2025

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Pensamiento Adversarial

ESTRATEGIAS PARA LA RESILIENCIA DIGITAL

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número treinta y cinco [35]
Agosto de 2025

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder Programa de Maestría en Ciberseguridad

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Desarrollo Tecnológico CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Adm. Libardo Cárdenas Corral
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Introducción

En un mundo cada vez más interconectado y dependiente de sistemas digitales, la ciberseguridad ya no se limita a responder ante incidentes: exige anticipar las acciones de adversarios capaces de explotar vulnerabilidades, manipular contextos o corromper datos. Es aquí donde el pensamiento adversarial emerge como una competencia esencial: la capacidad de adoptar la perspectiva de un atacante y razonar estratégicamente sobre el escenario de amenazas, para reforzar la resiliencia digital y ejercer competencias de poder en el ciberespacio.

El marco curricular *Cybersecurity Curricula 2017*(ACM, 2017) ya destacaba el pensamiento adversarial como unidad de conocimiento clave, señalando que no basta con proteger; es necesario pensar como el atacante para detectar puntos débiles y construir defensas más robustas. Estudios recientes han profundizado esta idea, vinculándola con dinámicas de poder, inteligencia ofensiva y estrategias de mitigación que trascienden lo técnico.

El informe *Adversarial Machine Learning and Cybersecurity* (Musser et al., 2023) examina cómo las vulnerabilidades en los sistemas de IA pueden ser explotadas por actores adversos, y plantea políticas y marcos regulatorios para contrarrestar esos riesgos, promoviendo una cultura de anticipación y control estratégico. (Center for Security and Emerging Technology et al., 2021)

Otro estudio, *Evolving techniques in cyber threat hunting: A systematic review* (Mahboubi et al., 2024), revisa cómo los equipos de caza de amenazas "threat hunting" emplean pensamiento adversarial para no solo responder a ataques visibles, sino buscar señales débiles, patrones latentes y proactividad en la defensa.(Mahboubi et al., 2024)

También, *Enhancing Cybersecurity Mindset through Rock-Paper-Scissors-Inspired Learning* aborda métodos pedagógicos innovadores para cultivar el pensamiento estratégico adversarial en estudiantes, usando simulaciones lúdicas que exigen anticipar decisiones y evaluar trade-offs[1], fortaleciendo competencias cognitivas y de poder en escenarios emergentes(Servin, 2025)

De este modo, el pensamiento adversarial y las competencias de poder no solo suponen conocimiento técnico, sino una conjunción de habilidades críticas, imaginativas y estratégicas: anticipación, riesgo calculado, creatividad ofensiva defensiva, conciencia ética y capacidad de traducir inteligencia en ventaja operativa. Este boletín explorará entonces cuatro ejes temáticos fundamentales: la conceptualización del pensamiento adversarial; las competencias de poder como capacidades estratégicas; las aplicaciones en inteligencia ofensiva, IA y sistemas complejos; y los retos éticos y pedagógicos para formar estos modos de pensar.

[1] Intercambio en el que se gana algo al sacrificar otra cosa

Pensamiento Adversarial

ESTRATEGIAS PARA LA RESILIENCIA DIGITAL

Autores

Luis Fernando Zambrano Hernandez
Docente Investigador
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

Hernando José Peña Hidalgo
Docente Investigador
CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-3477-2645

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-0392-1983

Néstor Raúl Cárdenas Corral
Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: orcid.org/0000-0003-3691-0148

Daniel Felipe Palomo Luna
Docente Esp. Seguridad Informática
Universidad Nacional Abierta y a Distancia
ORCID: https://orcid.org/0009-0004-9507-4295

Conceptualización del pensamiento adversarial en ciberseguridad

El pensamiento adversarial en ciberseguridad implica la capacidad de pensar desde la perspectiva del atacante: anticipar sus tácticas, técnicas y motivaciones, para diseñar defensas que no solo respondan, sino que prevengan. Esta forma de pensar combina análisis estratégico, creatividad, conocimiento técnico profundo, y conciencia ética.

Algunos artículos recientes aportan marcos conceptuales útiles:

Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems: examina cómo definir modelos de ataque adversarial realistas contra sistemas de detección de intrusos basados en aprendizaje automático, y plantea escenarios donde los atacantes tienen conocimiento parcial del sistema. (Apruzzese et al., 2022). Lo anterior, muestra que no todos los ataques asumen omnisciencia; la anticipación y la modelación de amenazas con limitaciones reales es clave.

A Framework for Cyber Threat Modeling and Risk Assessment in Smart Cities environments: Presenta un método que combina STRIDE, diagramas de flujos de datos y mapeo con MITRE ATT&CK para

identificar amenazas adversariales en infraestructuras urbanas críticas. (Ouaissa et al., 2025), esto hace notar que pensar adversarialmente requiere imaginar el entorno completo, los activos, flujos de información y amenazas potenciales, y cómo las adversidades se expresan en escenarios reales.

Threat Modeling of Cyber-Physical Systems – A Case Study Using STRIDE: Propone aplicar el modelo STRIDE para sistemas ciberfísicos, lo cual obliga a adoptar la perspectiva del atacante para anticipar amenazas como spoofing, tampering, etc. (Khalil et al., 2023). Esto implica mapear amenazas específicas en componentes del sistema, prever sus estrategias, y estimar impacto para diseñar respuestas.

Multi-aspects AI-based modeling and adversarial learning for Cybersecurity Intelligence and Robustness ofrece un panorama amplio de cómo los modelos de IA pueden ser susceptibles a ataques adversariales, y cómo construir resiliencia mediante técnicas de robustez, aprendizaje adversarial, defensa de modelos, etc. (Sarker, 2023). En este sentido, el pensamiento adversarial no es solo táctica tradicional, sino también entender cómo la IA puede ser explotada, y anticipar ataques sofisticados.

The Human Factor in AI Red Teaming: Perspectives from Social and Collaborative Computing: Explora cómo en ejercicios de red team hay factores humanos: sesgos, limitaciones cognitivas, preparación, elección de escenarios, etc. Estop nos invita a pensar de forma adversarial, también significa considerar qué tan probable es que el atacante tenga ciertos errores, qué tan preparado esté, qué información tenga; no es solo técnica, es también humana.

Competencias de Poder en Ciberseguridad

En el ámbito de la ciberseguridad, las competencias de poder se refieren a la capacidad de individuos, equipos u organizaciones para anticipar, influir y controlar dinámicas adversariales en el ciberespacio. Este concepto incorpora tanto habilidades técnicas como estratégicas, cognitivas y éticas, que permiten transformar la inteligencia y el pensamiento adversarial en ventaja operativa y resiliente.

Un referente reciente, *Evolving techniques in cyber threat hunting: A systematic review* (Mahboubi et al., 2024), analiza cómo los equipos

de *threat hunting* ya no solo reaccionan ante incidentes, sino que se adelantan mediante métodos avanzados: reconocimiento de tácticas, técnicas y procedimientos (TTPs), integración de detección proactiva y entrenamiento adversarial de sistemas. Lo anterior permite evidenciar que el adversario presenta una postura ofensiva-defensiva. (Mahboubi et al., 2024). Por otro lado, el articulo ***A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats*** evidencia que la colaboración entre organizaciones, el uso riguroso de estándares de inteligencia de amenazas (CTI), y la implementación de tecnologías adaptativas elevan la posición táctica y estratégica de las entidades expuestas a amenazas digitales, permitiéndoles proyectar poder (capacidad de influencia) más allá de su perímetro técnico. (Santos et al., 2025). Así mismo el artículo ***Assessing Power and Hierarchy in Cyberspace: An Approach of Power Transition Theory* (Lorci)** ofrece una mirada macro: traza métricas de poder digital entre estados, considerando factores como la economía digital, capacidades políticas cibernéticas y recursos de información. Este enfoque permite entender que competencias de poder no solo se aplican a nivel organizacional, sino también en la arena internacional, donde actores estatales compiten por influencia. (Lorci, 2024)

Desde la dimensión humana, ***Fuzzy to Clear: Elucidating the Threat Hunter Cognitive Process and Cognitive Support Needs*** resalta cómo los threat hunters desarrollan modelos mentales que les permiten anticipar comportamientos del adversario, refinar hipótesis en sesiones reales de caza de amenazas, y los apoyos cognitivos que necesitan (herramientas visuales, aprendizaje colaborativo, retroalimentación constante) para ejercer poder predictivo y estratégico. (Milani et al., 2024). Finalmente, ***DeepHunter: A Graph Neural Network Based Approach for Robust Cyber Threat Hunting*** ilustra una instancia técnico-operativa de pensamiento adversarial aplicado: el desarrollo de un sistema robusto de búsqueda de amenazas persistentes usando redes neuronales de grafos para modelar relaciones entre indicadores, lo que fortalece la capacidad de respuesta anticipada frente a adversarios sofisticados. (Wei et al., 2021)

Aplicación de Pensamiento Adversarial con una Metodología de Pruebas de Penetración - PTES

El pensamiento adversarial se hace operativo cuando se articula en distintos escenarios dentro de una metodología de pruebas de penetración ética. A continuación se propone un flujo integral que combina PTES (Penetration Testing Execution Standard), NIST SP 800-115 y MITRE ATT&CK para emular adversarios de forma controlada y transformar los hallazgos en decisiones técnicas y estratégicas —sin proporcionar instrucciones de explotación ni pasos peligroso.

1. Pre-Engagement: Definición del Adversario y sus Objetivos. En lugar de solo definir el alcance técnico, esta fase se centra en caracterizar al adversario. Se pregunta: ¿A quién estamos emulando? ¿Es un ciberdelincuente con motivación financiera, un actor patrocinado por un estado, o un insider malicioso? Se define no solo lo que se puede probar, sino también el por qué y con qué intención se hará.
Ejemplo, el objetivo no es solo "obtener acceso", sino "exfiltrar información confidencial de clientes" o "interrumpir la cadena de suministro". Este enfoque le da un propósito estratégico a la prueba desde el inicio.

2. Inteligencia y Reconocimiento: Mapeo de la Huella Digital del Adversario. Esta etapa va más allá de un simple escaneo de puertos. Se trata de pensar como el adversario y buscar la información que él buscaría. Se analizan las redes sociales, los foros de la dark web y las bases de datos de vulnerabilidades no solo para encontrar información técnica, sino para identificar a los empleados clave, sus hábitos y las tecnologías utilizadas. Se construye un perfil de la huella digital de la organización desde la perspectiva del atacante, priorizando los puntos de entrada que son más probables de ser explotados por el adversario definido en la fase 1.
3. Modelado de Amenazas y Planificación de la Emulación: Creación del Plan de Ataque. Aquí, el **pensamiento adversarial se vuelve el motor de la operación**. Se usan los hallazgos de reconocimiento para diseñar una campaña de ataque basada en MITRE ATT&CK. No se trata de ejecutar todas las TTPs, sino de seleccionar aquellas que un atacante real usaría en el contexto de la organización.
Ejemplo, si se descubrió que la empresa utiliza una versión antigua de un software, el plan de emulación podría centrarse en las TTPs de "Explotación de Software Público" (T1190). Este enfoque asegura que la prueba sea relevante, no solo una lista de vulnerabilidades genéricas, sino una simulación de un ataque dirigido.

4. Explotación y Post-Explotación: Ejecución de la Cadena de Muerte Adversarial. En esta fase, cada acción tiene un propósito alineado con los objetivos del adversario. La explotación no es un fin en sí misma, sino un medio para lograr la post-explotación. Se simulan los pasos de un atacante: una vez que se obtiene acceso inicial, se usan TTPs de movimiento lateral, escalada de privilegios y persistencia, siguiendo

la lógica de un adversario que busca profundizar su acceso y mantener el control del entorno. Se documentan las defensas que el equipo de seguridad de la organización logró detectar, las que no detectó y las contramedidas que se lograron evadir. Esto permite no solo identificar fallos, sino también evaluar la capacidad de detección y respuesta de la organización.

5. Análisis y Toma de Decisiones: De Hallazgo Técnico a Implicación Estratégica. Esta fase es la culminación del pensamiento adversarial. Los hallazgos técnicos se traducen en riesgos de negocio. En lugar de solo decir "se encontró una vulnerabilidad de Cross-Site Scripting", el informe dirá "esta vulnerabilidad podría ser usada por un adversario para comprometer la sesión de un administrador y robar credenciales, lo que les permitiría acceder a datos sensibles de clientes y causar una violación de datos". Se conecta cada TTP utilizada con el impacto potencial en la confidencialidad, integridad y disponibilidad. Esto ayuda a los líderes de la empresa a tomar decisiones estratégicas basadas en el riesgo real y no solo en una lista de vulnerabilidades.

6. Reporte y Limpieza: Comunicación del Riesgo Adversarial y Recomendaciones. El informe final se presenta desde la perspectiva del adversario. Se describe la historia del ataque: cómo se inició, qué rutas se tomaron y qué objetivos se lograron. Las recomendaciones no solo se enfocan en parches, sino en mejoras holísticas para la postura de seguridad de la organización.

Tabla 1.

Sinergia entre Pensamiento adversarial - PTES & NIST

Fase PTES	NIST SP 800-115	Pensamiento Adversarial	Cómo se integra
1. Pre-Engagement	Planificación y Acuerdos. Se definen los alcances y reglas de la prueba.	Definición del Adversario. Se enfoca en el "quién" y el "por qué" del ataque.	Se define el tipo de atacante (ej. criminal, estado, insider) y sus objetivos, como robar datos o interrumpir servicios, en lugar de solo listar los activos a probar.
2. Inteligencia y Reconocimiento	Recopilación de información sobre el objetivo, escaneos de red y mapeo de la infraestructura.	Mapeo de la Huella Digital. Se busca información de la misma manera que lo haría un atacante.	Se utiliza información de fuentes públicas (OSINT) y escaneos de red para identificar a las personas y tecnologías que un adversario podría explotar.
3. Modelado de Amenazas	Análisis de vulnerabilidades para identificar riesgos.	Creación del Plan de Ataque. Se seleccionan las tácticas y técnicas (TTPs) de MITRE ATT&CK más probables de ser usadas por el adversario definido.	Se diseñan las siguientes fases de la prueba para simular una campaña de ataque dirigida, enfocada en los TTPs específicos que un atacante real podría usar.
4. Explotación y Post-Explotación	Verificación de la explotación de vulnerabilidades y acceso a los sistemas.	Ejecución de la Cadena de Muerte. Cada acción tiene un propósito para lograr el objetivo final.	Se utilizan técnicas de movimiento lateral, escalada de privilegios y persistencia para emular un ataque sostenido, no solo un simple acceso inicial. Se evalúa la capacidad de detección de la organización.
5. Análisis y Toma de Decisiones	Análisis y clasificación de hallazgos según su impacto.	Traducción del Riesgo. Se convierte un hallazgo técnico en un riesgo para el negocio.	Se relaciona cada vulnerabilidad y TTP con el impacto potencial en la confidencialidad, integridad y disponibilidad, facilitando la toma de decisiones estratégicas.
6. Reporte y Limpieza	Documentación final de los hallazgos y las acciones realizadas.	Narrativa del Ataque. Se comunica cómo el adversario habría logrado sus objetivos.	El informe final presenta una historia del ataque, explicando el camino que siguió el adversario y sus objetivos, además de las recomendaciones técnicas y estratégicas para mejorar la postura de seguridad.

La siguiente tabla presenta un esquema técnico entre PTES ⇄ Pensamiento adversarial ⇄ Acciones prácticas, herramientas y entregables

PTES — FASE	ACCIÓN DESDE PENSAMIENTO ADVERSARIAL (QUÉ PENSAR / QUÉ PRIORIZAR)	EJEMPLO PRÁCTICO / TÉCNICAS (QUÉ HACER)	HERRAMIENTAS SUGERIDAS (USO RESPONSABLE)	PRODUCTO ENTREGABLE	CRITERIOS DE EVALUACIÓN
1. PRE-ENGAGEMENT (ACUERDO Y ALCANCE)	Definir el perfil del adversario (motivación, recursos, nivel de acceso) y escenarios objetivos; establecer reglas y límites (legalidad, alcance).	Crear 2 perfiles adversarios: *script kiddie*, *APT con recursos moderados*. Priorizar objetivos: exfiltración, sabotaje, espionaje.	Documentación/plantillas (plantilla de perfil adversario, reglas de engagement).	Documento de Alcance y Perfil de Adversario + Carta de autorización.	Coherencia del perfil con objetivos; claridad legal; aceptación por cliente/instructor.
2. INTELLIGENCE GATHERING (RECONOCIMIENTO)	Pensar como adversario: ¿qué fuentes usaría? ¿qué información pública y contextual explotable existe? Buscar vectores no técnicos (personal, proveedores).	Fingerprinting, subdominios, empleados, correos, exposiciones de servicios, Opensource + búsquedas en dark web para credenciales. Crear lista priorizada de objetivos y TTPs probables.	Recon: Shodan, Censys, DNSenum, Amass, Sublist3r, Maltego, Recon-ng, Google dorking, OSINT tools.	Registro de hallazgos (IOCs iniciales), mapa de activos, lista priorizada de vectores.	Cobertura de fuentes, novedad/accionable de IOCs, priorización justificable.
3. THREAT MODELING (MODELADO DE AMENAZA & PLANIFICACIÓN)	Convertir inteligencia en árboles de ataque / escenarios: ¿cómo encadenaría vulnerabilidades el adversario? Priorizar rutas con mayor probabilidad/impacto.	Construir attack trees, mapear TTPs a MITRE ATT&CK, estimar requerimientos para cada camino (skill, tiempo, herramientas). Definir hipótesis de explotación.	Modelado: draw.io, Mitre ATT&CK Navigator, ThreatModeler, Microsoft Threat Modeling Tool.	Attack trees, matriz de TTPs ↔ activos, plan de prueba con hipótesis.	Razonamiento lógico, correspondencia TTP-activo, plausibilidad del adversario.
4. VULNERABILITY ANALYSIS (ANÁLISIS DE VULNERABILIDADES)	Buscar debilidades explotables conforme al perfil adversario: preferir vectores realistas (configuraciones, credenciales, phishing).	Escaneo activo selectivo, fuzzing limitado, revisión de configuración, credential stuffing, análisis de APIs. Probar autenticación multifactor bypass técnicas si el perfil lo justifica (simulado).	Nmap, Nessus/OpenVAS (con permiso), Burp Suite, Nikto, dirb, wfuzz, sqlmap (con límites).	Inventario de vulnerabilidades priorizadas con contexto adversarial.	Relevancia práctica (exploitability), prioridad alineada a objetivo adversario.
5. EXPLOITATION (EXPLOTACIÓN CONTROLADA)	Ejecutar cadenas de explotación que un atacante real emplearía, priorizando persistencia y evasión y midiendo impacto real.	Explotar credenciales válidas, chaining (vuln web → pivot → RCE → escalate), mimikatz (simulado), lateral movement, pruebas de phishing (captura de credenciales en ambiente controlado).	Metasploit, Cobalt Strike (solo en entornos controlados / educativos y con permiso), Empire (en lab), psexec (laboratorio), BloodHound para AD.	Pruebas de concepto (PoC), logs de explotación, rutas de pivot documentadas, capturas de pantalla/recordings.	Realismo (¿sería práctica la cadena?), control ético, evidencia reproducible, impacto medible.
6. POST-EXPLOITATION (PERSISTENCIA, EXFILTRACIÓN, LIMPIEZA)	Simular objetivos finales del adversario: mover/escoger datos de interés, establecer persistencia y encubrir actividad. Medir cómo detectarían/mitigarían.	Exfiltración simulada (pequeña muestra), establecimiento de backdoor temporal, creación de artefactos de persistencia, limpieza parcial para probar detección.	Herramientas de post-explotación: Meterpreter, Mimikatz (lab), Rclone (simular exfiltración), scripts de persistencia (simulados).	Informe de actividades post-explotación: vectores usados, datos accedidos (anonymized), recomendaciones técnicas.	Niveles de acceso alcanzados, impacto simulado, detección por controles existentes (si se instrumentó).
7. REPORTING (INFORME & RECOMENDACIONES)	Traducir hallazgos en **productos estratégicos**: informes técnicos para operativos y resúmenes ejecutivos para dirección; priorizar mitigaciones que desarmen la cadena adversarial.	Mapear cada hallazgo a recomendaciones prácticas (parche, segmentación, detección, política, formación). Incluir MITRE ATT&CK mapping y playbooks.	Plantillas de informe (executive + technical), MITRE ATT&CK mapping tools, matrixes de priorización (CVSS + impacto).	Informe ejecutivo + informe técnico + PoC anexos + playbook de detección/respuesta.	Claridad, accionabilidad, priorización costo-beneficio, trazabilidad de PoC.

Conclusiones

El análisis desarrollado en este boletín permite afirmar que el pensamiento adversarial constituye un pilar esencial para fortalecer la resiliencia digital de las organizaciones. Adoptar la perspectiva del atacante no solo facilita la identificación de vulnerabilidades técnicas, sino que también impulsa una cultura de anticipación estratégica frente a las dinámicas cambiantes del ciberespacio.

En primer lugar, la conceptualización del pensamiento adversarial evidencia que este enfoque integra componentes técnicos, cognitivos y éticos. No se trata únicamente de ejecutar pruebas o simular ataques, sino de comprender motivaciones, limitaciones humanas y contextos organizacionales para modelar escenarios realistas de amenaza. Esta visión integral enriquece los marcos de seguridad tradicionales y fomenta defensas más adaptativas.

En segundo lugar, el abordaje de las competencias de poder en ciberseguridad mostró que la capacidad de influir y controlar dinámicas adversariales trasciende lo técnico. Implica proyectar ventaja operativa a partir del análisis colaborativo, la inteligencia de amenazas y la capacidad de coordinar acciones en múltiples niveles (individual, organizacional y estatal). Así, el poder en el ciberespacio se construye sobre la conjunción de capacidades técnicas, estratégicas y de gestión del conocimiento.

Finalmente, la aplicación práctica a través de la metodología PTES, enriquecida con referentes como NIST SP 800-115 y MITRE ATT&CK, permitió demostrar que el pensamiento adversarial puede integrarse de manera sistemática en los procesos de pruebas de penetración. La traducción de hallazgos técnicos en riesgos estratégicos ofrece un insumo valioso para la toma de decisiones de alto nivel, vinculando la seguridad digital con la continuidad del negocio y la protección de activos críticos.

En conjunto, los hallazgos permiten concluir que el pensamiento adversarial no es únicamente una técnica, sino una competencia transversal y evolutiva que debe cultivarse en la academia, en la gestión organizacional y en la política pública. Su incorporación en la formación de profesionales de la ciberseguridad, así como en los procesos institucionales de defensa digital, contribuye a consolidar una postura proactiva frente a amenazas emergentes y a construir ecosistemas más resilientes y sostenibles.

Referentes

ACM. (2017). *CYBERSECURITY CURRICULA 2017*. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems. *Digital Threats: Research and Practice*, *3*(3), 1-19. https://doi.org/10.1145/3469659

Center for Security and Emerging Technology, Fedasiuk, R., Weinstein, E., & Puglisi, A. (2021). *China's Foreign Technology Wish List*. Center for Security and Emerging Technology. https://doi.org/10.51593/20210009

Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber-Physical Systems—A Case Study of a Microgrid System. *Computers & Security*, *124*, 102950. https://doi.org/10.1016/j.cose.2022.102950

Lorci, E. (2024). Assessing Power and Hierarchy in Cyberspace: An Approach of Power Transition Theory. *Applied Cybersecurity & Internet Governance*. https://doi.org/10.60097/ACIG/190481

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, *232*, 104004. https://doi.org/10.1016/j.jnca.2024.104004

Milani, A. M. P., Starr, A., Hill, S., Curtis, C., Anderson, N., Moreno-Lumbreras, D., & Storey, M.-A. (2024). *Fuzzy to Clear: Elucidating the Threat Hunter*

Cognitive Process and Cognitive Support Needs (Versión 3). arXiv. https://doi.org/10.48550/ARXIV.2408.04348

Ouaissa, M., Ouaissa, M., Nadifi, Z., El Himer, S., Al Masmoudi, Y., & Kartit, A. (2025). A framework for cyber threat modeling and risk assessment in smart city environments. *Frontiers in Computer Science*, *7*, 1647179. https://doi.org/10.3389/fcomp.2025.1647179

Santos, P., Abreu, R., Reis, M. J. C. S., Serôdio, C., & Branco, F. (2025). A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. *Sensors*, *25*(14), 4272. https://doi.org/10.3390/s25144272

Sarker, I. H. (2023). Multi-aspects AI -based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *SECURITY AND PRIVACY*, *6*(5), e295. https://doi.org/10.1002/spy2.295

Servin, C. (2025). Enhancing Cybersecurity Mindset through Rock-Paper-Scissors: A Hands-On Approach to Adversarial Thinking. *Proceedings of the 30th ACM Conference on Innovation and Technology in Computer Science Education V. 2*, 763-763. https://doi.org/10.1145/3724389.3730792

Wei, R., Cai, L., Yu, A., & Meng, D. (2021). *DeepHunter: A Graph Neural Network Based Approach for Robust Cyber Threat Hunting* (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2104.09806

Contáctenos

📧 **Correo electrónico:** csirt@unad.edu.co
🌐 **Página web:** https://csirt.unad.edu.co

🛡️ El CSIRT Académico UNAD está siempre disponible para apoyarte ante consultas o inquietudes relacionadas con la protección de la información en la universidad. No dudes en ponerte en contacto con nuestro equipo para recibir asesoría, reportar incidentes o recibir orientación en temas de seguridad digital. ¡Tu seguridad es nuestra prioridad!