPV4. • 10 IP dedicadas IPV6 (Se debe incluir suministro, instalación, configuración y soporte 24/7). • Servidor configurado en DualStack con soporte para IPV4 e IPV6. • Suministro del servicio Cloud DNS con soporte Dual Stack, que permita al servidor DNS contar con IPV4 e IPV6. • Se verificará el estado del Dual Stack en https://ready.chair6.net/, tanto para la IPV4/IPV6 como para los dominios como para los servidores DNS PROTECCIÓN ATAQUE DDOS A NIVEL DE DATACENTER Y FIREWALL COMERCIAL: Sí. Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge a nivel de RED en el DATACENTER. BASE DE DATOS: MySQL, PostgreSQL y demás sujetas a necesidad de la entidad con réplicas automáticas para respaldo, recuperación y failover. LENGUAJES DE PROGRAMACIÓN: Javascript/Java/PHP/Perl/Phyton y demás sujetos a necesidad de la entidad. SOFTWARE: Apache/PhpMyAdmin/Tomcat/Joomla/Wordpress/Dupral sujeto a versiones requeridas por la entidad. REPORTES: Dentro del panel deberá disponer de un informe mensual de transferencia (tráfico) web y de los intentos de intrusión. Acceso a estadísticas completas.				
3	**ESPECIFICACIONES TÉCNICAS EMAIL MARKETING** GESTOR DE PLANTILLAS: Disponer de un editor dinámico de textos y contenidos, en el cual se puedan insertar imágenes y audios en los diseños. MULTIUSUARIO Y CREACIÓN DE ROLES: El sistema debe permitir la creación de usuario y roles de acuerdo a la necesidad de la entidad sin restricción. ENVÍOS DESDE DIFERENTES CORREOS AUTORIZADOS DE LA ENTIDAD: La plataforma debe permitir el envío desde diferentes y múltiples correos de remitentes de la entidad sin restricción y con cuentas de usuarios al panel de email marketing diferentes. Ejemplos remitentes: prensa@boyaca.gov.co, boletin@boyaca.gov.co, etc	**CUMPLE**	2. Cumplimiento Especificaciones Tecnicas.pdf	15-17	

	PLANTILLAS PROFESIONALES PREDISEÑADAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML. DISEÑOS Y PLANTILLAS RESPONSIVAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML GESTIÓN DE CONTACTOS Y SUSCRIPTORES: Permitir crear listas de contactos y suscriptores teniendo la opción de organizarlos y clasificarlos de acuerdo con filtros como por ejemplo ciudad, rango de edad, género, etc. Cada suscriptor debe ser único y poder pertenecer a múltiples segmentos y listas de distribución. IMPORTAR/EXPORTAR CONTACTOS: Opción de cargar y exportar en forma masiva desde un archivo Excel o .CSV (esta actividad estará a cargo del contratista y será realizada en caso de migración o a solicitud de la entidad) NÚMERO DE SUSCRIPTORES: Ilimitados sin restricción CREACIÓN Y ENVÍO DE CAMPAÑAS: Cuando se cree un boletín el envío se puede realizar de inmediato o pueda ser programado para ser envío en una fecha y hora específica. NÚMERO DE ENVÍOS EN EL MES: Ilimitados FORMULARIOS: Permitir crear formularios de la suscripción a su lista de correos para insertar en su página Web REPORTES: Generar reportes en tiempo real a la información detallada de correos recibidos, abiertos, rebotados y visitas a enlaces incluidos en su mensaje. SISTEMA ANTI SPAM: Sí. Los correos enviados cumplen con leyes anti- spam, incluida la Ley CAN-SPAM de los Estados Unidos. CANCELACIÓN DE SUSCRIPCIÓN: Sí. Incluir el enlace de cancelación de suscripción en las campañas de correo electrónico. SEGURIDAD SSL: Sí. REDES SOCIALES: Permitir integrar enlaces a los perfiles sociales de la entidad. GOOGLE ANALYTICS: Permitir Integración con Google Analytics SEGUIMIENTO ANÓNIMO Y "FINGERPRINTING": Sí AUTOMATIZACIÓN MULTICANAL NATIVA: Flujos de trabajo Notificaciones Web Push: Enviar un mensaje al navegador del usuario., mensajes de Foco: Mostrar pop-ups o barras personalizadas en tu web basadas en el segmento del usuario (ej: mostrar un cupón solo a quien ya ha comprado antes). FILTROS Y SEGMENTACIÓN: Etiquetas, clics, visitas a URLs específicas, valor de campos personalizados, puntos de lead scoring e incluso la tecnología que usa el usuario. SEGMENTOS TRANSVERSALES: Posibilidad de mover contactos entre listas automáticamente, contactos disponibles en múltiples listas. SUSCRIPCIÓN A SOUNCLOUD PARA CARGA DE AUDIOS: Plan con la capacidad de subida Ilimitado, que soporte formatos mp3, wav, flac, etc. Con posibilidad de publicar en otras plataformas. El proveedor entregará las credenciales de acceso a la plataforma https://soundcloud.com/ por el término de la vigencia del contrato.				

PERSONAL MÍNIMO REQUERIDO					
El proponente deberá acreditar que cuenta con el personal mínimo requerido para ejecutar el presente contrato, mediante certificaciones suscrita por el Representante Legal en la que manifieste que dispone de los perfiles acordes al objeto del contrato y determinar su disponibilidad de tiempo, actividades a desarrollar y experiencia					NO CUMPLE. No se adjuntó certificación suscrita por Representante Legal
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**PERFIL** Un ingeniero de sistemas o electrónico con especialización en seguridad informática. **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico Especialización en Seguridad Informática Certificado ISO 27001/2022 vigente **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube, demostrada mediante la	**NO CUMPLE**			No se acredita personal con experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube. No se acredita personal con experiencia en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas.

	presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. Acreditar en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso. • Copia diploma Especialista en Seguridad informática. • Certificado internacional Auditor líder ISO 27001/2022 verificable online vigente. No se admiten cursos, se debe contar con certificado internacional vigente.				
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**NO CUMPLE**			No se acredita personal con experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web. No se aporta documentación solicitada del personal requerido.
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**NO CUMPLE**			No acredita personal con experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux. No se aporta documentación solicitada del personal requerido.
EXPERIENCIA MÍNIMA REQUERIDA					

ITEM	DESCRIPCIÓN	CUMPLE/ NO CUMPLE	ARCHIVO	No. FOLIOS	OBSERVACIÓN
1	El proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas cuyo objeto sea igual o similar al presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera: De conformidad a la Circular Conjunta de fecha junio de 2019 de Despacho del Gobernador y Secretaría de Contratación, el proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas, cuyo objeto sea igual o similar al del presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera. **Número de contratos con los cuales el proponente cumple la experiencia acreditada** / **Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)** De 1 hasta 2 — 75% De 3 hasta 4 — 120% De 5 hasta 6 — 150%	NO CUMPLE			No se presentan contratos y/o certificaciones con entidades públicas o privadas tal cual como se solicita en el presente proceso.

3. OFERTA PRESENTADA POR INSTITUTO DE EDUCACION PARA EL TRABAJO Y EL DESARROLLO HUMANO LULOPY SAS POR VALOR DE $116.000.000,00

ESPECIFICACIONES TÉCNICAS REQUERIDAS Propuesta Técnica Anexo 05.					
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**ESPECIFICACIONES TÉCNICAS MÍNIMA DEL HOSTING** SERVIDOR: Cloud Privado Dedicado DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar 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). CERTIFICACIONES DATACENTER: 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**. 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 certificado.	NO CUMPLE	FORMATOS OFERTA GOB BOYACA.pdf	8-14	No se aporta certificación firmada por el representante legal ni evidencias, ni certificado partner o facturas. No se aportan certificaciones del Datacenter.

	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. MANEJO/ADMINISTRACIÓN: Servidor administrado 100% contratista NAVEGACIÓN: 7*24*365 días del año, del 99.6% mensual de alta disponibilidad. COPIAS DE RESPALDO: Incluido. Opción de restaurar en el Cpanel con soporte técnico 7x24. Suministro de un software o sistema comercial para realizar copias de respaldo de los sitios web, bases de datos y todos los archivos alojados en el servidor. El software debe permitir restaurar de forma individual las copias de seguridad de bases de datos, emails, DNS, o full backup de los sitios desde el cpanel/WHM con soporte técnico 7x24 a solicitud de la entidad. Copias completas mensuales, semanales y diarias de seguridad de los datos en servidores externos, 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 Validar y verificar las copias de seguridad permanente de todo el contenido del servidor hasta de 15 días atrás. MIGRACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. INSTALACIÓN Y CONFIGURACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. SOPORTE TÉCNICO ESPECIALIZADO, AUDITORÍA Y MANTENIMIENTO: 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 Business. • 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. SEGURIDAD Y CAPA DE BORDE (CLOUDFLARE BUSINESS): El contratista deberá proveer e implementar una capa de seguridad basada en Cloudflare Business Plan, que cumpla estrictamente con las siguientes funcionalidades: • Redireccionamiento por IP y CNAME (CNAME Flattening): Capacidad de resolución de registros CNAME en el ápice del dominio (dominio raíz) para permitir la redirección de tráfico y gestión de IP de destino sin necesidad de modificar los servidores DNS autoritativos de la entidad, garantizando flexibilidad en la infraestructura. • WAF (Web Application Firewall): Protección activa contra el Top 10 de OWASP, incluyendo bloqueos automáticos para Inyecciones SQL, Cross-Site Scripting (XSS) y mitigación de vulnerabilidades de "Día Cero" mediante reglas administradas. • Mitigación Anti-DDoS Avanzada: Protección ilimitada contra ataques de denegación de servicio en las capas 3, 4 y 7 (volumétricos y de aplicación) con prioridad en la red global de Cloudflare.				

	• Ocultación de IP (Proxy Inverso): Enmascaramiento total de la dirección IP real del servidor de origen para prevenir ataques directos a la infraestructura física. • Certificación SSL/TLS: Implementación de cifrado de extremo a extremo con soporte para TLS 1.3 y gestión automática de certificados. Reglas de Filtrado Dinámico (WAF Custom Rules): Capacidad de crear reglas de firewall personalizadas basadas en geolocalización (IP Colombia), comportamiento de usuario y reputación de IP.				
2	**ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR CLOUD DEDICADO** **HARDWARE MÍNIMO Y ESCALABLE** PROCESADOR: Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 36 cores, verificables durante toda la vigencia por supervisor, auto escalable a mayor potencia en caso de altos niveles de tráfico. MEMORIA RAM: 256 GB DDR5 4800 Mhz auto escalable a más memoria RAM en caso de altos niveles de tráfico. DISCO DURO: 4 discos de 2TB C/U en estado sólido con tecnología NVME Auto escalable en tamaño caso de alcanzar tope de consumo, configurado RAID 10. Verificable desde el Panel. ESPACIO PARA BACKUP REMOTO: 5 TB externo con acceso usuario y clave mediante SSH para transferencia las copias de seguridad desde el servidor cpanel. Cloud. Verificable desde el Panel Cloud. Las credenciales de acceso se deben entregar al supervisor para descargar de backups mensuales durante toda la vigencia del contrato RED HACIA Y DESDE INTERNET: 1 tarjeta de red de 1Gb garantizado ANCHO DE BANDA: Ilimitado **CARACTERISTICAS** PANEL DE CONTROL CPANEL: El contratista realizará la entrega formal del servidor licenciado con panel de control Cpanel /WHM para 200 usuarios, mediante un entorno "Ready-to-Host", cumpliendo con los siguientes hitos de configuración y transferencia de conocimiento: 1. Consolidado de Credenciales y Accesos Matriz de Acceso Seguro: Entrega de llaves SSH, credenciales de usuario root y accesos administrativos al WHM/cPanel bajo protocolos de cifrado. 2. Configuración de Software Entorno de Ejecución: Verificación de la instalación de CloudLinux y cPanel/WHM en sus versiones estables más recientes, incluyendo la configuración de perfiles MultiPHP (desde versiones legacy como 5.3 hasta actuales)., entre otros. 3. Verificación de la Licencia: La licencia se podrá verificar en https://verify.cpanel.net/app/verify con la IP principal asignada al servidor. MANEJO/ADMINISTRACIÓN: Administración Integral de Servidor: Administración Proactiva y Gestión Full-Managed: El contratista asumirá la administración total (100%) del ecosistema de servidor, garantizando la operatividad, seguridad y rendimiento óptimo mediante las siguientes facultades y responsabilidades: 1. Gestión de Infraestructura y Sistema Operativo Aprovisionamiento y Despliegue: Instalación, configuración inicial y despliegue de instancias basadas en AlmaLinux/CloudLinux bajo estándares de industria. Ciclo de Vida del Software: Gestión completa de actualizaciones de Kernel (mediante KernelCare si aplica), parches de seguridad críticos y actualizaciones de sistema operativo sin interrupción de servicio. Hardening (Endurecimiento): Implementación de políticas de seguridad a nivel de OS, cierre de puertos no esenciales,	CUMPLE	FORMATOS OFERTA GOB BOYACA.pdf	14-22	

	configuración de firewalls proactivos e Imunify360 para mitigación de ataques en tiempo real. 2. Administración del Stack de Aplicaciones (Middleware) Optimización de Web Server & PHP: Configuración y tunning de Apache/Nginx/Litespeed y manejadores PHP (FPM/lsapi) según los requerimientos de carga de la entidad. Gestión de Bases de Datos: Administración avanzada de MySQL/MariaDB, incluyendo optimización de variables de entorno, limpieza de logs y monitoreo de consultas lentas (Slow Queries). Ecosistema cPanel/WHM: Administración total del panel, gestión de cuentas, configuración de respaldos (locales y remotos) y monitoreo de integridad de servicios. 3. Conectividad y Servicios de Red Arquitectura de DNS Redundante: Configuración y mantenimiento de clústeres DNS para garantizar la resolución de nombres con tolerancia a fallos. Gestión de Correo y Transferencia: Administración y parcheo de Exim (SMTP), Dovecot (IMAP/POP3) y servicios de FTP, asegurando la correcta entregabilidad de correos y seguridad en transferencias. Seguridad Perimetral y CDN: Integración y gestión de capas de protección externa como Cloudflare, incluyendo reglas de firewall, optimización de caché y gestión de certificados SSL/TLS. 4. Monitoreo y Soporte Continuo Monitoreo 24/7: Supervisión constante de métricas críticas (CPU, RAM, I/O de disco y carga de red) para la resolución preventiva de incidentes. Soporte On-Demand: Capacidad de respuesta inmediata para cualquier requerimiento técnico o aplicación adicional que la entidad solicite para garantizar la continuidad del negocio. SISTEMA OPERATIVO: El servidor debe ser suministrado con el Sistema Operativo CloudLinux OS Shared Pro (o versión superior vigente), configurado y optimizado para entornos de alta criticidad, cumpliendo con las siguientes especificaciones técnicas: • Aislamiento de Recursos (LVE): Implementación de la tecnología Lightweight Virtualized Environment para encapsular cada cuenta de usuario, garantizando que picos de consumo de CPU, RAM o procesos (como los observados en el pool de PHP-FPM) no afecten la disponibilidad de los demás servicios del servidor. • Aislamiento del Sistema de Archivos (CageFS): Activación obligatoria de CageFS para evitar que un usuario pueda ver o acceder a archivos, procesos o información de configuración de otros usuarios o del sistema raíz, mitigando ataques de escalada de privilegios o infecciones cruzadas entre cuentas. • Selector de PHP Hardened: Disponibilidad de múltiples versiones de PHP con parches de seguridad para versiones antiguas (vía HardenedPHP), permitiendo la ejecución segura de aplicaciones que aún no han sido migradas a versiones 8.x. • Monitoreo de Rendimiento en Tiempo Real: Configuración de herramientas de análisis para identificar de forma inmediata qué usuario o script está generando una carga anómala o sufriendo un ataque de denegación de servicio (DoS). • MySQL Governor: Implementación de límites de uso de la base de datos por usuario para evitar que consultas lentas o ataques de inyección saturen el servicio MariaDB/MySQL. SOPORTE PARA DOMINIOS INDEPENDIENTES: Licencia para mínimo 200 dominios con Cpanel independientes. CERTIFICADO SSL: Wildcard, con cifrado SHA-2 y mínimo de 2048 bits y encriptación 128 Mb. Incluye instalación y				

	configuración para el dominio boyaca.gov.co y los subdominios alojados en el servidor. Se debe suministrar reemisiones del certificado ilimitados cada vez que se requiera la instalación en servidores locales de la entidad para servidores Windows y Linux con soporte 24/7 incluido SERVICIOS PARA ADMINISTRACIÓN: Acceso root SSH al servidor Cloud, FTP, VNC, DNS, acceso al servidor mediante sistema de rescate. ACTIVIDAD ESPECIALIZADA: 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). • 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. LICENCIA ANTIVIRUS: Sistema de análisis, detección y prevención de spam, malware, ramsomware y virus en tiempo real. Instalado, configurado y en ejecución para mínimo 100 dominios. Antivirus basado en inteligencia artificial con Cortafuegos avanzado, IDS / IPS, Detección de malware, Defensa proactiva, Manejo de reputación, entre otros con licencia comercial para todos los dominios. LICENCIA SOFTWARE COMERCIAL PARA PARCHADO AUTOMÁTICO DE SCRIPTS Y VULNERABILIDADES: Software de seguridad para realizar el parchado automático de scripts y páginas de todos los sitios del servidor en tiempo real. FIREWALL: Red/Servidor. Firewall Instalado, configurado y en ejecución. 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 DDoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios. IP DEDICADAS: • 4 IPs dedicadas IPV4. • 10 IP dedicadas IPV6 (Se debe incluir suministro, instalación, configuración y soporte 24/7). • Servidor configurado en DualStack con soporte para IPV4 e IPV6. • Suministro del servicio Cloud DNS con soporte Dual Stack, que permita al servidor DNS contar con IPV4 e IPV6. • Se verificará el estado del Dual Stack en https://ready.chair6.net/, tanto para la IPV4/IPV6 como para los dominios como para los servidores DNS PROTECCIÓN ATAQUE DDOS A NIVEL DE DATACENTER Y FIREWALL COMERCIAL: Sí. Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge a nivel de RED en el DATACENTER. BASE DE DATOS: MySQL, PostgreSQL y demás sujetas a necesidad de la entidad con réplicas automáticas para respaldo, recuperación y failover. LENGUAJES DE PROGRAMACIÓN: Javascript/Java/PHP/Perl/Phyton y demás sujetos a necesidad de la entidad. SOFTWARE: Apache/PhpMyAdmin/Tomcat/Joomla/Wordpress/Dupral sujeto a versiones requeridas por la entidad. REPORTES: Dentro del panel deberá disponer de un informe mensual de transferencia (tráfico) web y de los intentos de intrusión. Acceso a estadísticas completas.				
3	**ESPECIFICACIONES TÉCNICAS EMAIL MARKETING** GESTOR DE PLANTILLAS: Disponer de un editor dinámico de textos y contenidos, en el cual se puedan insertar imágenes y audios en los diseños. MULTIUSUARIO Y CREACIÓN DE ROLES: El sistema debe permitir la creación de usuario y roles de acuerdo a la necesidad de la entidad sin restricción. ENVÍOS DESDE DIFERENTES CORREOS AUTORIZADOS DE LA ENTIDAD: La plataforma debe permitir el envío desde diferentes y múltiples correos de remitentes de la entidad sin restricción y con cuentas de usuarios al panel de email marketing diferentes. Ejemplos remitentes: prensa@boyaca.gov.co, boletin@boyaca.gov.co, etc PLANTILLAS PROFESIONALES PREDISEÑADAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML. DISEÑOS Y PLANTILLAS RESPONSIVAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML GESTIÓN DE CONTACTOS Y SUSCRIPTORES: Permitir crear listas de contactos y suscriptores teniendo la opción de organizarlos y clasificarlos de acuerdo con filtros como por ejemplo ciudad, rango de edad, género, etc. Cada suscriptor debe ser único y poder pertenecer a múltiples segmentos y listas de distribución. IMPORTAR/EXPORTAR CONTACTOS: Opción de cargar y exportar en forma masiva desde un archivo Excel o .CSV (esta actividad estará a cargo del contratista y será realizada en caso de migración o a solicitud de la entidad) NÚMERO DE SUSCRIPTORES: Ilimitados sin restricción CREACIÓN Y ENVÍO DE CAMPAÑAS: Cuando se cree un boletín el envío se puede realizar de inmediato o pueda ser programado para ser envío en una fecha y hora específica. NÚMERO DE ENVÍOS EN EL MES: Ilimitados FORMULARIOS: Permitir crear formularios de la suscripción a su lista de correos para insertar en su página Web REPORTES: Generar reportes en tiempo real a la información detallada de correos recibidos, abiertos, rebotados y visitas a enlaces incluidos en su mensaje. SISTEMA ANTI SPAM: Sí. Los correos enviados cumplen con leyes anti- spam, incluida la Ley CAN-SPAM de los Estados Unidos. CANCELACIÓN DE SUSCRIPCIÓN: Sí. Incluir el enlace de cancelación de suscripción en las campañas de correo electrónico. SEGURIDAD SSL: Sí. REDES SOCIALES: Permitir integrar enlaces a los perfiles sociales de la entidad.	**CUMPLE**	FORMATOS OFERTA GOB BOYACA.pdf	22-24	

	GOOGLE ANALYTICS: Permitir Integración con Google Analytics SEGUIMIENTO ANÓNIMO Y "FINGERPRINTING": Sí AUTOMATIZACIÓN MULTICANAL NATIVA: Flujos de trabajo Notificaciones Web Push: Enviar un mensaje al navegador del usuario., mensajes de Foco: Mostrar pop-ups o barras personalizadas en tu web basadas en el segmento del usuario (ej: mostrar un cupón solo a quien ya ha comprado antes). FILTROS Y SEGMENTACIÓN: Etiquetas, clics, visitas a URLs específicas, valor de campos personalizados, puntos de lead scoring e incluso la tecnología que usa el usuario. SEGMENTOS TRANSVERSALES: Posibilidad de mover contactos entre listas automáticamente, contactos disponibles en múltiples listas. SUSCRIPCIÓN A SOUNCLOUD PARA CARGA DE AUDIOS: Plan con la capacidad de subida Ilimitado, que soporte formatos mp3, wav, flac, etc. Con posibilidad de publicar en otras plataformas. El proveedor entregará las credenciales de acceso a la plataforma https://soundcloud.com/ por el término de la vigencia del contrato.				

PERSONAL MÍNIMO REQUERIDO					
El proponente deberá acreditar que cuenta con el personal mínimo requerido para ejecutar el presente contrato, mediante certificaciones suscrita por el Representante Legal en la que manifieste que dispone de los perfiles acordes al objeto del contrato y determinar su disponibilidad de tiempo, actividades a desarrollar y experiencia					NO CUMPLE. No se adjuntó certificación suscrita por Representante Legal
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**PERFIL** Un ingeniero de sistemas o electrónico con especialización en seguridad informática. **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico Especialización en Seguridad Informática Certificado ISO 27001/2022 vigente **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. Acreditar en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso. • Copia diploma Especialista en Seguridad informática. • Certificado internacional Auditor líder ISO 27001/2022 verificable online vigente. No se admiten cursos, se debe contar con certificado internacional vigente.	**NO CUMPLE**			No se acredita personal con experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube. No se acredita personal con experiencia en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. No se aporta documentación solicitada del personal requerido.
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional.	**NO CUMPLE**			No se acredita personal con experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web. No se aporta documentación solicitada del personal requerido.

	Acreditar experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.				
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**NO CUMPLE**			No acredita personal con experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux. No se aporta documentación solicitada del personal requerido.

EXPERIENCIA MÍNIMA REQUERIDA

ITEM	DESCRIPCIÓN	CUMPLE/ NO CUMPLE	ARCHIVO	No. FOLIOS	OBSERVACIÓN
1	El proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas cuyo objeto sea igual o similar al presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera: De conformidad a la Circular Conjunta de fecha junio de 2019 de Despacho del Gobernador y Secretaría de Contratación, el proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas, cuyo objeto sea igual o similar al del presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera. **Número de contratos con los cuales el proponente cumple la experiencia acreditada** / **Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)** De 1 hasta 2 — 75% De 3 hasta 4 — 120% De 5 hasta 6 — 150%	NO CUMPLE			No se presentan contratos y/o certificaciones con entidades públicas o privadas tal cual como se solicita en el presente proceso.

4. OFERTA PRESENTADA POR RYD POR VALOR DE $128.325.000,00

ESPECIFICACIONES TÉCNICAS REQUERIDAS Propuesta Técnica Anexo 05.					
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**ESPECIFICACIONES TÉCNICAS MÍNIMA DEL HOSTING** SERVIDOR: Cloud Privado Dedicado DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar 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). CERTIFICACIONES DATACENTER: 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**. 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 certificado. 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. MANEJO/ADMINISTRACIÓN: Servidor administrado 100% contratista NAVEGACIÓN: 7*24*365 días del año, del 99.6% mensual de alta disponibilidad. COPIAS DE RESPALDO: Incluido. Opción de restaurar en el Cpanel con soporte técnico 7x24. Suministro de un software o sistema comercial para realizar copias de respaldo de los sitios web, bases de datos y todos los archivos alojados en el servidor. El software debe permitir restaurar de forma individual las copias de seguridad de bases de datos, emails, DNS, o full backup de los sitios desde el cpanel/WHM con soporte técnico 7x24 a solicitud de la entidad. Copias completas mensuales, semanales y diarias de seguridad de los datos en servidores externos, 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 Validar y verificar las copias de seguridad permanente de todo el contenido del servidor hasta de 15 días atrás. MIGRACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas	**NO CUMPLE**	ANEXOS RYD.pdf	4-10	No se aporta certificación firmada por el representante legal ni evidencias, ni certificado partner o facturas. No se aportan Certificaciones del Datacenter ni enlaces URl oficiales.

	actuales de php, extensiones, mysql y demás parámetros configurados e instalados. INSTALACIÓN Y CONFIGURACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. SOPORTE TÉCNICO ESPECIALIZADO, AUDITORÍA Y MANTENIMIENTO: 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 Business.				

	• 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. SEGURIDAD Y CAPA DE BORDE (CLOUDFLARE BUSINESS): El contratista deberá proveer e implementar una capa de seguridad basada en Cloudflare Business Plan, que cumpla estrictamente con las siguientes funcionalidades: • Redireccionamiento por IP y CNAME (CNAME Flattening): Capacidad de resolución de registros CNAME en el ápice del dominio (dominio raíz) para permitir la redirección de tráfico y gestión de IP de destino sin necesidad de modificar los servidores DNS autoritativos de la entidad, garantizando flexibilidad en la infraestructura. • WAF (Web Application Firewall): Protección activa contra el Top 10 de OWASP, incluyendo bloqueos automáticos para Inyecciones SQL, Cross-Site Scripting (XSS) y mitigación de vulnerabilidades de "Día Cero" mediante reglas administradas. • Mitigación Anti-DDoS Avanzada: Protección ilimitada contra ataques de denegación de servicio en las capas 3, 4 y 7 (volumétricos y de aplicación) con prioridad en la red global de Cloudflare. • Ocultación de IP (Proxy Inverso): Enmascaramiento total de la dirección IP real del servidor de origen para prevenir ataques directos a la infraestructura física. • Certificación SSL/TLS: Implementación de cifrado de extremo a extremo con soporte para TLS 1.3 y gestión automática de certificados. Reglas de Filtrado Dinámico (WAF Custom Rules): Capacidad de crear reglas de firewall personalizadas basadas en geolocalización (IP Colombia), comportamiento de usuario y reputación de IP.				
2	**ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR CLOUD DEDICADO** **HARDWARE MÍNIMO Y ESCALABLE** PROCESADOR: Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 36 cores, verificables durante toda la vigencia por supervisor, auto escalable a mayor potencia en caso de altos niveles de tráfico. MEMORIA RAM: 256 GB DDR5 4800 Mhz auto escalable a más memoria RAM en caso de altos niveles de tráfico. DISCO DURO: 4 discos de 2TB C/U en estado sólido con tecnología NVME Auto escalable en tamaño caso de alcanzar tope de consumo, configurado RAID 10. Verificable desde el Panel. ESPACIO PARA BACKUP REMOTO: 5 TB externo con acceso usuario y clave mediante SSH para transferencia las copias de seguridad desde el servidor cpanel. Cloud. Verificable desde el Panel Cloud. Las credenciales de acceso se deben entregar al supervisor para descargar de backups mensuales durante toda la vigencia del contrato RED HACIA Y DESDE INTERNET: 1 tarjeta de red de 1Gb garantizado ANCHO DE BANDA: Ilimitado	**CUMPLE**	ANEXOS RYD.pdf	10-18	

	CARACTERISTICAS PANEL DE CONTROL CPANEL: El contratista realizará la entrega formal del servidor licenciado con panel de control Cpanel /WHM para 200 usuarios, mediante un entorno "Ready-to-Host", cumpliendo con los siguientes hitos de configuración y transferencia de conocimiento: 1. Consolidado de Credenciales y Accesos Matriz de Acceso Seguro: Entrega de llaves SSH, credenciales de usuario root y accesos administrativos al WHM/cPanel bajo protocolos de cifrado. 2. Configuración de Software Entorno de Ejecución: Verificación de la instalación de CloudLinux y cPanel/WHM en sus versiones estables más recientes, incluyendo la configuración de perfiles MultiPHP (desde versiones legacy como 5.3 hasta actuales)., entre otros. 3. Verificación de la Licencia: La licencia se podrá verificar en https://verify.cpanel.net/app/verify con la IP principal asignada al servidor. MANEJO/ADMINISTRACIÓN: Administración Integral de Servidor: Administración Proactiva y Gestión Full-Managed: El contratista asumirá la administración total (100%) del ecosistema de servidor, garantizando la operatividad, seguridad y rendimiento óptimo mediante las siguientes facultades y responsabilidades: 1. Gestión de Infraestructura y Sistema Operativo Aprovisionamiento y Despliegue: Instalación, configuración inicial y despliegue de instancias basadas en AlmaLinux/CloudLinux bajo estándares de industria. Ciclo de Vida del Software: Gestión completa de actualizaciones de Kernel (mediante KernelCare si aplica), parches de seguridad críticos y actualizaciones de sistema operativo sin interrupción de servicio. Hardening (Endurecimiento): Implementación de políticas de seguridad a nivel de OS, cierre de puertos no esenciales, configuración de firewalls proactivos e Imunify360 para mitigación de ataques en tiempo real. 2. Administración del Stack de Aplicaciones (Middleware) Optimización de Web Server & PHP: Configuración y tunning de Apache/Nginx/Litespeed y manejadores PHP (FPM/lsapi) según los requerimientos de carga de la entidad. Gestión de Bases de Datos: Administración avanzada de MySQL/MariaDB, incluyendo optimización de variables de entorno, limpieza de logs y monitoreo de consultas lentas (Slow Queries). Ecosistema cPanel/WHM: Administración total del panel, gestión de cuentas, configuración de respaldos (locales y remotos) y monitoreo de integridad de servicios. 3. Conectividad y Servicios de Red Arquitectura de DNS Redundante: Configuración y mantenimiento de clústeres DNS para garantizar la resolución de nombres con tolerancia a fallos. Gestión de Correo y Transferencia: Administración y parcheo de Exim (SMTP), Dovecot (IMAP/POP3) y servicios de FTP, asegurando la correcta entregabilidad de correos y seguridad en transferencias. Seguridad Perimetral y CDN: Integración y gestión de capas de protección externa como Cloudflare, incluyendo reglas de firewall, optimización de caché y gestión de certificados SSL/TLS. 4. Monitoreo y Soporte Continuo				

	Monitoreo 24/7: Supervisión constante de métricas críticas (CPU, RAM, I/O de disco y carga de red) para la resolución preventiva de incidentes. Soporte On-Demand: Capacidad de respuesta inmediata para cualquier requerimiento técnico o aplicación adicional que la entidad solicite para garantizar la continuidad del negocio. SISTEMA OPERATIVO: El servidor debe ser suministrado con el Sistema Operativo CloudLinux OS Shared Pro (o versión superior vigente), configurado y optimizado para entornos de alta criticidad, cumpliendo con las siguientes especificaciones técnicas: • Aislamiento de Recursos (LVE): Implementación de la tecnología Lightweight Virtualized Environment para encapsular cada cuenta de usuario, garantizando que picos de consumo de CPU, RAM o procesos (como los observados en el pool de PHP-FPM) no afecten la disponibilidad de los demás servicios del servidor. • Aislamiento del Sistema de Archivos (CageFS): Activación obligatoria de CageFS para evitar que un usuario pueda ver o acceder a archivos, procesos o información de configuración de otros usuarios o del sistema raíz, mitigando ataques de escalada de privilegios o infecciones cruzadas entre cuentas. • Selector de PHP Hardened: Disponibilidad de múltiples versiones de PHP con parches de seguridad para versiones antiguas (vía HardenedPHP), permitiendo la ejecución segura de aplicaciones que aún no han sido migradas a versiones 8.x. • Monitoreo de Rendimiento en Tiempo Real: Configuración de herramientas de análisis para identificar de forma inmediata qué usuario o script está generando una carga anómala o sufriendo un ataque de denegación de servicio (DoS). • MySQL Governor: Implementación de límites de uso de la base de datos por usuario para evitar que consultas lentas o ataques de inyección saturen el servicio MariaDB/MySQL. SOPORTE PARA DOMINIOS INDEPENDIENTES: Licencia para mínimo 200 dominios con Cpanel independientes. CERTIFICADO SSL: Wildcard, con cifrado SHA-2 y mínimo de 2048 bits y encriptación 128 Mb. Incluye instalación y configuración para el dominio boyaca.gov.co y los subdominios alojados en el servidor. Se debe suministrar reemisiones del certificado ilimitados cada vez que se requiera la instalación en servidores locales de la entidad para servidores Windows y Linux con soporte 24/7 incluido SERVICIOS PARA ADMINISTRACIÓN: Acceso root SSH al servidor Cloud, FTP, VNC, DNS, acceso al servidor mediante sistema de rescate. ACTIVIDAD ESPECIALIZADA: 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).				

	• 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. LICENCIA ANTIVIRUS: Sistema de análisis, detección y prevención de spam, malware, ramsomware y virus en tiempo real. Instalado, configurado y en ejecución para mínimo 100 dominios. Antivirus basado en inteligencia artificial con Cortafuegos avanzado, IDS / IPS, Detección de malware, Defensa proactiva, Manejo de reputación, entre otros con licencia comercial para todos los dominios. LICENCIA SOFTWARE COMERCIAL PARA PARCHADO AUTOMÁTICO DE SCRIPTS Y VULNERABILIDADES: Software de seguridad para realizar el parchado automático de scripts y páginas de todos los sitios del servidor en tiempo real. FIREWALL: Red/Servidor. Firewall Instalado, configurado y en ejecución. 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 DDoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios. IP DEDICADAS: • 4 IPs dedicadas IPV4. • 10 IP dedicadas IPV6 (Se debe incluir suministro, instalación, configuración y soporte 24/7). • Servidor configurado en DualStack con soporte para IPV4 e IPV6. • Suministro del servicio Cloud DNS con soporte Dual Stack, que permita al servidor DNS contar con IPV4 e IPV6. • Se verificará el estado del Dual Stack en https://ready.chair6.net/, tanto para la IPV4/IPV6 como para los dominios como para los servidores DNS PROTECCIÓN ATAQUE DDOS A NIVEL DE DATACENTER Y FIREWALL COMERCIAL: Sí. Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge a nivel de RED en el DATACENTER. BASE DE DATOS: MySQL, PostgreSQL y demás sujetas a necesidad de la entidad con réplicas automáticas para respaldo, recuperación y failover. LENGUAJES DE PROGRAMACIÓN: Javascript/Java/PHP/Perl/Phyton y demás sujetos a necesidad de la entidad. SOFTWARE: Apache/PhpMyAdmin/Tomcat/Joomla/Wordpress/Dupral sujeto a versiones requeridas por la entidad. REPORTES: Dentro del panel deberá disponer de un informe mensual de transferencia (tráfico) web y de los intentos de intrusión. Acceso a estadísticas completas.				
3	**ESPECIFICACIONES TÉCNICAS EMAIL MARKETING** GESTOR DE PLANTILLAS: Disponer de un editor dinámico de textos y contenidos, en el cual se puedan insertar imágenes y audios en los diseños.	**CUMPLE**	ANEXOS RYD.pdf	18-20	

	MULTIUSUARIO Y CREACIÓN DE ROLES: El sistema debe permitir la creación de usuario y roles de acuerdo a la necesidad de la entidad sin restricción. ENVÍOS DESDE DIFERENTES CORREOS AUTORIZADOS DE LA ENTIDAD: La plataforma debe permitir el envío desde diferentes y múltiples correos de remitentes de la entidad sin restricción y con cuentas de usuarios al panel de email marketing diferentes. Ejemplos remitentes: prensa@boyaca.gov.co, boletin@boyaca.gov.co, etc PLANTILLAS PROFESIONALES PREDISEÑADAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML. DISEÑOS Y PLANTILLAS RESPONSIVAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML GESTIÓN DE CONTACTOS Y SUSCRIPTORES: Permitir crear listas de contactos y suscriptores teniendo la opción de organizarlos y clasificarlos de acuerdo con filtros como por ejemplo ciudad, rango de edad, género, etc. Cada suscriptor debe ser único y poder pertenecer a múltiples segmentos y listas de distribución. IMPORTAR/EXPORTAR CONTACTOS: Opción de cargar y exportar en forma masiva desde un archivo Excel o .CSV (esta actividad estará a cargo del contratista y será realizada en caso de migración o a solicitud de la entidad) NÚMERO DE SUSCRIPTORES: Ilimitados sin restricción CREACIÓN Y ENVÍO DE CAMPAÑAS: Cuando se cree un boletín el envío se puede realizar de inmediato o pueda ser programado para ser envío en una fecha y hora específica. NÚMERO DE ENVÍOS EN EL MES: Ilimitados FORMULARIOS: Permitir crear formularios de la suscripción a su lista de correos para insertar en su página Web REPORTES: Generar reportes en tiempo real a la información detallada de correos recibidos, abiertos, rebotados y visitas a enlaces incluidos en su mensaje. SISTEMA ANTI SPAM: Sí. Los correos enviados cumplen con leyes anti- spam, incluida la Ley CAN-SPAM de los Estados Unidos. CANCELACIÓN DE SUSCRIPCIÓN: Sí. Incluir el enlace de cancelación de suscripción en las campañas de correo electrónico. SEGURIDAD SSL: Sí. REDES SOCIALES: Permitir integrar enlaces a los perfiles sociales de la entidad. GOOGLE ANALYTICS: Permitir Integración con Google Analytics SEGUIMIENTO ANÓNIMO Y "FINGERPRINTING": Sí AUTOMATIZACIÓN MULTICANAL NATIVA: Flujos de trabajo Notificaciones Web Push: Enviar un mensaje al navegador del usuario., mensajes de Foco: Mostrar pop-ups o barras personalizadas en tu web basadas en el segmento del usuario (ej: mostrar un cupón solo a quien ya ha comprado antes). FILTROS Y SEGMENTACIÓN: Etiquetas, clics, visitas a URLs específicas, valor de campos personalizados, puntos de lead scoring e incluso la tecnología que usa el usuario. SEGMENTOS TRANSVERSALES: Posibilidad de mover contactos entre listas automáticamente, contactos disponibles en múltiples listas. SUSCRIPCIÓN A SOUNCLOUD PARA CARGA DE AUDIOS: Plan con la capacidad de subida Ilimitado, que soporte formatos mp3, wav, flac, etc. Con posibilidad de publicar en otras plataformas. El proveedor entregará las credenciales de acceso a la plataforma https://soundcloud.com/ por el término de la vigencia del contrato.				

PERSONAL MÍNIMO REQUERIDO	
El proponente deberá acreditar que cuenta con el personal mínimo requerido para ejecutar el presente contrato, mediante certificaciones suscrita por el Representante Legal en la que manifieste que dispone de los perfiles acordes al objeto del contrato y determinar su disponibilidad de tiempo, actividades a desarrollar y experiencia	NO CUMPLE. No se adjuntó certificación suscrita por Representante Legal

ITEM	DESCRIPCIÓN	CUMPLE/NO CUMPLE	ARCHIVO	No. FOLIOS	OBSERVACIÓN
1	**PERFIL** Un ingeniero de sistemas o electrónico con especialización en seguridad informática. **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico Especialización en Seguridad Informática Certificado ISO 27001/2022 vigente	**NO CUMPLE**	HOJA DE VIDA RAUL - ELECTRICO.pdf	1-24	Se aporta título de un ingeniero Electrónico, especializado en Gerencia de Proyectos y NO con especialización en Seguridad Informática.

	EXPERIENCIA MÍNIMA El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. Acreditar en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso. • Copia diploma Especialista en Seguridad informática. • Certificado internacional Auditor líder ISO 27001/2022 verificable online vigente. No se admiten cursos, se debe contar con certificado internacional vigente.		HOJA DE VIDA ING SISTEMAS.zip 11. TARJETAS DE ALEJANDRO.pdf Hoja de vida Alejandro Rojas Andrade.pdf	 1-3 1-6	No aporta el Certificado internacional Auditor líder ISO 27001/2022. Se aporta título de un ingeniero de sistemas con especialización en telecomunicaciones, no anexa certificaciones de experiencia específica ni documentación anexa solicitada.
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**NO CUMPLE**	hoja de vida personal - ing sistemas.pdf	1-10	Se aporta título de un ingeniero de sistemas, no anexa certificaciones de experiencia específica ni documentación anexa solicitada.
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así:	**NO CUMPLE**			No acredita personal con experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux. No se aporta documentación solicitada del personal requerido.

	• Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.				

EXPERIENCIA MÍNIMA REQUERIDA					
ITEM	**DESCRIPCIÓN**	**CUMPLE/ NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	El proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas cuyo objeto sea igual o similar al presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera: De conformidad a la Circular Conjunta de fecha junio de 2019 de Despacho del Gobernador y Secretaría de Contratación, el proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas, cuyo objeto sea igual o similar al del presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera. **Número de contratos con los cuales el proponente cumple la experiencia acreditada** / **Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)** De 1 hasta 2 — 75% De 3 hasta 4 — 120% De 5 hasta 6 — 150%	**NO CUMPLE**	EXP 2.pdf GISS 2131 - MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE INFRAESTRUCTURA TECNOLOGICA PARA ALMACENAMIENTO DE DATOS, SERVIDORES DE ALTO RENDIMIENT.pdf	1-10 1-4	En archivo presentado se evidencia documento denominado COMUNICACIÓN DE ACEPTACIÓN DE OFERTA SPC-CMC-089-2024, no obstante, el mismo no corresponde a certificación de contrato ejecutado o liquidado o a su respectiva acta de liquidación. El objeto no es igual o similar al del presente proceso. El objeto no es igual o similar al del presente proceso.

5. OFERTA PRESENTADA POR MIHOSTING SAS POR VALOR DE $141.490.000,00

ESPECIFICACIONES TÉCNICAS REQUERIDAS Propuesta Técnica Anexo 05.					
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**ESPECIFICACIONES TÉCNICAS MÍNIMA DEL HOSTING** SERVIDOR: Cloud Privado Dedicado DATACENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar 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). CERTIFICACIONES DATACENTER: 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**. 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	**CUMPLE**	ANEXO 5 Propuesta Tecnica.pdf ANEXO 5 Propuesta Tecnica_Datacenter.pdf	1-7 18-28	

	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 certificado. 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. MANEJO/ADMINISTRACIÓN: Servidor administrado 100% contratista NAVEGACIÓN: 7*24*365 días del año, del 99.6% mensual de alta disponibilidad. COPIAS DE RESPALDO: Incluido. Opción de restaurar en el Cpanel con soporte técnico 7x24. Suministro de un software o sistema comercial para realizar copias de respaldo de los sitios web, bases de datos y todos los archivos alojados en el servidor. El software debe permitir restaurar de forma individual las copias de seguridad de bases de datos, emails, DNS, o full backup de los sitios desde el cpanel/WHM con soporte técnico 7x24 a solicitud de la entidad. Copias completas mensuales, semanales y diarias de seguridad de los datos en servidores externos, 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 Validar y verificar las copias de seguridad permanente de todo el contenido del servidor hasta de 15 días atrás. MIGRACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. INSTALACIÓN Y CONFIGURACIÓN: Migrar la página web con dominio boyaca.gov.co en todas las páginas y portales alojados en el servidor actual, base datos, configuraciones personalizadas actuales de php, extensiones, mysql y demás parámetros configurados e instalados. SOPORTE TÉCNICO ESPECIALIZADO, AUDITORÍA Y MANTENIMIENTO: 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 Business. • 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. SEGURIDAD Y CAPA DE BORDE (CLOUDFLARE BUSINESS): El contratista deberá proveer e implementar una capa de seguridad basada en Cloudflare Business Plan, que cumpla estrictamente con las siguientes funcionalidades: • Redireccionamiento por IP y CNAME (CNAME Flattening): Capacidad de resolución de registros CNAME en el ápice del dominio (dominio raíz) para permitir la redirección de tráfico y gestión de IP de destino sin necesidad de modificar los servidores DNS autoritativos de la entidad, garantizando flexibilidad en la infraestructura. • WAF (Web Application Firewall): Protección activa contra el Top 10 de OWASP, incluyendo bloqueos automáticos para Inyecciones SQL, Cross-Site Scripting (XSS) y mitigación de vulnerabilidades de "Día Cero" mediante reglas administradas.				

	• Mitigación Anti-DDoS Avanzada: Protección ilimitada contra ataques de denegación de servicio en las capas 3, 4 y 7 (volumétricos y de aplicación) con prioridad en la red global de Cloudflare. • Ocultación de IP (Proxy Inverso): Enmascaramiento total de la dirección IP real del servidor de origen para prevenir ataques directos a la infraestructura física. • Certificación SSL/TLS: Implementación de cifrado de extremo a extremo con soporte para TLS 1.3 y gestión automática de certificados. Reglas de Filtrado Dinámico (WAF Custom Rules): Capacidad de crear reglas de firewall personalizadas basadas en geolocalización (IP Colombia), comportamiento de usuario y reputación de IP.				
2	**ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR CLOUD DEDICADO** **HARDWARE MÍNIMO Y ESCALABLE** PROCESADOR: Intel Xeon Gold 6554S (2.2 Ghz/3 Ghz)) o superior de mínimo 36 cores, verificables durante toda la vigencia por supervisor, auto escalable a mayor potencia en caso de altos niveles de tráfico. MEMORIA RAM: 256 GB DDR5 4800 Mhz auto escalable a más memoria RAM en caso de altos niveles de tráfico. DISCO DURO: 4 discos de 2TB C/U en estado sólido con tecnología NVME Auto escalable en tamaño caso de alcanzar tope de consumo, configurado RAID 10. Verificable desde el Panel. ESPACIO PARA BACKUP REMOTO: 5 TB externo con acceso usuario y clave mediante SSH para transferencia las copias de seguridad desde el servidor cpanel. Cloud. Verificable desde el Panel Cloud. Las credenciales de acceso se deben entregar al supervisor para descargar de backups mensuales durante toda la vigencia del contrato RED HACIA Y DESDE INTERNET: 1 tarjeta de red de 1Gb garantizado ANCHO DE BANDA: Ilimitado **CARACTERISTICAS** PANEL DE CONTROL CPANEL: El contratista realizará la entrega formal del servidor licenciado con panel de control Cpanel /WHM para 200 usuarios, mediante un entorno "Ready-to-Host", cumpliendo con los siguientes hitos de configuración y transferencia de conocimiento: 1. Consolidado de Credenciales y Accesos Matriz de Acceso Seguro: Entrega de llaves SSH, credenciales de usuario root y accesos administrativos al WHM/cPanel bajo protocolos de cifrado. 2. Configuración de Software Entorno de Ejecución: Verificación de la instalación de CloudLinux y cPanel/WHM en sus versiones estables más recientes, incluyendo la configuración de perfiles MultiPHP (desde versiones legacy como 5.3 hasta actuales)., entre otros. 3. Verificación de la Licencia: La licencia se podrá verificar en https://verify.cpanel.net/app/verify con la IP principal asignada al servidor. MANEJO/ADMINISTRACIÓN: Administración Integral de Servidor: Administración Proactiva y Gestión Full-Managed: El contratista asumirá la administración total (100%) del ecosistema de servidor, garantizando la operatividad, seguridad y rendimiento óptimo mediante las siguientes facultades y responsabilidades: 1. Gestión de Infraestructura y Sistema Operativo Aprovisionamiento y Despliegue: Instalación, configuración inicial y despliegue de instancias basadas en AlmaLinux/CloudLinux bajo estándares de industria.	**CUMPLE**	ANEXO 5 Propuesta Tecnica.pdf	7-15	

	Ciclo de Vida del Software: Gestión completa de actualizaciones de Kernel (mediante KernelCare si aplica), parches de seguridad críticos y actualizaciones de sistema operativo sin interrupción de servicio. Hardening (Endurecimiento): Implementación de políticas de seguridad a nivel de OS, cierre de puertos no esenciales, configuración de firewalls proactivos e Imunify360 para mitigación de ataques en tiempo real. 2. Administración del Stack de Aplicaciones (Middleware) Optimización de Web Server & PHP: Configuración y tunning de Apache/Nginx/Litespeed y manejadores PHP (FPM/lsapi) según los requerimientos de carga de la entidad. Gestión de Bases de Datos: Administración avanzada de MySQL/MariaDB, incluyendo optimización de variables de entorno, limpieza de logs y monitoreo de consultas lentas (Slow Queries). Ecosistema cPanel/WHM: Administración total del panel, gestión de cuentas, configuración de respaldos (locales y remotos) y monitoreo de integridad de servicios. 3. Conectividad y Servicios de Red Arquitectura de DNS Redundante: Configuración y mantenimiento de clústeres DNS para garantizar la resolución de nombres con tolerancia a fallos. Gestión de Correo y Transferencia: Administración y parcheo de Exim (SMTP), Dovecot (IMAP/POP3) y servicios de FTP, asegurando la correcta entregabilidad de correos y seguridad en transferencias. Seguridad Perimetral y CDN: Integración y gestión de capas de protección externa como Cloudflare, incluyendo reglas de firewall, optimización de caché y gestión de certificados SSL/TLS. 4. Monitoreo y Soporte Continuo Monitoreo 24/7: Supervisión constante de métricas críticas (CPU, RAM, I/O de disco y carga de red) para la resolución preventiva de incidentes. Soporte On-Demand: Capacidad de respuesta inmediata para cualquier requerimiento técnico o aplicación adicional que la entidad solicite para garantizar la continuidad del negocio. SISTEMA OPERATIVO: El servidor debe ser suministrado con el Sistema Operativo CloudLinux OS Shared Pro (o versión superior vigente), configurado y optimizado para entornos de alta criticidad, cumpliendo con las siguientes especificaciones técnicas: • Aislamiento de Recursos (LVE): Implementación de la tecnología Lightweight Virtualized Environment para encapsular cada cuenta de usuario, garantizando que picos de consumo de CPU, RAM o procesos (como los observados en el pool de PHP-FPM) no afecten la disponibilidad de los demás servicios del servidor. • Aislamiento del Sistema de Archivos (CageFS): Activación obligatoria de CageFS para evitar que un usuario pueda ver o acceder a archivos, procesos o información de configuración de otros usuarios o del sistema raíz, mitigando ataques de escalada de privilegios o infecciones cruzadas entre cuentas. • Selector de PHP Hardened: Disponibilidad de múltiples versiones de PHP con parches de seguridad para versiones antiguas (vía HardenedPHP), permitiendo la ejecución segura de aplicaciones que aún no han sido migradas a versiones 8.x. • Monitoreo de Rendimiento en Tiempo Real: Configuración de herramientas de análisis para identificar de forma inmediata qué usuario o script está generando una carga anómala o sufriendo un ataque de denegación de servicio (DoS).				

	• MySQL Governor: Implementación de límites de uso de la base de datos por usuario para evitar que consultas lentas o ataques de inyección saturen el servicio MariaDB/MySQL. SOPORTE PARA DOMINIOS INDEPENDIENTES: Licencia para mínimo 200 dominios con Cpanel independientes. CERTIFICADO SSL: Wildcard, con cifrado SHA-2 y mínimo de 2048 bits y encriptación 128 Mb. Incluye instalación y configuración para el dominio boyaca.gov.co y los subdominios alojados en el servidor. Se debe suministrar reemisiones del certificado ilimitados cada vez que se requiera la instalación en servidores locales de la entidad para servidores Windows y Linux con soporte 24/7 incluido SERVICIOS PARA ADMINISTRACIÓN: Acceso root SSH al servidor Cloud, FTP, VNC, DNS, acceso al servidor mediante sistema de rescate. ACTIVIDAD ESPECIALIZADA: 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). • 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. LICENCIA ANTIVIRUS: Sistema de análisis, detección y prevención de spam, malware, ramsomware y virus en tiempo real. Instalado, configurado y en ejecución para mínimo 100 dominios. Antivirus basado en inteligencia artificial con Cortafuegos avanzado, IDS / IPS, Detección de malware, Defensa proactiva, Manejo de reputación, entre otros con licencia comercial para todos los dominios. LICENCIA SOFTWARE COMERCIAL PARA PARCHADO AUTOMÁTICO DE SCRIPTS Y VULNERABILIDADES:				

	Software de seguridad para realizar el parchado automático de scripts y páginas de todos los sitios del servidor en tiempo real. FIREWALL: Red/Servidor. Firewall Instalado, configurado y en ejecución. 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 DDoS y escaneos de puertos, con licencia comercial con licencia para todos los dominios. IP DEDICADAS: • 4 IPs dedicadas IPV4. • 10 IP dedicadas IPV6 (Se debe incluir suministro, instalación, configuración y soporte 24/7). • Servidor configurado en DualStack con soporte para IPV4 e IPV6. • Suministro del servicio Cloud DNS con soporte Dual Stack, que permita al servidor DNS contar con IPV4 e IPV6. • Se verificará el estado del Dual Stack en https://ready.chair6.net/, tanto para la IPV4/IPV6 como para los dominios como para los servidores DNS PROTECCIÓN ATAQUE DDOS A NIVEL DE DATACENTER Y FIREWALL COMERCIAL: Sí. Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge a nivel de RED en el DATACENTER. BASE DE DATOS: MySQL, PostgreSQL y demás sujetas a necesidad de la entidad con réplicas automáticas para respaldo, recuperación y failover. LENGUAJES DE PROGRAMACIÓN: Javascript/Java/PHP/Perl/Phyton y demás sujetos a necesidad de la entidad. SOFTWARE: Apache/PhpMyAdmin/Tomcat/Joomla/Wordpress/Dupral sujeto a versiones requeridas por la entidad. REPORTES: Dentro del panel deberá disponer de un informe mensual de transferencia (tráfico) web y de los intentos de intrusión. Acceso a estadísticas completas.				
3	**ESPECIFICACIONES TÉCNICAS EMAIL MARKETING** GESTOR DE PLANTILLAS: Disponer de un editor dinámico de textos y contenidos, en el cual se puedan insertar imágenes y audios en los diseños. MULTIUSUARIO Y CREACIÓN DE ROLES: El sistema debe permitir la creación de usuario y roles de acuerdo a la necesidad de la entidad sin restricción. ENVÍOS DESDE DIFERENTES CORREOS AUTORIZADOS DE LA ENTIDAD: La plataforma debe permitir el envío desde diferentes y múltiples correos de remitentes de la entidad sin restricción y con cuentas de usuarios al panel de email marketing diferentes. Ejemplos remitentes: prensa@boyaca.gov.co, boletin@boyaca.gov.co, etc PLANTILLAS PROFESIONALES PREDISEÑADAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML. DISEÑOS Y PLANTILLAS RESPONSIVAS: Plantillas en formato HTML. Importación de HTML y URL. Posibilidad de escoger entre 850 plantillas en formato HTML GESTIÓN DE CONTACTOS Y SUSCRIPTORES: Permitir crear listas de contactos y suscriptores teniendo la opción de organizarlos y clasificarlos de acuerdo con filtros como por ejemplo ciudad, rango de edad, género, etc. Cada suscriptor debe ser único y poder pertenecer a múltiples segmentos y listas de distribución. IMPORTAR/EXPORTAR CONTACTOS: Opción de cargar y exportar en forma masiva desde un archivo Excel o .CSV (esta actividad estará a cargo del contratista y será realizada en caso de migración o a solicitud de la entidad) NÚMERO DE SUSCRIPTORES: Ilimitados sin restricción CREACIÓN Y ENVÍO DE CAMPAÑAS: Cuando se cree un boletín el envío se puede realizar de inmediato o pueda ser programado para ser envío en una fecha y hora específica. NÚMERO DE ENVÍOS EN EL MES: Ilimitados FORMULARIOS: Permitir crear formularios de la suscripción a su lista de correos para insertar en su página Web REPORTES: Generar reportes en tiempo real a la información detallada de correos recibidos, abiertos, rebotados y visitas a enlaces incluidos en su mensaje.	**CUMPLE**	ANEXO 5 Propuesta Tecnica.pdf	15-17	

	SISTEMA ANTI SPAM: Sí. Los correos enviados cumplen con leyes anti- spam, incluida la Ley CAN-SPAM de los Estados Unidos. CANCELACIÓN DE SUSCRIPCIÓN: Sí. Incluir el enlace de cancelación de suscripción en las campañas de correo electrónico. SEGURIDAD SSL: Sí. REDES SOCIALES: Permitir integrar enlaces a los perfiles sociales de la entidad. GOOGLE ANALYTICS: Permitir Integración con Google Analytics SEGUIMIENTO ANÓNIMO Y "FINGERPRINTING": Sí AUTOMATIZACIÓN MULTICANAL NATIVA: Flujos de trabajo Notificaciones Web Push: Enviar un mensaje al navegador del usuario., mensajes de Foco: Mostrar pop-ups o barras personalizadas en tu web basadas en el segmento del usuario (ej: mostrar un cupón solo a quien ya ha comprado antes). FILTROS Y SEGMENTACIÓN: Etiquetas, clics, visitas a URLs específicas, valor de campos personalizados, puntos de lead scoring e incluso la tecnología que usa el usuario. SEGMENTOS TRANSVERSALES: Posibilidad de mover contactos entre listas automáticamente, contactos disponibles en múltiples listas. SUSCRIPCIÓN A SOUNCLOUD PARA CARGA DE AUDIOS: Plan con la capacidad de subida Ilimitado, que soporte formatos mp3, wav, flac, etc. Con posibilidad de publicar en otras plataformas. El proveedor entregará las credenciales de acceso a la plataforma https://soundcloud.com/ por el término de la vigencia del contrato.				

PERSONAL MÍNIMO REQUERIDO					
El proponente deberá acreditar que cuenta con el personal mínimo requerido para ejecutar el presente contrato, mediante certificaciones suscrita por el Representante Legal en la que manifieste que dispone de los perfiles acordes al objeto del contrato y determinar su disponibilidad de tiempo, actividades a desarrollar y experiencia				**CUMPLE**	
ITEM	**DESCRIPCIÓN**	**CUMPLE/NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**
1	**PERFIL** Un ingeniero de sistemas o electrónico con especialización en seguridad informática. **NIVEL DE FORMACIÓN ACADÉMICA** Título de ingeniero de sistemas o electrónico Especialización en Seguridad Informática Certificado ISO 27001/2022 vigente **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en administración, aseguramiento y seguridad de servidores Linux y servicios Cloud en la nube, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. Acreditar en los últimos dos (2) años experiencia en implementación de sistemas de Seguridad de la Información ISO 27001 en entidades públicas. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso. • Copia diploma Especialista en Seguridad informática. • Certificado internacional Auditor líder ISO 27001/2022 verificable online vigente. No se admiten cursos, se debe contar con certificado internacional vigente.	**CUMPLE**	PERFILES EQUIPO TRABAJO.pdf	2-47	
	PERFIL Un ingeniero de sistemas o electrónico	**CUMPLE**	PERFILES EQUIPO TRABAJO.pdf	48-55	

	NIVEL DE FORMACIÓN ACADÉMICA Título de ingeniero de sistemas o electrónico **EXPERIENCIA MÍNIMA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años como implementador de portales Web en CMS Wordpress y administrador de bases de datos Mysql Server para contenidos web, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.				
	PERFIL Un ingeniero de sistemas o electrónico **NIVEL DE FORMACIÓN ACADÉMICA** El proponente deberá suministrar la hoja de vida del ingeniero quien deberá tener por lo menos dos (2) años experiencia profesional como ingeniero de sistemas o electrónico, contados a partir de la expedición de la tarjeta profesional. Acreditar experiencia específica en los últimos dos (2) años en implementación y configuración de servicios de hosting, firewall web, migración y base de datos y administración de servidores linux, demostrada mediante la presentación de mínimo dos (2) certificaciones de experiencia a partir de la expedición de la respectiva tarjeta profesional. **DOCUMENTOS ANEXOS** Para acreditar este requisito, el proponente deberá aportar los siguientes documentos del personal requerido así: • Tarjeta y/o Matricula Profesional • Certificado de vigencia de la tarjeta profesional o matricula expedido por la autoridad competente, cuya fecha de expedición no sea superior a tres (3) meses anteriores a la fecha de cierre del presente proceso.	**CUMPLE**	PERFILES EQUIPO TRABAJO.pdf	56-77	

EXPERIENCIA MÍNIMA REQUERIDA					
ITEM	**DESCRIPCIÓN**	**CUMPLE/ NO CUMPLE**	**ARCHIVO**	**No. FOLIOS**	**OBSERVACIÓN**

1	El proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas cuyo objeto sea igual o similar al presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera: De conformidad a la Circular Conjunta de fecha junio de 2019 de Despacho del Gobernador y Secretaría de Contratación, el proponente deberá acreditar experiencia mediante la presentación de contratos y/o certificaciones con entidades públicas o privadas, cuyo objeto sea igual o similar al del presente proceso. La verificación del número de contratos para la acreditación de experiencia se realizará de la siguiente manera. **Número de contratos con los cuales el proponente cumple la experiencia acreditada** / **Valor mínimo a certificar (como % del Presupuesto Oficial expresado en SMMLV)** De 1 hasta 2 — 75% De 3 hasta 4 — 120% De 5 hasta 6 — 150%	**CUMPLE**	EXPERIENCIA MIHOSTING SAS_2_contratos.pdf GOBERNACIÓN DE NARIÑO GN2724-2023 GOBERNACIÓN DE BOYACÁ Contrato 3046 – 2022	1-87 93-109	

Cordialmente,

SANDRA MILENA URRUTIA PEREZ
Secretaria de TIC Y Gobierno Abierto

VoBo. CAMILO ANDRES DELGADO
Director de Sistemas de Información

Revisó: Laura Díaz - Profesional Externo
Proyectó: Claudia Rocio Pineda F. - Profesional Universitario
Lowell Ferney Suárez – Profesional Externo