



www.esmihosting.co - www.ciberwebhost.com - www.mihosting.co - www.esmihosting.com
gerencia@mihosting.co

MIHOSTING S.A.S. NIT: 900724548-6

San Juan de Pasto, 29 de septiembre de 2026

Señores:

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

Asunto: **Renovación Alquiler Servidores Hosting**

Cordial Saludo,

De acuerdo a su solicitud me permito hacer llegar una propuesta para la renovación del servicio de Alquiler de servidores Hosting para su importante entidad, que tiene como objeto **"Se requiere el contratar un servicio de Hosting con 3 servidores en la nube para los servicios DNS y sitios WEB y aplicaciones institucionales en un modelo que funcione bajo estándares de virtualización compatibles con IPV4 e IPV6"**

De acuerdo a lo solicitado se **añade 1 servidor adicional a lo actualmente contratado.**

COSTO ANUAL: \$39.000.000

El costo por la renovación del servidor durante un año es de TREINTA Y NUEVE MILLONES DE PESOS MCTE (39.000.000), incluye impuestos y retenciones.

Atentamente,


JORGE LUIS VILLEGAS MAGUINA
MIHOSTING SAS

Se requiere el contratar un servicio de Hosting con 3 servidores en la nube para los servicios DNS y sitios WEB y aplicaciones institucionales en un modelo que funcione bajo estándares de virtualización compatibles con IPV4 e IPV6

ESPECIFICACIONES TECNICAS

FICHA TECNICA: ALQUILER HOSTING EN LA NUBE CON COMPATIBILIDAD IPV4 E IPV6	
SERVIDOR 1 - PRINCIPAL LINUX (CPANEL+CLOUD LINUX OS + LITESPPED+IMUNIFY 360 + JETBACKUPS)	
ITEMS	DESCRIPCIÓN
TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	32 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	1000 GB SSD NVME(VERIFICABLE)
RAM	32 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	CloudLinuxOS (VERIFICABLE)
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD
ACCESO CONSOLA HOSTING	LICENCIA CPANEL
DISPONIBILIDAD	99.96 %
SERVIDOR WEB	LITESPEED / LS CACHE INCLUIDO(VERIFICABLE)
FTP	SI
FIREWALL Y DETECCIÓN DE PREVENCIÓN DE INTRUSOS	SI – EJEMPLO: IMUNIFY 360

BASADO EN INTELIGENCIA ARTIFICIAL	
SERVIDOR 2 ADVISER LINUX - CPANEL	
ITEMS	DESCRIPCIÓN
TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	24 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	500 GB SSD NVME(VERIFICABLE)
RAM	16 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	Alma Linux
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD
ACCESO CONSOLA HOSTING	LICENCIA CPANEL(VERIFICABLE)
DISPONIBILIDAD	99.96 %
SERVIDOR WEB	APACHE
FTP	SI
FIREWALL Y DETECCIÓN DE PREVENCIÓN DE INTRUSOS BASADO EN INTELIGENCIA ARTIFICIAL	SI – EJEMPLO: IMUNIFY 360
SERVIDOR 3 LINUX	
ITEMS	DESCRIPCIÓN

TIPO CLOUD HOSTING	SERVIDOR CLOUD DEDICADO
PROCESADORES	8 CORES(Núcleos) Ejemplo: Intel Xeon Gold o AMD Epyc de mínimo 2.4 Ghz (VERIFICABLE)
DATASTORE/ ALMACENAMIENTO	250 GB SSD NVME(VERIFICABLE)
RAM	8 GB garantizada y dedicada (VERIFICABLE)
SISTEMA OPERATIVO	Alma Linux
SOPORTE DE BASE DE DATOS	MySQL, Maria DB, PostgreSQL
Compatibilidad IPV4 e IPV6	1-2 Direcciones IPV4 1-16 Direcciones IPV6
USAR Y CONFIGURAR LAS IPV4 E IPV6 SUMINISTRADA POR LA ENTIDAD EN DATACENTER DEL PROVEEDOR	SI, incluido sin costo adicional. En caso de migración se realizará la migración de las IP actuales de la Entidad en el actual Datacenter al nuevo Datacenter.
ARQUITECTURA	CLOUD

CARACTERISTICAS PARA TODOS LOS SERVIDORES

FULL BACKUP SERVIDOR NAS + SOFTWARE COMERCIAL + FULLBACKUP IMAGEN	- Suministro de Software comercial para el backup y copias de seguridad con retención de 15 días. Ejemplo: JETBACKUP o similar(No se admiten software libre o gratuito) - Suministro, configuración e implementación de un sistema de almacenamiento en red (NAS) de alto rendimiento, destinado al respaldo de hasta 3 servidores virtuales (VPS). El sistema debe garantizar una capacidad de almacenamiento neto usable de 5 TB bajo un esquema de redundancia que permita la falla de hasta dos unidades de disco sin pérdida de datos (RAIDZ2 o equivalente)." - Conectividad y Seguridad: - El contratista debe garantizar la integración del NAS en un Datacenter geográficamente distinto al de los servidores de origen.
---	--

- La comunicación se realizará mediante una VLAN privada y vRack virtual independiente, asegurando aislamiento total de la red pública y garantizando latencias mínimas para el tráfico de backup.
- Configuración Lógica (NAS/ZFS):
- Estructura de Datos: Se deberán configurar Datasets independientes para cada una de las 15 VPS, aplicando cuotas de disco si la supervisión lo requiere.
- Optimización: Se debe habilitar compresión (LZ4) y deduplicación para optimizar el uso de los recursos.
- Entregables y Acceso:
- Entrega de credenciales de administración total al supervisor del contrato.
- Configuración de accesos granulares (usuarios/passwords o llaves SSH) independientes para que cada VPS solo tenga visibilidad de su propio Dataset asignado.
- Especificaciones Técnicas mínimas NAS:

Procesador: Mínimo 16 Cores físicos (o combinación de núcleos/hilos que sumen 16 hilos de procesamiento de alto rendimiento).

Memoria RAM: Mínimo 16-32 GB RAM DDR4/DDR5 con corrección de errores (ECC) indispensable para la integridad de datos en sistemas tipo NAS

Almacenamiento de Sistema: 2 unidades SSD NVME (mínimo 240 GB) configuradas en Mirror (Espejo) para el sistema operativo del servidor NAS

Configuración de Discos y Rendimiento

1. (Pool de Datos): Garantizar 5 TB usables con protección y las unidades de aceleración solicitadas, el proponente debe cumplir con: Almacenamiento Masivo

	2.Unidad de Caché (L2ARC): 1 unidad SSD NVMe de 500 GB dedicada para aceleración de lectura. 3.Unidad de Log (SLOG): 1 unidad SSD NVMe de 20 GB (o superior) de alta resistencia (High Endurance) para acelerar las escrituras sincrónicas y proteger el log de transacciones.
DATACENTER (requisito habilitante)	- DATACENTER DE LOS SERVIDORES CLOUD VPS: DATA-CENTER CON MÍNIMO 99.98% UPTIME: El proponente deberá certificar en su oferta técnica a el Datacenter en el cual se alojará el servicio mediante una certificación firmada por el representante legal, además de entregar evidencias de un vínculo con el datacenter (Certificado Partner o Facturas pago último mes) El proponente deberá aportar, junto con la Certificación del Datacenter, las siguientes certificaciones que el Datacenter debe cumplir como mínimo, sin excepción, acompañadas de un enlace a la URL oficial y vigente del sitio web del Datacenter: 1. ISO_IEC_27001ISO 27001, 27017 y 27018 2. ISO 27701 3. RGPD 4. SOC 1, 2 y 3 5. CSA STAR 6. HIPAA e HITECH 7. PCI-DSS 8. SWIPO 9. ISO 14001 10. ISO 50001 11. Política de Seguridad del datacenter La no entrega de estos requisitos técnicos dará como resultado el rechazo de la propuesta. SEGMENTO DE IP ACTUALES CONTRATADAS CON EL DATACENTER DONDE SE ALOJARÁ EL SERVICIO:

	El proponente deberá indicar en su oferta técnica el segmento de direcciones IP (o, en su defecto, el número de sistema autónomo – ASN) en el cual se alojará el servicio. Dicho segmento deberá coincidir con el registro público de proveedores de infraestructura (LACNIC/ARIN) a nombre del Datacenter y el Proponente. En caso de adjudicación del proceso, el proponente no podrá, bajo ninguna circunstancia, alojar el servidor en centros de cableado o cuartos de TI que no cumplan con los requisitos establecidos en el presente documento. Todo cambio o traslado del servidor durante la vigencia del contrato deberá ser informado oportunamente al supervisor para su autorización. El supervisor validará las direcciones IP asignadas durante toda la ejecución contractual.										
SERVICIO VPN NETBIRD AUTOALOJADO (P2P ESTRICTO)	- El contratista, como proveedor de la infraestructura de hosting, suministrará, instalará, configurará, operará y mantendrá una red privada virtual NetBird en modalidad autoalojada (self-hosted), con modelo de conectividad punto a punto (P2P) estricto, como único medio de acceso administrativo a los dos (2) servidores cPanel/WHM contratados + 1 servidor Linux <table border="1"> <thead> <tr> <th>Elemento</th><th>Requisito</th></tr> </thead> <tbody> <tr> <td>Servidores cubiertos</td><td>2 servidores cPanel/WHM (Servidor 1 y Servidor 2) + 1 Servidor Linux</td></tr> <tr> <td>Acceso SSH (root)</td><td>Solo por VPN y solo con par de llaves pública/privada; contraseña deshabilitada</td></tr> <tr> <td>Acceso WHM</td><td>Solo por VPN</td></tr> <tr> <td>Acceso cPanel</td><td>Solo por VPN</td></tr> </tbody> </table>	Elemento	Requisito	Servidores cubiertos	2 servidores cPanel/WHM (Servidor 1 y Servidor 2) + 1 Servidor Linux	Acceso SSH (root)	Solo por VPN y solo con par de llaves pública/privada; contraseña deshabilitada	Acceso WHM	Solo por VPN	Acceso cPanel	Solo por VPN
Elemento	Requisito										
Servidores cubiertos	2 servidores cPanel/WHM (Servidor 1 y Servidor 2) + 1 Servidor Linux										
Acceso SSH (root)	Solo por VPN y solo con par de llaves pública/privada; contraseña deshabilitada										
Acceso WHM	Solo por VPN										
Acceso cPanel	Solo por VPN										

	Autenticación del dispositivo	Par de llaves WireGuard por dispositivo, más SSO y MFA del usuario
	Puertos administrativos en la interfaz pública	Todos cerrados (SSH, WHM y cPanel)
	Plataforma VPN	NetBird autoalojado, instancia dedicada y exclusiva para la entidad
	Plano de datos	Túnel WireGuard directo entre pares, sin relay ni TURN
	Vigencia	Igual al plazo de ejecución del contrato de hosting
	Costo	Incluido en el valor ofertado; sin licencias adicionales a cargo de la entidad
- Arquitectura Requerida El plano de control se aloja en una instancia dedicada del contratista y solo coordina; el tráfico administrativo viaja por túneles directos entre cada administrador y cada servidor. Arquitectura NetBird autoalojada · plano de control y túneles P2P Las líneas punteadas son señalización y configuración; las líneas de color son el único camino del tráfico administrativo. - Modelo de conectividad P2P estricto - Todo el tráfico administrativo viaja por túneles WireGuard directos entre el dispositivo del administrador y el servidor; ningún componente del contratista puede reenviar ese tráfico. - Requisitos obligatorios		

1. Plano de datos exclusivamente P2P: cada sesión es un túnel WireGuard cifrado de extremo a extremo entre los dos pares.
2. El servicio de relay de NetBird y el servidor TURN no se despliegan ni se configuran. Solo se permite STUN, únicamente para el descubrimiento de direcciones (ICE).
3. Cada servidor cPanel acepta tráfico entrante UDP en el puerto WireGuard del agente NetBird (por defecto 51820/UDP), para que la conexión directa se logre aunque el administrador esté detrás de NAT o CGNAT.
4. El plano de control (Management, Signal, proveedor de identidad y consola) solo intercambia configuración, llaves públicas y candidatos de conexión. Nunca transporta tráfico de administración.
5. Las llaves privadas WireGuard se generan y permanecen en cada dispositivo; el servidor de gestión solo conoce llaves públicas.
6. Cada servidor cPanel es un par (peer) con su propio agente NetBird. No se usan routing peers, rutas de red ni la función Networks para alcanzarlos.
7. Sin salida a internet por la VPN: no se configuran exit nodes ni túnel completo (full tunnel).
8. Los dos servidores no se ven entre sí por la VPN, salvo que la entidad lo autorice por escrito para una necesidad concreta (por ejemplo, transferencias de cuentas entre servidores).
9. Si dos pares no logran conexión directa, la conexión falla. El contratista corrige la causa (firewall, NAT, puertos) sin habilitar relay.
10.
 - **Modelos y configuraciones prohibidos(No se aceptan)**

Prohibido	Motivo
Concentrador hub-and-spoke o gateway VPN central	El tráfico pasa por un tercero y crea un punto único de falla
Relay de NetBird o TURN como respaldo	Rompe el modelo P2P aunque solo se use en fallas
Routing peer, subnet router o túnel sitio a sitio	Un nodo intermedio reenvía tráfico hacia los servidores
OpenVPN, IPsec/IKEv2, L2TP, PPTP o VPN SSL	Modelos cliente-servidor distintos al exigido
NetBird Cloud u otro plano de control SaaS	El control quedaría fuera de la infraestructura dedicada
Exit nodes o full tunnel	Mezcla navegación general con el canal administrativo
Túneles SSH, port forwarding o bastiones como sustituto	Evaden el control de acceso de la VPN

- Verificación. El comando netbird status -d en cada servidor y en cada equipo administrador debe mostrar tipo de conexión **P2P** para todos los pares, nunca **Relayed**.

- Funcionalidades mínimas de NetBird:

La plataforma se entrega con todas las funciones siguientes activas y configuradas; las marcadas como deseables suman valor técnico pero no son habilitantes.

Funcionalidad	Exigencia	Carácter
Consola web de administración	Autoalojada, publicada solo por HTTPS con certificado TLS válido	Obligatoria

	Proveedor de identidad (IdP)	IdP integrado o externo compatible con OIDC; inicio de sesión único (SSO)	Obligatoria
	Autenticación multifactor	MFA obligatoria para todo usuario de la VPN y de la consola	Obligatoria
	Roles de usuario	La entidad tiene rol de propietario o administrador de la consola; el contratista, rol de administrador	Obligatoria
	Grupos	Grupos separados para servidores, administradores de la entidad y administradores del contratista	Obligatoria
	Políticas de acceso	Por grupo origen, grupo destino, protocolo y puerto; la política por defecto que permite todo se elimina	Obligatoria
	Verificación de postura (posture checks)	Versión mínima de NetBird, versión mínima de sistema operativo, ubicación geográfica y rango de red de origen, según defina la entidad	Obligatoria
	Llaves de alta (setup keys)	De un solo uso, con expiración y	Obligatoria

		grupo asignado; revocadas una vez usadas	
	Expiración de sesión	Reautenticación periódica de los pares de usuario, con plazo definido por la entidad (recomendado 24 horas)	Obligatoria
	DNS interno	Resolución de los servidores por nombre dentro de la VPN	Obligatoria
	Registro de actividad	Eventos de altas, bajas, cambios de política, inicios de sesión y cambios de configuración	Obligatoria
	API REST y tokens	API disponible para auditoría y automatización, con tokens de acceso con expiración	Obligatoria
	Clientes	Agente en Linux para los servidores; clientes para Windows, macOS y Linux para los administradores	Obligatoria
	Resistencia cuántica (Rosenpass)	Habilitable sobre los túneles WireGuard	Deseable
	Clientes móviles	Android e iOS para atención de emergencias	Deseable

- **Actualizaciones.** El contratista mantiene la plataforma en la versión estable vigente y aplica los parches de seguridad publicados por el fabricante en un plazo máximo de 15 días hábiles, previa notificación a la entidad.

- **Endurecimiento de los servidores cPanel/WHM**

Ningún servicio de administración responde en la interfaz pública: SSH, WHM y cPanel solo se alcanzan por la VPN y con autenticación por llaves. Afuera solo quedan el puerto UDP del túnel NetBird y los servicios de publicación que el contrato incluya.

SSH (root)

- Autenticación por contraseña deshabilitada: PasswordAuthentication no y KbdInteractiveAuthentication no.
- Root solo con par de llaves: PermitRootLogin prohibit-password, llaves Ed25519 personales, una por administrador, con la llave privada protegida por frase de paso y sin llaves compartidas.
- SSH restringido a la dirección o rango NetBird del servidor (por defecto 100.64.0.0/10), tanto en sshd_config como en el firewall.
- Opción de WHM para permitir autenticación SSH por contraseña desactivada, para que las actualizaciones de cPanel no la reactiven.
- El acceso SSH o SFTP de las cuentas cPanel, si se habilita, también es solo con llave y solo por la VPN.

WHM

- Puerto 2087/TCP permitido solo desde el rango NetBird; 2086/TCP cerrado.
- Subdominio de servicio whm.<dominio> deshabilitado o bloqueado, porque expone WHM por los puertos 80/443 y evadiría la VPN.
- Autenticación de dos factores de WHM activa para root y revendedores.

	• Protección contra fuerza bruta (cPHulk o equivalente) activa. cPanel • Puerto 2083/TCP permitido solo desde el rango NetBird; 2082/TCP cerrado. • Subdominio de servicio cpanel.<dominio> deshabilitado o bloqueado, porque expone el panel por los puertos 80/443 y evadiría la VPN. • Autenticación en dos capas: el dispositivo entra a la VPN con su par de llaves WireGuard y el usuario inicia sesión en cPanel con contraseña y segundo factor (2FA) obligatorio. • cPanel no admite inicio de sesión web con llaves SSH; el factor de llave pública/privada lo aporta el túnel WireGuard, sin el cual el panel no es alcanzable.
SEGURIDAD Y SOPORTE ESPECIALIZADO (Habilitante se debe presentar hoja de vida)	Se requiere como mínimo las siguientes actividades durante toda la ejecución del contrato, realizadas directamente por un Ingeniero de Sistemas Especialista en Seguridad Informática, certificado en Ciberseguridad o Auditor Líder ISO27001/2022, con experiencia en implementación de Sistema de de Seguridad en entidades públicas, vinculado al proyecto, el cual no puede cambiarse durante toda la ejecución del contrato: - Migración, configuración, revisión de seguridad continua de la infraestructura adquirida, inclusive subdominios. Soporte Técnico 24/7 y asesoría especializada por un especialista en seguridad informática por doce (12) meses. - Auditoría y asesoría permanente, frente a cualquier situación relacionada con incidentes y vulnerabilidades, y defensa proactiva ante ataques informáticos durante toda la ejecución del contrato de todos los sitios alojados en el servidor en actividades mínimas como:

	- Mitigación de ataques de Denegación de Servicio (DDoS/Flood): Capacidad para identificar y filtrar ataques de inundación SYN (Layer 4) y ataques de aplicación (Layer 7) mediante el uso coordinado de Firewalls perimetrales y WAF. - Gestión de Seguridad Perimetral y Edge: Configuración de reglas estrictas en el Firewall Edge. - Hardening de Servidores Web (CPanel/WHM): Implementación de políticas de aislamiento de cuentas, saneamiento de versiones de PHP obsoletas y restricción de tráfico saliente para evitar que el servidor sea usado como nodo de ataque. - Forense y Limpieza de Malware en CMS: Identificación de vectores de entrada (exploits en plugins), eliminación de backdoors complejos, purga de inyecciones de spam SEO en bases de datos y restauración de integridad de archivos. - Administración Avanzada de Firewall Local (CSF/LFD): Configuración de listas de bloqueo dinámicas (como la red TOR), control de tasas de conexión (CT_LIMIT) y protección contra escaneos de puertos. - Entregar un reporte de versiones y componentes vulnerables, identificados mediante el software licenciado parchado con análisis de vulnerabilidades en los CMS más populares (Joomla, Wordpress, Drupal), una vez identificada la vulnerabilidad, el sistema debe permitir las actualizaciones pertinentes y las correcciones de seguridad. - Sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones proactivas y correctivas antes de que el ataque suceda. - En caso de incidentes y ataques El especialista será responsable de liderar el ciclo completo de respuesta ante incidentes (IR), que incluye la detección,
--	---

	contención, erradicación y, fundamentalmente, la elaboración de un Informe Técnico Forense y de Remediación. Este documento debe consolidar todas las evidencias recolectadas durante el ataque y las acciones correctivas aplicadas. El informe debe contener como mínimo: • Resumen Ejecutivo: Descripción no técnica del impacto del ataque en los servicios institucionales y el estado final de la seguridad. • Línea de Tiempo del Incidente (Timeline): Detalle cronológico desde la detección de los primeros síntomas (ej. lentitud por tráfico de IPs de Indonesia/red TOR) hasta la resolución total. • Identificación de Vectores de Entrada: Análisis de cómo el atacante logró vulnerar el sistema (ej. vulnerabilidad en el plugin Anywhere Elementor, archivos de verificación de Google inyectados o backdoors ocultos). • Evidencia Técnica y Logs: Consolidación de capturas de logs de Apache, reportes de Imunify360, procesos sospechosos en WHM y listado de direcciones IP bloqueadas. • Acciones de Contención y Limpieza: Detalle de las medidas tomadas: • Configuración del Firewall Edge y Cloudflare. • Limpieza manual de inyecciones de código en la base de datos (spam SEO). • Saneamiento de archivos del núcleo de WordPress. • Ajustes en los límites de procesos PHP-FPM y CURL. • Plan de Remediación y Mejora Continua: Recomendaciones de seguridad a corto y largo plazo
--	---

	(ej. política de contraseñas, actualización obligatoria de plugins, auditoría de red interna para detectar saltos laterales). Verificar el estado del servidor y realizar actualizaciones del software del servidor y las herramientas de Cpanel. Soporte técnico permanente vía web, correo electrónico, teléfono, chat, en caso de requerirse del ingeniero especialista en seguridad informática 24/7, tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. Aspectos que garanticen la seguridad del servidor. - Para 2 servidores cpanel: Sondeo permanente para identificar comportamientos sospechosos y actividades típicas de ataques de seguridad, permitiendo tomar acciones proactivas y correctivas antes de que el ataque suceda. - Para 2 servidores cpanel: Sistema de detección de virus y malware basado en inteligencia artificial licenciado para 300 dominios tipo Imunify360 u otros con licencias comercial que cumplan con lo solicitado, no se aceptan versiones inferiores a 360. - Server side que identifique y elimine amenazas de su servidor. - Actualizaciones diarias del software del servidor y las herramientas. - Para 2 servidores cpanel: Suministro de un software comercial licenciado para la protección avanzada de firewall que utiliza heurística en la nube e inteligencia artificial para detectar nuevas amenazas y proteger todos los servidores que ejecutan el software. El firewall es capaz de defenderse contra ataques de fuerza bruta, ataques DoS y escaneos de puertos, con licencia comercial, tipo Imunify360 u otros con licencias
--	---

	comercial que cumplan con lo solicitado, no se aceptan versiones inferiores a 360 en el caso de Ímunify - Soporte técnico permanente vía web, correo electrónico, teléfono, chat, o presencial en caso de requerirse del ingeniero especialista en seguridad informática. - Tiempo de respuesta ante eventualidades, máximo sesenta (60) minutos. Copias de seguridad permanente de todo el contenido del servidor hasta de un mes atrás. - Actualizaciones del sistema operativo del servidor, Sistema de análisis y prevención de ransomware, Monitoreo proactivo del servidor para verificar su disponibilidad Configurar el servicio de monitoreo “uptime” que notifique mediante alertas el estado de inactividad y rendimiento de los sitios web por separado
--	--