2025

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Ecosistemas Formativos Basados en TTX

UN MARCO ACADÉMICO-ESTRATÉGICO PARA DESARROLLAR INTELIGENCIA ADVERSARIAL Y LIDERAZGO

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 seis [36]
Septiembre 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

Licencia Atribución – Compartir igual

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

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

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
DOI: https://doi.org/10.22490/UNAD-csirt-b36

Introducción

La creciente sofisticación de las amenazas digitales y la expansión de superficies de ataque en sectores públicos, privados y educativos exigen

estrategias de formación que trasciendan el aprendizaje técnico tradicional y fomenten capacidades integrales para anticipar, responder y adaptarse ante escenarios de crisis cibernética. En este contexto, los Tabletop Exercises (TTX) emergen como una metodología transformadora capaz de articular investigación, innovación pedagógica y fortalecimiento institucional, actuando como puentes entre los marcos teóricos de la ciberseguridad, la toma de decisiones estratégicas y el desarrollo de pensamiento adversarial.

Los TTX han sido reconocidos como mecanismos efectivos para el entrenamiento en respuesta a incidentes y la adquisición de competencias de coordinación, comunicación y análisis crítico bajo presión, integrando dimensiones técnicas, organizativas y cognitivas (Angafor et al., 2020). Asimismo, su evolución hacia plataformas educativas digitales y ecosistemas híbridos ha demostrado impacto positivo en el aprendizaje activo y la evaluación de desempeño en contextos universitarios y profesionales .(Švábenský et al., 2024)

En coherencia, los desarrollos recientes impulsados por la comunidad académica y organismos especializados muestran que los TTX constituyen no solo ejercicios de simulación, sino instrumentos de investigación-acción que permiten medir comportamientos, identificar brechas y fortalecer capacidades institucionales de forma iterativa y fundamentada (Vykopal et al., 2024).

Así, esta propuesta posiciona los TTX como eje articulador para consolidar ecosistemas formativos resilientes, alineados con marcos de gobernanza en ciberseguridad y modelos educativos que privilegian la autonomía, la experiencia, la reflexión y la construcción colectiva de conocimiento. El objetivo es avanzar hacia una cultura académica y organizacional donde el pensamiento adversarial ético, el liderazgo decisional y la resiliencia digital se desarrollen con base en evidencia, práctica deliberada y mejora continua.

Ecosistemas Formativos Basados en TTX

Un marco académico-estratégico para desarrollar inteligencia adversarial y liderazgo

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: 0000-0003-3691-0148

Marco conceptual y Valor Organizacional del Ejercicio de Mesa (TTX)

En el ámbito de la Ciberseguridad, la preparación proactiva frente a incidentes no solo requiere controles técnicos robustos, sino también una cultura organizacional que desarrolle capacidades de respuesta, coordinación y aprendizaje continuo. En este sentido, los ejercicios de mesa conocidos como "Tabletop Exercise (TTX)" emergen como una metodología clave para articular esta preparación entre distintos niveles de la organización.

¿Qué es un ejercicio de mesa?

Según la Cybersecurity and Infrastructure Security Agency (CISA), un TTX es "una actividad de juego de roles en la que los jugadores responden a escenarios presentados por uno o más facilitadores CISA, (*Cybersecurity Tabletop Exercise Tips*, 2020). Los participantes suelen desempeñar sus roles reales (por ejemplo, jefe de TI, líder de comunicaciones, ejecutivo) o roles asignados para cubrir vacíos.

La redacción del paquete TTX de CISA indica que los recursos proporcionan "objetivos prediseñados, escenarios, preguntas de módulo, plantillas y referencias" para facilitar la construcción del ejercicio. Es decir: no se trata solamente de una "charla" sino de un ejercicio estructurado que simula una crisis, pone a prueba los roles, la comunicación, el plan de respuesta, y genera espacios de discusión y reflexión.

Valor organizacional de los TTX

La revisión de la literatura en el artículo de Angafor, Yevseyeva y He *"Game-based learning: A review of tabletop exercises for cybersecurity incident response training"*(Angafor et al., 2020) documenta que los TTX contribuyen a mejorar la conciencia, entendimiento y preparación de los equipos de respuesta a incidentes.

Entre los hallazgos específicos se señala que estos ejercicios permiten:

- Desarrollar tanto habilidades técnicas como *soft skills* (comunicación, trabajo en equipo, pensamiento crítico) que suelen faltar en formaciones puramente técnicas.
- Fomentar la toma de decisiones estratégicas bajo presión, es decir, pensamiento adversarial y respuesta informada.
- Identificar brechas en planes, procesos y roles antes de que ocurra un incidente real, reduciendo así el riesgo de "enseñanzas dolorosas" en plena crisis.

CISA enfatiza este valor al indicar que el objetivo del TTX no es que los jugadores actúen "perfectamente", sino que "trabajen como equipo y resuelvan cualquier área de problema en tiempos de paz; no habrá oportunidad de alinear al equipo en tiempos de guerra".

Concretamente, las organizaciones que emplean paquetes como los de CISA tienen acceso a más de 100 escenarios que abarcan desde ransomware, amenazas internas ("insider threats"), ataques a sistemas de control industrial, hasta disturbios civiles u otros tipos de crisis. (*CISA Tabletop Exercise Packages*, 2022) Este abanico amplio de escenarios demuestra el valor transversal del TTX como mecanismo de aprendizaje y de validación organizacional, no es solo para TI, sino para comunicaciones, departamentos legales, alta dirección, infraestructura crítica, operaciones y otras funciones clave.

Competencias de Poder e Inteligencia Adversarial en Ecosistemas Formativos Basados en TTX

El desarrollo de capacidades avanzadas en ciberseguridad exige transcender la formación técnica tradicional para integrar dimensiones de poder organizacional, pensamiento adversarial ético e inteligencia estratégica para la toma de decisiones en crisis. Los Tabletop Exercises (TTX) constituyen un mecanismo privilegiado para activar estas competencias, al simular escenarios de ataque donde convergen intereses, restricciones de recursos, ambigüedad informativa y presiones temporales reales.

De las habilidades técnicas al liderazgo estratégico y el poder de toma de decisión

En entornos reales de ciberincidentes, el conocimiento técnico es necesario, pero insuficiente. Los documentos consultados evidencia que los TTX permiten entrenar capacidades donde convergen liderazgo, autonomía, anticipación y gobernanza organizacional (Angafor et al., 2020). Estos ejercicios obligan a los participantes a ejercer poder decisional en condiciones

adversas, abordando preguntas críticas:

- ¿Quién autoriza la desconexión de sistemas críticos?
- ¿Cómo se gestiona la comunicación externa sin amplificar daños reputacionales?
- ¿Qué criterios definen el escalamiento a instancias directivas o reguladoras?

Este enfoque se alinea con la evidencia presentada en la literatura reciente, donde se documenta que los TTX elevan la madurez organizacional al exponer a los líderes a decisiones complejas y dinámicas no lineales de crisis (Vykopal et al., 2024).

El pensamiento adversarial como competencia cognitiva central

El "pensamiento adversarial" refiere a la capacidad de comprender las motivaciones, tácticas y patrones de comportamiento del atacante, anticipar movimientos y desarrollar estrategias correctivas y disuasorias. La revisión de (Vykopal et al., 2024) señala que los TTX son catalizadores de aprendizaje profundo en esta dimensión, al permitir a los participantes modelar el rol del adversario y sus escaladas lógicas.

Este proceso favorece:

- Construcción de modelos mentales sobre el comportamiento del atacante.
- Anticipación estratégica basada en hipótesis operativas.
- Evaluación continua de riesgos emergentes.
- Desarrollo de respuestas adaptativas y creativas.

Históricamente, estos ejercicios han sido utilizados en defensa estratégica y diplomacia; su entrada al dominio académico de ciberseguridad implica una evolución hacia modelos pedagógicos que combinan simulación, reflexión y evaluación basada en evidencia.

Articulación con marcos de resiliencia institucional y gobernanza

CISA subraya que los TTX fortalecen la coordinación entre áreas técnicas, directivas, legales y de comunicación, habilitando una gobernanza integrada de incidentes(*CISA Tabletop Exercise Packages*, 2022) . Esto coincide con la literatura académica, que sostiene que la participación multidisciplinaria en TTX incrementa la capacidad institucional para comprender interdependencias y gestionar el riesgo desde una perspectiva sistémica (Angafor et al., 2020).

Un aspecto clave es que la capacidad de poder organizacional no se limita al ejercicio del mando, sino a la habilidad de orquestar capacidades colectivas, sostener decisiones difíciles y activar mecanismos institucionales. Es decir, convertir la información técnica en acción estratégica.

Evidencia y oportunidades para el diseño didáctico con base en investigación

La propuesta educativa contemporánea basada en TTX, según (Švábenský et al., 2024), demuestra efectos en:

- Dinámicas colaborativas y roles críticos.
- Participación activa Vs conocimiento declarativo.
- Capacidad reflexiva (metacognición).
- Transferencia del aprendizaje a contextos reales.
- Evaluación continua de desempeño individual y colectivo.

Adicionalmente, la literatura evidencia que los TTX fortalecen el análisis crítico, la resiliencia organizacional y la capacidad para anticipar y gestionar escenarios de incertidumbre, elementos esenciales en contextos de seguridad digital y gestión de crisis. Como infraestructura didáctica avanzada, los TTX permiten implementar un aprendizaje situado, donde la experiencia se convierte en un mecanismo para generar conocimiento tácito y explícito de manera integrada.

De esta forma, se abre una oportunidad para articular el diseño instruccional con marcos de competencias institucionales, fortaleciendo aspectos como liderazgo adaptativo, ética en decisiones adversariales, comunicación estratégica, pensamiento sistémico e institucional, y gestión del riesgo en entornos complejos y dinámicos. En entornos educativos como la UNAD, este enfoque converge con el Modelo Heutagógico Unadista Solidario 5.0, favoreciendo procesos reflexivos, autónomos y colaborativos que promueven innovación educativa y aprendizaje transformador.

Ilustración 1.
Ciclo de aprendizaje experiencial aplicado a TTX

Elaboración propia utilizando Napkin.

Indicadores para medición y mejora continua

Los estudios sugieren que los TTX permiten recolectar datos sobre desempeño, roles, flujo de información y puntos de fallas organizacionales (Vykopal et al., 2024), Ejemplos de métricas documentadas incluyen:

- Tiempo de reconocimiento de incidente.

- Capacidad de coordinación e intercambio de información.
- Claridad en protocolos de escalamiento.
- Identificación de puntos críticos de comunicación.

Estas métricas permiten crear dashboards para seguimiento institucional y retroalimentación educativa.

En términos generales, los TTX constituyen un medio robusto para activar competencias esenciales en ciberseguridad que trascienden la técnica, poder organizacional, pensamiento adversarial, liderazgo decisional y resiliencia institucional. La literatura científica y las guías de CISA convergen al demostrar que estos ejercicios habilitan escenarios seguros para experimentar, fallar, aprender y mejorar, anclando el desarrollo profesional y académico en dinámicas reales de crisis y colaboración estratégica.

TTX como Eje Articulador Académico y Transformador Pedagógico

La implementación de los ejercicios de mesa (TTX) en ambientes educativos y formativos representa una evolución pedagógica significativa; pasa de ser un recurso ad-hoc de entrenamiento a convertirse en el eje articulador de un ecosistema formativo que integra competencias técnicas, cognitivas, organizativas y estratégicas.

Convirtiendo el TTX en columna vertebral del currículo formativo

En un contexto académico, vincular un TTX al currículo exige plantearlo no como evento aislado sino como mecanismo estructural que:

- sustenta módulos de aprendizaje activo, por ejemplo, cursos de "Cybersecurity Incident Response Management o Aprendizaje Automático Aplicado a la Ciberseguridad o Intrusdión y Testing"
- conecta roles institucionales reales (Líder de gestión de incidentes, Especialista en normatividad y cumplimiento, Arquitecto de soluciones técnicas, dirección, TI, legal, comunicaciones) con simulaciones reales de crisis
- se alinea con competencias del programa (pensamiento adversarial, liderazgo decisional, coordinación interfuncional)
  Por ejemplo, el estudio "Research and Practice of Delivering Tabletop Exercises" platea cómo los TTX pueden articularse dentro de cursos de computing y ciberseguridad, proporcionando métodos, métricas y recomendaciones para su entrega y evaluación.

De igual manera, en "From Paper to Platform: Evolution of a Novel Learning Environment for Tabletop Exercises" se documenta que la adopción de una plataforma digital (INJECT Exercise Platform)

permitió que el TTX trascendiera el formato tradicional («papel y lápiz») y se convirtiera en componente sistemático del plan de estudios, permitiendo capturar datos, analizar desempeño y retroalimentar.

Diseño, ejecución y evaluación del ciclo TTX en un contexto formativo

El diseño de un TTX académico institucional debe contemplar fases claras: (i) definición de objetivos de aprendizaje, (ii) preparación del escenario y roles (iii) ejecución del ejercicio (iv) sesión de debriefing[1] y reflexión (v) informe "After Action Report" y mejora continua. Este ciclo se alinea con la guía de la Cybersecurity and Infrastructure Security Agency (CISA) para ejercicios de mesa.
En el trabajo citado de Švábenský y Vykopal, se destaca que la retroalimentación automatizada de la plataforma permitió comparar desempeño de equipos y ajustar iteraciones futuras, lo cual evidencia que el TTX no solo es formativo sino también investigativo, donde se recogen datos reales para análisis y mejora (Švábenský et al., 2024).

Por otra parte, en el estudio de (Ottis, 2014) "Light Weight Tabletop Exercise for Cybersecurity Education" se presenta un formato de bajo costo y carga docente, exitoso para la educación de posgrado, enfatizando que las discusiones de roles, el intercambio de información y la comunicación son vitales (Ottis, 2014b).

Métricas, datos de aprendizaje y generación de evidencias

Para consolidar el TTX como eje articulador, es importante contar con datos que permitan evidenciar aprendizaje, cambio de comportamiento, mejora de procesos y fortalecimiento institucional. El trabajo de Švábenský et al. destaca que la plataforma de TTX generó datos de interacción (por ejemplo, número de decisiones por equipo, tiempo de respuesta, escalamiento, injects respondidos), facilitando análisis comparativos entre cohortes (Švábenský et al., 2024).

Desde un diseño de boletín o informe institucional, estos datos pueden transformarse en gráficos de:

- número de decisiones críticas tomadas por el equipo durante el ejercicio
- tiempo promedio de escalamiento a la alta dirección
- porcentaje de roles que identificaron brechas de respuesta

[1] Revisión o análisis posterior a una experiencia, actividad o evento, con el objetivo de reflexionar, aprender y mejorar a partir de lo ocurrido.

Convergencia entre el modelo institucional (MHUS 5.0) y el enfoque TTX

Dado que la Universidad Nacional Abierta y a Distancia, UNAD opera bajo el marco del Modelo Heutagógico Unadista Solidario 5.0 (MHUS 5.0), el TTX se convierte en una herramienta ideal para activar los principios del modelo: aprendizaje activo, autónomo, reflexivo, conectado con comunidad. El TTX permite a los estudiantes (o participantes institucionales) asumir roles activos en la simulación, reflexionar sobre sus decisiones desde el contexto, retroalimentar procesos institucionales y vincular resultados con mejoras reales.

Además, la evidencia académica sugiere que el TTX facilita la transición del conocimiento declarativo al conocimiento procedimental y estratégico. Por ejemplo, la revisión sistemática de Švábenský y Vykopal. describe que los TTX permiten trabajar análisis, toma de decisiones y comunicación en equipo bajo presión (Vykopal et al., 2024).

Recomendaciones para su incorporación efectiva en el boletín y diseño institucional

Para asegurar que el TTX actúe como eje articulador en la academia se recomienda:

- Vincular explícitamente los objetivos del TTX con competencias institucionales (liderazgo, resiliencia digital, pensamiento adversarial)
- Integrar el recurso de CISA como base práctica (escenario, módulo de preguntas, plantillas) para contextualización institucional
- Diseñar sesiones de TTX con roles reales de la organización
- Definir métricas de desempeño antes y después del ejercicio y presentar resultados en formato gráfico que evidencien mejora (participación, coordinación, identificación de brechas)
- Documentar los resultados en un Informe Post-Acción, integrándolo al informe institucional para asegurar la trazabilidad entre el ejercicio de simulación y las acciones reales de mejora continua.
- Establecer continuidad, teniendo en cuenta que el TTX no es un evento único, sino parte de un ciclo repetitivo de mejora.

Integración Estratégica del Recurso CISA en Programas Académicos y Ecosistemas Institucionales de Ciberseguridad

La incorporación de los paquetes de ejercicios de mesa en ciberseguridad de CISA (*CISA Tabletop Exercise Packages*, 2022) en entornos educativos e institucionales constituye una oportunidad estratégica para fortalecer

capacidades profesionales, robustecer procesos organizacionales y consolidar una cultura de seguridad digital basada en evidencia. La clave radica en no utilizar los ejercicios como actividades aisladas, sino convertirlos en un mecanismo transversal de formación, gobernanza digital y mejora continua, articulado con competencias del currículo y objetivos institucionales.

CISA como fuente de simulación de crisis

CISA dispone de un conjunto de ejercicios estructurados con objetivos, escenarios, preguntas, plantillas y formatos de informe posteriores, diseñados para fortalecer la preparación ante incidentes en entidades públicas y privadas. Entre los escenarios incluidos se encuentran ataques de ransomware, amenazas internas, interrupción de servicios críticos y afectaciones a entornos industriales y operativos (ICS/OT)[2]. Estas guías permiten desarrollar ejercicios realistas y alineados con amenazas actuales reconocidas por autoridades internacionales de ciberseguridad.

En contextos universitarios y gubernamentales, este material ofrece una base sólida para realizar simulaciones rigurosas sin partir desde cero, asegurando pertinencia, consistencia metodológica y adecuación a marcos regulatorios.

Alineación curricular y desarrollo de competencias

La evidencia académica demuestra que la incorporación sistemática de ejercicios de mesa en programas de ciberseguridad mejora la toma de decisiones en condiciones de incertidumbre, el pensamiento crítico, y la capacidad para operar bajo presión (Angafor et al., 2020).

En educación superior, estos ejercicios se integran de forma ideal en cursos de:

- Respuesta a incidentes y gestión de crisis
- Ciberseguridad defensiva y ofensiva
- Gobernanza y políticas de seguridad
- Gestión del riesgo cibernético
- Ingeniería de sistemas críticos

Estudios evidencian que el uso de plataformas educativas para TTX facilita registrar datos de interacción, evaluar desempeño y retroalimentar al estudiante de manera objetiva, convirtiendo este método en una estructura académica continua y no en una práctica soportada por anectodtas (Švábenský et al., 2024).

Uso institucional: CSIRT académico y gobernanza

Además del ámbito formativo, los ejercicios CISA se pueden

[2] Sistemas de Control Industrial/Tecnología Operativa

integrarse a la gestión institucional como herramienta para fortalecer:

Tabla 1.
Ejemplo de aplicación Institucional

Área institucional	Contribución de los ejercicios CISA
Gobernanza TI	Prueba de planes, procesos y roles
Talento humano	Desarrollo de competencias críticas
Comunicaciones	Entrenamiento en gestión de crisis reputacional
Riesgo y cumplimiento	Validación de protocolos y escalamiento
Dirección institucional	Preparación para crisis de alto impacto
Investigación aplicada	Producción de datos para análisis académico

Elaboración propia

Investigaciones en educación superior han demostrado la efectividad de ejercicios de mesa de bajo costo para preparar equipos académicos y profesionales en ambientes reales y simulados (Ottis, 2014).

Metodología de adopción para impacto sostenido

Para garantizar continuidad e impacto, se recomienda implementar un ciclo institucional:

1. Definición de objetivos y competencias
2. Selección del escenario CISA adecuado
3. Asignación de roles reales
4. Ejecución del ejercicio con registro de decisiones
5. Informe de lecciones aprendidas
6. Ajuste y mejora de procesos institucionales

ISACA coincide en que los ejercicios de mesa fortalecen la madurez en gestión de incidentes y la capacidad estratégica de respuesta (Wlosinski, 2022).

Aporte a investigación, acreditación y mejora continua

Los ejercicios TTX permiten capturar información sobre comportamiento, decisiones, comunicación y madurez digital, lo cual habilita:

- Investigación aplicada en ciberseguridad
- Producción científica basada en simulaciones controladas
- Evidencia para procesos de acreditación.

Buenas Prácticas, Desafíos y Métricas de Éxito para la Implementación de Ejercicios TTX en Educación y Gestión Institucional

La implementación de ejercicios de mesa (TTX) en ecosistemas académicos y organizacionales exige no solo el uso de escenarios adecuados, sino un andamiaje metodológico riguroso que garantice impacto formativo, valor institucional y mejora continua. A partir de las recomendaciones de CISA, la evidencia académica disponible y guías estratégicas como las emitidas por ISACA, se identifican buenas prácticas, desafíos y métricas esenciales para lograr resultados sostenibles y medibles.

Buenas prácticas para la planificación y ejecución de TTX

a) Definición clara de objetivos y competencias
Los ejercicios deben alinearse con objetivos específicos de aprendizaje, competencias institucionales y marcos operativos de ciberseguridad. La literatura señala la necesidad de articular conocimientos técnicos con habilidades estratégicas, comunicación efectiva y toma de decisiones bajo presión (Angafor et al., 2020).

b) Selección contextualizada de escenarios
El catálogo CISA facilita ejercicios que pueden adaptarse a ambientes educativos, gubernamentales y de operación crítica, permitiendo seleccionar amenazas relevantes como ransomware, divulgación de datos o interrupción operacional (*CISA Tabletop Exercise Packages*, 2022).

c) Roles y cadena de mando realista
Tanto CISA como ISACA destacan la importancia de involucrar perfiles diversos: dirección, TI, comunicaciones, legal, riesgo y soporte operativo (Wlosinski, 2022). Esto fortalece la interoperabilidad institucional y evita ejercicios centrados únicamente en equipos técnicos.

d) Sesión estructurada de retroalimentación (debriefing)
Los estudios de Švábenský y Vykopal demuestran que el análisis posterior es tan importante como el ejercicio mismo, ya que consolida aprendizajes, genera conciencia situacional y permite recolectar datos para investigación (Vykopal et al., 2024).

e) Ciclo iterativo de mejora
La repetición de ejercicios con ajustes progresivos mejora madurez e institucionalización, alineándose con modelos como MHUS 5.0 y enfoques de calidad educativa.

Principales desafíos identificados

Los referentes analizados destacan limitaciones comunes:

Tabla 2.
Limitaciones comunes identificadas en el análisis literario

Desafío	Fuente
Limitada medición de aprendizaje y desempeño real	Švábenský et al., 2024 (arXiv: 2404.10988)
Foco excesivo en aspectos técnicos, descuidando componentes comunicativos y de gobernanza	Angafor et al., 2020 (DOI: 10.1002/spy2.126)
Escasa participación interdisciplinaria	ISACA, 2022
Escenarios poco realistas o excesivamente genéricos	CISA Exercise Tips
Falta de continuidad (TTX como evento único)	Ottis, 2014 (DOI: 10.1515/jhsem-2014-0031)

Elaboración propia

Métricas para evaluar impacto

La evidencia científica sugiere indicadores que permiten evaluar éxito e institucionalización:

Indicadores de desempeño operativo

- Tiempo de identificación del incidente
- Tiempo de escalamiento a actores clave
- Precisión y claridad en decisiones

Indicadores de coordinación y comunicación

- Flujo de información entre roles
- Cumplimiento de responsabilidades RACI
- Calidad de los informes posteriores

Indicadores de aprendizaje y madurez

- Evaluación pre/post ejercicio
- Autoevaluación y coevaluación estructurada
- Evidencias reflexivas y metacognitivas
- Niveles de participación interfuncional.

En estudios como el de Vykopal et al. (2024), el uso de plataformas permite capturar estos datos automáticamente y transformarlos en insumos para investigación y retroalimentación institucional.

Recomendaciones accionables para el contexto universitario e institucional

En coherencia con los hallazgos derivados de la literatura académica y las directrices emitidas por organismos especializados como CISA e ISACA, las siguientes recomendaciones sintetizan acciones estratégicas que permiten fortalecer la adopción de ejercicios de mesa en entornos universitarios y de gestión pública. Estas acciones están orientadas a garantizar que los TTX trasciendan la simulación operativa y se consoliden como instrumentos de formación integral, evaluación basada en desempeño, fortalecimiento institucional y generación de evidencia para procesos de mejora continua y aseguramiento de la calidad. Su implementación sistemática posibilita articular competencias técnicas y estratégicas, promover la participación interdisciplinaria, fomentar la toma de decisiones informada y documentar aprendizajes para avanzar hacia niveles superiores de madurez en ciberseguridad y gobernanza digital.

Tabla 3.

Recomendaciones generadas a partir del análisis literario

Acción	Beneficio
Utilizar plantillas CISA y guías ISACA	Estandarización y rigor
Registrar métricas y generar informes post-ejercicio	Mejora continua y trazabilidad
Integrar altos directivos y dependencias no TI	Madurez organizacional real
Publicar resultados sistematizados	Valor académico y reputacional
Incorporar reflexión individual y colectiva	Aprendizaje profundo (MHUS 5.0). De forma especifica para la UNAD

Elaboración propia

La integración de ejercicios TTX requiere rigor metodológico y visión estratégica. Su éxito se fundamenta en objetivos claros, participación interdisciplinaria, medición verificable y compromiso institucional continuo. Adoptados bajo un enfoque académico-operativo, se convierten en

herramientas esenciales para fortalecer capacidades reales, desarrollar pensamiento adversarial responsable y consolidar resiliencia digital en instituciones educativas y organizaciones públicas o privadas.

Ejercicios de Mesa para el Fortalecimiento de las Capacidades de Ciberseguridad Según CIS

El documento *Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team* del Center for Internet Security (CIS) (*Six Tabletop Exercises to Help Prepare Your Cybersecurity Team*, 2025) propone una guía práctica para fortalecer equipos de ciberseguridad mediante ejercicios de simulación estratégica. Su propósito es facilitar que organizaciones de distintos sectores analicen riesgos, practiquen respuesta ante incidentes y desarrollen capacidades operativas y de gestión frente a amenazas digitales emergentes.

Objetivo y Alcance

El documento presenta seis escenarios de ejercicio diseñados para poner a prueba procesos internos, capacidades técnicas, mecanismos de escalamiento, comunicación institucional y toma de decisiones bajo presión. Cada escenario incluye preguntas de reflexión para promover análisis crítico, identificación de brechas y acciones de mejora continua. Adicionalmente, se establecen controles CIS asociados para orientar la madurez de la seguridad organizacional.

Lineamientos de Ejecución

Además, establece que los ejercicios deben ser guiados por un facilitador, incluir actores relevantes de la organización y centrarse en el aprendizaje. Se sugiere:

- Leer y comprender el escenario de forma grupal
- Identificar decisiones críticas
- Simular flujos de respuesta internos
- Evaluar capacidades técnicas, administrativas y operativas
- Documentar lecciones aprendidas y brechas detectadas
- Ejecutar acciones de mejora posteriores

Este enfoque busca fortalecer la cultura organizacional en seguridad digital y fomentar la colaboración entre áreas técnicas y administrativas.

Tabla 4.

Resumen de los Escenarios propuestos por CIS[3]

Nº	Nombre del Escenario	Situación Simulada	Proceso/Capacidad Evaluada	Tipo de Amenaza	Activo o Función Impactada
1	**The Quick Fix**	Aplicación apresurada de un parche crítico genera indisponibilidad del sistema	Gestión de cambios y control de versiones	Insider (error interno)	Red interna - acceso de usuarios
2	**A Malware Infection**	Malware ingresa vía dispositivo externo personal y se propaga a sistemas corporativos	Detección, contención y conciencia del usuario	Accidental insider	Integridad de la red y equipos
3	**The Unplanned Attack**	Grupo activista anuncia ataque sin avisar vector específico	Preparación estratégica y monitoreo	Hacktivista	Sistemas corporativos (variable - desconocido)
4	**The Cloud Compromise**	Brecha en proveedor cloud expone datos sensibles institucionales	Respuesta a incidente, gestión de terceros y comunicación	Actor externo	Datos en la nube - servicios cloud
5	**Financial Break-in**	Fraude financiero tras intrusión física y uso indebido de credenciales	Respuesta a incidente, auditoría, control de accesos	Externa con componente interno comprometido	Sistemas financieros - datos RRHH
6	**The Flood Zone**	Desastre natural más ataque ransomware simultáneo que bloquea operaciones	Continuidad operativa, gestión de crisis y respuesta a ransomware	Actor externo	Operaciones críticas - servicios de emergencia

Elaboración propia, construida desde el documento Six Scenarios to Help Prepare Your Cybersecurity Team de CIS.

Integración de Buenas Prácticas

El documento también proporciona:

- Recomendaciones metodológicas para la conducción de ejercicios
- Enlaces a herramientas gratuitas y recursos formativos
- Referencias a los Controles CIS para fortalecer políticas y procedimientos
- Sugerencias para reforzar auditoría, control de accesos, capacitación y respuesta a incidentes.

Este recurso de CIS constituye un instrumento valioso para organizaciones que buscan elevar su madurez en ciberseguridad. A través de escenarios realistas, preguntas orientadoras y alineación con controles reconocidos, permite:

- Evaluar capacidades actuales de respuesta
- Identificar vulnerabilidades procedimentales y técnicas
- Fortalecer la cultura de seguridad digital

[3] https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team

- Fomentar aprendizaje colaborativo y mitigación proactiva

Su naturaleza práctica lo convierte en una herramienta adaptable a entornos corporativos, gubernamentales y académicos, apoyando estrategias integrales de preparación ante ciberamenazas y gestión de riesgos.

Conclusiones

Los Tabletop Exercises (TTX) se consolidan como un componente estratégico para fortalecer la cultura institucional de ciberseguridad y la formación avanzada en escenarios de toma de decisiones frente a incidentes. Su implementación en la academia y particularmente en la UNAD evidencia que:

1. Transforman el aprendizaje tradicional, permitiendo pasar de modelos centrados en contenidos a experiencias inmersivas que desarrollan análisis crítico, pensamiento adversarial ético y liderazgo para la gestión de crisis.

2. Integran dimensiones técnicas, cognitivas y organizacionales, preparando a los participantes para operar en entornos inciertos con comunicación efectiva, priorización estratégica y gestión del riesgo.

3. Generan evidencia objetiva y medible para procesos de mejora continua, acreditación y madurez institucional, articulando métricas y ciclos de aprendizaje experiencial.

4. Se alinean con el Modelo Heutagógico Unadista Solidario 5.0, potenciando autonomía, aprendizaje colaborativo, investigación aplicada y construcción colectiva del conocimiento.

5. Fortalecen el rol del CSIRT Académico UNAD como articulador entre academia, gestión estratégica y cultura organizacional de seguridad digital, contribuyendo a ecosistemas institucionales resilientes.

Recomendaciones finales para las instituciones

Para maximizar el impacto y sostenibilidad de los TTX, se recomienda que las entidades académicas y públicas:

1. Institucionalicen los TTX como práctica recurrente, articulada al plan académico o de entrenamiento, operativo y de seguridad digital.
2. Definan métricas de madurez y desempeño, integrando evidencias cuantitativas y cualitativas en procesos de seguimiento e informes.
3. Vinculen equipos multidisciplinarios (dirección, TI, comunicaciones, legal, riesgo, talento humano) para fortalecer la gobernanza y la coordinación interfuncional.
4. Aprovechen recursos abiertos de CISA y FEMA para garantizar rigor metodológico, pertinencia y actualización permanente.
5. Documenten resultados y retroalimenten procesos, asegurando trazabilidad hacia planes de mejora curricular, institucional y operativa.
6. Impulsen investigación aplicada basada en datos reales generados en los ejercicios, fortaleciendo producción científica, innovación y transferencia de conocimiento.
7. Aseguren formación continua para facilitadores, desarrollando capacidades técnicas, pedagógicas y estratégicas para orientar ejercicios avanzados.

Implementadas de manera sistemática, estas acciones permitirán consolidar ecosistemas formativos resilientes, alineados con estándares internacionales y las demandas emergentes de la seguridad digital global.

Referentes

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *SECURITY AND PRIVACY*, *3*(6), e126. https://doi.org/10.1002/spy2.126

CISA Tabletop Exercise Packages. (2022). https://www.cisa.gov/sites/default/files/2023-02/ctep_fact_sheet_v._11_16_2021_final.pdf

Cybersecurity Tabletop Exercise Tips. (2020). CISA. https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf

Ottis, R. (2014a). Light Weight Tabletop Exercise for Cybersecurity Education. *Journal of Homeland Security and Emergency Management*, *11*(4), 579-592. https://doi.org/10.1515/jhsem-2014-0031

Ottis, R. (2014b). Light Weight Tabletop Exercise for Cybersecurity Education. *Journal of Homeland Security and Emergency Management*, *11*(4), 579-592. https://doi.org/10.1515/jhsem-2014-0031

Six Tabletop Exercises to Help Prepare Your Cybersecurity Team. (2025). CIS. https://www.cisecurity.org/insights/white-papers/six-tabletop-exercises-prepare-cybersecurity-team

Švábenský, V., Vykopal, J., Horák, M., Hofbauer, M., & Čeleda, P. (2024). From Paper to Platform: Evolution of a Novel Learning Environment for Tabletop Exercises. *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, 213-219. https://doi.org/10.1145/3649217.3653639

Vykopal, J., Čeleda, P., Švábenský, V., Hofbauer, M., & Horák, M. (2024). Research and Practice of Delivering Tabletop Exercises. *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1*, 220-226. https://doi.org/10.1145/3649217.3653642

Wlosinski. (2022). *Cybersecurity Incident Response Exercise Guidance*. ISACA.

Contáctenos

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

El CSIRT Académico UNAD está 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!