

De la pirámide de *Threat Profiling* a la Pirámide de Actores de Amenaza 2026

Origen, límites y una actualización del modelo de seis niveles para la era de la inteligencia artificial

Sebastián Vargas Yáñez · CEO de TTPSEC · Investigador doctoral en seguridad de IA
ORCID [0000-0003-1782-3153](https://orcid.org/0000-0003-1782-3153) · 29 de octubre de 2026

Resumen

La pirámide de seis niveles de actores de amenaza sigue siendo una herramienta didáctica útil, pero en 2026 clasifica mal: ordena *quién* es el atacante cuando lo que hoy discrimina es *qué capacidad pone en juego en una operación concreta*. Este artículo reconstruye la genealogía del modelo, desde la matriz genérica de amenaza de Sandia (2007, 2012) y la taxonomía del Defense Science Board (2013) hasta su primera aparición corporativa fechada, en una patente de T-Mobile USA (prioridad 2014). Con evidencia de 2025–2026 (ENISA, Verizon DBIR, Microsoft y el honeypot HIVE-AI), muestra que cuatro supuestos de la lámina popular dejaron de cumplirse. Propone la Pirámide de Actores de Amenaza 2026: los mismos seis niveles, ordenados por modo de operación; la IA como multiplicador transversal y no como séptimo nivel; y un perfil de seis dimensiones que separa la capacidad del atacante de la exposición y el impacto de la organización. Cierra con las amenazas a la validez y una agenda de validación empírica.

Palabras clave: perfilamiento de amenazas, actores de amenaza, inteligencia de amenazas, gestión de riesgo, IA generativa, Defense Science Board.

1. Introducción

Tesis. La pirámide de seis niveles que usamos para perfilar atacantes sigue siendo útil, pero en 2026 ordena mal: ordena *quién* es el actor cuando lo que hoy discrimina es *qué capacidad pone en juego en una operación concreta*. Propongo mantener los seis niveles, cambiar la variable que los ordena y tratar la IA como un amplificador transversal, no como un séptimo piso.

En 2019, desde el CSIRT de Redbanc, analizamos mucho esta pirámide. Era la lámina que todos tenían en la presentación: verde abajo, rojo arriba, *script kiddies* en la base y naciones en la punta. Funcionaba porque era simple. Siete años después, esa misma simplicidad se volvió un riesgo.

Tres hallazgos de 2026 lo muestran. ENISA constata que la distinción entre cibercrimen, hacktivismo y actividad con nexo estatal sigue difuminándose. Verizon mide que la explotación de vulnerabilidades ya supera al abuso de credenciales como vector de entrada. Y Microsoft sostiene que la IA da a actores poco sofisticados una persistencia que antes era exclusiva de las agencias de inteligencia. Si un mismo grupo opera en tres pisos según el día, el piso deja de describir al grupo.

Antes de proponer nada, fui a buscar de dónde sale realmente la pirámide. La respuesta es más interesante de lo que recordaba.

2. El origen: no es una pirámide, son dos modelos pegados

La lámina «Threat Profiling» circula desde hace una década casi siempre sin autor. Su aparición fechada más antigua que encontré es la FIG. 1 de la patente *Recombinant threat modeling* de T-Mobile USA, de los inventores Gregory Reith y Brett Peppe ([US 10,216,938 B2](#)). La patente tiene prioridad del 5 de diciembre de 2014; la solicitud se publicó el 9 de junio de 2016 y la concesión llegó en febrero de 2019. El OCR de la portada de la solicitud muestra los elementos de la lámina: un rótulo de actor por nivel (de *script kiddies* a naciones), el eje intención/capacidad y los multiplicadores financiamiento, activos y tecnología. Esa figura, a su vez, ensambla dos trabajos del gobierno de EE.UU. publicados con meses de diferencia (Figura 1 y Tabla 1).

La pirámide del Defense Science Board (2013)

El informe *Resilient Military Systems and the Advanced Cyber Threat* fue un estudio de 18 meses de un grupo de trabajo para el Secretario de Defensa de EE.UU. Su taxonomía agrupa seis niveles en tres pares. Los niveles I y II explotan vulnerabilidades conocidas. Los III y IV tienen recursos y pericia para descubrir vulnerabilidades nuevas. Los V y VI invierten miles de millones de dólares y años para *crear* vulnerabilidades, incluso en sistemas bien protegidos. El ancho de cada piso representa la cantidad de practicantes, no el riesgo. El ejemplo de nivel VI del propio informe es analógico: el proyecto GUNMAN, en el que la inteligencia soviética modificó máquinas de escribir IBM Selectric de la embajada de EE.UU. en Moscú.

El DSB dejó dos advertencias que casi nadie copió a la lámina, y que son la clave de esta actualización. La primera: los actores de nivel alto usan la técnica más baja que les sirva, para esconderse en el ruido de los niveles inferiores. La segunda: los Estados pueden actuar mediante proxies, de modo que un grupo de nivel medio accede a capacidades de nivel alto. Además, su modelo de riesgo trataba la consecuencia como un parámetro separado de la amenaza. El autor original ya advertía, en otras palabras, que el nivel describe una capacidad y no una identidad.

La matriz de Sandia (2007–2012)

La franja inferior de la lámina (intensidad, sigilo, tiempo, personal, conocimiento, acceso y los multiplicadores financiamiento, activos y tecnología) viene de la matriz genérica de amenaza de Sandia National Laboratories. Su motivación era justamente evitar las etiquetas: sus autores criticaban que los modelos de la época fueran poco más que una progresión de rótulos, que refuerzan prejuicios y oscurecen la capacidad real. Propusieron describir la amenaza por atributos medibles, en dos familias (compromiso y recursos) y con ocho niveles.

Hay un detalle fino. Sandia trata el financiamiento, los activos y la tecnología como *multiplicadores*: potencian atributos, pero no cambian el nivel de la amenaza. La lámina popular los puso en la misma fila que el resto. Esa confusión importa en 2026, porque la IA es precisamente un multiplicador.

De la patente a la lámina de referencia

La patente no cita al DSB, pero usa su misma escala I–VI y la combina con los atributos de Sandia; la filiación es una inferencia por coincidencia, no una cita. Desde ahí la lámina circuló sin atribución entre consultoras, cursos y blogs. Telenor llevó los seis niveles al lenguaje de arquitectura defendible en 2020, con un dato útil: un nivel 6 puede asignar más de cien personas a una sola operación por etapas. En el camino se perdieron las advertencias del DSB y la lógica de atributos de Sandia.

El modelo tampoco está solo. La Tabla 2 lo sitúa junto a otras escalas de adversario. Lo relevante es la columna de impacto: los esquemas que se usan para gestionar riesgo (NIST SP 800-30, DSB) separan el impacto del nivel del adversario; la lámina popular los funde.

Tabla 1. Genealogía documentada del modelo de seis niveles de actores de amenaza

Año	Fuente	Tipo	Aporte al modelo	Verificación
2007	Duggan et al., SAND2007-5791 (Sandia)	Laboratorio	Matriz genérica de amenaza: 8 niveles definidos por atributos, sin rótulos de actor	FP
2012	Mateski et al., SAND2012-2427 (Sandia)	Laboratorio	Familias compromiso (intensidad, sigilo, tiempo) y recursos (personal técnico, conocimiento, acceso); multiplicadores (financiamiento, activos, tecnología)	FP
2013	Defense Science Board, Resilient Military Systems	Gobierno	Taxonomía de 6 niveles en 3 pares (explotar, descubrir, crear vulnerabilidades); advierte uso de proxies y técnica mínima	FP
2014	Reith y Peppe, US 2016/0162690 A1 y US 10,216,938 B2 (T-Mobile USA)	Industria	"Threat pyramid" (FIG. 1): actores por nivel, intención/capacidad y multiplicadores (financiamiento, activos, tecnología)	FP*
c. 2016–2019	Lámina "Threat Profiling" en circulación	Difusión	Reproduce la FIG. 1 sin atribución; fusiona la pirámide DSB con la franja Sandia	P
2020	Kvarvåg y Kall (Telenor Group)	Industria	Aplica los 6 niveles a arquitectura defendible; nivel 6 con más de 100 personas por operación	FP
2026	Este artículo	Propuesta	Niveles por modo de operación; IA como multiplicador transversal; perfil de 6 dimensiones	—

FP = verificado en fuente primaria. P = parcial: coincidencia por OCR, sin cotejo visual. — = no aplica.

* Prioridad: provisional 62/088,479 (5 dic. 2014); solicitud publicada el 9 jun. 2016; patente concedida el 26 feb. 2019. El contenido de la FIG. 1 se identificó por el OCR de la portada de la publicación A1; las etiquetas "Global 25 / 150 / 2000" no se pudieron cotejar.

La patente no cita al Defense Science Board; la filiación conceptual con DSB (2013) es una inferencia por coincidencia de la escala I–VI.

Tabla 2. Escalas de adversario comparables: unidad clasificada, niveles y tratamiento del impacto

Esquema	Año	Niveles	Atributos que ordenan	Unidad clasificada	¿Separa impacto del nivel?
Sandia, matriz genérica de amenaza	2007/2012	8	Compromiso (intensidad, sigilo, tiempo); recursos (personal técnico, conocimiento, acceso)	Amenaza	No reportado
MITRE, niveles de amenaza (Bodeau et al.)	2010	5	Capacidad, intención, focalización	Adversario	No reportado
NIST SP 800-30 Rev. 1	2012	5 por atributo	Capacidad, intención, focalización (Apéndice D)	Adversario	Sí: el impacto es un factor de riesgo distinto
Defense Science Board	2013	6	Capacidad y recursos: explotar, descubrir, crear vulnerabilidades	Actor	Sí: consecuencia como parámetro de riesgo aparte (p. 6)
MITRE Cyber Prep 2.0 (Bodeau y Graubart)	2017	5 clases	Metas, alcance, horizonte temporal, persistencia y sigilo, capacidades	Clase de adversario	Parcial: las clases se nombran por su efecto
Aerospace SPARTA	s. f.	7	Habilidad, malicia, motivación, métodos	Actor	No reportado
Pirámide de Actores 2026 (esta propuesta)	2026	6 + 6 dimensiones	Capacidad y persistencia observadas; IA como multiplicador	Operación	Sí: D5 y D6 fuera del eje

"No reportado" significa que la fuente no lo trata explícitamente; no equivale a afirmar que el esquema carezca de esa propiedad.

MITRE (2010): Unsophisticated, Limited, Moderate, Significant, Advanced. NIST SP 800-30: Very Low a Very High por atributo; páginas de las Tablas D-3 a D-5 no cotejadas.

La lámina popular funde complejidad e impacto en un eje; el DSB, su fuente conceptual, sí los separaba.

Genealogía documentada del modelo de seis niveles (2007–2026)

Nodos equiespaciados: el eje horizontal ordena la secuencia, no es proporcional al tiempo.

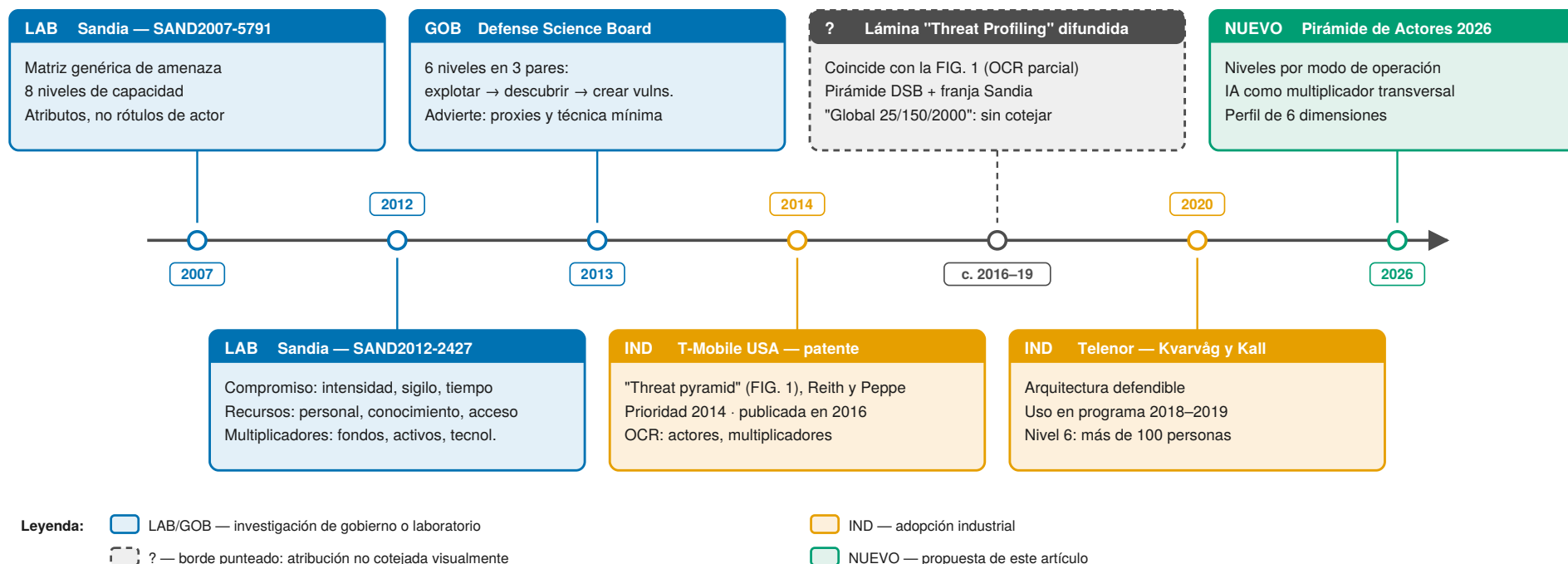


Figura 1. Genealogía documentada del modelo de seis niveles (2007–2026). Azul: investigación de laboratorio o de gobierno; naranja: adopción industrial; verde: esta propuesta. La caja de borde punteado marca la difusión de la lámina "Threat Profiling", cuya coincidencia con la FIG. 1 de la patente de T-Mobile se estableció por OCR y no por cotejo visual. Nodos equiespaciados: el eje ordena la secuencia, no es proporcional al tiempo.

3. Qué envejeció: cuatro supuestos que ya no se sostienen

El modelo no está equivocado: está desalineado con cómo se organiza hoy la oferta de ataque. Cuatro supuestos implícitos de la lámina dejaron de cumplirse. La Tabla 3 resume la evidencia.

1. Identidad del actor = capacidad. La lámina asigna cada tipo de actor a un piso. Pero la economía del ransomware como servicio, los intermediarios de acceso inicial y los mercenarios comerciales separaron quién opera de quién desarrolla: un afiliado con poca pericia alquila capacidades de nivel IV. ENISA constata que las categorías de amenaza siguen difuminándose y que operadores criminales, hacktivistas y con nexo estatal recurren cada vez más a vectores, herramientas y enfoques similares. El rótulo «hacktivista» no dice qué capacidad tiene el grupo esta semana.

2. Lo de abajo es ruido; lo de arriba es lo grave. La pirámide sugiere que el impacto crece con el piso. Los datos de 2025 no lo respaldan de forma lineal. ENISA analizó 8.257 incidentes: el 51,3 % fueron DDoS, el tipo más frecuente. Sin embargo, el mismo informe concluye que la actividad financiera, encabezada por el ransomware, es la de mayor impacto a corto plazo, y que el ciberespionaje lo es a largo plazo. A la inversa, una intrusión oportunista sobre un sistema OT expuesto puede tener consecuencias de nivel VI.

3. Las defensas se apilan por piso. La columna derecha de la lámina asigna «firewall, AV» a la base y «contrainteligencia» a la punta. Hoy la entrada dominante es transversal. Según el Verizon DBIR 2026, la explotación de vulnerabilidades subió al 31 % de los accesos iniciales (20 % el año anterior) y el 48 % de las brechas involucró a un tercero (30 % el año anterior). La cadena de suministro, que el DSB reservaba al nivel V, es hoy la puerta de casi cualquier nivel.

4. La tecnología es un dato fijo. Sandia ya advertía que la tecnología disponible limita atributos como el tiempo y el conocimiento. La IA generativa y agéntica movió ese límite para todos a la vez. Microsoft sostiene que la IA comprime la cadena de ataque de los actores sofisticados de días a segundos. Eso no sube a nadie de piso por sí solo, pero acorta la distancia entre pisos.

Tabla 3. Evidencia empírica de 2025–2026 usada para fundamentar la actualización

Fuente	Indicador	Valor	Referencia de comparación	Periodo	Ubicación
<i>Vectores de entrada y terceros</i>					
Verizon DBIR 2026	Explotación de vulnerabilidades como acceso inicial	31 %	20 % en la edición 2025	nov. 2024 – oct. 2025	pp. 10, 15
Verizon DBIR 2026	Abuso de credenciales como acceso inicial	13 %	22 % en la edición 2025	nov. 2024 – oct. 2025	pp. 10, 16
Verizon DBIR 2026	Brechas con participación de un tercero	48 %	30 % en la edición 2025	nov. 2024 – oct. 2025	pp. 11, 20
Verizon DBIR 2026	Vulnerabilidades KEV completamente remediadas	26 %	38 % en la edición 2025	2025	pp. 10, 17
Verizon DBIR 2026	Brechas con ransomware	48 %	44 % en la edición 2025	nov. 2024 – oct. 2025	pp. 11, 30
<i>Distribución del volumen frente al impacto</i>					
ENISA ETL 2026	Incidentes DDoS	51,3 %	Tipo de incidente más frecuente	ene.–dic. 2025	pp. 7, 11
ENISA ETL 2026	Incidentes de acceso no autorizado	39,5 %	—	ene.–dic. 2025	pp. 7, 11
ENISA ETL 2026	Accesos no autorizados que explotaron una vulnerabilidad	60,4 %	Solo del 5,2 % con vector identificado	ene.–dic. 2025	p. 11
ENISA ETL 2026	Amenaza de mayor impacto	Cualitativo	Financiera: corto plazo · espionaje: largo plazo	ene.–dic. 2025	pp. 10, 13
<i>Efecto de la IA</i>					
Microsoft MDDR 2026	Compresión de la cadena de ataque en actores sofisticados	días → segundos	Cualitativo	2025–2026	Resumen ejecutivo, p. 3
HIVE-AI (Vargas Yáñez y Tobón, 2026)	Ataques contra APIs de IA generativa	16 683	1 229 IP de 50 países	20 días de operación	Resumen
HIVE-AI (Vargas Yáñez y Tobón, 2026)	Sesiones de escaneo automatizado / sondeo con inyección / adaptativas	~76 / 22 / 2 %	Muestra validada, n = 100	2026	Cuerpo del artículo

Verizon DBIR 2026: más de 31 000 incidentes y 22 000 brechas confirmadas en 145 países. ENISA ETL 2026: 8 257 incidentes analizados (p. 9). — = sin comparación pertinente.

Las proporciones de HIVE-AI provienen de una muestra de validación de 100 sesiones y no deben leerse como cifras poblacionales.

4. La propuesta 2026: la misma escalera, otra variable

La Pirámide de Actores de Amenaza 2026 conserva los seis niveles y el gradiente de capacidad y persistencia. Cambia tres cosas: los pisos se nombran por *modo de operación* y no por tipo de actor; el ancho se declara ilustrativo; y cada nivel lleva su uso de IA y su defensa prioritaria (Figura 2 y Tabla 4).

Tabla 4. Correspondencia entre la lámina original y la Pirámide de Actores 2026

Nivel	Lámina original (tipo de actor)	Propuesta 2026 (modo de operación)	Criterio de capacidad (DSB 2013)	Defensa prioritaria 2026
VI	Naciones	Estratégico: operaciones sostenidas	Operaciones de espectro completo a escala, simultáneas	Segmentación industrial; recuperación ensayada
V	Atacantes patrocinados por Estados	Avanzado: campañas dirigidas	Crea vulnerabilidades en el ciclo de vida o la cadena de suministro	Control de privilegios; vigilancia de terceros
IV	Crimen organizado, cibermercenarios	Organizado: crimen como servicio	Equipos organizados que descubren vulnerabilidades nuevas	Copias inmutables; parcheo priorizado
III	Grupos criminales, hacktivistas	Coordinado: campañas y herramientas	Descubre y usa código malicioso desconocido	Mitigación DDoS; gestión de crisis
II	Criminales, empleados descontentos	Operativo: acceso y herramientas disponibles	Desarrolla herramientas sobre vulnerabilidades públicas	Mínimo privilegio; verificación por otro canal
I	Script kiddies, actores no maliciosos	Oportunista: barrera de entrada reducida	Usa exploits conocidos desarrollados por otros	Autenticación resistente al phishing

Los criterios de capacidad parafrasean la Tabla 2.1 del Defense Science Board (2013, p. 22). El nivel se asigna por la operación observada, no por el rótulo del actor.

El impacto no se infiere del nivel: se evalúa por separado (Tabla 5, D6).

La decisión de diseño más importante es la separación de ejes. La lámina original ponía complejidad e impacto en el mismo eje vertical. La versión 2026 los separa: el eje vertical es capacidad y persistencia, y el impacto se evalúa aparte, en el perfil de la operación. Por eso el piso I advierte que un ataque simple también puede causar un impacto crítico.

Leída así, la propuesta no rompe con el DSB. Vuelve a su advertencia original (el nivel es capacidad, no identidad) y a la intención de Sandia (describir por atributos, no por rótulos), que la versión popular había perdido.

De la lámina original a la Pirámide de Actores 2026: mismos seis niveles, otra variable de orden

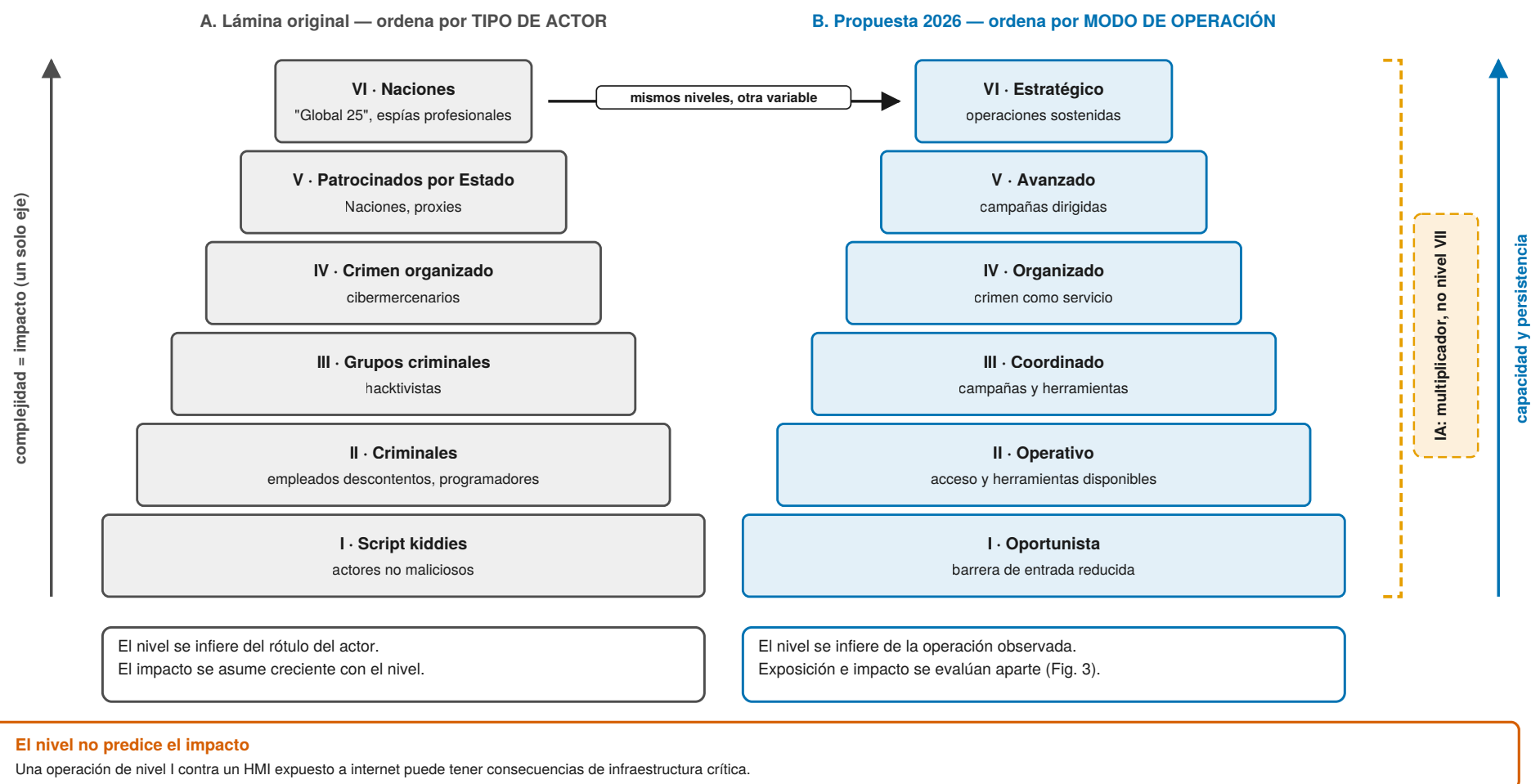


Figura 2. De la lámina original (A) a la Pirámide de Actores 2026 (B). Se conservan los seis niveles, pero cambia la variable que los ordena: tipo de actor frente a modo de operación. La IA se representa como multiplicador transversal (corchete discontinuo), no como séptimo nivel. La exposición y el impacto se evalúan fuera de la pirámide (Figura 3).

5. La IA no es un piso nuevo: es un multiplicador

La tentación obvia era agregar un nivel VII «atacante con IA». Lo descarté porque repite el error que Sandia quiso evitar: convertir una tecnología en una identidad. En términos de la matriz original, la IA es un multiplicador: potencia el personal técnico efectivo, el conocimiento y el tiempo sin cambiar por sí sola el nivel del actor. La propuesta la representa como una franja que atraviesa los seis pisos, con tres roles:

- **IA para atacar:** phishing personalizado, clonación de voz y video, reconocimiento y automatización. Microsoft observa uso de IA en reconocimiento, ingeniería social, desarrollo de malware y exploits, y actividad posterior al compromiso.
- **IA como objetivo:** inyección de instrucciones, fuga de datos y abuso de herramientas y permisos de agentes. Verizon reporta que el 67 % de los usuarios accede a servicios de IA con cuentas no corporativas desde equipos de la empresa.
- **IA para defender:** correlación de alertas y apoyo a la respuesta, con validación humana, registros y permisos limitados.

El efecto neto es una compresión vertical de la pirámide. La IA baja la barrera de entrada de los pisos I a III y acelera los ciclos de los pisos IV a VI. Lo que no entrega automáticamente es lo que sigue separando a un nivel VI: escala, simultaneidad, acceso humano cercano y capacidad de crear vulnerabilidades en el ciclo de vida.

La IA reduce barreras de entrada; no convierte automáticamente a cualquier actor en una amenaza avanzada.

Lo vimos con datos propios. En HIVE-AI, el honeypot multiservicio para APIs de IA generativa que publicamos con Sergio Tobón en el *International Journal of Information Security*, registramos 16.683 ataques desde 1.229 IP de 50 países en 20 días de operación. En una muestra validada de 100 sesiones, cerca del 76 % fue escaneo automatizado, el 22 % sondeo de múltiples fachadas con intentos de inyección y apenas el 2 % actividad adaptativa de tipo dirigido. Traducido a la pirámide: el objetivo cambió a las APIs de IA, pero el grueso del tráfico sigue operando en los pisos I y II.

6. Perfil de la operación: cómo aplicar el modelo

El nivel de la pirámide es una conclusión, no un punto de partida. Se llega a él evaluando seis dimensiones de la operación observada (Figura 3 y Tabla 5). Las cuatro primeras describen al atacante y heredan la lógica del DSB y de Sandia; las dos últimas describen a la organización y son el aporte nuevo, porque el riesgo es relacional.

Tabla 5. Dimensiones del perfil de la operación: definición, evidencia observable y escala propuesta

Dim.	Dimensión	Definición operacional	Evidencia observable	Escala propuesta	Origen
D1	Intención	Finalidad que persigue la operación	Datos objetivo, reivindicación, demanda de rescate	Nominal: lucro, espionaje, ideología, sabotaje	DSB 2013 (intent)
D2	Capacidad	Conocimiento y herramientas puestos en juego, propios o alquilados	Novedad del exploit, ofuscación, uso de servicios criminales	Ordinal 1–6 (criterios de la Tabla 4)	Sandia 2012 (personal, conocimiento)
D3	Acceso	Posición lograda dentro de sistemas restringidos	Cuentas usadas, privilegios, relación de confianza con terceros	Ordinal: ninguno, usuario, privilegiado, tercero de confianza	Sandia 2012 (acceso)
D4	Persistencia	Duración, sigilo y continuidad tras la detección	Tiempo de permanencia, borrado de registros, reingreso	Ordinal: días, semanas, meses, años	Sandia 2012 (intensidad, sigilo, tiempo)
D5	Exposición	Superficie de la víctima alcanzable por la operación	Activos expuestos: nube, datos, OT, sistemas de IA	Ordinal: baja, media, alta	Nueva (cf. targeting, MITRE Cyber Prep)
D6	Impacto	Efecto real o potencial sobre la organización	Interrupción, pérdida financiera, efecto físico	Ordinal: bajo, medio, alto, crítico	Nueva; eje separado del nivel

Las escalas son una propuesta del autor y aún no se han validado empíricamente (véase la Tabla 6).

D1–D4 describen al atacante y determinan el nivel (salvo D1, que orienta la probabilidad); D5–D6 describen a la organización y entran en el riesgo.

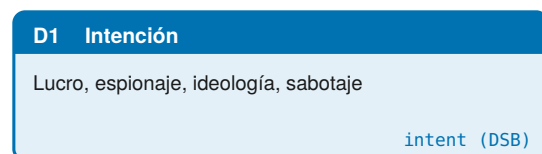
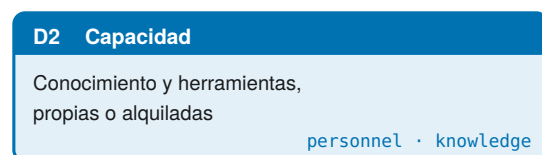
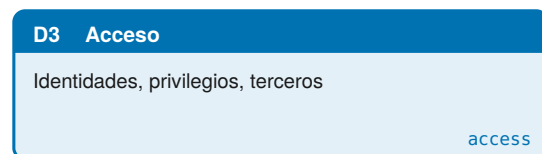
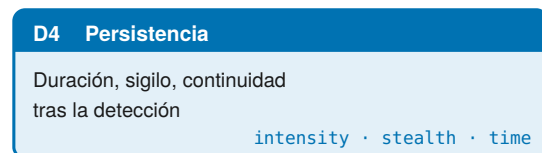
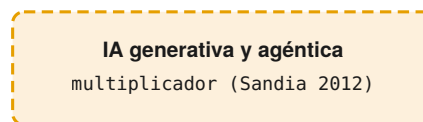
El procedimiento propuesto tiene cinco pasos:

- 1. Describir antes de etiquetar.** Registrar las seis dimensiones con evidencia: TTP mapeadas a MITRE ATT&CK, línea de tiempo y vector de entrada.
- 2. Ubicar el nivel por capacidad y persistencia.** Elegir el piso más parecido, como recomendaba Sandia, y no el que calza con el rótulo del grupo.
- 3. Separar lo propio de lo alquilado.** Si la capacidad viene de un servicio (RaaS, intermediario de acceso, kit con IA), registrarlo: distingue al operador de la cadena que lo sostiene.
- 4. Cruzar con exposición e impacto.** Una operación de nivel I contra un HMI expuesto a internet se gestiona como incidente crítico.
- 5. Elegir defensas por dimensión, no por piso.** Acceso: identidad y terceros. Persistencia: detección y caza de amenazas. Impacto: copias inmutables y recuperación ensayada.

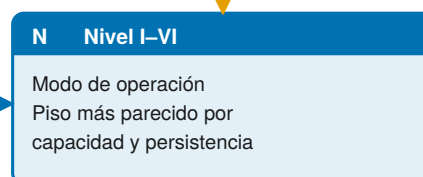
Ejemplo ilustrativo (caso hipotético). Una empresa sanitaria detecta el cifrado de servidores de su red corporativa; la red OT está segmentada. La intención es lucro. La capacidad es alta pero alquilada: un afiliado de una plataforma RaaS. El acceso se obtuvo con credenciales de un proveedor de mantenimiento remota y la persistencia duró once días antes del cifrado. La exposición incluye servidores *historian* conectados a la red IT, y el impacto potencial alcanza la operación de las plantas. Resultado: nivel IV por modo de operación, con exposición e impacto de infraestructura crítica. La lámina antigua lo habría archivado como «crimen organizado» y habría propuesto antivirus y SIEM.

Perfil de la operación: de seis dimensiones observables al nivel, al riesgo y a la defensa

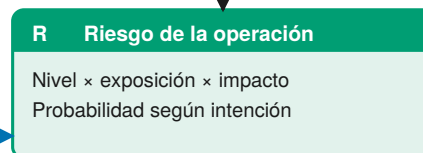
ATACANTE — atributos heredados (DSB 2013, Sandia 2012)



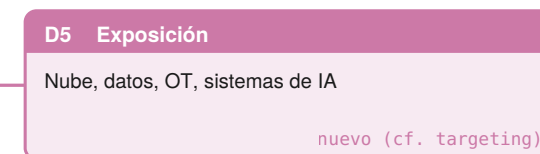
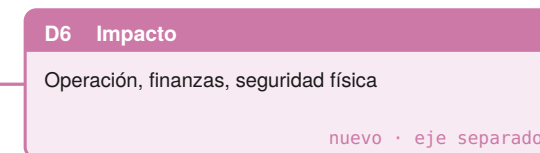
amplifica D2 y D4



probabilidad



ORGANIZACIÓN — atributos nuevos



Defensas por dimensión, no por piso

D3 Acceso → identidad y terceros · D4 Persistencia → detección y caza de amenazas · D6 Impacto → copias inmutables y recuperación ensayada

Línea continua: el atributo determina el nodo de destino. Línea discontinua: modula sin determinar (la intención orienta la probabilidad; la IA amplifica capacidad y persistencia).

Figura 3. Perfil de la operación. D1–D4 describen al atacante y se heredan del DSB (2013) y de Sandia (2012); D5–D6 describen a la organización y son el aporte nuevo. Línea continua: el atributo determina el nodo de destino. Línea discontinua: lo modula sin determinarlo. Los atributos originales de Sandia figuran en fuente monoespaciada.

7. Límites del modelo y agenda de validación

Una propuesta seria tiene que decir dónde falla. La Tabla 6 resume las principales amenazas a la validez. Los seis niveles ordenan, pero no miden: sumar o promediar niveles no tiene sentido. La atribución es incierta, porque los actores de nivel alto se disfrazan de nivel bajo a propósito. Las fuentes describen lo que se reporta y no todo lo que ocurre, y en Latinoamérica hay pocos datos públicos y casi ninguno sobre OT. Y el modelo es una síntesis didáctica: no es una clasificación oficial ni una escala estadística.

Tabla 6. Amenazas a la validez del modelo propuesto y mitigaciones

Tipo	Amenaza específica	Mitigación propuesta
Constructo	Las seis dimensiones pueden no ser independientes (capacidad y persistencia covarían)	Análisis de correlación sobre casos codificados; fusionar dimensiones si $r > 0,7$
Constructo	La escala ordinal se trata como si midiera distancias iguales entre niveles	Prohibir sumas o promedios de niveles; reportar solo medianas y modas
Interna	Atribución incompleta: los actores de nivel alto imitan técnicas de nivel bajo	Registrar el nivel con su grado de confianza; reclasificar al obtener nueva evidencia
Externa	Fuentes sesgadas hacia lo que se reporta; escasez de datos de Latinoamérica y de OT	Complementar con telemetría propia (honeypots) y datos de CSIRT regionales
Conclusión	Baja concordancia entre analistas al asignar el nivel	Prueba de concordancia (kappa de Fleiss) y panel Delphi antes de uso operativo

Clasificación de amenazas a la validez según la convención constructo, interna, externa y de conclusión.

La agenda para validarlo es concreta. Primero, un panel Delphi de analistas de CTI de la región. Segundo, una prueba de concordancia entre evaluadores (kappa de Fleiss) que clasifique los mismos casos con la lámina antigua y con la nueva. Tercero, un mapeo de los grupos documentados en MITRE ATT&CK contra los seis niveles. Si dos analistas no llegan al mismo piso con la misma evidencia, el modelo tiene que corregirse.

8. Conclusión

Mi postura es simple: dejemos de usar la pirámide para ponerle nombre al enemigo y usémosla para medir la operación que tenemos al frente. El nivel describe lo que el atacante puede hacer y por cuánto tiempo; la exposición y el impacto los pone la organización.

La IA hace este cambio urgente. Cuando un afiliado de nivel I opera con herramientas que hace tres años eran de nivel IV, defender «por piso» deja huecos justo donde más duele. Si enseñas esta lámina, o la tienes en el informe de riesgo de tu directorio, revisa qué variable está ordenando. Si es el tipo de actor, estás usando la versión de 2013.

Referencias

- Bodeau, D., Fabius-Greene, J., & Graubart, R. (2010). *How do you assess your organization's cyber threat level?* The MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/10_2914.pdf
- Bodeau, D., & Graubart, R. (2017). *Cyber Prep 2.0: Motivating organizational cyber strategies in terms of preparedness* (MTR150264). The MITRE Corporation. <https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf>
- Defense Science Board. (2013). *Task force report: Resilient military systems and the advanced cyber threat*. U.S. Department of Defense. <https://apps.dtic.mil/sti/pdfs/ADA569975.pdf>

- Duggan, D. P., Thomas, S. R., Veitch, C. K. K., & Woodard, L. (2007). *Categorizing threat: Building and using a generic threat matrix* (SAND2007-5791). Sandia National Laboratories. https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/14-Categorizing_Threat.pdf
- European Union Agency for Cybersecurity. (2026). *ENISA Threat Landscape 2026*. <https://doi.org/10.2824/0806036>
- Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Kvarvåg, E., & Kall, P. (2020). *Security architecture design phase: The concept of a threat intelligence driven defendable architecture*. Telenor Group. <https://www.telenor.com/security-architecture-design-phase-the-concept-of-a-threat-intelligence-driven-defendable-architecture/>
- Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). *Cyber threat metrics* (SAND2012-2427). Sandia National Laboratories. <https://www.osti.gov/biblio/1039394>
- Microsoft. (2026). *Microsoft Digital Defense Report 2026: Executive summary*. <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2026-Microsoft-DDR-Exec-Summary.pdf>
- Reith, G. R., & Peppe, B. C. (2019). *Recombinant threat modeling* (U.S. Patent No. 10,216,938 B2; publicación de solicitud US 2016/0162690 A1). T-Mobile USA. <https://patents.google.com/patent/US10216938>
- The Aerospace Corporation. (s. f.). *Threat levels to space systems*. SPARTA. <https://sparta.aerospace.org/related-work/threat-levels>
- Vargas Yáñez, S., & Tobón, S. (2026). Hive-AI: A defended multi-service honeypot framework for generative AI APIs. *International Journal of Information Security*, 25, 158. <https://doi.org/10.1007/s10207-026-01307-0>
- Verizon. (2026). *2026 Data breach investigations report*. <https://www.verizon.com/business/resources/T343/reports/2026-dbir-data-breach-investigations-report.pdf>

Nota sobre figuras y uso de IA. Las Figuras 1–3 son esquemas conceptuales sin datos medidos, dibujados como código SVG (paleta Okabe–Ito, legibles en escala de grises). La redacción y las figuras contaron con asistencia de un modelo de lenguaje (Claude, Anthropic). No se usó generación de imágenes con IA. Todas las cifras se verificaron en las fuentes citadas al 29 de octubre de 2026.