METODOLOGÍA SAPIENT-OT VERSIÓN LITE

Safety-first Assessment Passive Intelligence Ethical Non-intrusive Testing for Operational Technology

RESUMEN EJECUTIVO

La metodología SAPIENT-OT representa un paradigma revolucionario en la evaluación de ciberseguridad para entornos de Tecnología Operacional (OT). Desarrollada específicamente para superar las limitaciones críticas de las metodologías tradicionales de pentesting, SAPIENT-OT prioriza la **seguridad operacional** y la **continuidad de procesos industriales** sin comprometer la exhaustividad de la evaluación de seguridad.

Diferenciación Clave

- **100% No Invasiva:** Cero riesgo de interrupción operacional
- **Safety-First:** La seguridad funcional prevalece sobre la ciberseguridad
- **Específica para OT:** Diseñada para protocolos y sistemas industriales
- **Multi-framework:** Integra cumplimiento con IEC 62443, NIST SP 800-82, NERC CIP

FUNDAMENTOS DE LA METODOLOGÍA

Principios Fundamentales

1. PRINCIPIO SAFETY-FIRST

- La seguridad funcional (safety) **SIEMPRE** prevalece sobre la ciberseguridad
- Tolerancia **CERO** a interrupciones de procesos críticos
- Respeto absoluto por sistemas SIS (Safety Instrumented Systems)
- Preservación incondicional de ventanas de mantenimiento programadas

2. ENFOQUE 100% NO INVASIVO

- Eliminación total de técnicas de explotación activa
- Uso exclusivo de análisis pasivo y simulación teórica
- Proof-of-concept sin impacto operacional
- Técnicas de reconocimiento ultra-conservadoras

3. ESPECIALIZACIÓN OT

- Comprensión profunda de protocolos industriales (Modbus, DNP3, EtherNet/IP, OPC UA)
- Análisis específico del Modelo Purdue
- Consideración de sistemas legacy industriales
- Integración con marcos de seguridad funcional

4. COMPLIANCE MULTI-FRAMEWORK

- Alineación simultánea con múltiples marcos regulatorios
- Mapeo directo a IEC 62443, NIST SP 800-82, NERC CIP
- Preparación para NIS2 y Cyber Resilience Act
- Evidencia auditable para compliance

METODOLOGÍA: FASES DETALLADAS

FASE 1: PLANIFICACIÓN Y SAFETY ASSESSMENT

Objetivos Principales

- Establecer contexto de seguridad operacional
- Definir alcance técnico sin riesgo
- Identificar sistemas críticos y restricciones
- Establecer protocolos de comunicación con operaciones

Actividades Críticas

Reunión de Stakeholders Obligatorios:

- Plant Manager/Director de Planta (autoridad final)
- CISO/Responsable de Seguridad (líder técnico)
- Safety Manager (responsable sistemas SIS)
- Operations Manager (ventanas mantenimiento)
- IT/OT Network Engineer (conocimiento infraestructura)

Evaluación de Impacto en Seguridad:

- Identificación de sistemas SIS y análisis SIL
- Mapeo de criticidad de procesos
- Definición de sistemas fuera de alcance
- Establecimiento de protocolos de emergencia

Documentación Legal Específica:

- NDA adaptado para entornos industriales
- Limitación de responsabilidad operacional
- Acuerdos de no interferencia con safety
- Protocolos de manejo de información sensible

Entregables Fase 1

- Plan de Evaluación Técnica OT-específico
- Matriz de Criticidad de Sistemas
- Protocolos de Comunicación 24/7
- Marco Legal y de Compliance

FASE 2: RECONOCIMIENTO PASIVO ESPECIALIZADO

Objetivos Principales

- Mapeo completo del panorama OT sin generar tráfico
- Identificación de arquitectura y topología real

- Análisis de exposición externa específica industrial
- Correlación con threat intelligence OT

Actividades Críticas

OSINT Industrial Avanzado:

Fuentes Específicas OT:
• Registros públicos de telecomunicaciones industriales
• Documentación técnica expuesta (P&ID, diagramas eléctricos)
• Certificaciones industriales públicas
• Bases de datos ambientales y de seguridad
• Información de proveedores OT específicos

Google Hacking para Sistemas Industriales:

Dorks Especializados:
• intitle:"SIMATIC WinCC" OR "WinCC Runtime"
• intitle:"FactoryTalk View SE"
• intitle:"ClearSCADA" OR "Geo SCADA"
• site:empresa.com filetype:pdf "P&ID"
• "empresa" AND "Modbus" AND "configuration"

Discovery de Red Ultra-Conservador:

- Temporización 1 paquete por 2 segundos máximo
- Escaneo paralelo limitado (máximo 1 hilo)
- Timeouts extendidos 5x normales
- Monitorización continua respuesta sistemas

Herramientas Principales

- **GRASSMARLIN** (NSA): Análisis 100% pasivo redes industriales
- **Shodan:** Búsqueda sistemas OT expuestos
- **Maltego:** Transforms específicos infraestructura crítica
- **Nmap:** Configuración ultra-safe para OT

Entregables Fase 2

- Inventario Completo de Activos OT
- Mapeo de Topología de Red
- Análisis de Exposición Externa
- Baseline de Threat Intelligence

FASE 3: ANÁLISIS DE VULNERABILIDADES

Objetivos Principales

- Identificación exhaustiva de vulnerabilidades sin impacto
- Clasificación específica para entornos OT
- Priorización basada en criterios industriales
- Validación de falsos positivos

Actividades Críticas

Escaneo Automático Ultra-Seguro:

Configuración Nessus OT:
• Retrasos obligatorios: 8-10 segundos entre peticiones
• Verificaciones concurrentes: Máximo 2 por dispositivo
• Plugins: Solo "safe" y "non-intrusive"
• Exclusiones: DoS, buffer overflow, cambios configuración

Análisis Manual por Protocolo:

Modbus TCP/RTU:

- Enumeración Function Codes sin modificar estados
- Análisis respuestas excepción
- Mapeo espacio direcciones
- Testing autenticación

DNP3:

- Evaluación SAv5 (Secure Authentication)
- Análisis respuestas no solicitadas
- Verificación integridad datos
- Testing mensajes broadcast

OPC UA:

- Gestión certificados X.509
- Configuración cifrado
- Métodos autenticación
- Control autorización RBAC

Clasificación Avanzada de Vulnerabilidades

CVSS v3.1 Adaptado para OT:

Modificadores Específicos Industriales:
• Safety Systems: +1.8x (impacto personas/ambiente)
• 24/7 Operations: +1.2x (sin ventanas mantenimiento)
• Production Critical: +1.4x (impacto continuidad)

Mapeo MITRE ATT&CK for ICS:

- Initial Access (TA0108): Valid Accounts, External Remote Services

- Execution (TA0109): Command-Line Interface, Scripting
- Impact (TA0119): Manipulation of Control, Loss of Safety

Entregables Fase 3

- Inventario Detallado de Vulnerabilidades
- Matriz de Priorización OT-específica
- Mapeo Compliance (IEC 62443, NIST, NERC CIP)
- Plan de Remediación Priorizado

FASE 4: SIMULACIÓN CONTROLADA DE EXPLOTACIÓN

Objetivos Principales

- Demostrar viabilidad de ataques sin ejecución real
- Desarrollar escenarios de impacto realistas
- Análisis de cadenas de ataque complejas
- Simulación en entornos seguros

Metodología de Explotación Simulada

Sistemas con Prohibición Total:

- Safety Instrumented Systems (SIS)
- Sistemas Control Proceso Crítico
- Equipos Legacy sin soporte
- Sistemas durante alta demanda operacional

Desarrollo de Entornos de Testing:

Laboratorios OT Seguros:
• Hardware representativo (PLCs, HMIs, historians)
• Simuladores software para dispositivos críticos
• Topología de red replicada
• Datos configuración sanitizados

Técnicas de Proof-of-Concept No Destructivo:

- Verificación autenticación sin bypass completo
- Demostración capacidad acceso sin explotación
- Análisis vulnerabilidades red sin interferencia
- Testing protocolos sin comandos control

Análisis de Cadenas de Ataque

Ejemplo: Compromiso Estación Ingeniería

1. Compromiso Inicial → Spear phishing ingeniero
2. Escalada Privilegios → Vulnerabilidad local

3. Movimiento Lateral → Credenciales caché
4. Manipulación Proceso → Modificación lógica PLC
5. Impacto Realizado → Degradación eficiencia

Entregables Fase 4

- Escenarios de Ataque Documentados
- Análisis de Cadenas de Impacto
- Simulaciones en Digital Twins
- Evaluación de Controles Compensatorios

FASE 5: ANÁLISIS DE IMPACTO OPERACIONAL

Objetivos Principales

- Cuantificar impacto real en operaciones industriales
- Evaluar efectos en cascada
- Análisis de impacto multi-dimensional
- Simulación de escenarios sin ejecución

Marco de Evaluación de Impacto

Matriz Multi-Dimensional:

Dimensión	Nivel 1 (Bajo)	Nivel 2 (Medio)	Nivel 3 (Alto)	Nivel 4 (Crítico)
Safety	Sin impacto SIS	Degradación menor	Compromiso parcial	Pérdida completa
Operacional	Degradación <10%	Reducción 10-25%	Parada parcial	Parada completa
Económico	<€10K pérdidas	€10K-€100K	€100K-€1M	>€1M pérdidas
Regulatorio	Notificación requerida	Investigación probable	Multas significativas	Suspensión licencias

Análisis de Movimientos Laterales:

- Mapeo rutas ataque sin movimiento real
- Identificación puntos pivote críticos
- Análisis interdependencias sistemas
- Evaluación controles segmentación

Metodología de Simulación de Impacto

Escenario Ejemplo - Sector Energético:

Compromiso Sistema Control Turbina:
• Impacto Directo: Parada 500MW = €200K/hora
• Costes Reinicio: €2M
• Impacto Red Regional: Activación reservas costosas
• Investigación Regulatoria: Autoridad eléctrica nacional

Entregables Fase 5

- Matriz de Impacto Cuantificado
- Análisis de Efectos en Cascada
- Escenarios de Impacto por Sector
- Recomendaciones de Mitigación

FASE 6: EVIDENCIAS Y ANÁLISIS FORENSE

Objetivos Principales

- Recopilación evidencias sin impacto operacional
- Preservación cadena custodia industrial
- Cumplimiento requisitos regulatorios
- Protección información sensible

Metodología de Recopilación Específica OT

Categorización de Evidencias:

Evidencias Sistema Control:
• Programas PLC y configuraciones
• Bases datos historians
• Archivos configuración SCADA/HMI
• Scripts automatización

Evidencias Comunicación Red:
• Tráfico protocolos industriales
• Comunicaciones wireless industriales
• Análisis timing comunicaciones
• Captura pasiva mediante TAPs

Técnicas No Invasivas:

- Network TAPs físicos (sin latencia)
- Mirror ports con configuración conservadora
- Captura memoria volátil en sistemas críticos
- Análisis logs sistemas industriales

Framework de Gestión de Evidencias

Clasificación Sensibilidad:

- **Información Seguridad Nacional:** Infraestructura crítica
- **Propietaria Proceso:** Recetas, parámetros optimización

- **Seguridad Funcional:** Configuraciones SIS, procedimientos emergencia
- **Regulatoria:** Datos compliance, historial incidentes

Protección y Cifrado:

- Cifrado AES-256 para almacenamiento
- Gestión claves criptográficas robusta
- Timestamps criptográficos verificables
- Verificación integridad continua

Entregables Fase 6

- Paquete Evidencias Forenses
- Documentación Cadena Custodia
- Análisis Compliance Regulatorio
- Protección Información Sensible

FASE 7: RECOMENDACIONES Y REMEDIACIÓN

Objetivos Principales

- Desarrollo recomendaciones específicas OT
- Priorización basada en criterios industriales
- Plan implementación sin impacto operacional
- Alineación con marcos regulatorios

Marco de Recomendaciones OT-Específico

Categorización por Impacto:

Recomendaciones Safety-Critical:

- Mejoras sistemas SIS sin compromiso función
- Validación niveles SIL post-implementación
- Análisis modos fallo para cambios propuestos
- Documentación según ciclo vida seguridad

Recomendaciones Continuidad Operacional:

- Implementación durante ventanas mantenimiento
- Diseño con redundancia y resiliencia
- Procedimientos rollback rápido
- Coordinación equipos operacionales 24/7

Metodología de Priorización

Algoritmo Scoring Integrado:

```
Score = (Safety Impact × 0.40) + (Operational × 0.25) +
        (Regulatory × 0.15) + (Business × 0.10) +
        (Technical × 0.05) + (Threat × 0.05)
```

Clasificación:
• 9.0-10.0: CRÍTICO (0-24 horas)
• 7.0-8.9: ALTO (24-72 horas)
• 5.0-6.9: MEDIO (1-4 semanas)
• 3.0-4.9: BAJO (1-6 meses)

Plan de Acción Estructurado

Fase Inmediata (0-72 horas):

- Vulnerabilidades críticas safety
- Quick wins sin impacto operacional
- Controles mitigatorios temporales
- Comunicación ejecutiva obligatoria

Fase Programada (1-4 semanas):

- Mejoras estructurales sistemas
- Segmentación red y firewalls
- Endurecimiento configuraciones
- Training equipos especializados

Fase Transformación (6+ meses):

- Actualizaciones mayores sistemas
- Frameworks seguridad comprehensivos
- Capacidades SOC avanzadas
- Cumplimiento completo estándares

Entregables Fase 7

- Plan Remediación Priorizado
- Roadmap Implementación Temporal
- Guías Técnicas Específicas
- Marco Seguimiento y Mejora Continua

FASE 8: INFORMES Y COMUNICACIÓN

Objetivos Principales

- Comunicación efectiva múltiples audiencias
- Protección información sensible

- Cumplimiento requisitos legales
- Seguimiento implementación

Tipología de Informes Específicos

Informe Ejecutivo:

Estructura Optimizada:
• Dashboard visual estado seguridad
• Hallazgos críticos (máximo 5)
• Impacto cuantificado en términos negocio
• ROI estimado recomendaciones
• Cronograma implementación realista

Informe Técnico Detallado:

Contenido Especializado:
• Metodología SAPIENT-OT aplicada
• Análisis arquitectura industrial
• Vulnerabilidades con evidencias
• Correlación frameworks (CVE, CWE, MITRE)
• Recomendaciones implementación específicas

Informe Compliance:

Mapeo Multi-Framework:
• IEC 62443: Security Levels y Foundational Requirements
• NIST SP 800-82: Familias control y RMF
• NERC CIP: Estándares específicos utilities
• NIS2: Requisitos entidades esenciales

Consideraciones Seguridad y Confidencialidad

Clasificación Información:

- **Crítica Seguridad Nacional:** Protección gubernamental
- **Propietaria Proceso:** Acuerdos confidencialidad específicos
- **Seguridad Funcional:** Restricciones acceso personal autorizado
- **Técnica Sensible:** Cifrado y controles acceso granular

Aspectos Legales:

- Revisión consejo legal obligatoria
- Coordinación autoridades regulatorias
- Cumplimiento plazos notificación
- Protección privilegio attorney-client

Entregables Fase 8

- Suite Informes Multi-Audiencia
- Documentación Compliance

- Protocolos Distribución Segura
- Framework Seguimiento Continuo

MATRIZ DE RIESGOS INTEGRADA

Modelo de Evaluación Específico OT

La matriz de riesgos SAPIENT-OT™ integra consideraciones únicas de entornos industriales:

Dimensiones de Evaluación

1. **Impacto Safety (40%):** Sistemas SIS, rating SIL, peligros proceso
2. **Criticidad Operacional (25%):** Disponibilidad, redundancia, costes downtime
3. **Exposición Regulatoria (15%):** Cumplimiento normativo, sanciones
4. **Impacto Negocio (10%):** Pérdidas financieras, recuperación
5. **Severidad Técnica (5%):** CVSS adaptado, exploitabilidad
6. **Probabilidad Amenaza (5%):** Intelligence, capacidades adversario

Ejemplo de Aplicación

Vulnerabilidad: Bypass autenticación SIS

• Safety Impact: 10/10 (Sistemas críticos vida)
• Operational: 8/10 (Parada emergencia probable)
• Regulatory: 9/10 (Violación normas safety)
• Business: 8/10 (Pérdidas millonarias)
• Technical: 7/10 (Exploit disponible)
• Threat: 6/10 (APT capabilities requeridas)

Score Final: 9.2/10 → CRÍTICO (Acción 0-24h)

INDICADORES Y KPIs DE EVALUACIÓN

Framework de Métricas OT-Específico

KPIs Estratégicos (Executive Dashboard)

Postura Seguridad General: 78/100 (Objetivo: 85/100)
Tiempo Medio Detección: 4.2 horas (Objetivo: <3 horas)
Vulnerabilidades Críticas: 0 (Objetivo: 0)
Cumplimiento IEC 62443: 60% (Objetivo: 85%)
Madurez Seguridad: 2.15/5.0 (Objetivo: 2.8/5.0)

KPIs Tácticos (Management Operacional)

Disponibilidad Sistemas: 99.6% (Baseline: 99.7%)
Latencia Red OT: 18ms (Baseline: 15ms)
False Positives/Día: 12 (Objetivo: <20)
Tiempo Respuesta HMI: 250ms (Baseline: 200ms)

Métricas ROI y Valor Negocio

Inversión Total Programa: €680,000
Beneficios Anuales: €1,030,000
ROI: 151% (Payback: 8.0 meses)
Prevención Incidentes: €920,000/año
Eficiencias Operacionales: €105,000/año

COMPARATIVA CON METODOLOGÍAS TRADICIONALES

Limitaciones Metodologías Existentes

Aspecto	OWASP	OSSTMM	PTES	SAPIENT-OT
Enfoque Safety	No considerado	Ausente	Básico	**PRIORITARIO**
Protocolos OT	No incluidos	Limitado	Básico	**COMPLETO**
Técnicas No Invasivas	20%	30%	40%	**95%**
Compliance Industrial	Web-focused	Genérico	Genérico	**MULTI-FRAMEWORK**
Consideración SIL/SIS	No	No	No	**SÍ**
Impacto Producción	Aceptable	Medio	Medio	**PROHIBIDO**

Ventajas Competitivas Demostradas

Reducción Riesgos Operacionales:

- 100% reducción incidentes relacionados evaluación
- Ahorros €500K-€2M por evitar paradas no planificadas
- Tasa aceptación 95% equipos operacionales

Cumplimiento Regulatorio:

- Aceptación sin observaciones auditores múltiples marcos
- Evidencia auditable completa
- Mapeo directo requisitos específicos sector

Eficiencia Tiempo y Recursos:

- Tiempo total comparable metodologías tradicionales
- Eliminación fases explotación activa
- Reducción significativa tiempo remediación

HERRAMIENTAS Y TECNOLOGÍAS

Stack Tecnológico Especializado

Reconocimiento y Discovery

OSINT Industrial:
• Maltego + Transforms industriales
• Shodan + queries OT específicas
• Censys + certificate intelligence
• GRASSMARLIN (NSA) + análisis pasivo

Network Discovery:
• Nmap + configuración ultra-safe
• Wireshark + dissectors OT
• NetworkMiner + reconstrucción sesiones
• TAPs físicos + mirror ports

Análisis Vulnerabilidades

Escaners Adaptados:
• Nessus Professional + plugins OT
• OpenVAS + NVTs industriales
• Qualys VMDR + assets industriales
• PLCScan + protocolos específicos

Análisis Protocolos:
• ModbusPal + simulación segura
• S7comm tools + análisis Siemens
• DNP3 analyzers + utilities focus
• OPC UA Expert + configuración seguridad

Forense y Evidencias

Recopilación Pasiva:
• Forensic TAPs + captura completa
• WinPmem/LiME + memoria volátil
• FTK Imager + imaging sistemas críticos
• Volatility + análisis memoria avanzado

Gestión Evidencias:
• Blockchain + cadena custodia
• HSMs + gestión claves criptográficas
• Secure storage + clasificación automática
• Legal holds + compliance frameworks

CASOS DE USO Y SECTORES VALIDADOS

Sectores de Aplicación Exitosa

Energía y Utilities

Aplicaciones Validadas:
• Centrales térmicas/nucleares/renovables
• Subestaciones transmisión/distribución
• Plantas procesamiento gas natural
• Sistemas gestión demanda

Resultados Típicos:
• Mejora 85% postura ciberseguridad
• Cumplimiento NERC CIP sin observaciones
• Cero impacto operaciones durante evaluación

Manufactura Avanzada

Sectores Específicos:
• Automoción (líneas ensamblaje)
• Aeroespacial (manufactura precisión)
• Electrónica (fabricación semiconductores)
• Farmacéutico (procesos críticos)

Características Únicas:
• Sistemas MES complejos
• Robótica industrial avanzada
• Digital twins procesos
• Industria 4.0 integrada

Químico y Petroquímico

Entornos Críticos:
• Refinerías petróleo
• Plantas petroquímicas
• Procesamiento gas
• Manufactura química fina

Consideraciones Especiales:
• Sistemas SIL 3/4 obligatorios
• Sustancias peligrosas
• Procedimientos emergencia estrictos
• Cumplimiento ambiental crítico

IMPLEMENTACIÓN Y ADOPCIÓN

Roadmap de Implementación Organizacional

Fase 1: Preparación (Mes 1)

Actividades Clave:
• Training inicial equipos internos
• Adaptación herramientas específicas

• Establecimiento protocolos comunicación
• Validación marco legal específico

Entregables:
• Equipo certificado SAPIENT-OT
• Toolkit herramientas configurado
• Procedimientos internos definidos
• Contratos/NDAs adaptados

Fase 2: Piloto (Meses 2-3)

Alcance Piloto:
• Selección subsistema no crítico
• Aplicación metodología completa
• Validación resultados
• Refinamiento procedimientos

Objetivos:
• Demostrar valor sin riesgo
• Entrenar equipos práctica real
• Establecer baselines métricas
• Obtener buy-in operacional

Fase 3: Despliegue (Meses 4-12)

Expansión Gradual:
• Evaluación sistemas críticos
• Integración procesos normales
• Establecimiento KPIs continuo
• Optimización basada experiencia

Resultados Esperados:
• Postura seguridad mejorada 60-80%
• Cumplimiento regulatorio completo
• Cultura seguridad OT establecida
• ROI demostrado cuantitativamente

CERTIFICACIÓN Y COMPETENCIAS

Programa de Certificación SAPIENT-OT

Niveles de Certificación

Practitioner Level:
• Comprensión fundamentos metodología
• Aplicación técnicas básicas
• Conocimiento protocolos industriales
• Capacidad evaluaciones supervisadas

Specialist Level:
• Liderazgo evaluaciones independientes
• Desarrollo recomendaciones complejas
• Expertise sectores específicos
• Training otros profesionales

Expert Level:
• Diseño programas seguridad OT
• Consultoría estratégica C-level
• Desarrollo metodología avanzada
• Publicación investigación sector

Requisitos de Competencia

Conocimientos Técnicos:
• Protocolos industriales (Modbus, DNP3, OPC UA)
• Sistemas control (PLC, DCS, SCADA, HMI)
• Seguridad funcional (IEC 61508/61511)
• Frameworks seguridad (IEC 62443, NIST)

Experiencia Práctica:
• 3+ años entornos industriales
• Proyectos seguridad OT demostrados
• Conocimiento sectores específicos
• Certificaciones complementarias

CONTACTO Y RECURSOS

Información del Autor

José Israel Nadal Vidal

- CISO & Chief Information Security Officer
- Red Team Specialist & DPO Certificado
- Master en Seguridad Informática y Hacking Ético
- Certificaciones: ISO 27001 Lead Auditor, Claroty CIE, Tenable OT Expert

Recursos Adicionales

Documentación:
• Guías implementación detalladas
• Plantillas contratos/NDAs
• Herramientas análisis específicas
• Casos uso sector por sector

Training:
• Cursos certificación online
• Workshops prácticos presenciales
• Consultoría implementación
• Soporte técnico especializado