Catálogo de Servicios IT Gestionados

ConsultasIT — Soluciones tecnológicas para PyMEs en Ecuador

Acerca de este documento

Este catálogo detalla los servicios IT gestionados que ofrece ConsultasIT a pequeñas y medianas empresas ecuatorianas. Está organizado por categoría y describe qué incluye cada servicio, a qué tipo de empresa está dirigido, y los resultados típicos que nuestros clientes obtienen.

Todos nuestros servicios se prestan bajo un modelo de mensualidad fija con alcance claramente definido — no hay costos sorpresa, ni tarifas por hora ocultas. Nuestro objetivo es que usted sepa exactamente qué obtiene y cuánto cuesta antes de firmar.

1. Administración de Infraestructura

Monitoreo 24/7 de servidores y redes

Supervisión continua del estado de sus servidores, equipos de red, y servicios críticos. Nuestra plataforma recolecta métricas cada 60 segundos y emite alertas automáticas ante cualquier anomalía. Respuesta a incidentes críticos en menos de 15 minutos durante horario hábil, y menos de 30 minutos fuera de horario.

Incluye:

- Monitoreo de CPU, memoria, disco, red y servicios por servidor
- Alertas por correo electrónico y WhatsApp en tiempo real
- Panel de control web con históricos de 90 días
- Reporte mensual de disponibilidad y tendencias
- Integración con nuestra mesa de ayuda para tickets automáticos

Gestión de parches y actualizaciones

Aplicación controlada de parches de seguridad y actualizaciones del sistema operativo en ventanas de mantenimiento negociadas con usted. Todos los parches se prueban primero en entornos de staging cuando es posible, y siempre se generan snapshots antes de aplicar cambios críticos.

Incluye:

- Parcheo mensual de Linux (Ubuntu, Debian, AlmaLinux) y Windows Server
- Gestión de actualizaciones de Docker, bases de datos y servicios clave
- Snapshots pre-cambio y plan de rollback documentado
- Reporte de CVEs pendientes y su nivel de criticidad

2. Administración de Nube y Hosting

Gestión de VPS y servidores dedicados

Administramos servidores VPS y dedicados tanto en proveedores ecuatorianos como internacionales (DigitalOcean, Vultr, AWS Lightsail, EcuaVPS). Nos encargamos del aprovisionamiento inicial, configuración segura, hardening y mantenimiento continuo.

Servicios incluidos:

- Aprovisionamiento e imagen base endurecida (SSH sin password, firewall, fail2ban)
- Configuración de servicios web (nginx, Apache, Caddy) con SSL vía Let's Encrypt
- Gestión de bases de datos (MySQL, PostgreSQL, MariaDB)
- Backups automáticos diarios con retención configurable
- Migración entre proveedores sin downtime para sitios estáticos, <15 min para dinámicos

Backups y recuperación ante desastres

Diseñamos e implementamos estrategias de respaldo con la regla 3-2-1: tres copias de los datos, en dos medios distintos, con una copia offsite. Probamos la restauración trimestralmente para garantizar que los backups realmente funcionan cuando son necesarios.

Objetivos de servicio:

Métrica	Objetivo estándar	Objetivo premium
RPO (punto máximo de pérdida)	24 horas	4 horas
RTO (tiempo de recuperación)	8 horas	2 horas
Retención de backups	30 días	90 días + archivado anual
Pruebas de restauración	Trimestral	Mensual

3. Seguridad Gestionada

Hardening y cumplimiento base

Configuración segura inicial siguiendo los lineamientos de CIS Benchmarks y las mejores prácticas del sector. Esto sienta las bases para cualquier auditoría de seguridad posterior o requerimiento de cumplimiento.

Controles implementados:

- Deshabilitación de autenticación por contraseña en SSH; solo llaves Ed25519/RSA 4096
- Firewall por host (ufw/firewalld) con política deny-all por defecto
- fail2ban para SSH, nginx, Postfix y servicios expuestos
- Usuarios sin privilegios sudo innecesarios; segregación por rol
- Registro centralizado de logs con retención de 90 días para análisis forense
- Configuración segura de TLS (solo 1.2+, cifrado moderno, HSTS en sitios web)

Respuesta a incidentes de seguridad

En caso de brecha sospechada, seguimos un protocolo estandarizado: contención, recolección de evidencia forense, análisis de causa raíz, erradicación, y endurecimiento post-incidente. Proporcionamos un informe ejecutivo en las primeras 48 horas y uno técnico detallado dentro de los siguientes 5 días hábiles.

Evaluaciones de vulnerabilidad

Escaneos trimestrales de vulnerabilidades externas sobre sus servicios públicos, con priorización según criticidad real en su entorno (no solo CVSS base). Acompañamos cada hallazgo con un plan de remediación concreto y plazos realistas.

4. Aplicaciones y Desarrollo

Administración de stack web

Gestión completa de aplicaciones web basadas en stacks modernos, incluyendo despliegue continuo, optimización de rendimiento, y resolución de incidentes en producción.

Stacks soportados:

- WordPress y WooCommerce con optimización de caché (Redis, Varnish)
- Aplicaciones Node.js con PM2 o systemd para supervisión de procesos
- Django / Flask con gunicorn y nginx como reverse proxy
- Next.js / React con despliegue Vercel o self-hosted
- Aplicaciones Laravel / PHP-FPM
- Contenedores Docker con docker-compose o Kubernetes

CI/CD y automatización

Implementación de pipelines de integración y despliegue continuo usando GitHub Actions, GitLab CI, o Jenkins. Incluye tests automatizados, escaneos de seguridad en el pipeline, y despliegues con capacidad de rollback en un solo clic.

5. Soporte a Usuarios Finales

Mesa de ayuda para PyMEs

Soporte técnico para los empleados de su empresa en temas cotidianos: correo electrónico, impresoras, VPN, suites de oficina, herramientas de colaboración. Respondemos vía WhatsApp, email y llamada telefónica, con tiempos de respuesta acordes al nivel de servicio contratado.

Canales y tiempos de respuesta:

Severidad	Ejemplo	Primera respuesta
Crítica	Servicio caído afectando todo el equipo	15 minutos
Alta	Usuario bloqueado no puede trabajar	1 hora
Media	Función secundaria no funciona	4 horas
Baja	Solicitud de cambio o consulta general	1 día hábil

Nuestro Proceso de Onboarding

Del primer contacto a servicio activo en 10 días

Día 1 — Descubrimiento

Reunión inicial (virtual o presencial) para entender su negocio, inventario de equipos, y retos actuales. Sin compromiso, sin costo.

Días 2-3 — Evaluación técnica

Auditoría remota de su infraestructura actual. Identificamos riesgos, ineficiencias y oportunidades de mejora inmediata. Entregamos un informe ejecutivo con hallazgos priorizados.

Día 4 — Propuesta

Presentamos un plan con el alcance exacto de servicios recomendados, cronograma de implementación, e inversión mensual. Sin letra chica.

Días 5-7 — Implementación base

Instalamos nuestra plataforma de monitoreo, configuramos acceso seguro, documentamos su entorno, y establecemos los canales de comunicación con su equipo.

Días 8-9 — Remediación prioritaria

Resolvemos los problemas críticos identificados en la evaluación: parches urgentes, respaldos faltantes, configuraciones inseguras.

Día 10 — Go-live y capacitación

Sesión de capacitación con su equipo sobre cómo abrir tickets, uso del panel de monitoreo, y protocolos de emergencia. Desde este momento, el servicio está activo 24/7.

Casos de Uso Típicos

Tienda en línea con WooCommerce

Cliente típico: comercio minorista con 1,000–20,000 visitas diarias.
Retos: caídas durante promociones, pagos fallidos por lentitud, vulnerabilidades en plugins desactualizados.
Nuestra solución: hosting dedicado con caché Redis, monitoreo de transacciones, parcheo semanal de WordPress/plugins, backups cada 4 horas durante días de alto tráfico.
Resultado: uptime de 99.95%, tiempo de carga <1.2s desde Ecuador, cero pérdidas por vulnerabilidades conocidas.

Consultorio médico con historia clínica digital

Cliente típico: clínica privada con 3–15 médicos y sistema de HC (OpenEMR, MedicalCross, o propio).
Retos: protección de datos sensibles, cumplimiento con normativa ecuatoriana de protección de datos, acceso remoto seguro para médicos.
Nuestra solución: servidor dedicado con cifrado de disco, VPN WireGuard para acceso remoto, backups cifrados offsite, logs de auditoría de accesos.
Resultado: cumplimiento documentado, recuperación probada ante ransomware hipotético en <2 horas.

Empresa con 20–100 empleados y correo corporativo

Cliente típico: PyME con operación en varias ciudades, correo corporativo en dominio propio, uso intensivo de Google Workspace o Microsoft 365.
Retos: phishing dirigido, cuentas comprometidas, pérdida de productividad por lentitud de VPN y archivos compartidos.
Nuestra solución: filtro antispam avanzado, autenticación multifactor obligatoria, capacitación anti-phishing, Nextcloud para archivos internos, respuesta a incidentes 24/7.
Resultado: 90% menos phishing exitoso, pérdida de productividad por incidentes IT reducida de 8 horas/mes a <1 hora/mes por empleado.

Próximos Pasos

Si alguno de los servicios descritos resuena con sus retos actuales, nos encantaría agendar una llamada de descubrimiento de 30 minutos — sin costo y sin compromiso — para entender mejor su situación y determinar si somos un buen fit.

Cómo contactarnos:

Web: https://consultasit.com

Solicitud de consultoría: https://consultasit.com/#contacto

Ubicación: Quito, Ecuador — con soporte remoto nacional

ConsultasIT existe para que las PyMEs ecuatorianas puedan enfocarse en su negocio, no en apagar incendios de IT. Hablemos.