INGENIERÍA DE CIBERDEFENSA SOBERANA · FORENSIA DIGITAL · CONTINUIDAD OPERATIVA

WANADI TACTICAL

Blindamos la continuidad operativa de la Banca, Telecomunicaciones, Retail e Infraestructuras Críticas mediante **Inmunización en Caliente (Zero-Downtime)**, **Auditoría Forense Inmutable** y **Sistemas Operativos Soberanos**.

"The Internet assumes connectivity. Wanadi assumes failure."

JURISDICCIÓN & SEDE	IMPACTO EN PRODUCCIÓN	PRIVACIDAD Y DATOS	ESTÁNDAR PERICIAL
Estados Unidos (LLC)	**0% Tiempo de Caída**	**100% Air-Gapped / Local**	**NIST SP 800-86 & ISO**
Operaciones LatAm & Global	Zero-Downtime Hot Patching	Cero Exfiltración a la Nube	Cadena Custodia SHA-512

Wanadi Tactical LLC es miembro oficial del **NVIDIA Inception program**
Prioridad de Patente Internacional OMPI: **PCT/IB2026/062116** (157 países)

© 2026 NVIDIA, the NVIDIA logo, and NVIDIA Inception are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries.

DIAGNÓSTICO DE RIESGO OPERATIVO

Por Qué la Ciberseguridad Tradicional Falla en el Momento Crítico

Las organizaciones enfrentan hoy una tormenta perfecta: vulnerabilidades explotadas en minutos, actualizaciones oficiales que rompen sistemas en producción y soluciones en la nube que exponen datos confidenciales.

RIESGO 01 · INTERRUPCIÓN DE NEGOCIO

El Dilema de Actualizar vs. Caer en Producción

Ante alertas críticas como **PHP2Shell (CVE-2026-109618)** y la falla global en compresión **Brotli / HTTP2Shell (CVE-2026-111497)** en Node.js, Python y PHP, actualizar librerías en caliente rompe dependencias y provoca caídas costosas.

- El 65% de la infraestructura crítica opera con módulos que no admiten reinicios ni cambios bruscos de versión.
- Una sola hora de caída cuesta entre **$5,000 y $50,000+ USD** en ventas perdidas y multas de SLA.

RIESGO 02 · AUDITORÍAS CIEGAS Y LENTAS

Consultoras que Entregan PDFs de Papel, No Soluciones

Las firmas tradicionales cobran decenas de miles de dólares por auditorías que tardan semanas, instalan agentes intrusivos que degradan el rendimiento y entregan diagnósticos teóricos sin remediar el servidor.

- Cerrar un puerto o editar una configuración hoy **no detecta ni erradica al intruso que entró ayer**.
- Falta de evidencia criptográfica válida ante juntas directivas, reguladores (SBS, SUDEBAN, NIS2) y aseguradoras.

RIESGO 03 · DEPENDENCIA FRÁGIL DE LA NUBE

Exfiltración de Datos y Colapso de Conectividad

El incidente global de julio de 2024 (8.5 millones de máquinas caídas por un parche defectuoso en modo kernel) y los apagones de red demostraron que depender 100% de nubes externas es un punto único de fallo.

- Los WAFs en la nube obligan a desviar el tráfico DNS corporativo y no inspeccionan la memoria interna del servidor.
- Cuando cae el enlace de fibra o Internet, los puestos de mando quedan completamente incomunicados.

ARQUITECTURA INTEGRAL DE DEFENSA

Nuestras Tres Líneas de Soluciones Corporativas

Tecnología propietaria desarrollada en Estados Unidos que protege desde el código en ejecución de sus servidores actuales hasta sus estaciones de administración y comunicaciones de emergencia.

PILAR 01 · SERVIDORES

Tepuy Core™ & Anticuerpos Digitales

Motor de auditoría forense no intrusiva e **inmunización en caliente (Hot Virtual Patching)** para servidores Linux y Windows en producción.

- **Inmunización en 15 minutos:** Bloquea exploits críticos (ej. *PHP2Shell*) en el proxy y en el runtime sin recompilar ni apagar el servidor.
- **12 Motores Forenses:** Caza de *webshells* en memoria RAM, registros, tareas ocultas y contenedores Docker.
- **Cero Escritura (WORM):** Inspección 100% segura sin alterar el disco del cliente.

PILAR 02 · ESTACIONES SOC

Sentinel OS™ (SO Soberano)

El primer sistema operativo táctico inmutable con particionamiento atómico A/B e Inteligencia Artificial 100% local para *Jump Hosts*, SOCs y Salas de Crisis.

- **Inmune a Ransomware y Fallos:** Raíz de solo lectura verificada por hardware (`dm-verity` + TPM 2.0) con reversión automática en **<5 segundos**.
- **Doctrina Air-Gapped:** Cero telemetría hacia nubes externas; máxima confidencialidad bancaria e industrial.
- **Agentes IA Locales:** Diagnóstico autónomo sin conectar datos sensibles a Internet.

PILAR 03 · COMUNICACIONES

Kuntur Continuity SDK™ (Malla Offline)

Infraestructura y protocolo de comunicaciones resilientes que mantiene conectados a sus equipos y sucursales cuando colapsan Internet y la telefonía celular.

- **Red en Malla Autónoma:** Transmisión salto a salto vía Bluetooth Low Energy (BLE) y Wi-Fi Direct sin requerir antenas ni satélites.
- **Cifrado de Grado Militar:** Arquitectura criptográfica *Noise XX + Double Ratchet*.
- **Integración Empresarial:** Incorporado nativamente en Sentinel OS™ o integrable en apps móviles corporativas.

SOLUCIÓN DE URGENCIA INMEDIATA · ZERO-DOWNTIME

Tepuy Digital Antibody Suite™: PHP2Shell & Brotli (HTTP2Shell)

Proteja hoy mismo sus APIs, pasarelas de pago y servidores en **Node.js, Python, PHP (5.4 a 8.5) y Docker** contra el desbordamiento en **Brotli (CVE-2026-111497)** y **PHP2Shell (CVE-2026-109618 / 109619 / 115560)** con 0% caída.

ARQUITECTURA DE 5 CAPAS EN 15 MINUTOS

¿Qué hace nuestro Anticuerpo Digital en su Servidor?

- **1. Escudo Perimetral (Edge Virtual Patch):** Reglas quirúrgicas en Nginx, Apache o LiteSpeed que interceptan y destruyen el payload malicioso antes de que toque el motor de PHP.
- **2. Blindaje de Runtime en Caliente (FPM Pools):** Anclaje inmutable de directivas de seguridad mediante `php_admin_value` con recarga suave (*graceful reload*) y **0% pérdida de sesiones activas**.
- **3. Caza Forense Retrospectiva (YARA v20 Hunter):** Barrido profundo de memoria RAM, `/tmp` y directorios web para confirmar que ningún atacante haya inyectado una *webshell* desde el Día Cero.
- **4. Verificación Matemática y Rollback en 1 Clic:** Comprobación automatizada de inmunidad y script de reversión determinista instantánea.

POR QUÉ NO BASTA CON "EDITAR EL PHP.INI"

Ventaja frente a Parches Manuales o Actualizar Versiones

CRITERIO OPERATIVO	ACTUALIZACIÓN / MANUAL	ANTICUERPO WANADI
Node.js, Python y PHP (5.4–8.5)	❌ Sin soporte oficial	**✓ 100% Cubierto**
Riesgo de Romper la Aplicación	Alto (Incompatibilidad)	**✓ Cero (No toca código)**
Tiempo de Caída (Downtime)	Horas o días de migración	**✓ 0 Segundos (En caliente)**
Detecta Hackers ya Adentro	❌ No audita el servidor	**✓ Barrido Forense YARA**
Certificado Legal de Cumplimiento	❌ Sin validez pericial	**✓ Acta Criptográfica SHA-512**

DIAGNÓSTICO PROFUNDO CON CERO ALTERACIÓN

Tepuy Core™ M2: Los 12 Motores Forenses de Inspección

Nuestra plataforma ejecuta una radiografía completa de sus servidores, bases de datos y estaciones de trabajo bajo protocolo **WORM (Write-Once-Read-Many)**, garantizando que ni un solo byte de su operación sea modificado durante la auditoría.

MOTOR 01-03

Sistemas Windows & Logs

- **Hivex Registry:** Extracción offline de colmenas SAM y SYSTEM.
- **EVTX Parser:** Reconstrucción de accesos e intrusiones.
- **Tareas Ocultas:** Detección de persistencia en Cron/Systemd/Tasks.

MOTOR 04-06

Memoria RAM & Malware

- **Volatile RAM Extractor:** Caza de procesos ocultos e inyecciones DLL.
- **YARA v20 Hunter:** Detección de ransomware, troyanos y webshells.
- **Entropía Shannon:** Localización de binarios cifrados o empaquetados.

MOTOR 07-09

Red, Cloud & Contenedores

- **Docker & SUID Audit:** Detección de escapes de contenedores y privilegios.
- **Sockets & ARP:** Mapeo de conexiones laterales no autorizadas.
- **AI-as-C2 Hunter:** Bloqueo de fugas de datos hacia APIs externas.

MOTOR 10-12

Criptografía & Custodia

- **Auditoría Post-Cuántica (PQC):** Evaluación de llaves débiles (FIPS 203/204).
- **Credenciales IAM:** Hallazgo de claves expuestas en archivos `.env` y código.
- **Ledger SHA-512:** Sello criptográfico inmutable con código QR verificable.

Entregable Ejecutivo Inmediato: Al finalizar la sesión, la Directiva recibe el **Informe Pericial con Score de Seguridad**, matriz de riesgos priorizada y los paquetes de remediación listos para aplicar.

NIST SP 800-86 COMPLIANT

BLINDAJE PARA PUESTOS DE MANDO, SOC Y SERVIDORES DE SALTO

Sentinel OS™: El Sistema Operativo que No Puede Ser Secuestrado

No requiere cambiar las computadoras de oficina de su personal. **Sentinel OS™** se despliega estratégicamente en las consolas desde donde sus administradores controlan la red (*Jump Hosts*), estaciones de tesorería/banca y Salas de Crisis Ejecutivas.

ARQUITECTURA ANTI-FRÁGIL

¿Por qué Sentinel OS™ supera a cualquier estación tradicional?

- **Raíz Inmutable (Imposible de Infectar Permanentemente):** El sistema operativo corre en modo de solo lectura verificado bloque a bloque por hardware (`dm-verity`). Cualquier intento de instalar ransomware o troyanos desaparece por completo al reiniciar.
- **Particionamiento Atómico A/B (Cero Pantallas Azules):** Las actualizaciones se aplican en una partición secundaria inactiva. Si algo falla, el sistema regresa a la versión sana en **menos de 5 segundos**.
- **Candado Físico TPM 2.0:** La bóveda de datos está sellada al chip criptográfico de la máquina; si roban el disco duro, es imposible leerlo en otro equipo.
- **Comunicaciones de Emergencia Integradas:** Incluye nativamente el protocolo de malla sin Internet para coordinar crisis durante apagones.

3 FORMATOS DE IMPLEMENTACIÓN

Adaptado a la Necesidad de su Organización

1. Sentinel Lite™ (Live Tactical USB WORM)

Memoria USB industrial blindada que convierte cualquier laptop en una estación de auditoría forense segura en 60 segundos sin tocar el disco interno.

2. Sentinel Pro™ (Estación SOC & Jump Host M.2)

Para los ingenieros que administran servidores críticos, firewalls, switches de telecomunicaciones y bases de datos financieras.

3. Sentinel Sovereign™ (Appliance Físico para Sala de Crisis)

Mini-PC industrial rugerizada llave en mano con IA local y malla autónoma para continuidad de mando de la Junta Directiva.

ANÁLISIS COSTO-BENEFICIO PARA EL COMITÉ DIRECTIVO

Por Qué los Líderes Eligen a Wanadi Tactical

Combinamos la velocidad quirúrgica de una intervención automatizada con el rigor probatorio de la forensia de grado militar, a una fracción del costo y tiempo de las alternativas tradicionales.

DIMENSIÓN EVALUADA	HACERLO INTERNAMENTE (TI PROPIO)	CONSULTORAS TRADICIONALES / WAF CLOUD	WANADI TACTICAL LLC
Tiempo de Respuesta ante Día Cero	Semanas de pruebas para no romper aplicaciones en producción.	Días de trámites, desvío de tráfico DNS y configuración externa.	**15 minutos en caliente (sin reiniciar servidores ni cortar el servicio).**
Impacto en Sistemas Legados	Alto riesgo de caída al forzar actualizaciones de versión.	No protegen a nivel de proceso interno ni versiones sin soporte.	**Protección total desde versiones antiguas hasta actuales sin tocar código.**
Detección de Intrusos Previos	Limitada a revisión manual de logs superficiales.	Un WAF perimetral no revisa si el servidor ya fue infectado antes.	**Barrido Forense YARA v20 en memoria RAM y disco incluido.**
Privacidad y Soberanía de Datos	Variable según herramientas gratuitas utilizadas.	El tráfico y los datos confidenciales pasan por nubes de terceros.	**100% En Sitio / Air-Gapped. Sus datos jamás salen de su empresa.**
Respaldo Legal y Regulatorio	Sin validez pericial externa.	Reportes genéricos automáticos.	**Certificado Criptográfico SHA-512 bajo norma NIST SP 800-86.**
Inversión Estimada	$15,000 – $40,000 USD (en horas hombre y caídas operativas).	$24,000 – $60,000+ USD anuales en contratos forzosos.	**Desde $2,500 – $4,500 USD con retorno de inversión inmediato.**

INVERSIÓN TRANSPARENTE Y ESCALABLE

Paquetes Comerciales y Garantía de Acreditación

Inicie con una intervención táctica inmediata para resolver sus riesgos más urgentes hoy mismo, con el beneficio de acreditar el **50% de su inversión inicial** si decide escalar a nuestra protección anual continua en los primeros 30 días.

OPCIÓN 01 · ENTRADA INMEDIATA

Inmunización Táctica & Auditoría Forense

$4,500 USD / Pago Único

Ideal para blindar servidores críticos expuestos a *PHP2Shell* y *Brotli HTTP2Shell (CVE-2026-111497)* sin detener la operación.

- Parcheo virtual perimetral (Nginx/Apache) + blindaje de runtime en caliente (0% downtime).
- Barrido forense retrospectivo con nuestros 12 motores y reglas YARA v20.
- Acta Pericial y Certificado Criptográfico SHA-512 para Directiva y Auditores.
- **Garantía Comercial:** Se acredita **$2,250 USD (50%)** a favor si contrata el Plan Anual en 30 días.

OPCIÓN 02 · PROTECCIÓN CONTINUA SOC

Licencia Anual Sentinel OS Pro™

$12,000 USD / Nodo / Año

Estación forense inmutable y blindaje continuo para equipos de TI, administración de red y banca.

- Unidad M.2 NVMe / Estación con **Sentinel OS Pro™** (raíz inmutable + rollback A/B en <5s).
- Incluye todos los paquetes de **Anticuerpos Digitales** del año sin costo adicional.
- Auditorías forenses trimestrales certificadas con sello SHA-512.
- Opción de entrada rápida por hardware portátil: **Sentinel Lite™ USB WORM por $2,500 USD**.

OPCIÓN 03 · BLINDAJE INTEGRAL C-LEVEL

Sala de Crisis Sentinel Sovereign™

$35,000 USD / Llave en Mano

Soberanía tecnológica total para Juntas Directivas, Centros de Datos, Telcos e Infraestructura Crítica.

- Despliegue de **2 Nodos Hardware Rugerizados (Wanadi Tactical Box)** con TPM 2.0 e IA local.
- Red de comunicación de emergencia sin Internet (Malla **Kuntur / Chasqui** BLE + Wi-Fi Direct).
- Inmunización de hasta 10 servidores críticos de producción y protocolo de respuesta a incidentes.
- Capacitación ejecutiva y simulacro de continuidad de negocio para el equipo directivo.

EXPERIENCIA REAL EN INFRAESTRUCTURA CRÍTICA

Dirección Ejecutiva y Respaldo Internacional

Wanadi Tactical está liderada por especialistas con más de 15 años protegiendo y operando redes de telecomunicaciones, plataformas bancarias y operaciones corporativas en América Latina y Estados Unidos.

FOUNDER, CEO & LEAD SYSTEMS ARCHITECT

Juan Carlos Díaz Parisca

Arquitecto de Sistemas de Misión Crítica y Ciberdefensa con más de 15 años de trayectoria en el sector de telecomunicaciones y banca (**CANTV, Movistar, Banco de Venezuela**).

- Creador de la arquitectura **Tepuy Core™**, **Sentinel OS™** y del protocolo criptográfico de malla sin Internet.
- Postulado al programa global **AAIF Ambassador de The Linux Foundation** en estándares de IA Local y seguridad agéntica.

CO-FOUNDER & CHIEF FINANCIAL OFFICER

Diego Fabrizio Vera Flores

Especialista en Gobernanza Financiera, Estructuración de Negocios B2B, Cumplimiento Normativo y Gestión de Riesgos Corporativos.

- Lidera la estructuración contractual, modelos de retorno de inversión (ROI) para clientes corporativos y alianzas estratégicas en la región andina y EE. UU.
- Coordinador de transparencia financiera internacional con *Open Source Europe* (Bélgica).

CHIEF MARKETING & INSTITUTIONAL OFFICER

Carolina Santini

Estratega de Comunicación Corporativa C-Level, Posicionamiento Internacional y Relaciones Institucionales B2B.

- Dirige la vinculación con cámaras empresariales, juntas directivas y programas de adopción tecnológica corporativa.
- Especialista en traducción de riesgos cibernéticos complejos a estrategias de continuidad de negocio para la Alta Dirección.

Validación & Propiedad Intelectual: PoC de campo en **VTC Cargo** · Patente OMPI PCT/IB2026/062116 (157 países).
Ecosistema Institucional: Wanadi Tactical LLC es miembro oficial del **NVIDIA Inception program** · I+D EE. UU. y Europa.

© 2026 NVIDIA, the NVIDIA logo, and NVIDIA Inception are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries.

RUTA DE IMPLEMENTACIÓN RÁPIDA EN 3 PASOS

Asegure la Continuidad de su Operación Hoy Mismo

Nuestro proceso de incorporación está diseñado para brindarle resultados tangibles y verificables en menos de 48 horas, sin burocracia ni interrupciones para su equipo de tecnología.

PASO 01 · DÍA 1 (30 MINUTOS)

Sesión Ejecutiva & NDA

Reunión confidencial (remota o presencial) con nuestra dirección técnica para evaluar su topología actual, versiones de servidores expuestos y prioridades de continuidad.

PASO 02 · DENTRO DE 24-48 HORAS

Inmunización / Diagnóstico WORM

Despliegue en caliente del **Anticuerpo Digital** (0% caída de servicio) o ejecución de auditoría forense de 12 motores bajo modalidad de cero escritura en disco.

PASO 03 · ENTREGA Y CERTIFICACIÓN

Acta Pericial SHA-512 & Blindaje

Entrega del Dictamen Ejecutivo para la Junta Directiva con sello criptográfico inmutable y activación de su crédito del 50% para escalar a **Sentinel OS™**.

CONTACTO DIRECTO DE DIRECCIÓN EJECUTIVA

Juan Carlos Díaz Parisca · Diego Fabrizio Vera Flores

Correo: jparisca@wanaditactical.com | **Web:** wanaditactical.com | **WhatsApp:** +58 414-2831076

AGENDAR DIAGNÓSTICO TÁCTICO

Disponibilidad inmediata para emergencias 24/7

© 2026 WANADI TACTICAL LLC · Todos los derechos reservados · Propiedad Intelectual Protegida (EE. UU.)