2026

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Europa Frente al Riesgo Digital

CÓMO LA UE ESTÁ FORTALECIENDO SU RESPUESTA EN CIBERSEGURIDAD

Este documento se construye con base en la guía The ENISA Cybersecurity Exercise Methodology: End-to-end guide on how to plan, run and evaluate an exercise, como referente técnico para contextualizar los avances de la Unión Europea en el fortalecimiento de su respuesta estratégica y operativa en ciberseguridad.

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 [37]
Marzo de 2026

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

Contenido

Introducción

La ciberseguridad dejó hace tiempo de ser un asunto exclusivamente técnico para convertirse en una prioridad estratégica de gobiernos, organizaciones y sectores críticos. En un entorno marcado por amenazas cada vez más sofisticadas, persistentes y transfronterizas, la capacidad de anticipar, coordinar y responder eficazmente ya no depende solo de contar con tecnologías de protección, sino también de fortalecer la preparación institucional y el aprendizaje continuo.

En ese contexto, la Unión Europea ha venido consolidando un enfoque más robusto de ciberresiliencia, en el que la regulación, la cooperación y el entrenamiento práctico se articulan como piezas complementarias. La metodología de ejercicios de ciberseguridad promovida por ENISA refleja precisamente esa evolución, propone pasar de la reacción improvisada a la preparación estructurada, mediante ejercicios diseñados para evaluar capacidades, identificar brechas y mejorar la toma de decisiones bajo presión.

Este boletín presenta una lectura académica y aplicada de ese enfoque, explicando las seis fases que componen la metodología y resaltando su valor para el fortalecimiento de la respuesta organizacional frente a incidentes y crisis cibernéticas. Más allá del caso europeo, el análisis permite reconocer lecciones útiles para otros contextos, especialmente para América Latina y el Caribe, donde la madurez en ciberseguridad sigue siendo desigual y donde avanzar hacia esquemas de preparación más sistemáticos resulta cada vez más urgente.

Europa frente al riesgo digital: cómo la UE está fortaleciendo su respuesta en ciberseguridad

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

La preparación como estrategia: el enfoque europeo detrás de la metodología ENISA

La introducción de The ENISA Cybersecurity Exercise Methodology[1] debe leerse como parte de una evolución más amplia de la política europea de ciberseguridad, en la que la preocupación ya no se limita a la protección técnica de sistemas, sino que incorpora preparación institucional, coordinación entre actores, capacidad de respuesta y aprendizaje posterior a incidentes. En ese sentido, el documento no surge de forma aislada, responde a una necesidad real de la Unión Europea de fortalecer la resiliencia organizacional frente a amenazas cada vez más frecuentes, complejas y transfronterizas. Esa lectura se ve respaldada por el ENISA Threat Landscape 2025, que reporta el análisis de 4.875 incidentes y señala que el entorno de amenazas sigue dominado por vectores como el phishing, mientras el ransomware conserva un impacto especialmente severo sobre organizaciones y sectores críticos(ENISA, 2025).

Desde esa perspectiva, la metodología de ENISA se entiende mejor no solo como una guía para "hacer ejercicios", sino como una herramienta para cerrar una brecha estratégica, la distancia entre la existencia de normas o

[1] https://www.enisa.europa.eu/sites/default/files/2026-02/The%20ENISA%20Cybersecurity%20Exercise%20Methodology.pdf

capacidades formales y la capacidad real de actuar bajo presión. Ese marco coincide con lo planteado por ENISA en Best Practices for Cyber Crisis Management, donde se advierte que la gestión de crisis cibernéticas en la UE ha evolucionado de forma significativa y debe abordarse como un ciclo integrado de prevención, preparación, respuesta y recuperación (ENISA, s. f.-a). En otras palabras, el valor del documento está en traducir la política europea en práctica operativa, algo que resulta esencial cuando los incidentes dejan de ser eventos netamente técnicos y pasan a comprometer continuidad, confianza pública y coordinación institucional (ENISA, 2026).

Además, esta introducción cobra más sentido al contrastarla con la evidencia sobre madurez sectorial presentada por ENISA NIS360 - 2024. Ese informe muestra que la madurez en ciberseguridad no es homogénea dentro de la Unión; sectores como electricidad, telecomunicaciones y banca presentan niveles más altos, mientras otros sectores recién regulados o menos consolidados exhiben madurez moderada o inferior, lo que obliga a priorizar acciones de fortalecimiento (ENISA, 2025b). Bajo esa lógica, la metodología de ejercicios no debe verse como un complemento opcional, sino como un mecanismo para evaluar capacidades, identificar brechas y acelerar la madurez operativa allí donde la criticidad sectorial supera la preparación efectiva.

En síntesis, la introducción del documento sitúa al lector en una idea central, en el enfoque europeo actual, la ciberseguridad no se agota en la regulación ni en la tecnología, sino que exige entrenamiento, coordinación, evaluación y mejora continua. Por eso, el texto de ENISA funciona como un puente entre la estrategia de la Unión Europea y la necesidad concreta de que organizaciones y sectores críticos ensayen su respuesta antes de enfrentar una crisis real.

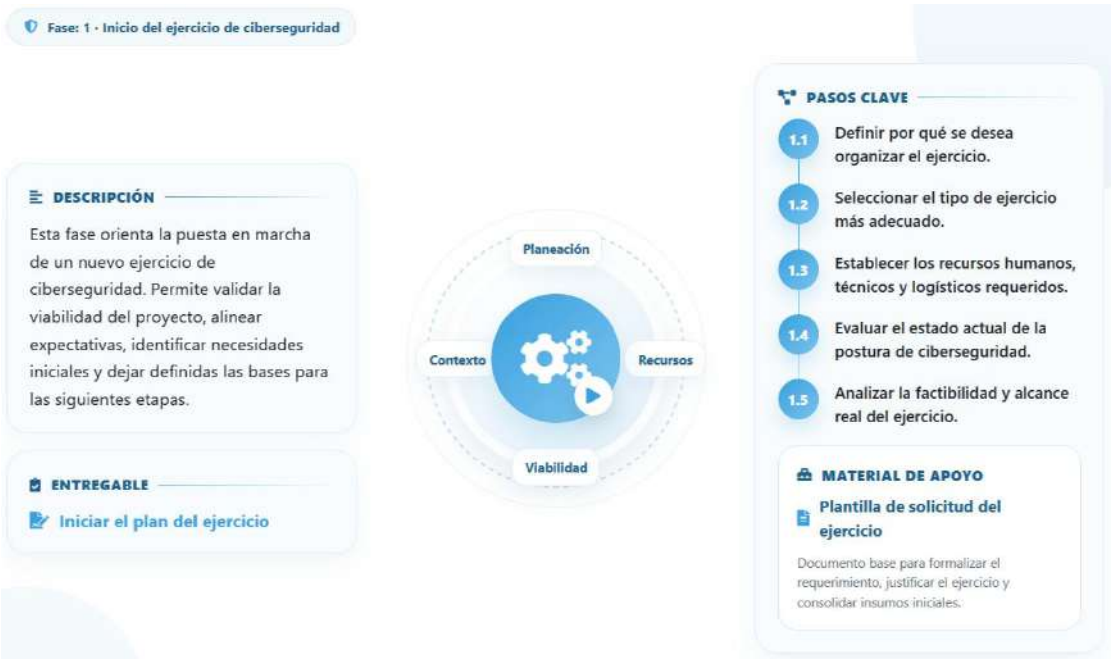
De la planeación a la mejora: las seis fases de la metodología ENISA

La metodología de ENISA organiza los ejercicios de ciberseguridad en seis fases encadenadas: iniciación, diseño, preparación, ejecución, evaluación y proyección de resultados. Esta secuencia no es decorativa; responde a una lógica de madurez, donde cada etapa prepara la siguiente y evita que el ejercicio se convierta en una simulación improvisada sin impacto real. En conjunto, las seis fases

permiten pasar de la intención estratégica a la acción operativa, y de la acción al aprendizaje institucional.

Fase 1. Iniciación: el punto donde se define si el ejercicio tiene sentido

La fase de iniciación cumple una función crítica, antes de hablar de escenarios, jugadores o métricas, obliga a la organización a responder una pregunta incómoda pero esencial ¿para qué se quiere hacer el ejercicio?. ENISA plantea que toda decisión de avanzar debe comenzar por comprender el propósito de fondo, el "why", ya sea a nivel institucional, organizacional o gubernamental. Ese propósito no equivale todavía a un objetivo técnico, más bien actúa como la razón estratégica que da legitimidad al ejercicio, moviliza actores y alinea el proceso con metas más amplias. Dicho sin maquillaje: si una organización no tiene claro por qué quiere entrenarse, probablemente tampoco sabrá qué necesita mejorar (ENISA, 2026).



Desde esa lógica, la iniciación no se limita a una idea general de "hagamos un simulacro". La metodología aterriza esta fase en cinco tareas concretas: definir el propósito, escoger el tipo de ejercicio, identificar los recursos requeridos, valorar la postura actual de ciberseguridad, revisar la viabilidad real del proceso.

ENISA incluso la describe como la fase que determina la viabilidad del proyecto, fija expectativas y deja planteados los requerimientos para las etapas posteriores. Es, en esencia, el filtro que separa un

ejercicio útil de uno armado por cumplir.

Uno de los aportes más valiosos de esta fase es que obliga a elegir entre distintos tipos de ejercicio según los objetivos y capacidades disponibles. La metodología distingue, por ejemplo, entre ejercicios basados en discusión, orientados al análisis, la coordinación y la toma de decisiones, y ejercicios operativos, enfocados en validar procedimientos, capacidades técnicas y respuestas en entornos simulados. Esta distinción es clave porque evita un error bastante común, que es el de creer que todos los ejercicios sirven para todo.

La iniciación también introduce una mirada realista sobre los recursos. ENISA subraya que un ejercicio serio exige personas, tecnología, presupuesto y tiempo. Además, advierte que el involucramiento temprano de actores internos y externos es decisivo, especialmente cuando se necesita apoyo de la alta dirección, articulación entre áreas o dependencias o validación de prioridades. En esta fase, el mapeo de stakeholders no es un formalismo administrativo; es una condición para que el ejercicio tenga legitimidad, participación y capacidad de producir resultados aplicables.

Otro elemento central es la revisión de la postura de ciberseguridad. La metodología insiste en que antes de planear un ejercicio conviene entender capacidades, debilidades, vulnerabilidades y brechas de mejora. Para ello propone una aproximación de tres pasos:

- Evaluación general
- Análisis de vulnerabilidades
- Análisis de brechas.

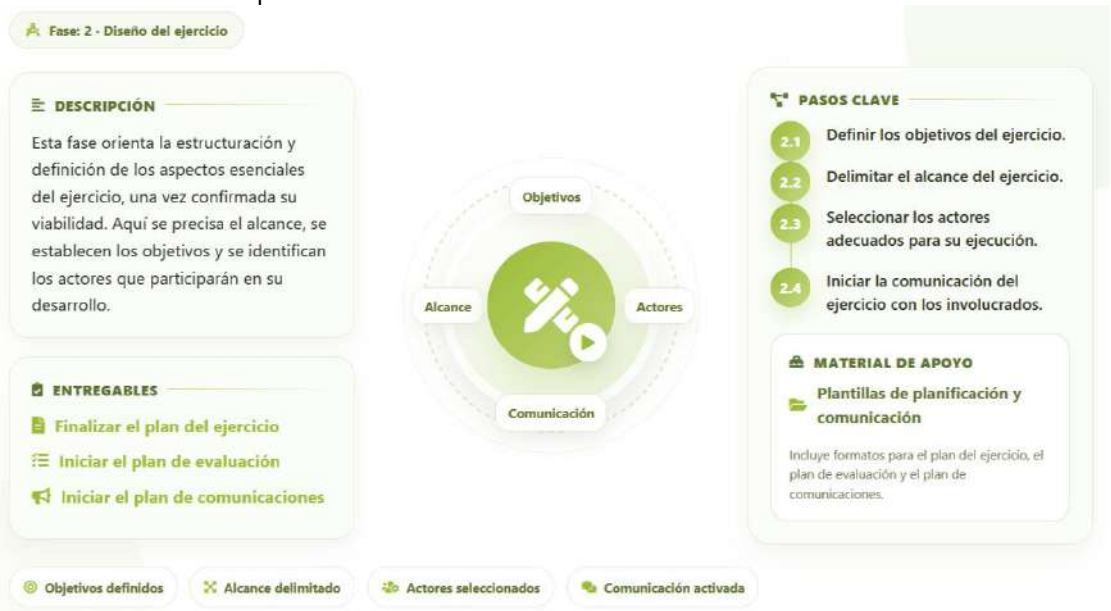
La idea de fondo es sencilla, pero potente, el ejercicio no debe construirse sobre supuestos, sino sobre necesidades reales. Si no se parte de un diagnóstico, el riesgo es terminar simulando una amenaza vistosa pero irrelevante para la realidad de la organización.

Finalmente, la fase de iniciación incorpora una verificación de factibilidad. ENISA plantea que, una vez entendida la postura de ciberseguridad, la organización debe evaluar si realmente tiene condiciones para ejecutar el ejercicio: alineación con prioridades estratégicas, disponibilidad de recursos, compatibilidad tecnológica, compromiso de actores clave y tiempo suficiente para planear sin afectar otras operaciones críticas. El cierre de esta fase desemboca en un entregable central: el plan del ejercicio,

concebido como el documento base que concentrará las decisiones y orientará todo el proceso posterior.

Fase 2. Diseño: convertir la intención en una estructura clara de ejercicio

Si la fase de iniciación responde por qué vale la pena hacer el ejercicio, la fase de diseño se encarga de definir qué se va a probar, con quién y bajo qué límites. ENISA presenta esta etapa como el momento en que, una vez confirmada la viabilidad del ejercicio, se estructuran sus aspectos esenciales: objetivos, alcance, jugadores y comunicación. En otras palabras, aquí el ejercicio deja de ser una buena idea y empieza a tomar forma operativa.



El primer componente del diseño es la definición de objetivos. La metodología insiste en que estos deben ser claros, medibles y alineados con las metas estratégicas de la organización, de modo que el ejercicio no se convierta en una actividad genérica sin capacidad de producir mejoras concretas. Para ello propone el uso del enfoque SMART y sugiere temas orientadores como estrategia, operación, factores humanos, mejora de procesos, continuidad del negocio y cumplimiento legal. Además, plantea tres preguntas que ayudan a aterrizar cada objetivo: qué se quiere lograr, quién debe lograrlo y cómo se medirá el éxito. Esa triada parece simple, pero evita uno de los errores más frecuentes en estos ejercicios: querer evaluar todo al mismo tiempo y terminar sin evidencia útil.

El segundo componente es el alcance. ENISA lo trata como una pieza crítica porque fija fronteras específicas, mantiene el foco del ejercicio y evita la deriva de misión. El alcance debe definir qué sistemas o infraestructuras serán puestos a prueba, qué límites organizacionales se incluyen, qué escenarios de amenaza se van a simular y qué restricciones temporales u operativas deben respetarse. La metodología también advierte sobre varios errores típicos: hacer un alcance demasiado amplio, demasiado estrecho, con límites mal definidos, con escenarios irreales o ignorando dependencias críticas. La lógica es bastante sensata: un ejercicio bien acotado que examine a fondo unos pocos procesos críticos vale más que uno ambicioso que apenas roce muchos frentes y no deje aprendizajes claros.

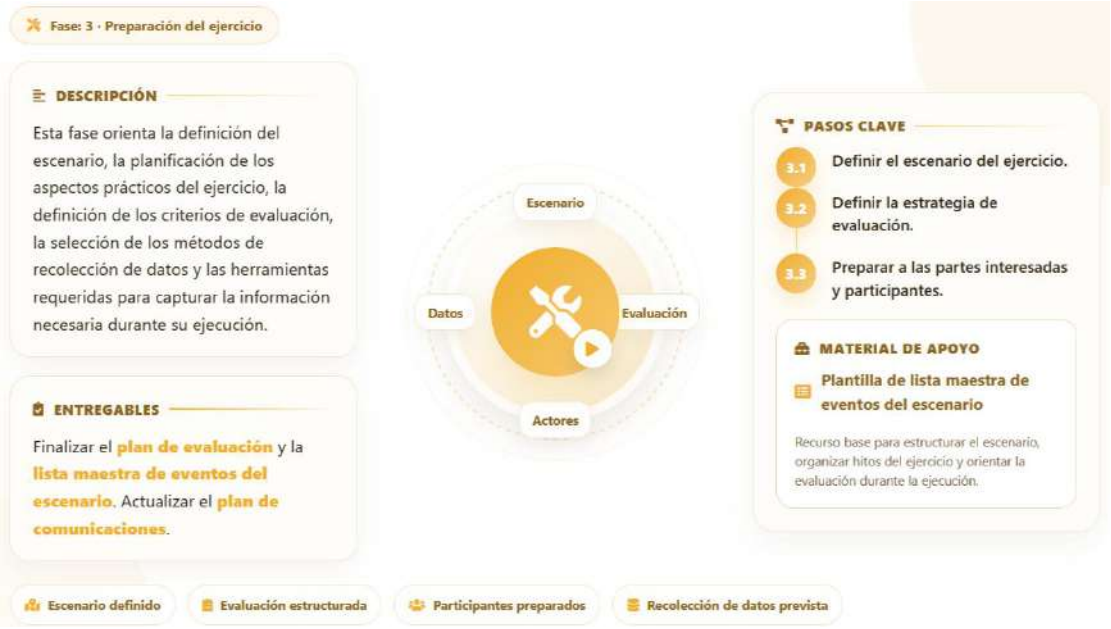
El tercer elemento del diseño es la selección de los jugadores. Aquí ENISA señala que los participantes deben representar a las personas que realmente responderían ante un incidente, contar con autoridad para tomar decisiones y tener disponibilidad real para participar. La metodología no se queda en cargos genéricos, sino que asocia perfiles concretos con funciones específicas: CISO, respondedor de incidentes, analista de inteligencia, investigador forense, perfiles legales y roles técnicos ofensivos o defensivos. Además, recuerda que en el contexto más amplio del ejercicio también pueden intervenir TI, comunicaciones, talento humano y alta dirección. Esto refuerza una idea importante para el boletín: la ciberseguridad, en el enfoque europeo, no se juega solo en el SOC ni en el área técnica; se pone a prueba como capacidad organizacional.

El cuarto componente es la comunicación. ENISA es bastante directa en esto: la comunicación efectiva es la columna vertebral de una buena planificación. Por eso recomienda iniciar el plan de comunicación desde la fase de diseño, no al final. Ese plan debe servir para generar conocimiento y respaldo antes del ejercicio, mantener el compromiso durante la preparación, asegurar coordinación durante la ejecución y capturar retroalimentación una vez termine. También propone acciones tempranas muy concretas, como identificar stakeholders internos y externos, definir mensajes clave y canales preferidos, realizar reuniones iniciales y sostener actualizaciones periódicas. Traducido al lenguaje del boletín: si la gente no entiende el ejercicio, no confía en él o no sabe qué papel cumple, el diseño ya empezó cojo.

El cierre de esta fase también es importante. ENISA indica que, una vez definidos el alcance, los equipos, los perfiles de jugadores y las capacidades que se desean evaluar, el plan del ejercicio debe quedar completado y deben iniciarse las bases del plan de evaluación y del plan de comunicación. Eso muestra que la fase de diseño no es solo conceptual; produce entregables concretos que conectan la intención estratégica con la preparación posterior.

Fase 3. Preparación: donde el ejercicio deja de ser una idea y comienza a tomar cuerpo

La fase de preparación cumple una función decisiva dentro de la metodología ENISA, porque es el momento en que el ejercicio se convierte en una experiencia estructurada, coherente y técnicamente viable. Si en la fase de diseño se definieron los objetivos, el alcance y los actores, aquí corresponde traducir todo eso en una narrativa operativa, en criterios de evaluación y en condiciones reales de alistamiento para los participantes. El documento lo resume con bastante claridad: esta etapa se orienta a definir el escenario, planear las cuestiones prácticas, establecer los criterios de evaluación, escoger los métodos de recolección de datos y preparar a los actores involucrados.



El primer núcleo de esta fase es la construcción del escenario. ENISA insiste en que los ejercicios de ciberseguridad deben apoyarse en escenarios realistas y convincentes, porque el escenario funciona como la columna narrativa que ordena

las actividades, las decisiones y la interacción entre los participantes. No se trata de inventar una historia espectacular para impresionar, sino de construir una situación plausible, alineada con los objetivos del ejercicio y con el panorama real de amenazas de la organización. Por eso la metodología recomienda partir del análisis del threat landscape[2] propio, identificar amenazas sectoriales probables y asociarlas con actores plausibles, como grupos criminales, hacktivistas o actores con vínculo estatal. Esa recomendación es bastante sensata: un ejercicio útil no es el más dramático, sino el que más se parece a los riesgos que realmente podrían materializarse.

Dentro de esa construcción del escenario, la metodología destaca tres elementos centrales: el actor de amenaza, el estado del mundo y la línea narrativa de lo que ocurrirá durante el ejercicio. El "estado del mundo" aporta el contexto previo, es decir, los antecedentes que ayudan a que los participantes entiendan qué ha venido ocurriendo antes del incidente simulado. La línea narrativa, por su parte, organiza lo que sucederá durante la ejecución y da sentido a la secuencia de eventos. ENISA advierte, además, que esta narrativa debe ser equilibrada: suficientemente realista para generar aprendizaje, pero no tan recargada ni tan teatral que termine confundiendo a los jugadores o desviando el foco de los objetivos.

El segundo núcleo de la preparación es la estrategia de evaluación. Aquí la metodología hace una afirmación clave: sin una evaluación adecuada, incluso un ejercicio bien diseñado se reduce a un evento de entrenamiento sin impacto duradero. En ese sentido, la evaluación no aparece al final como trámite, sino que se diseña desde antes de ejecutar el ejercicio. Su función es medir si los objetivos se alcanzaron, detectar brechas de capacidad o de proceso, y reunir evidencia que justifique futuras mejoras e inversiones. Dicho de forma simple, ENISA plantea que el valor de un ejercicio no está solo en realizarlo, sino en poder demostrar qué funcionó, qué falló y por qué.

Para lograrlo, la fase de preparación exige definir criterios de evaluación y métodos de recolección de

[2] Panorama actual de amenazas que permite identificar los riesgos y actores más probables para orientar el ejercicio.

datos. Eso implica decidir qué indicadores se observarán, cómo se medirán y con qué herramientas se obtendrá la información. La metodología subraya que esta previsión es necesaria para que, durante la ejecución, se capture evidencia útil y luego pueda analizarse de manera consistente. En ejercicios grandes, incluso recomienda conformar un equipo específico de evaluación con liderazgo y funciones diferenciadas, lo que refuerza la idea de que medir bien también forma parte del ejercicio, y no es un accesorio puesto al final para llenar un informe.

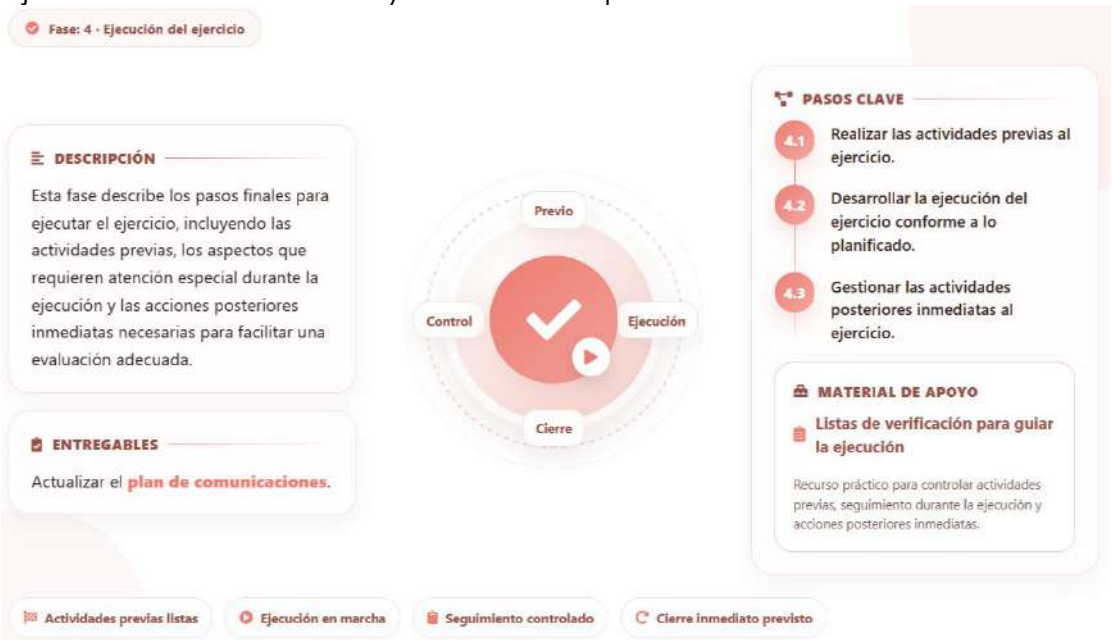
El tercer componente de esta fase es la preparación de los stakeholders, en especial de los jugadores. ENISA señala que una buena ejecución depende de que los participantes comprendan su rol, el contexto del escenario y las condiciones logísticas antes de empezar. Para eso propone elaborar una guía del jugador, que debe incluir una visión general del ejercicio, objetivos, alcance, reglas de participación, requerimientos técnicos, cronograma y datos logísticos esenciales. No es un detalle menor: esta guía busca que todos entren al ejercicio con una base común de información y que la experiencia no se vea afectada por vacíos de interpretación o improvisación.

La metodología también dedica atención a la forma en que esa información debe entregarse. Recomienda combinar documentación escrita, sesiones de briefing y espacios de preguntas, e incluso actividades de entrenamiento específico cuando el ejercicio lo requiera. Además, recalca que estas acciones deben estar integradas al plan de comunicación iniciado en la fase anterior, precisamente para asegurar que los actores estén informados, comprometidos y realmente preparados. El mensaje de fondo vuelve a ser coherente con toda la lógica del documento: un ejercicio sólido no depende solo del escenario o de la técnica, sino también de la claridad con que las personas entienden qué van a hacer y para qué lo van a hacer.

Fase 4. Ejecución: donde la planeación se somete a la realidad

La fase de ejecución es el punto en que meses de planificación se convierten en acción. ENISA la presenta como el momento en que el escenario cobra vida, los participantes ponen a prueba sus

capacidades bajo presión y los evaluadores recogen información crítica para la mejora. No es solo "hacer el ejercicio"; es el instante en que la organización comprueba si lo que definió en el papel realmente funciona cuando aparecen presión, incertidumbre, coordinación interáreas y necesidad de respuesta. La propia metodología resume esta etapa en tres momentos: actividades previas al ejercicio, ejecución del escenario y actividades posteriores inmediatas.



El primer bloque corresponde a las actividades previas a la ejecución. ENISA les da un peso importante porque funcionan como un último filtro de control antes de poner en marcha la simulación. Aquí se revisan las condiciones logísticas, la disponibilidad del entorno, la solidez del escenario y la preparación tanto del equipo de control como de los jugadores. La metodología es bastante clara: estas verificaciones finales, hechas horas o días antes, ayudan a evitar fallas que pueden arruinar incluso un ejercicio bien diseñado. En otras palabras, antes de evaluar la respuesta de una organización, primero hay que asegurarse de que el propio ejercicio no se estrelle por descuido.

Dentro de esas actividades previas, ENISA distingue varios controles concretos. En lo logístico, se debe confirmar que el espacio, los equipos, la conectividad y los canales de comunicación estén operativos. En cuanto al escenario, recomienda realizar dry runs[3] del

[3] Ensayos previos del ejercicio para comprobar que el escenario, la secuencia de eventos y la logística funcionen correctamente antes de la ejecución real.

MSEL[4] y verificar que los materiales narrativos e inyecciones estén listos. También subraya la necesidad de preparar al equipo de control, incluidos facilitadores y observadores, para que tengan claridad sobre sus funciones, la coordinación interna y los mecanismos de intervención. Finalmente, los jugadores deben haber confirmado su participación y recibido la información esencial para desempeñar su papel. La lógica es impecable: la improvisación puede servir para una obra de teatro experimental, pero para un ejercicio serio de ciberseguridad suele ser la ruta más corta al caos.

El segundo bloque es la ejecución propiamente dicha del escenario. Aquí los injects del MSEL se entregan a los jugadores según la secuencia prevista, pero con margen para ajustes dinámicos cuando la reacción de los participantes lo exige. ENISA insiste en que el equipo de control debe estar preparado para modificar el ritmo o la dirección del escenario en tiempo real para mantener realismo y utilidad. Este detalle es importante porque muestra que la ejecución no es mecánica; no se trata de "pasar diapositivas" ni de cumplir un guion rígido, sino de conducir una simulación creíble que permita observar comportamientos reales.

La metodología también diferencia con claridad entre ejercicios basados en discusión y ejercicios operativos. En los primeros, los facilitadores conducen el escenario mediante preguntas, dilemas y puntos de discusión orientados al análisis, la colaboración y la toma de decisiones. En los segundos, en cambio, se espera que los jugadores ejecuten acciones concretas y medibles dentro de un entorno simulado: análisis forense, comunicaciones de crisis, activación de procedimientos técnicos o coordinación entre equipos. Esta distinción es clave, porque demuestra que la ejecución adopta formas distintas según el tipo de ejercicio, aunque en ambos casos se busca observar la respuesta organizacional frente a un incidente creíble.

En los ejercicios operativos, además, ENISA concede un lugar central a la gestión del entorno técnico. La infraestructura debe mantenerse estable, coherente con el escenario y suficientemente realista para desafiar a los participantes sin

[4] Secuencia maestra de eventos del escenario que organiza las inyecciones, tiempos y desarrollo del ejercicio.

introducir fallas artificiales. Para ello se requiere monitorear la salud de los sistemas, verificar que los eventos simulados mantengan autenticidad y contar con capacidad de intervención rápida ante problemas de plataforma. El mensaje de fondo aquí es bastante fino: la tecnología debe apoyar el realismo del ejercicio, no convertirse en un obstáculo absurdo que distorsione la evaluación.

El tercer componente de esta fase es el monitoreo en tiempo real y el soporte durante la ejecución. ENISA señala que el equipo de control y los observadores deben documentar continuamente acciones, decisiones, comunicaciones y eventos críticos, incluyendo tanto las inyecciones previstas como las intervenciones adicionales que surjan durante la simulación. También recomienda captar retroalimentación inmediata en pausas o momentos designados. Esta recolección en vivo es esencial porque convierte la ejecución en evidencia, y sin evidencia no hay evaluación seria, solo impresiones.

Por último, la fase de ejecución no termina cuando se apaga la simulación. ENISA incluye aquí las actividades posteriores inmediatas, especialmente la organización de los datos recolectados y el debriefing[5] estructurado. Se deben conservar registros técnicos, comunicaciones, notas del equipo y retroalimentación de participantes, observadores y facilitadores. Además, el debriefing cumple funciones clave: permite reflexión, genera hallazgos, identifica oportunidades de mejora y fomenta aprendizaje compartido. Incluso la metodología distingue entre hotwash[6] y coldwash[7], mostrando que la conversación posterior también forma parte del valor del ejercicio

Fase 5. Evaluación: donde el ejercicio se convierte en aprendizaje útil

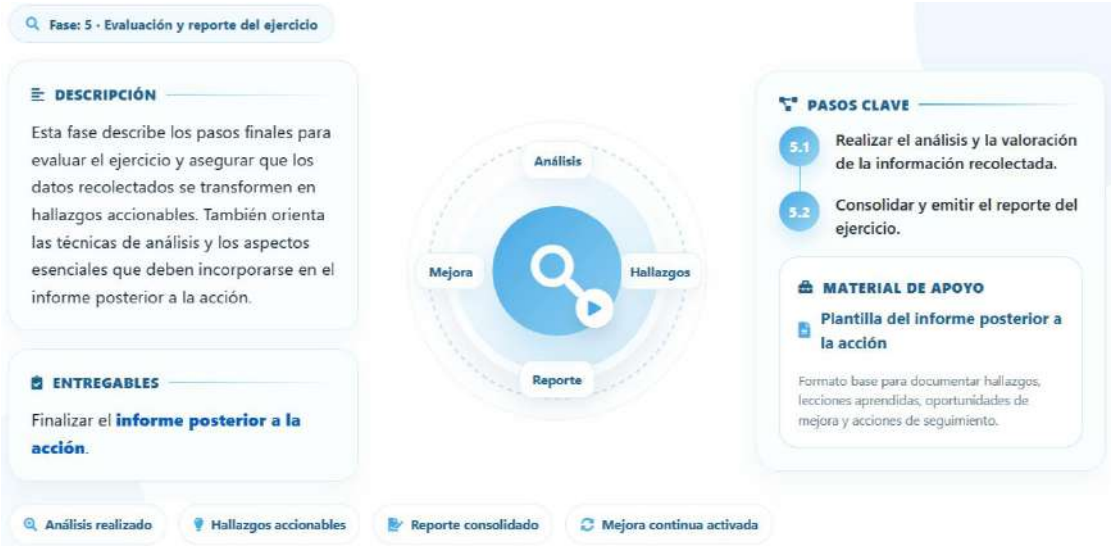
La fase de evaluación ocupa un lugar decisivo dentro de la metodología ENISA, porque es la etapa en la que el ejercicio deja de

[5] Sesión de revisión posterior, realizada después del hotwash, para analizar con mayor calma los resultados, hallazgos y lecciones aprendidas del ejercicio

[6] Sesión inmediata posterior al ejercicio para recoger impresiones, hallazgos iniciales y leacciones aprendidas

[7] Sesión de revisión posterior, realizada después del hotwash, para analizar con mayor calma los resultados, hallazgos y lecciones aprendidas del ejercicio.

ser una experiencia vivida y pasa a convertirse en evidencia, juicio crítico y posibilidad de mejora. El documento la presenta con una pregunta de fondo bastante clara: ¿se cumplieron los objetivos, ¿dónde estuvieron las fallas y qué explica esas brechas? Esa formulación no es menor, porque deja ver que evaluar no consiste en describir lo ocurrido de forma anecdótica, sino en transformar datos dispersos en hallazgos accionables. ENISA incluso advierte que, sin un análisis riguroso, hasta un ejercicio bien ejecutado termina reducido a otro entrenamiento más, sin impacto duradero.



Desde esa lógica, la evaluación parte del tratamiento de la información recolectada durante las fases previas. La metodología recuerda que los datos obtenidos suelen ser de dos tipos, cualitativos y cuantitativos, y que por eso no basta con acumular registros, entrevistas, observaciones o métricas: hay que aplicar técnicas distintas según la naturaleza de la evidencia. En otras palabras, el valor de esta fase no está en cuánto dato se recogió, sino en la capacidad de interpretarlo con método para producir conclusiones confiables y útiles para la organización.

En el caso de los datos cualitativos, ENISA pone el foco en insumos como entrevistas, observaciones y sesiones de debriefing, precisamente porque allí suelen aparecer percepciones, comportamientos, tensiones y fallas de coordinación que no siempre quedan visibles en una métrica. La idea central es que estos insumos deben analizarse de manera sistemática para extraer hallazgos significativos y no quedarse en impresiones generales. Esto es importante

para el boletín porque refuerza una idea muy propia del enfoque europeo: la respuesta en ciberseguridad no se evalúa solo en términos técnicos, sino también en dimensiones humanas, organizacionales y comunicativas.

Por su parte, el tratamiento de los datos cuantitativos busca ofrecer una lectura más medible del desempeño. La metodología vincula esta parte con la estrategia de evaluación definida desde la fase de preparación, donde se habían establecido indicadores, métricas y fuentes de datos. Así, la evaluación no arranca de cero; más bien verifica, con base en evidencia, si los tiempos de respuesta, la precisión en la detección, la efectividad de la coordinación o el nivel de cumplimiento realmente alcanzaron el estándar esperado. Esa coherencia entre preparación y evaluación es clave, porque evita que el análisis posterior se convierta en una lectura improvisada o arbitraria.

Un aspecto especialmente relevante es que ENISA no entiende la evaluación solo como análisis interno, sino también como producción de un resultado documental estructurado: el After-Action Report, o AAR[8]. Según la metodología, este informe es el instrumento que permite pasar de los hallazgos a las mejoras concretas, mediante una documentación cuidadosa de resultados, lecciones identificadas y recomendaciones. Además, el AAR no se concibe como un informe genérico: su circulación debe regirse por el Traffic Light Protocol, lo que permite ajustar el nivel de sensibilidad y divulgación de los hallazgos según el público destinatario. Ahí hay una idea bastante fina: aprender sí, pero sin regalar información sensible al mundo entero.

La estructura propuesta para el AAR también muestra el carácter práctico de esta fase. ENISA señala que normalmente debe incluir un resumen ejecutivo, una visión general del ejercicio, la metodología empleada, los hallazgos y lecciones identificadas, y un apartado orientado a los siguientes pasos o moving forward. Es decir, no se trata solo de registrar fortalezas y debilidades, sino de dejar trazada una ruta de acción para corregir brechas, reforzar capacidades y orientar futuras iteraciones. Evaluar, en este

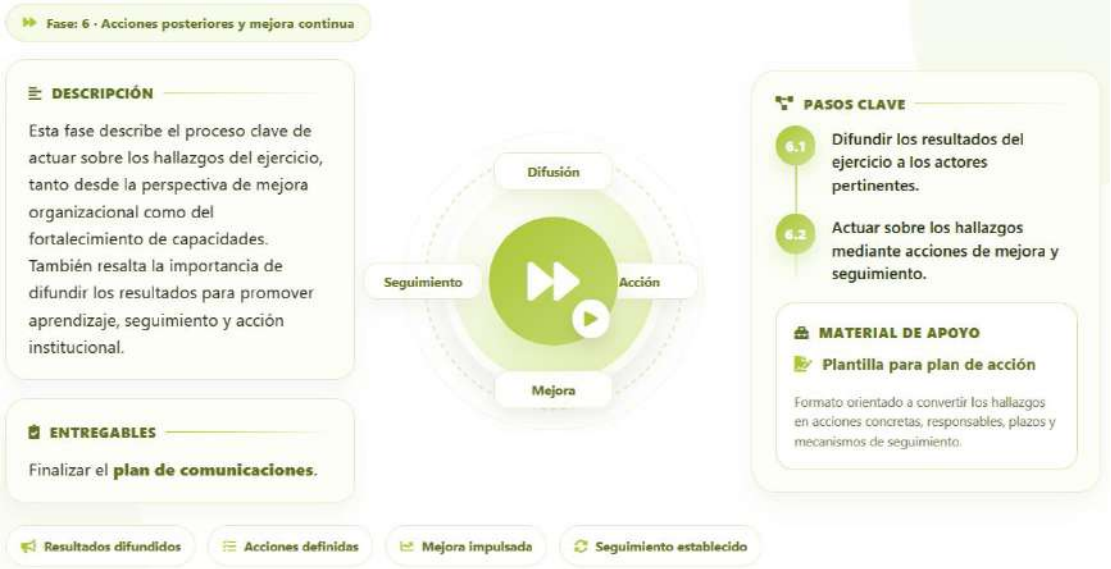
[8] Informe posterior al ejercicio que documenta hallazgos, lecciones aprendidas y acciones de mejora

marco, no es cerrar el ejercicio: es abrir el camino de mejora.

La metodología también introduce una advertencia útil: no siempre el mejor análisis es el más sofisticado. Entre los errores comunes menciona sobreanalizar conjuntos pequeños de datos, confundir correlación con causalidad o usar técnicas complejas cuando bastaría una lectura más simple y robusta. Esa precisión resulta valiosa porque aterriza la evaluación en un terreno realista: lo importante no es impresionar con análisis estadístico innecesario, sino obtener conclusiones claras que permitan fortalecer la preparación y la resiliencia organizacional.

Fase 6. Moving Forward[9]: cuando el ejercicio empieza a producir cambio real

La sexta fase de la metodología ENISA tiene un mérito poco glamuroso, pero decisivo: evita que todo el esfuerzo anterior termine archivado en un informe bonito y olvidado al mes siguiente. Bajo el título Moving Forward, esta etapa se concentra en dos tareas concretas: difundir los resultados del ejercicio y actuar sobre los hallazgos. El documento la presenta como el momento de traducir lo aprendido en mejora organizacional y en fortalecimiento del programa de desarrollo de capacidades. Dicho sin rodeos: aquí se define si el ejercicio sirvió para algo más que llenar una agenda institucional.



[9] Fase orientada a convertir los hallazgos del ejercicio en acciones concretas de mejora, seguimiento y fortalecimiento organizacional.

El primer componente es la difusión de resultados. ENISA sostiene que una difusión efectiva transforma un evento puntual en mejora sostenida, porque impide que los aprendizajes queden encerrados en un grupo pequeño y limita el desperdicio de la inversión realizada. En esta lógica, la diseminación cumple tres propósitos: rendición de cuentas, aprendizaje y acción. Sirve para demostrar que los recursos se utilizaron con sentido, para compartir lecciones dentro de la organización y para generar impulso hacia la implementación de mejoras. La idea central es potente: un ejercicio que no se comunica estratégicamente pierde parte de su valor, porque no mueve cultura, no corrige percepción de riesgo y no moviliza decisiones.

La metodología también es cuidadosa al señalar que no todos los públicos deben recibir el mismo mensaje ni el mismo nivel de detalle. Por eso propone ajustar la difusión según la audiencia, sus intereses y los canales que resulten más adecuados. Los jugadores necesitan comprender su desempeño y sus oportunidades de mejora; los planificadores deben aprovechar los resultados para perfeccionar futuros ejercicios; los observadores aportan retroalimentación especializada; el resto de la organización requiere aumentar conciencia sobre riesgos y medidas de mitigación; la alta dirección necesita una lectura ejecutiva del impacto y de las decisiones estratégicas; y, en ciertos casos, incluso la prensa o el público general pueden ser parte del proceso de comunicación. ENISA propone herramientas diferenciadas para cada uno, como AAR claros o restringidos, sesiones de briefing y debriefing, talleres, intranet, reportes internos, webinars, estudios de caso, infografías, publicaciones web y resúmenes ejecutivos. En el fondo, la lección es bastante clara: comunicar bien también es una forma de gobernar la ciberseguridad.

El segundo componente, probablemente el más importante, es actuar sobre los hallazgos. ENISA no se queda en la idea vaga de "tomar en cuenta las lecciones aprendidas", sino que propone un proceso concreto para construir un plan de acción efectivo. La primera tarea consiste en identificar y priorizar las mejoras a partir del AAR[10] y de las sesiones de retroalimentación. Eso implica

[10] Informe posterior al ejercicio que documenta hallazgos, lecciones aprendidas y acciones de mejora

consolidar debilidades, brechas y oportunidades detectadas, y ordenarlas según impacto, urgencia, severidad, facilidad de implementación, valor estratégico o posibilidad de obtener quick wins. Esta parte es clave porque pone freno a una tentación muy común: querer corregir todo a la vez y terminar corrigiendo poco o nada.

Luego viene la definición de alcance y responsabilidad. La metodología propone clasificar las mejoras según su propósito principal: cambios organizacionales orientados a corregir causas de fondo, o ajustes al programa de fortalecimiento de capacidades, como nuevas formaciones o ejercicios mejor diseñados. A cada acción debe asignársele un responsable claro, e incluso ENISA sugiere considerar matrices tipo RACI para precisar roles cuando los cambios sean complejos. Esta precisión importa mucho porque, sin propietario, la mejora se convierte en tierra de nadie. Y en tierra de nadie, casi siempre gana el olvido.

La fase continúa con la construcción formal del plan de acción. Aquí ENISA recomienda descomponer cada mejora en tareas específicas, definir plazos realistas y documentar responsables y tiempos en una hoja de ruta verificable. No se trata solo de tener una lista de buenas intenciones, sino de convertir los hallazgos en compromisos rastreables. El documento remata esta lógica con un cuarto paso: seguimiento y verificación. Allí se plantea la necesidad de realizar revisiones periódicas, comprobar si las acciones fueron realmente implementadas, medir si generaron las mejoras esperadas y adaptar el enfoque conforme evolucionen los resultados y el contexto. Esta parte le da a la metodología un aire de mejora continua bastante maduro: no basta con ejecutar cambios, hay que validar que funcionen.

Un detalle especialmente valioso es que ENISA no limita esta fase a corregir fallas puntuales del ejercicio más reciente. También plantea que algunos hallazgos deben provocar cambios en la manera en que toda la cartera de ejercicios se planifica, se conduce y se evalúa. Incluso considera buena práctica repetir el ejercicio una vez implementadas acciones correctivas o nuevas actividades de formación, precisamente para comprobar si los ajustes resolvieron las debilidades detectadas. Esa recomendación muestra que, en el enfoque europeo, un ejercicio no es un cierre en sí mismo, sino un insumo para ciclos sucesivos de maduración.

Conclusiones

La metodología de ENISA permite concluir que la respuesta europea en ciberseguridad se está consolidando sobre una lógica mucho más madura que la simple emisión de normas. El enfoque que refleja el documento no se limita a regular o recomendar buenas prácticas, sino que apuesta por desarrollar capacidades reales de preparación, coordinación, ejecución y mejora continua frente a incidentes y crisis cibernéticas. En esa medida, la estrategia de la Unión Europea muestra una evolución clara: pasar de la preocupación normativa a la construcción de resiliencia operativa.

Otro hallazgo relevante es que el valor de un ejercicio de ciberseguridad no radica únicamente en su ejecución, sino en la secuencia completa que lo sostiene. La metodología demuestra que un ejercicio útil debe comenzar con una intención estratégica clara, traducirse en objetivos y alcances bien definidos, prepararse con escenarios plausibles, ejecutarse con control y realismo, evaluarse con criterios verificables y, finalmente, convertirse en acciones de mejora. Esto refuerza una idea central para el boletín: la preparación no puede entenderse como un evento aislado, sino como un proceso estructurado de fortalecimiento institucional.

Asimismo, el documento deja ver que la ciberseguridad, en el enfoque europeo, no es solo un asunto técnico. A lo largo de las seis fases aparecen de manera constante elementos como liderazgo, coordinación interinstitucional, comunicación, toma de decisiones, asignación de responsabilidades y difusión de resultados. Eso significa que la capacidad de respuesta ante un incidente no depende únicamente de herramientas o equipos especializados, sino también de la forma en que la organización articula personas, procesos y decisiones bajo presión. En otras palabras, la resiliencia se construye tanto en el plano técnico como en el organizacional.

Finalmente, una conclusión especialmente importante es que ENISA no concibe los ejercicios como un fin en sí mismos, sino como un mecanismo para generar aprendizaje verificable y cambio real. La insistencia en la evaluación, el after-action report, la priorización de mejoras y el seguimiento posterior muestra que la metodología busca evitar que los ejercicios se conviertan en simulaciones vistosas pero estériles. Desde esta perspectiva, la principal fortaleza del enfoque europeo está en entender que la ciberresiliencia no se declara: se ensaya, se mide, se corrige y se vuelve a poner a prueba. Recomendaciones finales
un ecosistema digital más confiable, sostenible y centrado en las personas.

Recomendaciones

Existen iniciativas regionales relevantes, lo cual indica que el problema no es la ausencia total de esfuerzos, sino su fragmentación, su diferente nivel de madurez y la falta de una articulación más sistemática entre diagnóstico, respuesta, formación y ejercicios. Para América Latina y el Caribe, la primera recomendación es institucionalizar ciclos periódicos de evaluación de madurez en ciberseguridad y usarlos como base de política pública. La región ya cuenta con una línea de trabajo concreta desarrollada por la OEA/CICTE, el BID y el Global Cyber Security Capacity Centre de la Universidad de Oxford, que sirve precisamente para medir capacidades y orientar decisiones. La recomendación, entonces, no es inventar otro termómetro, sino usar mejor el que ya existe y convertir sus hallazgos en hojas de ruta nacionales y sectoriales (Porrúa et al., 2025).

Pasar del diagnóstico a la preparación operativa mediante programas regulares de ejercicios de ciberseguridad. Aquí la región tampoco parte de cero: el propio reporte regional de 2025 destaca que la red CSIRTAméricas, liderada por la OEA, conecta 52 CSIRTs de 22 países para facilitar respuesta a incidentes, intercambio de información y fortalecimiento de capacidades. Lo que falta es conectar esa capacidad regional con una metodología de ejercicios más estructurada, de extremo a extremo, como la propuesta por ENISA. En la práctica, esto significa que los países de la región deberían usar sus redes CSIRT no solo para reaccionar, sino también para ensayar escenarios, probar decisiones, medir tiempos de respuesta y estandarizar lecciones aprendidas antes de la próxima crisis (Porrúa et al., 2025).

Fortalecer la fuerza laboral de ciberseguridad con una lógica regional de roles, competencias y trayectorias formativas. También aquí ya hay una base aprovechable: la OCDE documentó en 2023 la evolución de la demanda de profesionales en Chile, Colombia y México, y mostró que el crecimiento del mercado laboral va acompañado de exigencias más claras en certificaciones, estándares y perfiles técnicos. Esa evidencia sugiere que la región necesita algo más que cursos aislados: requiere marcos compartidos de habilidades, mejor alineación entre oferta educativa y demanda laboral, y rutas de formación técnica y profesional que permitan escalar talento con velocidad y pertinencia. Sin gente preparada, la estrategia termina siendo un PowerPoint caro (OECD, 2023).

Avanzar hacia una mayor convergencia estratégica entre países. El análisis comparado de seis países latinoamericanos muestra que la región ha venido desarrollando estrategias nacionales, pero con ritmos, enfoques y alcances muy desiguales. Esa heterogeneidad no es un detalle menor, porque complica la cooperación, debilita la confianza y genera respuestas asimétricas ante incidentes transfronterizos. Por eso conviene impulsar un núcleo mínimo común para las estrategias nacionales y sectoriales: gobernanza clara, gestión de riesgos, coordinación de crisis, reglas de notificación, protección de infraestructura crítica, desarrollo de capacidades y cooperación internacional. No se trata de uniformar todo, sino de asegurar un piso compartido para que la interoperabilidad regional no dependa del azar (Urbanovics, 2022).

Consolidar un mecanismo regional de inteligencia aplicada y aprendizaje compartido. Esa lógica ya está asomando en iniciativas como el Latin America and Caribbean Cybersecurity Observatory, citado en literatura reciente como espacio de revisión y sistematización de experiencias avanzadas en políticas y prácticas de ciberseguridad. La región debería aprovechar y expandir este tipo de esfuerzos para producir no solo benchmarking, sino también repositorios de escenarios, tipologías de incidentes, prácticas efectivas, errores recurrentes y modelos de madurez reutilizables por gobiernos, sectores críticos y academia. Sin memoria regional, cada país termina aprendiendo solo y pagando la matrícula completa (Figueroa et al., 2025).

El fortalecimiento regional no se debe constituir únicamente desde la lógica técnica o securitaria, sino también desde una perspectiva democrática y de derechos. La literatura reciente sobre América Latina advierte que la creación de capacidades en ciberseguridad no ocurre en el vacío: se cruza con disputas geopolíticas, riesgos de vigilancia y dinámicas de desinformación. Por eso, cualquier agenda regional seria debería incluir salvaguardas de transparencia, supervisión institucional, protección de derechos fundamentales y control sobre el uso de capacidades estatales. La región necesita más capacidad, sí, pero no a costa de normalizar respuestas opacas o expansivas que después nadie pueda contener (Henshaw, 2024).

Referentes

ENISA. (s. f.-a). *Best Practices for Cyber Crisis Management*. Recuperado https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

ENISA. (2025b). *ENISA NIS360 2024*. https://www.enisa.europa.eu/publications/enisa-nis360-2024#contentList

ENISA. (2025b). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

ENISA. (2026). *The ENISA Cybersecurity Exercise Methodology*. https://www.enisa.europa.eu/sites/default/files/2026-02/The%20ENISA%20Cybersecurity%20Exercise%20Methodology.pdf

Figueroa, V., Sánchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security*, *24*(3), 121. https://doi.org/10.1007/s10207-025-01024-0

Henshaw, A. (2024). Capacity Building and Cyber Insecurity in Latin America: Geopolitics, Surveillance, and Disinformation. En A. Mhajne & A. Henshaw (Eds.), *Critical Perspectives on*

Cybersecurity (1.ª ed., pp. 173-193). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197695883.003.0008

OECD. (2023). *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*. OECD Publishing. https://doi.org/10.1787/9400ab5c-en

Porrúa, M., Moncayo, G., Paz, S., Nowersztern, A., Bejarano, J. F., Baudino, M. F., Bordese, M. P., Barret, K.-A., Baena, C. E., Jaramillo, M., Garces, O., & Isidro, A. (2025). *2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean*. Inter-American Development Bank. https://doi.org/10.18235/0013872

Urbanovics, A. (2022). Cybersecurity Policy-Related Developments in Latin America. *Academic and Applied Research in Military and Public Management Science*, *21*(1), 79-94. https://doi.org/10.32565/aarms.2022.1.6

Contactenos

📧 **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!