INGENIERÍA DE CIBERDEFENSA · FORENSIA DIGITAL · CONTINUIDAD OPERATIVA

WANADI TACTICAL

Protegemos la continuidad operativa de banca, telecomunicaciones, comercio e infraestructuras críticas mediante defensa en caliente, auditoría forense y sistemas de control local.

«Internet presupone conectividad. Wanadi se prepara para su falla».

JURISDICCIÓN Y SEDE	IMPACTO OPERATIVO	PRIVACIDAD	METODOLOGÍA
Estados Unidos · LLC	Intervención sin paradas previstas	Procesamiento local · Sin nube	NIST SP 800-86 · SHA-512

DIAGNÓSTICO DE RIESGO OPERATIVO

Por qué la ciberseguridad tradicional falla en el momento crítico

Vulnerabilidades explotadas rápidamente, sistemas legados sensibles y dependencias externas que pueden interrumpir el negocio.

RIESGO 01 · INTERRUPCIÓN

Actualizar o detener la producción

Parchar servidores financieros, comerciales o de telecomunicaciones puede romper dependencias y provocar paradas.

- Los sistemas legados no siempre admiten reinicios o cambios bruscos.
- Impacto financiero estimado: pérdidas de USD 5.000 a 50.000+ por hora de caída operativa.

RIESGO 02 · AUDITORÍA

Informes sin corrección efectiva

Auditorías lentas o intrusivas que entregan diagnósticos, pero no necesariamente neutralizan amenazas activas.

- Cambiar una configuración no demuestra que un intruso previo haya sido erradicado.
- La dirección necesita evidencias trazables para evaluar el riesgo.

RIESGO 03 · DEPENDENCIA

Falla de nube y conectividad

Cuando el enlace de Internet o los proveedores externos fallan, una respuesta centralizada puede quedar inoperativa.

- Dependencia de servicios y rutas de red de terceros.
- Inspeccionar solo el perímetro no equivale a examinar los procesos internos.

ARQUITECTURA INTEGRAL DE DEFENSA

Tres líneas de soluciones corporativas

Tecnologías diseñadas para servidores, estaciones de mando y comunicaciones en contingencia.

PILAR 01 · SERVIDORES

Tepuy Core™ y Anticuerpos Digitales

Auditoría forense e intervención en caliente para servidores Linux y Windows.

- Controles perimetrales y refuerzo del entorno de ejecución.
- Inspección forense mediante herramientas de detección especializadas.
- Preservación y registro criptográfico de evidencias.

PILAR 02 · ESTACIONES DE MANDO

Sentinel OS™

Sistema operativo táctico para estaciones de seguridad, equipos de salto y salas de crisis.

- Raíz del sistema protegida en modo de solo lectura.
- Recuperación controlada y seguridad basada en hardware.
- Análisis local sin telemetría obligatoria en la nube.

PILAR 03 · COMUNICACIONES

Kuntur Continuity SDK™

Capa de continuidad operativa para aplicaciones y redes con conectividad intermitente.

- Comunicación entre dispositivos por BLE y Wi-Fi Direct.
- Sincronización y recuperación de operaciones pendientes.
- Integración en aplicaciones corporativas y de campo.

CONTENCIÓN Y REMEDIACIÓN CONTROLADA

Tepuy Digital Antibody Suite™

Protección multicapa frente a riesgos de ejecución y exposición web. Cada intervención se valida en el entorno del cliente.

CAPACIDADES DE INTERVENCIÓN

01 · PROTECCIÓN DEL ACCESO WEB
Controles de entrada para interceptar actividad maliciosa y reducir exposición.

02 · ESTABILIZACIÓN DEL ENTORNO
Refuerzo de protección compatible con el funcionamiento de servicios críticos.

03 · REVISIÓN FORENSE RETROSPECTIVA
Identificación de indicios de intrusión actual o previa en los activos autorizados.

04 · COMPROBACIÓN Y REVERSIÓN
Verificación de resultados, acta técnica y procedimientos de reversión.

ACTUALIZACIÓN MANUAL FRENTE A ANTICUERPOS

CRITERIO	ACTUALIZACIÓN	WANADI
Sistemas legados	Compatibilidad variable	Controles compensatorios
Riesgo de interrupción	Puede requerir migración	Cambios progresivos y controlados
Intrusiones previas	No se detectan por actualizar	Búsqueda forense adicional
Prueba de intervención	Registro de actividades	Evidencia sellada con SHA-512

Intervención acotada por alcance, autorización y pruebas de compatibilidad.

DIAGNÓSTICO PROFUNDO Y TRAZABILIDAD

Tepuy Core™ M.2: doce capacidades de inspección

Inspección técnica para reconstruir actividad, identificar riesgos y producir resultados documentados.

MOTORES 01–03

Windows y registros

▸ Configuración y rastros
Revisión de indicadores técnicos relevantes.

▸ Actividad de acceso
Reconstrucción de eventos y accesos sospechosos.

▸ Mecanismos de persistencia
Detección de cambios y ejecuciones no habituales.

MOTORES 04–06

Memoria y amenazas

▸ Ejecución activa
Análisis de indicios en procesos y memoria, según acceso.

▸ Patrones de amenazas
Correlación de indicadores de software malicioso.

▸ Archivos sospechosos
Identificación y clasificación de anomalías.

MOTORES 07–09

Red y contenedores

▸ Entornos virtualizados
Revisión de privilegios y configuración.

▸ Conexiones activas
Indicios de comunicaciones no autorizadas.

▸ Transferencias no habituales
Evaluación de indicadores de fuga de información.

MOTORES 10–12

Criptografía y custodia

▸ Criptografía
Revisión de algoritmos y debilidades.

▸ Credenciales
Búsqueda de secretos expuestos.

▸ Evidencia SHA-512
Huella criptográfica y registro de custodia.

ENTREGABLE EJECUTIVO Informe de hallazgos, matriz de riesgos y recomendaciones de remediación · Referencia metodológica: NIST SP 800-86

ESTACIONES DE SEGURIDAD Y SALAS DE CRISIS

Sentinel OS™: un entorno táctico de control local

SENTINEL OS

Diseñado para consolas administrativas, equipos de salto, estaciones de tesorería y coordinación durante incidentes.

CAPACIDADES DE PROTECCIÓN

▸ Integridad del entorno
Entorno de ejecución controlado con verificaciones de integridad.

▸ Recuperación ante fallos
Mecanismos de retorno seguro a una configuración operativa conocida.

▸ Protección criptográfica
Resguardo de datos y credenciales mediante controles locales.

▸ Continuidad operativa
Preparado para trabajar con infraestructura local y enlaces intermitentes.

MODALIDADES DE IMPLEMENTACIÓN

01 · SENTINEL LITE™
Unidad USB de arranque para auditoría y trabajo táctico portátil.

02 · SENTINEL PRO™
Estación de centro de seguridad y equipo de salto en formato M.2.

03 · SENTINEL SOVEREIGN™
Equipo industrial para sala de crisis con IA local y continuidad de comunicaciones.

Referencias de alineación: NIS2 · SBS · SUDEBAN · ISO/IEC 27001

COMPARATIVA PARA LA DIRECCIÓN

Una propuesta integrada de defensa y evidencia

Comparativa operativa frente a esquemas tradicionales de seguridad y consultoría.

CRITERIO	EQUIPO INTERNO	CONSULTORÍA / NUBE	WANADI TACTICAL
Respuesta ante urgencias	Pruebas y cambios programados	Procesos externos de aprobación	Intervención orientada a horas
Aplicaciones legadas	Actualizaciones complejas	Cobertura variable por producto	Controles compensatorios en sitio
Intrusión ya presente	Revisión interna de eventos	Perímetro y alertas externas	Investigación retrospectiva especializada
Protección de datos	Depende de herramientas locales	Puede requerir tráfico externo	Procesamiento local o aislado
Soporte de evidencia	Registros internos	Informes automatizados	Acta técnica y huellas SHA-512
Inversión referencial	USD 15.000–40.000*	USD 24.000–60.000+ / año*	Demostración táctica desde USD 2.500

Alcance y condiciones de cada servicio establecidos en la propuesta y el contrato.

INVERSIÓN Y ESCALABILIDAD

Tres modalidades de contratación corporativa

Esquemas de inversión escalables diseñados para proteger la operación desde el primer día.

OPCIÓN 01 · DEMOSTRACIÓN

Demostración táctica presencial (PoV)

USD 2.500 PAGO ANTICIPADO

Validación focalizada en un activo crítico y objetivos previamente acordados.

- Sesión técnica, validación de capacidades y evidencia de resultados.
- Alcance, autorizaciones y entregables definidos por escrito.
- 100% acreditable a Auditoría Express de USD 6.500 en 45 días.

OPCIÓN 02 · CONTINUIDAD

Licencia anual Sentinel OS Pro™

USD 12.000 POR NODO / AÑO

Estación de seguridad y protección continua para equipos de TI.

- Unidad M.2 y entorno de sistema inmutable.
- Paquetes de Anticuerpos Digitales según contrato.
- Auditorías trimestrales previstas en la oferta.

OPCIÓN 03 · ALTA DIRECCIÓN

Sala de Crisis Sentinel Sovereign™

USD 35.000 IMPLEMENTACIÓN

Plataforma de coordinación y respuesta para dirección y centros críticos.

- Dos equipos industriales de mando.
- Red local de emergencia con Kuntur.
- Intervención sobre hasta 10 servidores y simulacro.

La demostración se acredita solo a Auditoría Express dentro de 45 días; otras licencias y equipos se cotizan por separado.

DIRECCIÓN Y EXPERIENCIA DE CAMPO

Equipo directivo y despliegue regional

Conocimiento de infraestructuras empresariales, continuidad operativa y desarrollo de soluciones de misión crítica.

FUNDADOR · DIRECTOR GENERAL

Juan Carlos Díaz Parisca

Arquitecto principal de sistemas

Más de 15 años de trayectoria en arquitectura crítica para telecomunicaciones y banca.

- Arquitectura de Tepuy Core, Sentinel OS y continuidad local.
- Liderazgo técnico en diagnósticos e implementaciones.

COFUNDADOR · DIRECTOR FINANCIERO

Diego Fabrizio Vera Flores

Gobernanza financiera y tesorería

Estructuración comercial B2B, análisis de inversión y gestión de riesgos.

- Modelos de contratación y retorno de inversión.
- Coordinación financiera y alianzas institucionales.

MARKETING · RELACIONES INSTITUCIONALES

Carolina Santini

Comunicación corporativa

Posicionamiento institucional y comunicación estratégica.

- Relación con directivos y ecosistemas empresariales.
- Traducción de riesgos técnicos al lenguaje de negocio.

VALIDACIÓN EN CAMPO: prueba de concepto en operaciones logísticas internacionales (VTC Cargo).

RUTA DE INCORPORACIÓN EN TRES PASOS

Asegure la continuidad de su operación

Un proceso de evaluación, diagnóstico y entrega de evidencias adaptado a la criticidad de sus sistemas.

01 PRIMER CONTACTO

Sesión ejecutiva y confidencialidad

Reunión con la dirección técnica para revisar riesgos prioritarios, expectativas y condiciones de confidencialidad.

02 INTERVENCIÓN

Diagnóstico y controles técnicos

Auditoría e intervención acordadas con el cliente, sujeta a autorización, evaluación de riesgos y ventanas de cambio.

03 ENTREGA

Resultados y trazabilidad

Informe ejecutivo de hallazgos, plan de remediación y evidencias criptográficas de los trabajos realizados.

CONTACTO DIRECTO · WANADI TACTICAL LLC

Juan Carlos Díaz Parisca · Diego Fabrizio Vera Flores

jparisca@wanaditactical.com | wanaditactical.com | +58 414-2831076

WANADI TACTICAL LLC · © 2026 · Todos los derechos reservados · Contacto institucional