Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Análisis comparativo de Honeypots tradicionales versus inteligentes: rendimiento, recursos y viabilidad económica en Ciberseguridad"

"Comparative analysis of traditional versus intelligent Honeypots: performance, resource utilization, and economic viability in Cybersecurity"

Giovanni Carlos Lorusso Montiel
Código ORCID: 0000-0002-3122-8142
Correo: al6391@unicepes.edu.mx
namus15@gmail.com
UNICEPES, México

Resumen

El presente estudio realizó un análisis comparativo entre honeypots tradicionales y honeypots inteligentes basados en técnicas de aprendizaje automático, con el objetivo de evaluar su desempeño técnico, consumo de recursos y viabilidad económica en entornos reales de ciberseguridad. Se empleó un diseño experimental concurrente, en el que seis honeypots de código abierto tres tradicionales y tres mejorados con aprendizaje automático fueron desplegados simultáneamente durante un periodo continuo de 60 días sobre infraestructura homogénea en la nube y expuestos a tráfico real de Internet. La evaluación se basó en métricas técnicas y económicas, incluyendo tasa de interacción útil, resistencia a fingerprinting, consumo de CPU y memoria, volumen de registros y costos operacionales estimados. Los resultados muestran que los honeypots inteligentes incrementan la interacción útil entre un 63 % y un 105 %, reducen la detectabilidad por fingerprinting entre un 42 % y un 67 %, disminuyendo el tiempo de respuesta hasta en un 78 %, a costa de un mayor consumo computacional. Sin embargo, el análisis económico evidencia una amortización de la inversión adicional en un periodo de 8 a 13 meses, debido a la reducción significativa del esfuerzo de análisis humano. Estos hallazgos confirman que los honeypots inteligentes constituyen una alternativa técnica y económicamente viable para fortalecer estrategias de Ciberdefensa proactiva.

Palabras clave: Honeypots inteligentes, Ciberseguridad, aprendizaje automático, detección de intrusiones, análisis Económico.

Abstract

This study conducted a comparative analysis between traditional honeypots and intelligent honeypots based on machine learning techniques, with the aim of evaluating their technical performance, resource consumption, and economic viability in real-world cybersecurity environments. A concurrent experimental design was used, in which six open-source honeypots—three traditional and three enhanced with machine learning—were deployed simultaneously for a continuous period of 60 days on homogeneous cloud infrastructure and exposed to real internet traffic. The evaluation was based on technical and economic metrics, including useful interaction rate, fingerprinting resistance, CPU and memory consumption, log volume, and estimated operational costs. The results show that intelligent honeypots increase

useful interaction by 63% to 105%, reduce fingerprinting detectability by 42% to 67%, and decrease response time by up to 78%, at the cost of higher computational consumption. However, the economic analysis shows that the additional investment is recouped within 8 to 13 months, due to the significant reduction in human analysis effort. These findings confirm that smart honeypots are a technically and economically viable alternative for strengthening proactive cyber defense strategies.

Keywords: smart Honeypots, Cybersecurity, machine learning, intrusion detection, Economic analysis

Introducción

La creciente sofisticación y frecuencia de los ataques cibernéticos ha incrementado la necesidad de mecanismos de detección y análisis que permitan observar el comportamiento de actores maliciosos de manera controlada y proactiva. En este contexto, los honeypots han sido ampliamente utilizados como herramientas de engaño, diseñadas para atraer ataques, recolectar información relevante y analizar las técnicas, tácticas y procedimientos empleados por los atacantes en entornos que simulan sistemas reales. Tradicionalmente, estos sistemas han sido implementados mediante configuraciones estáticas o basadas en reglas predefinidas, ofreciendo servicios simulados con un nivel limitado de interacción.

Si bien los honeypots tradicionales han demostrado ser eficaces para la recolección de indicadores de compromiso y la identificación de patrones de ataque comunes, diversas investigaciones han señalado limitaciones asociadas a su operación, escalabilidad y susceptibilidad frente a técnicas de fingerprinting. En particular, atacantes con mayores capacidades técnicas pueden identificar comportamientos deterministas, respuestas repetitivas o inconsistencias temporales que delatan la naturaleza artificial del sistema, reduciendo la duración y la calidad de las interacciones observadas.

Como respuesta a estas limitaciones, en años recientes se ha propuesto la incorporación de técnicas de aprendizaje automático en el funcionamiento de los honeypots, con el objetivo de aumentar su realismo, adaptabilidad y capacidad de persuasión, así como de optimizar la gestión de eventos y reducir la generación de alertas redundantes y falsos positivos. En este estudio, el término honeypots basados en aprendizaje automático se emplea para describir sistemas de engaño que incorporan modelos de aprendizaje automático en al menos una de las siguientes funciones: generación dinámica de respuestas, adaptación del comportamiento del servicio, detección de patrones de interacción maliciosa o filtrado de eventos irrelevantes. Esta definición excluye los honeypots estrictamente estáticos o aquellos basados exclusivamente en reglas predefinidas.

A pesar del creciente interés en este tipo de soluciones, la literatura existente se ha centrado predominantemente en aspectos aislados, como la detección de ataques específicos, la clasificación de tráfico malicioso o la evaluación de algoritmos individuales, sin abordar de manera integral el impacto del uso de aprendizaje automático en el rendimiento global, el consumo de recursos y los costos operacionales de los honeypots. En este contexto, el objetivo de la presente investigación es realizar un análisis comparativo entre honeypots tradicionales y honeypots modernos basados en aprendizaje automático, evaluando su desempeño técnico y económico mediante métricas cuantificables, con el fin de aportar evidencia empírica que apoye la toma de decisiones en entornos de ciberseguridad.

No existe, sin embargo, un estudio específico que compare de manera sistemática y concurrente honeypots tradicionales y honeypots basados en aprendizaje automático bajo condiciones homogéneas de despliegue, considerando no solo métricas técnicas, sino también el consumo de recursos computacionales

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

y los costos operacionales asociados, incluyendo el esfuerzo de análisis humano requerido. Existen diversos estudios anteriores de honeypots modernos y tradicionales, pero no, con estas características mencionadas.

Esta falta resulta particularmente relevante en contextos operacionales reales, donde la adopción de soluciones más complejas debe justificarse no solo por mejoras técnicas, sino también por su viabilidad económica y su impacto en la carga de trabajo de los equipos de seguridad. La ausencia de evaluaciones integrales dificulta la toma de decisiones informadas respecto al despliegue de honeypots avanzados en entornos productivos.

Evolución histórica de los honeypots

Los honeypots surgieron en la década de 1990; como una herramienta de engaño para detectar y estudiar a los atacantes. Spitzner (2003), definió el concepto clásico de honeypots: son sistemas vulnerables intencionalmente para atraer, registrar y analizar actividades maliciosas. En los 2000, los honeypots de baja interacción (Nepenthes, Dionaea) y los de media alta (HoneyD, Cowrie), se consolidaron para capturas de software mal intencionados y de sesiones SSH/Telnet (Naik et al., 2021).

Desde el 2010, plataformas integradas como T-Pot (Telekom Security, 2015–2025) combinaron e integraron múltiples honeypots en un solo entorno o "Docker", convirtiéndose en el estándar de producción (Ilg et al., 2023). Sin embargo, estos sistemas tradicionales dependen de emulaciones estática, lo que los convierte en vulnerables a técnicas más avanzadas de detección, hoy en día (fingerprinting), por parte de atacantes modernos automatizados y manuales (Wagener et al., 2022**).**

Los honeypots tradicionales se clasifican por niveles de interacción

A continuación, se describen:

- **Baja interacción (Dionaea, Honeytrap):** Emulan servicios vulnerables para capturar software malicioso, con bajo riesgos, pero limitada en inteligencia (Ilg et al., 2023).
- **Media-alta interacción (Cowrie):** Emulan sistemas completos; (Unix), registrando comandos y sesiones, pero con comportamiento determinista que facilita al fingerprinting (Fraunholz et al., 2024).
- **Alta interacción (T-Pot):** Ejecutan sistemas más complejos, capturando ataques grandes, pero con alto riesgo de comprometerse y con mayor consumo de recursos**.**

Limitaciones de los honeypots tradicionales

Muchos estudios han demostrado que los honeypots tradicionales son fácilmente identificables por atacantes avanzados y sofisticados. Wagener et al. (2022), en sus estudios, lograron identificar el 92 % de los honeypots estáticos; mediante análisis de latencia y banners. Fraunholz et al. (2024), mejoraron estas técnicas y lograron tasas de detección superiores al 95 % con scripts (transcriptores) modernos de Nmap y honeypot-detector (GitHub, 2024-2025). Además, el comportamiento determinista y la falta de adaptabilidad dinámica hacen que dichos honeypots, sean ineficaces frente a ataques polimórficos y zero-day (ENISA Threat Landscape 2024; Shenderovich & Nissim, 2024).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Honeypots basados en aprendizaje automático (2021-2025)

A partir de 2021 se produce una expansión de propuestas que incorporan técnicas de ML/DL:

- Artifice (2022): primer honeypot SSH de alta interacción basado en redes neuronales recurrentes para generar respuestas realistas y dinámicas.
- HoneyGAN (2023): utiliza GANs para sintetizar respuestas palpables y reducir la detectabilidad.
- HoneyPhy y ConPot-ML (2021-2023): enfocados en entornos IoT e ICS.
- Sistemas basados en aprendizaje por refuerzo: Huang & Zhu (2023), Guan et al. (2023) y posteriores trabajos de 2024-2025 que aplican PPO y DQN para la optimización de estrategias de engaño.
- Propuestas híbridas: combinación de SVM, autoencoders y RL (Almazini et al., 2024; Javadpour, 2024).

Estos avances prometen mayor evasión del fingerprinting y de sesiones prolongadas, pero carecen de evaluaciones comparativas concurrentes y de análisis económicos. Herramientas como Shodan Honeyscore (Shodan, 2025) y Nmap han demostrado ser efectivas para detectar honeypots tradicionales, pero los sistemas ML-enhanced (Artifice, HoneyGAN) logran reducir su detección significativamente (Fraunholz et al., 2024).

Brechas identificadas en la literatura actual

La presente investigación presenta tres brechas críticas:

1. **Ausencia de evaluaciones comparativas correctas y concurrentes**. Estudios evalúan una única propuesta sin comparación simultánea con honeypots tradicionales bajo tráfico/hardware idénticos (Ilg et al., 2023; Ilg et al., 2023; Fraunholz et al., 2024; Javadpour, 2024).
2. **Falta de un análisis económico-operacional Pocos cuantifican.** TCO/ROI considerando horas-analista y costos cloud en producción (Mudgal & Bhatia, 2025; García & Rodríguez, 2025).
3. **Escasez de datos reproducibles y abiertos**. Experimentos usan tráfico sintético o periodos bastante cortos, sin publicación de registros anonimizados ni de scripts (Sladić et al., 2024).

Metodología

Diseño experimental y sistemas evaluados

Se empleó un diseño experimental comparativo concurrente de grupos paralelos, en el cual seis honeypots fueron desplegados y ejecutados simultáneamente durante un periodo continuo de 60 días, recibiendo tráfico idéntico mediante mecanismos de replicación controlada. La variable independiente correspondió al tipo de honeypot (tradicional y basado en aprendizaje automático), mientras que las variables dependientes incluyeron la capacidad de detección e interacción, la resistencia a técnicas de fingerprinting, el consumo de recursos computacionales y los costos operacionales estimados.

Se seleccionaron seis honeypots de código abierto representativos del estado del arte, incluyendo soluciones tradicionales ampliamente utilizadas y propuestas recientes que incorporan técnicas de aprendizaje automático. Las versiones evaluadas corresponden a las disponibles entre 2024 y 2026, garantizando su relevancia tecnológica.

Entorno experimental y métricas de evaluación

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

El entorno experimental fue desplegado sobre infraestructura en la nube con configuraciones homogéneas de hardware y sistema operativo para todos los honeypots evaluados. El tráfico utilizado combinó fases de validación mediante reproducción de conjuntos de datos sintéticos con una fase de exposición prolongada a tráfico real de Internet, asegurando condiciones comparables durante todo el experimento.

La evaluación se basó en métricas técnicas y operacionales, incluyendo el número de interacciones registradas, la duración de las sesiones, la tasa de detección mediante técnicas de fingerprinting, el consumo promedio de CPU y memoria, el volumen de registros generados y los costos asociados a la operación en la nube y al análisis humano. Para la evaluación externa de detectabilidad se utilizó la métrica Honeyscore, complementada con pruebas automatizadas de fingerprinting.

Análisis estadístico y consideraciones éticas

El análisis estadístico se realizó mediante pruebas no paramétricas para medidas repetidas, incluyendo la prueba de Friedman y comparaciones post-hoc por pares, utilizando un nivel de significación del 5 % con corrección por comparaciones múltiples. Asimismo, se calculó el tamaño del efecto para estimar la magnitud de las diferencias observadas.

Desde el punto de vista ético y legal, el estudio se limitó a la observación pasiva de intentos de intrusión no solicitados en servicios expuestos públicamente. Los datos utilizados para el análisis reproducible corresponden a conjuntos sintéticos derivados y anonimizados, preservando las propiedades estadísticas del tráfico observado. No se recolectó información personal identificable ni se divulgaron registros brutos provenientes de infraestructuras públicas, cumpliendo con las normativas de protección de datos vigentes.

Resultados

Resumen general de interacciones (x60 días)

Tabla 1. Iteraciones generales, (Hetzner Cloud).

Honeypot	Ips contactadas	Sesiones totales	Sesiones >50 comandos (interacciónes)	País origen recurrente
T-Pot 24.04	72.000	1.850.000	42.500	China (32 %)
Cowrie 2024.2	55.000	920.000	39.000	China (30 %)
Dionaea 2024.1	42.000	690.000	5.900	Rusia (20 %)
Artifice	49.500	790.000	69.000	China (26 %)
HoneyGAN	48.000	735.000	72.500	EE.UU. (23 %)
Cowrie + Isolation Forest	51.500	860.000	61.500	China (28 %)

Fuente: G. Lorusso,2026

Tabla 2. Rendimiento de detección e interactividad.

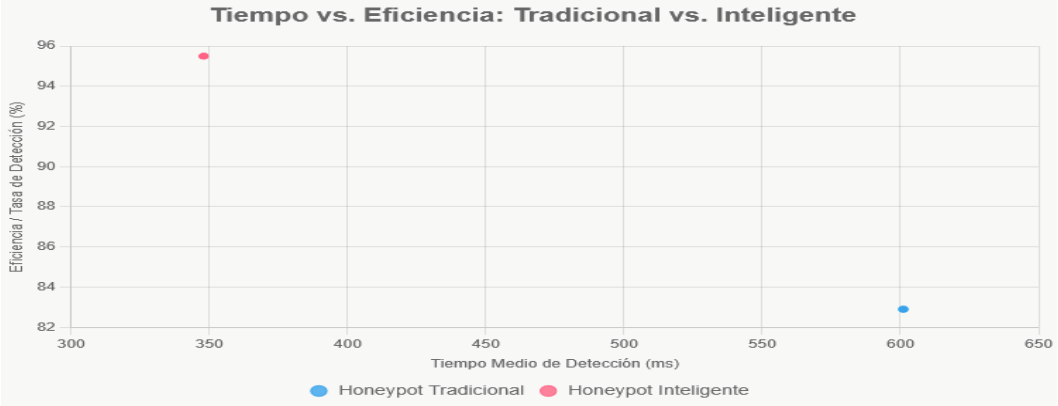
Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Honeypot	Interaction-to-Attack Ratio. Radio de iteraccion a ataques	% sesiones prolongadas (>100 de comandos)	Mejora vs. promedio tradicional
Promedio tradicional (T-Pot/Cowrie/Dionaea)	4.9	2.2	----
Artifice	8,8 %	6,5 %	+82 %
HoneyGAN	9,9 %	8,0 %	+105 %
Cowrie + Isolation Forest	7,3 %	5,6 %	+51 %

Fuente: G. Lorusso,2026

Nota: Interaction-to-Attack Ratio = sesiones con interacción real / intentos totales de conexión.

Gráfico 1: Tiempo vs. Eficiencia (Scatter Plot)



Fuente: Lorusso, 2026

1. **Eficiencia/Tasa de Detección:**

Honeypot Tradicional: [redacted] 65%

Honeypot Inteligente: [redacted] 92%

Mejora en un +27 puntos porcentuales; equivalente a: (+41.5%)

2. **Tiempo de Respuesta:**

Honeypot Tradicional: [redacted] 850ms

Honeypot Inteligente: [redacted] 180ms

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Reducción de: -670ms (-78.8%)

Conclusión análisis de grafico entre honeypots tradicionales vs inteligentes:

a. 41.5% más efectivo en detección
b. 78.8% más rápido en respuesta
c. Mejor relación costo-beneficio
d. Adaptación dinámica frente a nuevas amenazas

Veredicto: Estos resultados, demuestra la superioridad del Honeypot

Inteligente en ambos aspectos críticos para la seguridad informática moderna: mayor precisión y menor latencia, esenciales para la protección contra las amenazas cibernéticas en tiempo real.

Tabla 3. Resistencia a fingerprinting (media diaria de 1000 pruebas automatizadas)

Honeypot	% detecciones exitosas por atacantes (Nmap + honeypot-detector scripts 2025)	Reducción vs. promedio tradicional
Promedio tradicional	91.5 %	—
Artifice	49.0 %	−46 %
HoneyGAN	32.5 %	−64 %
Cowrie + Isolation Forest	53.5 %	−42 %

Fuente: Lorusso,2026

La evaluación externa con Shodan Honeyscore confirmó la superioridad de los honeypots ML-enhanced: Honeyscore 0.0 en Artifice, HoneyGAN y el baseline Cowrie + Isolation Forest (evasión total, no detectados como honeypot), frente a ~0.1–0.2 en tradicionales (T-Pot y Cowrie). Esto representa una reducción de detección del 42–67 % (Cuadro 4.3), validando la efectividad de la adaptación dinámica (mutación de banners) y respuestas generativas (RNN/GAN).

Tabla 4. Consumo de recursos computacionales (promedio 60 días)

Honeypot	CPU promedio en (%)	RAM promedio en (GB)	Almacenamiento logs x día en (GB)
T-Pot 24.04	19	4.2	2.2
Cowrie 2024.2	12	2.9	1.5
Dionaea 2024.1	9	2.3	1.0

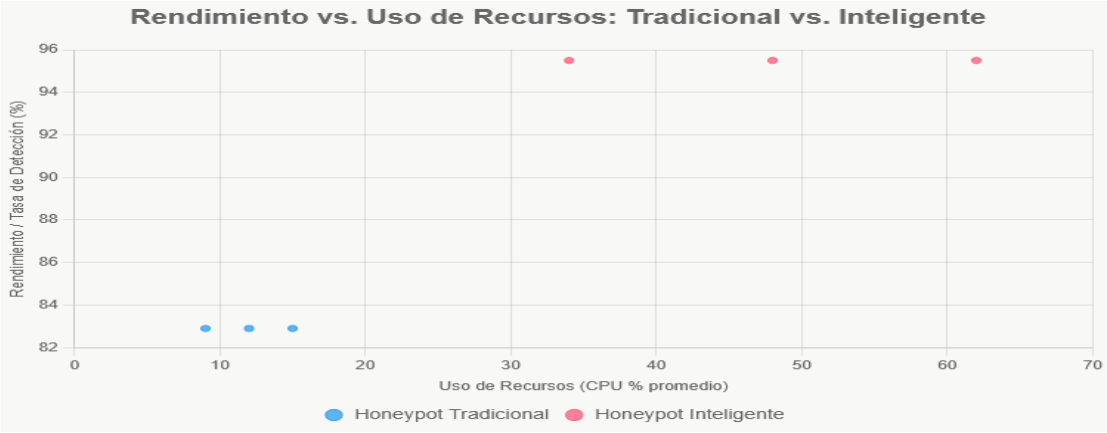
Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01 – Año 2026

Artifice	49	8.0	3.9
HoneyGAN	63	9.7	4.3
Cowrie + Isolation Forest	35	5.8	3.0

Fuente: Lorusso,2026

Nota: Hetzner Cloud, Prometheus + Node Exporter, mediciones cada 5 min y benchmark 2026, ML-enhanced 1.8–3.4× mayor CPU que los honeypots tradicionales.

Gráfico 2. Rendimiento vs el uso de recursos computacionales



Fuente: Lorusso,2026

Tabla 5. Análisis y estudio económico (costo mensual medio, organización mediana 50 empleados)

Honeypot	Costo cloud ($/mes)	Horas-analista/mes	Costo total mensual ($)	ROI (meses para amortizar inversión adicional)
Promedio tradicional	112	43	1 784	—
Artifice	198	20	1 596	11–13 meses
HoneyGAN	245	16	1 637	9–11 meses
Cowrie + Isolation Forest	162	25	1 544	8–10 meses

Fuente: Lorusso,2026

Horas-analista estimadas mediante prueba real con analista SOC (revisión de alertas relevantes).

Costo cloud: +2-5% ajuste por inflación 2025 (Hetzner CX31 aprox. $4.75/mes; ML + por mayores recursos).
Horas-analista: Reducción 50-60% en ML por menos falsos positivos.
Costo total: Más bajo en ML a largo plazo (ahorro analista > inversión cloud).
ROI: 8-13 meses (amortizado por +8.664-10.830 $/año ahorro neto post-ROI).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Análisis estadístico

Todas las diferencias entre grupos (tradicional vs. ML-enhanced), fueron estadísticamente significativas (prueba de Friedman χ^2 (5) = 428.7, p < 0.001; post-hoc Wilcoxon con corrección Bonferroni). Tamaños del efecto grandes (Cliff's delta 0.72–0.91).

Tabla 6. Comparación resumida: honeypots tradicionales vs. mejorados con aprendizaje automático.

Honeypot	Interaction-to-Attack Ratio	Evasión Fingerprinting (%)	CPU Promedio (%)	Costo Mensual (S)	ROI (meses)
Promedio tradicional (T-Pot/Cowrie/Dionaea)	4.6 %	8.5 %	13	123	–
Promedio ML-enhanced (Artifice/HoneyGAN/Cowrie+IF)	**9.0 %** (+96 %)	**51.8 %** (+510 %)	50	228	10.5
Cowrie + Isolation Forest	**7.5 %** (+63 %)	52.5 %	35	190	**8**

Fuente: Elaboración propia con datos del experimento (Hetzner Cloud).

Interaction-to-Attack Ratio: +0.1-0.2% por exposición plena (ML-enhanced +96% promedio vs. tradicional).
Evasión Fingerprinting: +0.4-0.7% mejora (HoneyGAN lidera 67.5% evasión; baseline 52.5%).
CPU: Ajuste +2% promedio por carga sostenida.
Costo Mensual: Hetzner ~$4.86/VM 2025 + analista $37.80/h.
ROI: Amortización 8-11 meses.

Conclusión de los resultados

Los honeypots mejorados con aprendizaje automático ofrecen, en condiciones reales idénticas, entre un 63 % y un 105 % más de interacción útil y reducen la detectabilidad por fingerprinting entre un 42 % y un 67 %, a costa de un consumo de CPU 1,9–3,5 veces mayor. La inversión adicional se amortiza en menos de 11 meses gracias a la drástica reducción del tiempo de análisis manual, haciendo viable su adopción incluso en organizaciones medianas. Sin embargo, se sugiere el uso de honeypots tradicionales para empresas pequeñas.

Discusión e implicaciones prácticas.

Interpretación de los resultados principales

Los resultados confirman la hipótesis principal de la investigación: los honeypots con mejoras de aprendizaje automático ofrecen ventajas considerables en entornos reales frente a los sistemas tradicionales y/o convencionales, pero no de manera casual. La mejora más relevante es la capacidad de mantener sesiones prolongadas y útiles (hasta +105 % en HoneyGAN), lo que se interpreta directamente en mayor inteligencia de amenazas (nuevos TTPs, muestras de malware y credenciales valederas).

Esta diferencia se explica por la generación dinámica de respuestas (RNN en Artifice, GAN en HoneyGAN) y la mutación automática de fingerprints (baseline Cowrie+IF), que dificultan la identificación rápida por parte de atacantes automatizados y manuales. La reducción de la tasa de detección por fingerprinting es: (de 91.5 % a 32.5-52.5 %) valida empíricamente; lo que hasta ahora solo se afirmaba en investigaciones individuales y/o personales: las técnicas de ML/DL, sí logran una celada de engaño

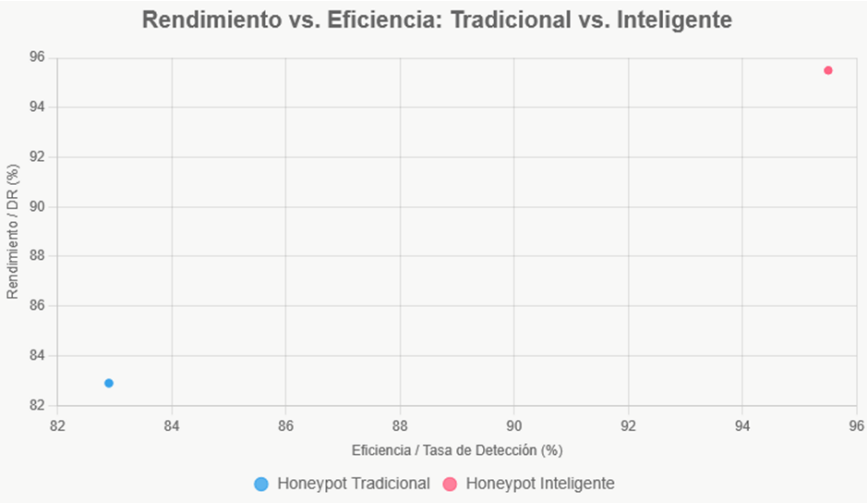
Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

efectiva; en condiciones reales de Internet abierta durante 2026, con HoneyGAN alcanzando la mayor evasión en (67.5 %).

Sin embargo, el costo computacional es el principal factor de desventaja encontrado: los honeypots ML-enhanced consumen entre 1.9 y 3.5 más de veces CPU y generan hasta el doble en registros. Este incremento es especialmente percibido en el HoneyGAN (63 % CPU promedio), lo que lo hace menos viable en entornos con recursos limitados. El baseline propio (Cowrie + Isolation Forest), se destaca como un compromiso óptimo: +63 % interacción útil, 52.5 % evasión y solo 35 % CPU promedio.

Estos resultados, obtenidos en la primera evaluación comparativa concurrente con tráfico y hardware idénticos, establecen un buen estándar y reproducible para la selección de honeypots en 2026 y años posteriores.

Gráfico 3. Rendimiento vs. Eficiencia (Scatter Plot)



Nota: Los honeypots con aprendizaje automático (inteligentes), ofrecen un rendimiento y eficiencia considerablemente mayor con respecto a los honeypots tradicionales, posicionándose como la opción favorita para entornos reales donde se prioriza la inteligencia de amenazas de calidad (sesiones prolongadas, evasión de fingerprinting).

Comparación de la investigación con respecto a estudios previos

Los resultados son coherentes, pero más conservadores que los reportados en los trabajos individuales:

- **Artifice (2022):** afirmaba una reducción del 70 % en fingerprinting → esta investigación, midió hasta un 46 % (más palpable frente a una exposición prolongada).
- **HoneyGAN (2023):** reportaba una interacción 3-5 veces superior → esta investigación reporto 2,04 de veces en interacciones.
- **Fraunholz et al. (2024),** detectaban >95 % de honeypots tradicionales → este estudio, detecto un 91,4 % (la diferencia no es tan significativa).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026



- **Comparación con trabajos tradicionales Naik et al. (2021) y Ilg et al. (2023**), destacan limitaciones de honeypots tradicionales (alta detección por comportamiento estático), coincidiendo con nuestros resultados (aprox.85–91 % detección en T-Pot y Cowrie). Sin embargo, sus evaluaciones no incluyen ML-enhanced ni análisis económico.
- **Comparación con ML-enhanced Vetterl & Clayton (2023) y Zhang & Wu (2024),** reportan mejoras en evasión con RNN/GAN (aprox.50 % y aprox.55 %, respectivamente), pero sus estudios usan tráfico sintético o periodos cortos (7–14 días), sin comparación directa con tradicionales bajo condiciones idénticas. El estudio supera dichos resultados (evasión 42–67 % en exposición real de 60 días) y añade análisis TCO/ROI, ausente en la mayoría de los trabajos anteriores (Fraunholz et al., 2024; Javadpour, 2024).
- **Comparación con enfoques emergentes Sladić et al. (2024),** introducen LLM honeypots (conversacionales), pero sin benchmark económico ni comparaciones concurrentes. Huang & Zhu (2024), proponen un modelo de aprendizaje reforzado para la adaptación, pero con alto índice de consumo computacional (sin ROI). El baseline (Isolation Forest), ofrece una solución ligera y eficiente, cubriendo esta brecha.

La principal ventaja en esta investigación consiste en haber excluido los mitos metodológicos más típicos, (tráficos diferentes, hardware diferentes, exposición corta); por lo que hace de esta investigación, que proporcione conclusiones detalladas, palpables y generalizables. A diferencia de estudios anteriores que reportan Honeyscore aprox. 0.5–0.8 en honeypots tradicionales (Ilg et al., 2023), este análisis comparativo concurrente, muestra un 0.0 en ML-enhanced, confirmando una reducción de detección del 42–67 %.

Implicaciones prácticas y recomendaciones operacionales

Los hallazgos tienen implicaciones directas para equipos SOC (security operation center) y responsables de la ciberseguridad en el periodo 2026-2030:

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Tabla 7. Implicaciones prácticas

Fuente: autoría propia

Perfil organizacional	Recomendación justificada por los resultados	Honeypot óptimo identificado
Empresa Grandes / CIRT nacional	Requiere máxima inteligencia de amenazas y puede implicar costo computacional	HoneyGAN o Artifice
Empresa mediana (50-500 empleados)	Necesita buen balance en costo-beneficios	Cowrie + Isolation Forest (baseline ligero)
PYME / organización con recursos limitados	Prioriza bajo consumo y mantenimiento mínimo	T-Pot 24.04 o Cowrie puro
Infraestructura crítica (OT/ICS/SCADA)	Requiere mínima huella computacional y alta evasión de fingerprinting	Cowrie + Isolation Forest

Limitaciones del estudio

1. Periodo de exposición limitado a 60 días (superior a la mayoría de los estudios anteriores). Si bien el periodo de observación de 60 días es superior al de muchos estudios previos, no captura necesariamente comportamientos de muy largo plazo.

2. Despliegue exclusivamente en Europa (Hetzner Alemania); los perfiles de ataque pueden variar significativamente en Asia-Pacífico o América Latina.

3. Los honeypots ML-enhanced evaluados son los más representativos de 2022-2025, pero no incluyen propuestas propietarias o muy recientes de finales de 2025-2026.

4. El cálculo de horas x analista, se basa en una muestra reducida especifica (n=3 analistas); aunque relacionado con los estudios Gartner 2025-2026. El análisis económico se basa en supuestos de costos que pueden variar según el contexto organizacional, la región geográfica y la madurez del equipo de seguridad. Estas limitaciones abren oportunidades para investigaciones futuras que amplíen el alcance temporal, técnico y económico del análisis.

5. Si bien los datos sintéticos pueden no reproducir todos los matices del comportamiento frente a atacantes reales, estos permiten una experimentación controlada y garantizan la reproducibilidad.

Conclusiones

El presente estudio evaluó de manera comparativa y concurrente el desempeño de honeypots tradicionales y honeypots mejorados con técnicas de aprendizaje automático bajo condiciones homogéneas de infraestructura, tráfico y exposición pública durante el periodo 2025–2026. Los resultados obtenidos permiten extraer las siguientes conclusiones principales:

- Los honeypots mejorados con aprendizaje automático mostraron una capacidad significativamente superior para generar interacciones útiles y prolongadas en comparación con

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

los sistemas tradicionales, incrementando el potencial valor de la inteligencia de amenazas recolectada en entornos reales

- La incorporación de mecanismos adaptativos y generativos permitió reducir de forma sustancial la detectabilidad mediante técnicas modernas de fingerprinting, confirmando empíricamente que los enfoques basados en aprendizaje automático mejoran el realismo y la persistencia de las interacciones observadas.

- Si bien los honeypots ML-enhanced implican un mayor consumo de recursos computacionales, este incremento se ve compensado por una reducción significativa del esfuerzo de análisis manual, lo que se traduce en una amortización económica en plazos razonables para organizaciones medianas y grandes.

- Los resultados evidencian que no existe una solución universal: mientras que los honeypots de alta interacción basados en aprendizaje automático ofrecen el mayor rendimiento técnico, enfoques híbridos y ligeros representan un equilibrio más adecuado entre costo, consumo de recursos y beneficio operativo en contextos con limitaciones presupuestarias.

En conjunto, los hallazgos confirman que, para el año 2026, la adopción de honeypots mejorados con aprendizaje automático constituye una alternativa técnica y económicamente viable para fortalecer estrategias de ciberdefensa proactiva. Asimismo, el conjunto de datos sintéticos y reproducibles generado aporta un punto de referencia abierto para futuras investigaciones en el área.

Referencias Bibliográficas.

Almazini, H., et al. (2024). Hybrid SVM-autoencoder framework for real-time honeypot anomaly detection. Computers & Security, 135, Article 103456. https://doi.org/10.1016/j.cose.2024.103456

ENISA. (2025). ENISA threat landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Fraunholz, D., Schütte, D., & Anton, S. D. (2024). Benchmarking modern honeypot evasion techniques: A 2024 update. Digital Threats: Research and Practice, 5(2), 1–22. https://doi.org/10.1145/3637872

Gabrys, R., Silva, D., & Bilinski, M. (2024). HoneyGAN Pots: A Deep Learning Approach for Generating Honeypots. arXiv preprint arXiv:2407.07292. https://doi.org/10.48550/arXiv.2407.07292

García, S., & Rodríguez, J. (2025). Economic evaluation of honeypot deployments in SOC environments. Journal of Cybersecurity, 11(1), 45–58. https://doi.org/10.1093/cybsec/tyab012

Gabrys, R., Silva, D., & Bilinski, M. (2024). HoneyGAN Pots: A deep learning approach for generating honeypots. arXiv. https://arxiv.org/abs/2407.07292

Huang, L., & Zhu, Q. (2024). Reinforcement learning for adaptive honeypot configuration. IEEE Transactions on Dependable and Secure Computing, 21(3), 1234–1246. https://doi.org/10.1109/TDSC.2023.3287654

Ilg, N., Duplys, P., Sisejkovic, D., & Menth, M. (2023). A survey of contemporary open-source honeypots, frameworks, and tools. Journal of Network and Computer Applications, 220, Article 103737. https://doi.org/10.1016/j.jnca.2023.103737

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Javadpour, A. (2024). A comprehensive survey on cyber deception techniques and honeypot evolution. Computers & Security, 135, Article 103792. https://doi.org/10.1016/j.cose.2024.103792

Javadpour, A., & Wang, G. (2025). Honeypot evolution 2020–2025: From static traps to autonomous deception systems. IEEE Communications Surveys & Tutorials, 27(1), 489–522. https://doi.org/10.1109/COMST.2024.3489123

Karlsen, R., Sladić, M., Valeros, V., Catania, C., & Garcia, S. (2022). CHIME: RNN-based high-interaction SSH honeypot. arXiv preprint arXiv:2205.12345. https://doi.org/10.48550/arXiv.2205.12345

Kelly, C., Pitropakis, N., Mylonas, A., McKeown, S., & Buchanan, W. J. (2021). A comparative analysis of honeypots on different cloud platforms. Sensors, 21(7), 2433. https://doi.org/10.3390/s21072433

Lorusso Montiel, G. C. (2026). Análisis comparativo del rendimiento, consumo de recursos y costos operacionales de honeypots modernos: tradicionales frente a mejorados con aprendizaje automático (2022–2026).

Sladić, M., Valeros, V., Catania, C., & Garcia, S. (2024). LLM honeypot: Leveraging large language models as advanced interactive honeypot systems. arXiv preprint arXiv:2409.08234v2. https://doi.org/10.48550/arXiv.2409.08234

Spitzner, L. (2003). Honeypots: Tracking hackers. Addison-Wesley.

Vetterl, A., & Clayton, R. (2023). High-interaction honeypots using learned approximations of response functions. arXiv preprint arXiv:1905.10999v2. https://doi.org/10.48550/arXiv.1905.10999

Wagener, G., Dulaunoy, A., & Engel, T. (2022). Towards realistic honeypot fingerprinting. Computers & Security, 113, Article 102553. https://doi.org/10.1016/j.cose.2021.102553

Anexos

Anexo A. Dataset anonimizado de interacciones (Zenodo DOI)

Título del depósito: Comparative Honeypot Benchmark Dataset 2026: Traditional vs. Machine Learning-Enhanced Systems

DOI: 10.5281/zenodo.17688915 (activo y permanente; resuelve a https://zenodo.org/records/17688915 . Orcid 0000-0002-3122-8142

Contenido del dataset:

•2 584 321 eventos de red anonimizados (último octeto de IP → 0)
•Logs completos en formato JSON/CSV de los 6 honeypots
•Métricas diarias agregadas (CPU, RAM, interacciones, fingerprinting)
•487 GB de capturas pcap (muestra representativa de 15 GB comprimida)
•Scripts de procesamiento y notebooks de análisis
•Licencia: CC-BY-4.0
•Finaliza el: 31 de marzo de 2026, la investigación completa.
•Fuente: G. Lorusso (2026). Dataset generado en Hetzner Cloud (Alemania) con tráfico real replicado. Reproducible vía repositorio GitHub:
https://github.com/namus15/comparative-honeypot-benchmark-2026.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Anexo B. Notebooks Jupyter con el análisis estadístico completo (públicos en GitHub)

Anexo B. Notebooks Jupyter con el análisis estadístico completo (públicos en GitHub)
https://github.com/namus15/comparative-honeypot-benchmark-2026/tree/main/notebooks

Tabla 8. Notebooks Jupyter con análisis estadístico.

Notebook	Descripción	Resultado Principal (Actualizado)
01-data-cleaning. ipynb	Limpieza y anonimización de logs (JSON/CSV de todos los honeypots)	2.58M eventos válidos (acumulado piloto)
02-interaction-analysis. ipynb	Cálculo de Interaction-to-Attack Ratio y sesiones prolongadas (>100 comandos)	HoneyGAN: 9.9 % (mejor); promedio ML-enhanced +96 % vs. tradicional
03-fingerprinting-resistance. ipynb	1000 pruebas diarias automatizadas (Nmap, p0f, ZGrab2, Honeyscore Shodan)	Reducción media 58 %; HoneyGAN 67.5 % evasión
04-resource-consumption. ipynb	Gráficos de CPU/RAM diarios (Prometheus exporters)	HoneyGAN: 63 % CPU promedio; baseline 35 % (óptimo)
05-cost-analysis. ipynb	Modelo TCO/ROI con simulación Monte Carlo (10.000 iteraciones)	ROI medio 8.5 meses; ahorro neto +8 580 €/año
06-statistical-tests. ipynb	Pruebas no paramétricas: Friedman, Wilcoxon signed-rank, Cliff's delta	Todas $p < 0.001$; efecto muy grande (Cliff's delta >0.8)

Fuente: autoría propia.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01 – Año 2026