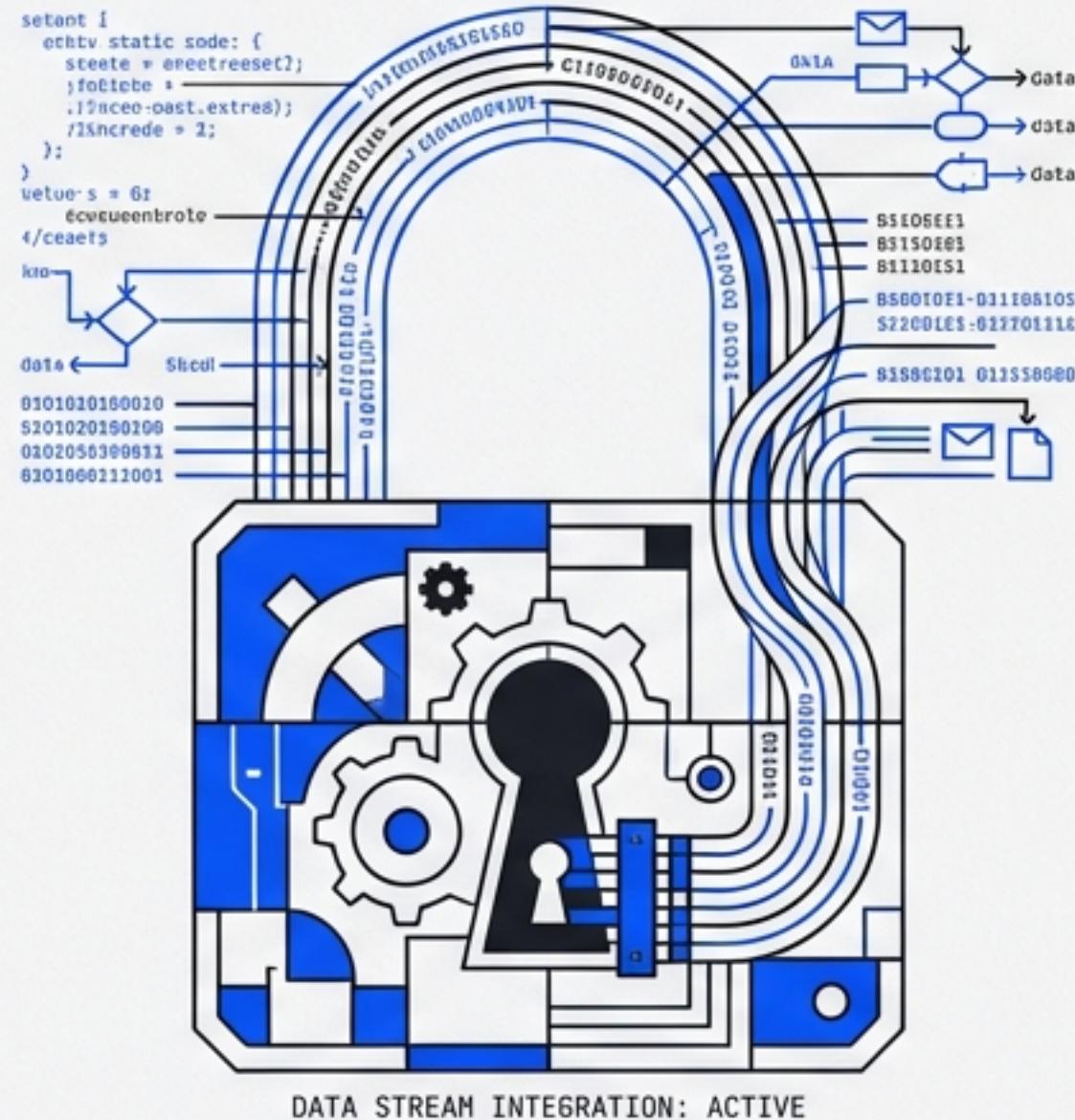


INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD

GUÍA OPERATIVA



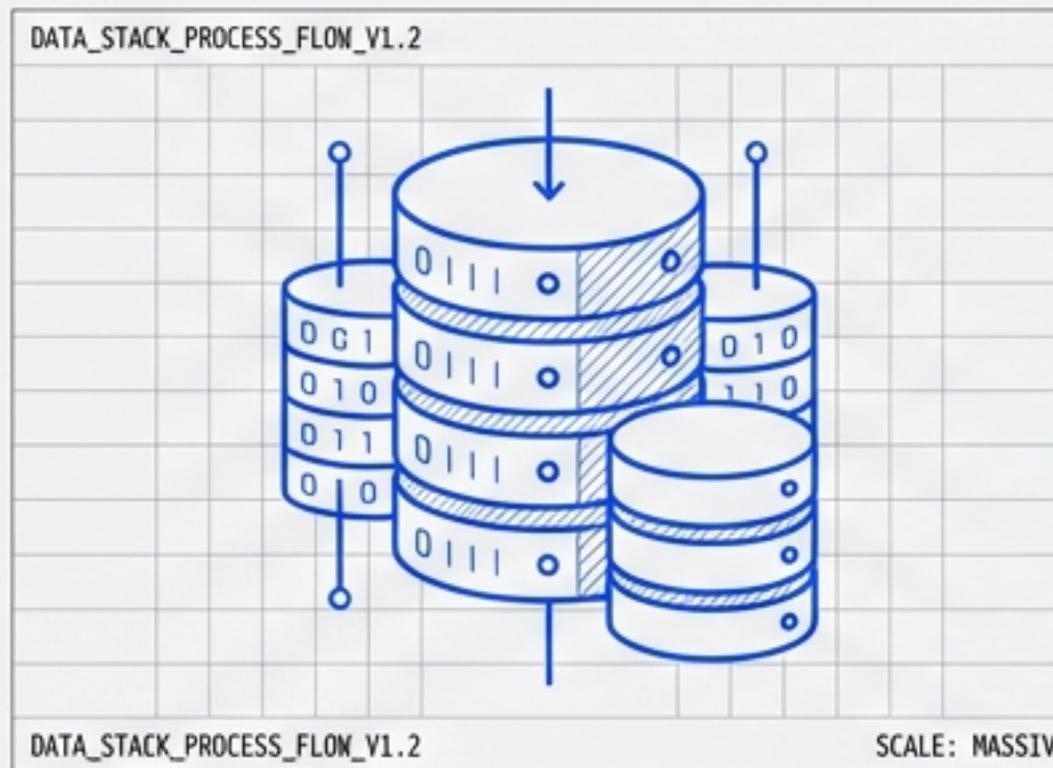
Estrategias, Prompting y Casos
de Uso para Profesionales

METODOLOGÍA: T-C-R-E-I
VERSIÓN: 1.0



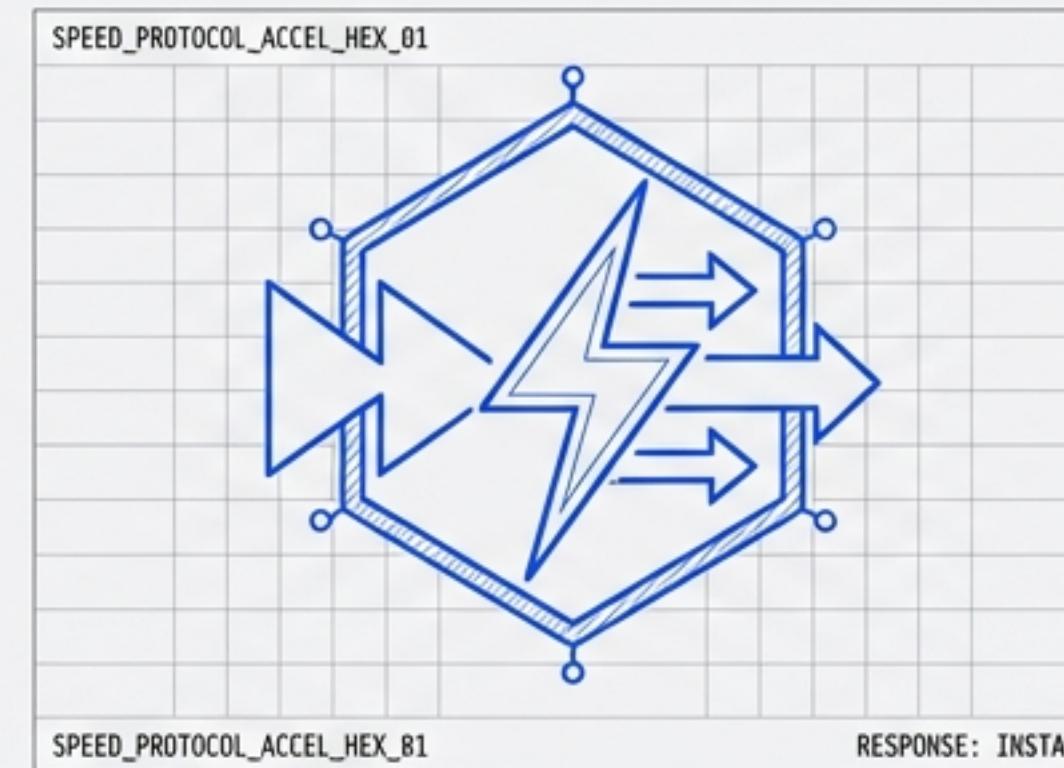
LA ADOPCIÓN TECNOLÓGICA COMO IMPERATIVO DE DEFENSA

En el panorama actual, la IA no es un lujo, es la única vía para adelantarse a las amenazas modernas. Su implementación transforma la operatividad del profesional de seguridad.



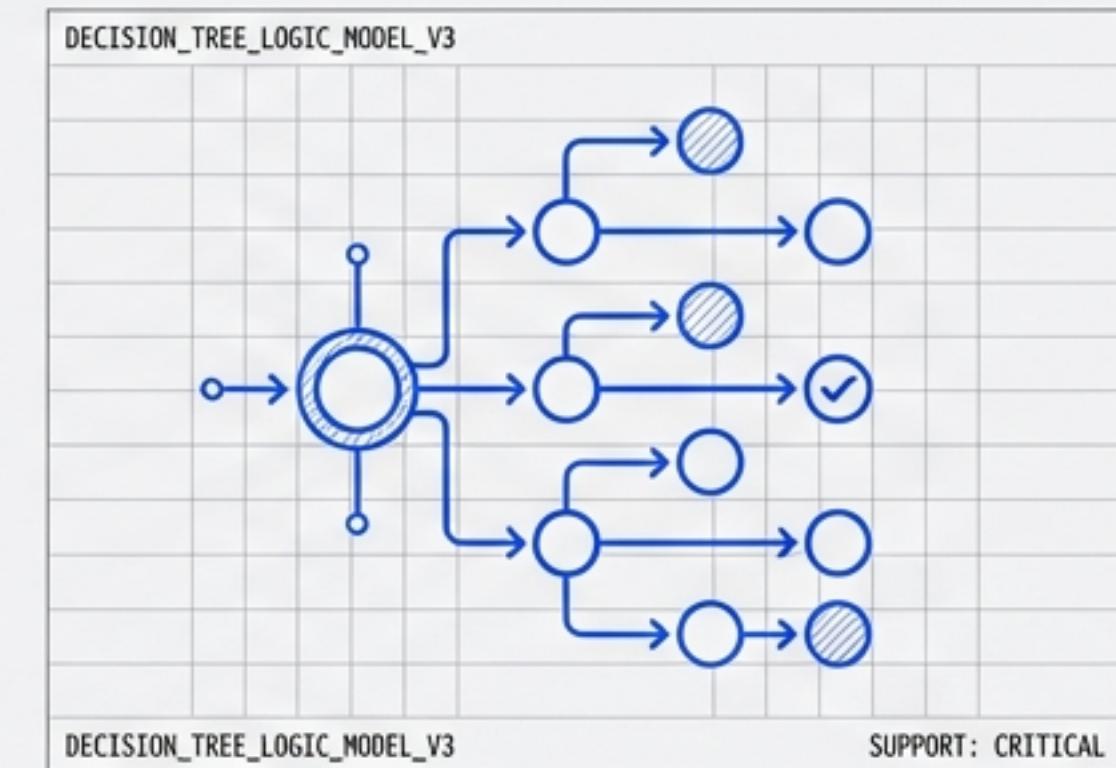
Análisis Masivo

Procesamiento de flujos de datos a escalas inalcanzables manualmente.



Agilidad

Aceleración drástica en las comunicaciones y reportes.



Decisión Informada

Soporte crítico para la toma de decisiones basada en datos.

LA IA COMO ARMA DE DOBLE FILO



EL ALIADO (DEFENSA)

- ✓ Aumento de productividad
- ✓ Análisis de datos y patrones
- ✓ Automatización de rutinas

LA AMENAZA (ATAQUE)

- ⚠ Ataques sofisticados automatizados
- ⚠ Evasión de detección
- ⚠ Explotación a alta velocidad

CONCLUSIÓN: Es vital dominar estas herramientas para proteger los propios sistemas y mantenerse un paso por delante.

IA GENERATIVA (GenAI): EL MOTOR OPERATIVO

Tecnología capaz de generar nuevo contenido mediante **instrucciones (prompts)**.

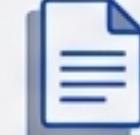


HERRAMIENTAS:

- Gemini
- ChatGPT
- Copilot
- Claude

CREACIÓN

Informes,
documentación,
datos sintéticos.



ANÁLISIS

Resumen de reportes,
transcripciones.



INVESTIGACIÓN

Consultas sobre
malware y ransomware.

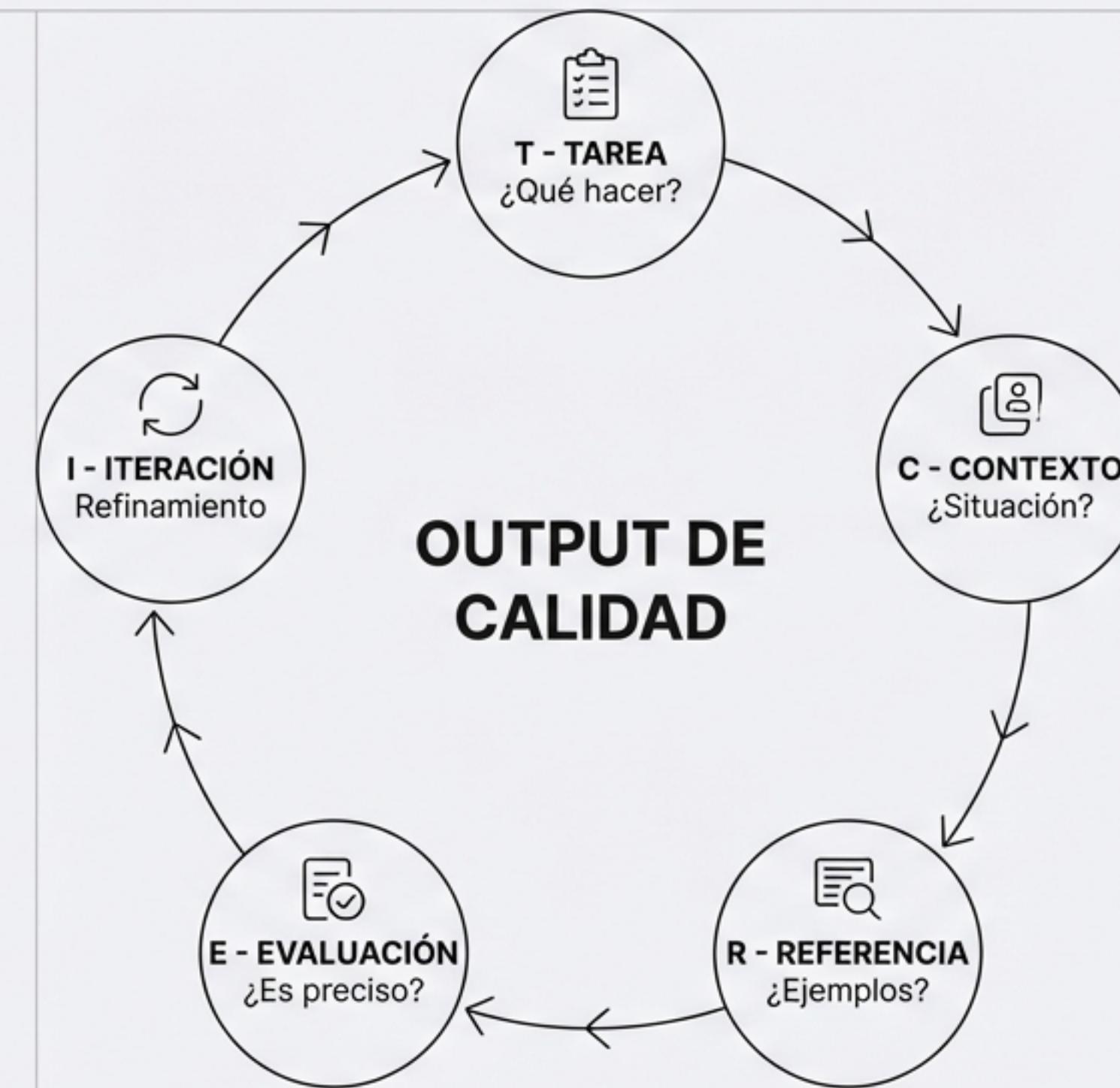


TRIAGE

Análisis de phishing,
depuración.



METODOLOGÍA DE PROMPTING: MARCO T-C-R-E-I



La calidad del resultado depende de la calidad de la instrucción.

CONFIGURACIÓN DEL PROMPT: TAREA Y CONTEXTO

1. TAREA (TASK)

PERSONA: Definir el rol (ej: 'Analista SOC Senior').

FORMATO: Definir la salida (Lista, JSON, Tabla).

2. CONTEXTO (CONTEXT)

✗ DEFICIENTE

"Ideas para un regalo de 30€"

✓ CONTEXTUALIZADO

"Ideas para un regalo de 30€ para una persona de 29 años que practica esquí y le gustan los deportes de invierno."

REFINAMIENTO: REFERENCIA, EVALUACIÓN E ITERACIÓN

REFINAMIENTO: REFERENCIA, EVALUACIÓN E ITERACIÓN

R - REFERENCIA



Añadir documentos previos
o guías de estilo para
emular lógicas específicas.

E - EVALUACIÓN



Análisis crítico: ¿Es
precisa la información?
¿Cumple el objetivo?

I - ITERACIÓN

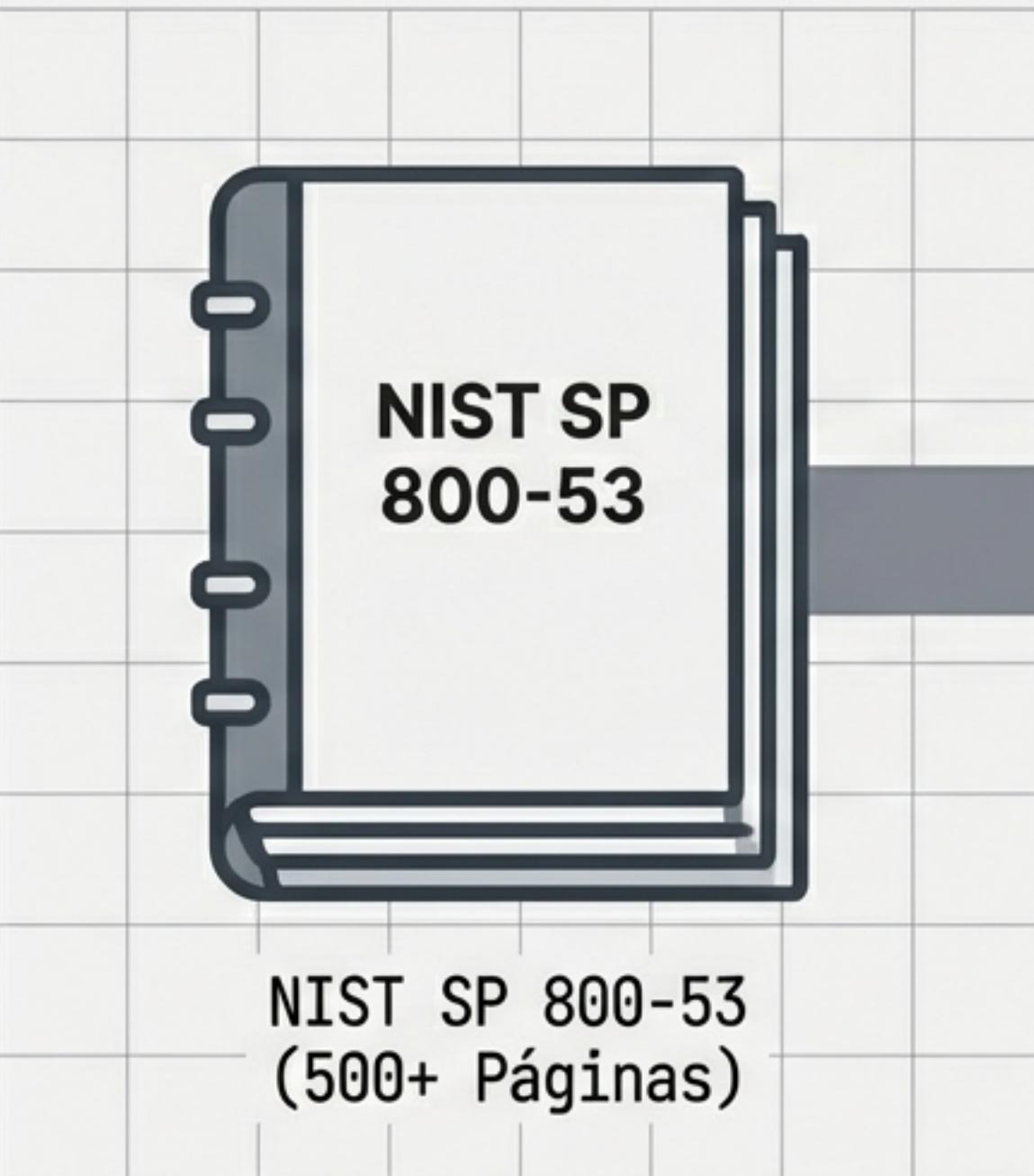


El ciclo de ajuste. La IA
funciona mejor mediante
ciclos repetidos.

INSIGHT: El primer resultado raramente es el producto final.

CASO DE USO A: CUMPLIMIENTO (NIST)

Navegando la complejidad de NIST SP 800-53



LOCALIZACIÓN

Identificación rápida: Control SI-5 (Seguridad y Privacidad).

TRADUCCIÓN

Explicación técnica simplificada para implementación.

ADAPTACIÓN

Distinción: Requisitos obligatorios vs. opcionales.

■ **PROMPT TIP:** Solicitar explicación por niveles ('Analista Junior' vs 'Estudiante').

CASO DE USO B: SEGURIDAD EN CÓDIGO (PYTHON)

Detección y corrección automática de vulnerabilidades en código Python.

INPUT (Con Error)	OUTPUT (Corregido por IA)
<p>División por cero: "usuarios" podría ser 0, provocando un error de ejecución crítico.</p> 	<pre>def calcular_metricas(usuarios): return total / usuarios # Riesgo</pre> <pre>try: return total / usuarios except ZeroDivisionError: return 0 # Manejo elegante</pre>



Depuración Automática

Identifica y aisla errores en el flujo de ejecución.



Control de Errores (Try/Except)

Añade bloques "try-except" para gestionar excepciones sin detener el programa.

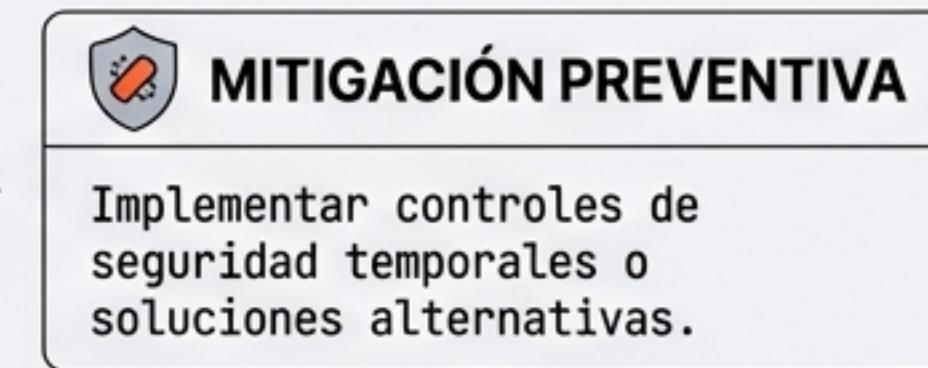
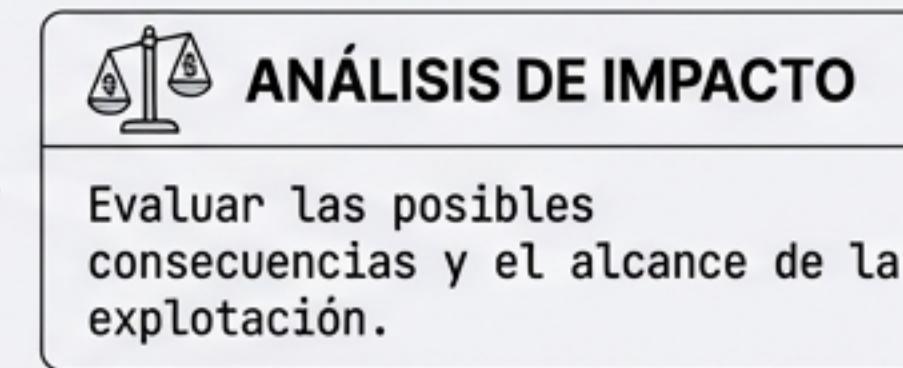
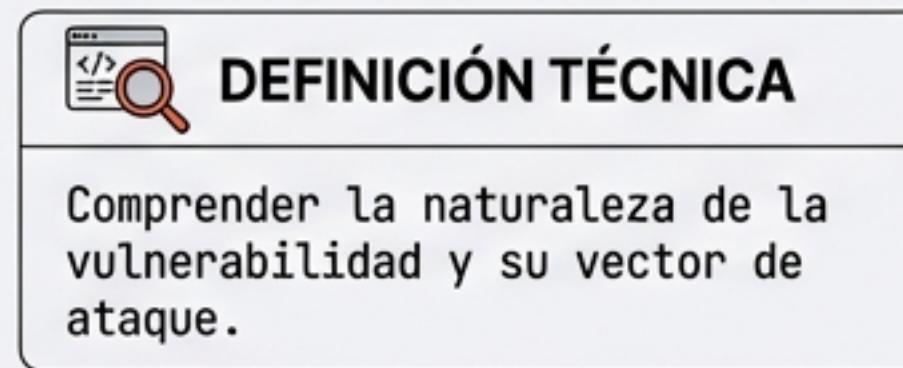
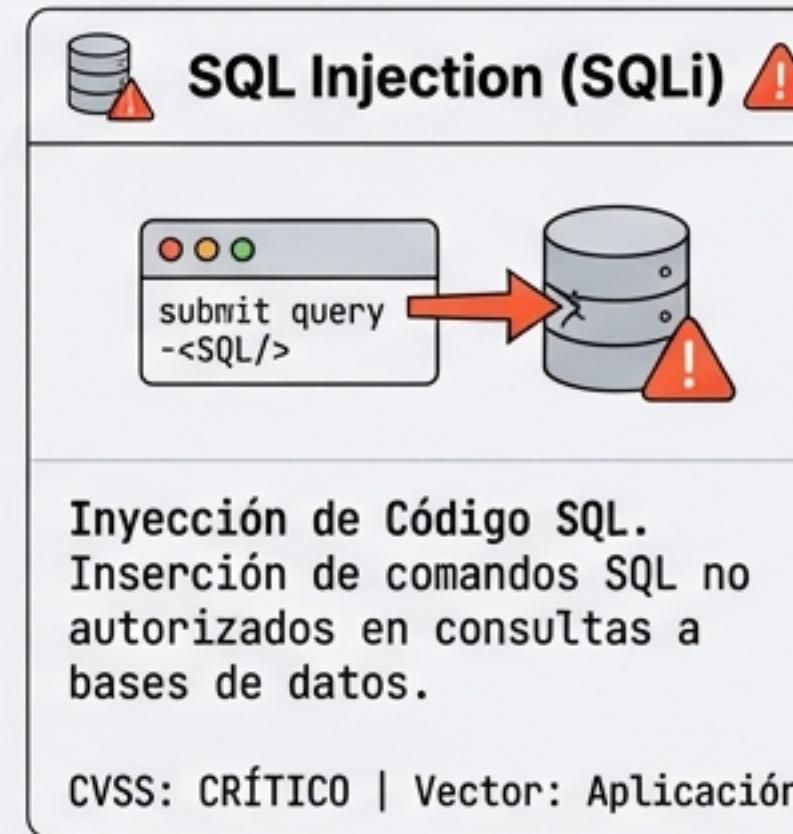
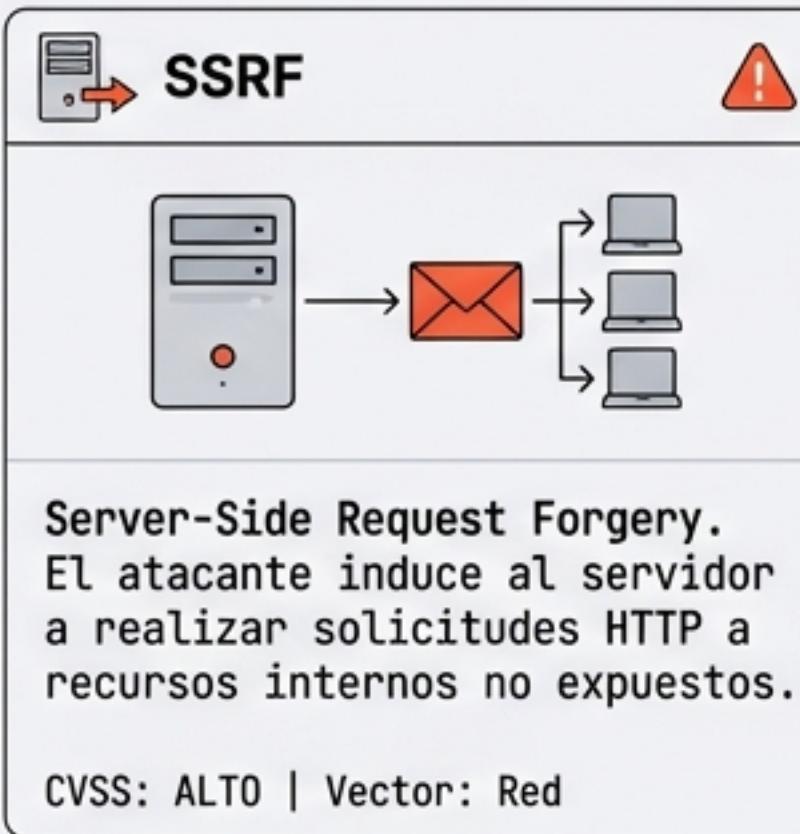


Generación de Documentación

Crea comentarios y documentación explicativa para el código corregido.

CASO DE USO C: ANÁLISIS DE VULNERABILIDADES

Identificación y mitigación sistemática de fallas de seguridad.

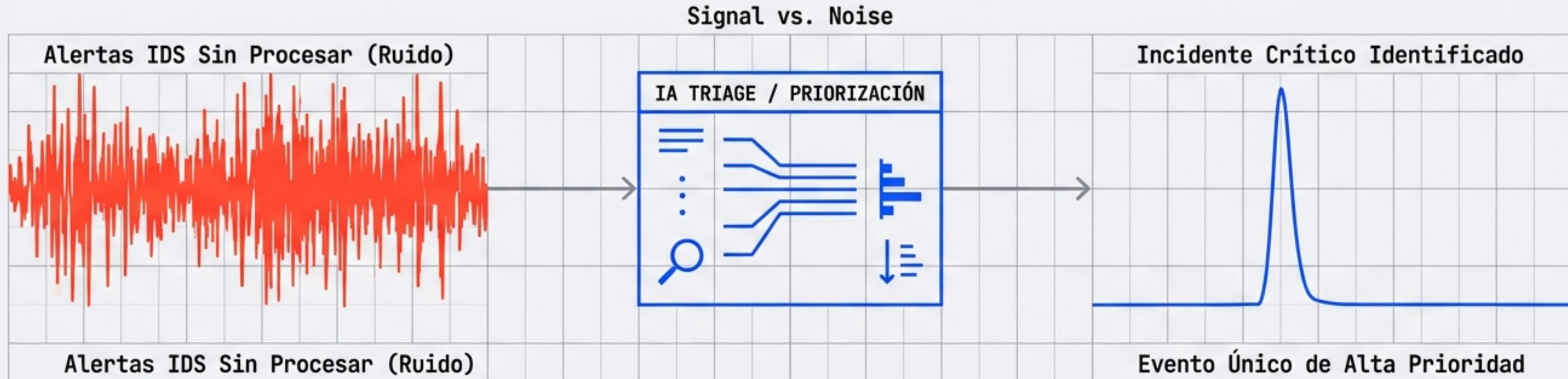


Sugerencias de contención antes del parche oficial.



CASO DE USO D: DETECCIÓN Y RESPUESTA (SOC)

Análisis y mitigación automatizada de amenazas en el centro de operaciones de seguridad.



	Priorización
	Clasificación por gravedad. Evaluación instantánea del riesgo basada en múltiples indicadores.

	Tácticas
	Detección de ataques de distracción (DDoS vs Intrusión). Correlación de eventos para diferenciar ataques reales de señuelos.

	Soporte IRP
	Redacción de procedimientos en tiempo real. Generación automática de pasos de respuesta y documentación para el analista.

EL PRINCIPIO HUMAN-IN-THE-LOOP

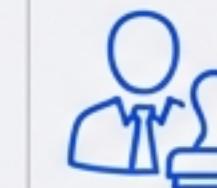


La IA es una herramienta complementaria, no un sustituto.



VERIFICACIÓN OBLIGATORIA

Contrastar siempre con fuentes confiables.



RESPONSABILIDAD FINAL

El profesional responde por la salida, no el algoritmo.



RESPONSABILIDAD FINAL

El profesional responde por la salida, no el algoritmo.

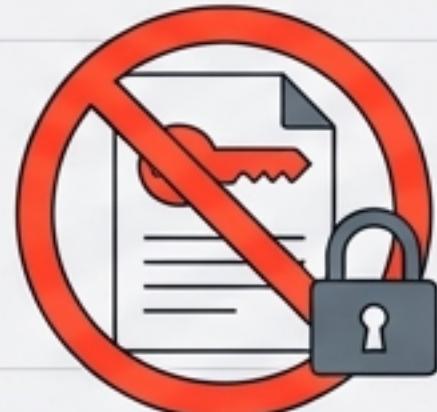


ENTRENAMIENTO HUMANO

Usar la inteligencia humana para refinar el sistema.

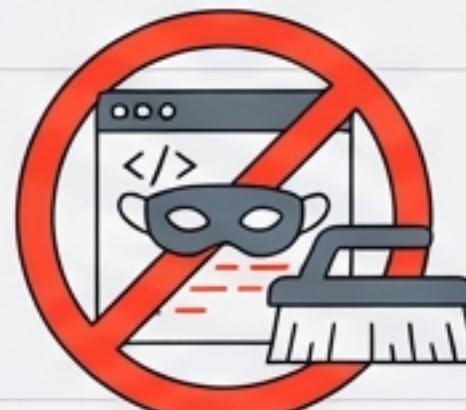
PRIVACIDAD Y DATOS: LA ZONA ROJA

WARNING / ALERTA



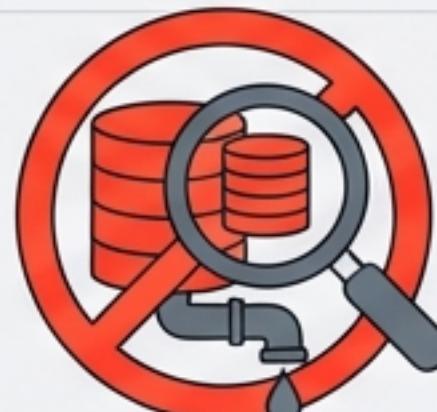
INFORMACIÓN CONFIDENCIAL

NUNCA introducir secretos comerciales o PII (Datos Personales).



SANITIZACIÓN DE CÓDIGO

Eliminar variables sensibles/IP antes de pegar en la IA.



PRECISIÓN DE CONTEXTO

El exceso de contexto aumenta el riesgo de fuga de datos.

CONSEJOS PARA LA EFICIENCIA

1



INPUT DE VOZ

Dictado para mensajes complejos rápidos.

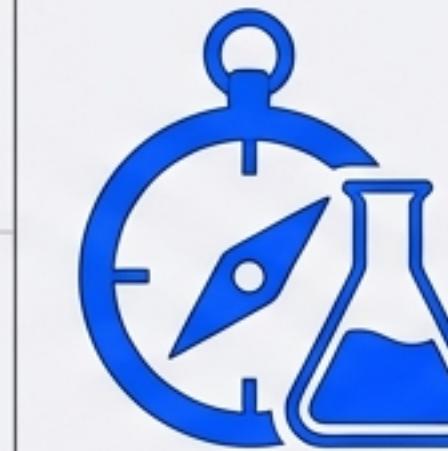
2



SIMULACIÓN (ROLEPLAY)

Entrevistas simuladas para practicar comunicación técnica.

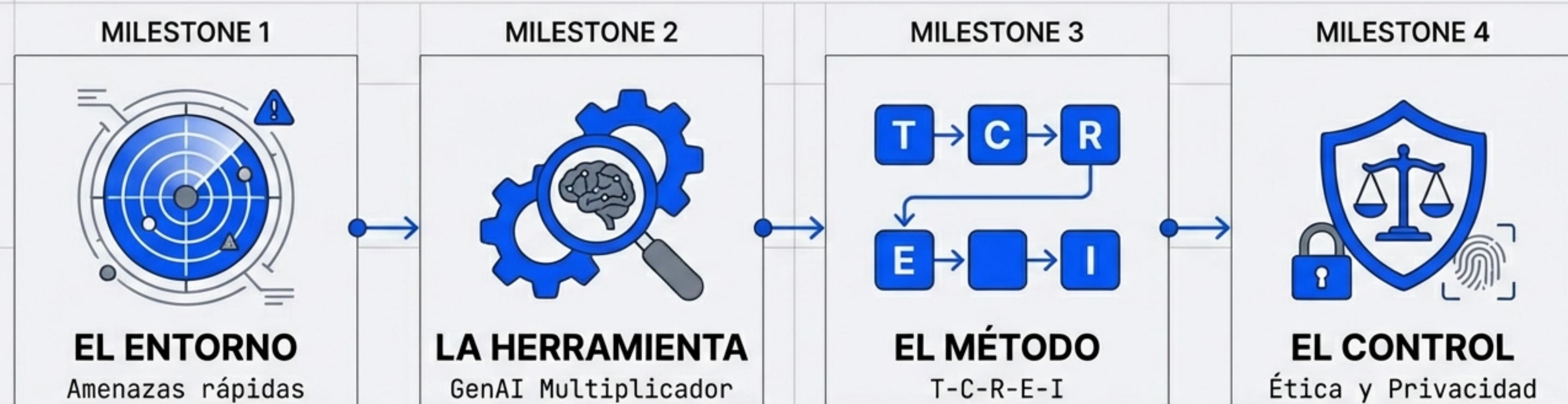
3



EXPLORACIÓN CONTINUA

Experimentación diaria con nuevas rutas de interacción.

CONCLUSIÓN: HACIA UNA OPERATIVA AUMENTADA



La adopción metodológica de la IA define la próxima generación de defensa en ciberseguridad.

FIN DE LA GUÍA