keep coding

Machine Learning y Ciberseguridad

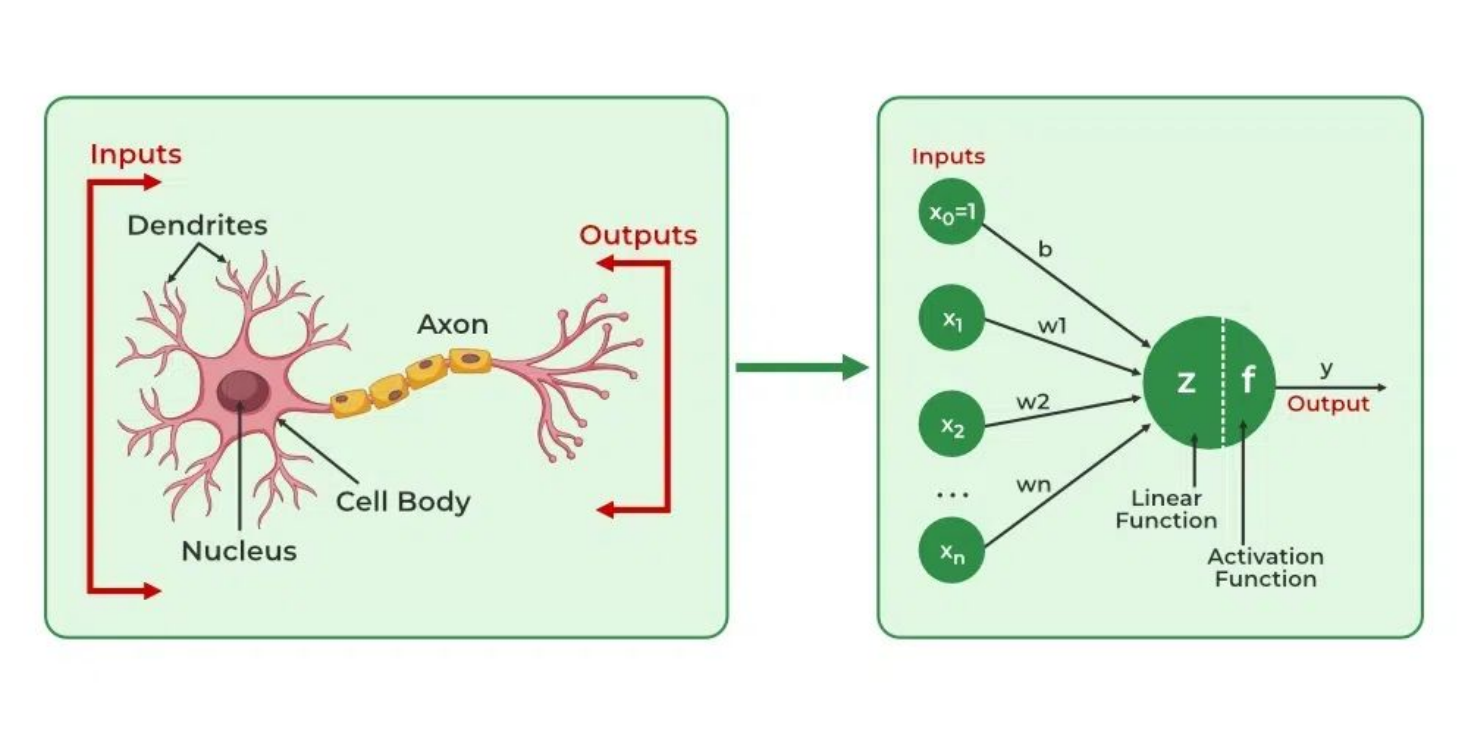
Deep Learning y el papel de la ciberseguridad

Índice

¿Qué es Deep Learning?

- DL es una rama de ML que usa redes neuronales profundas para aprender de datos complejos.
- Diferencia con ML tradicional: Maneja datos no estructurados como imágenes o texto automáticamente.
- En cyber: Predice ataques analizando patrones en logs o tráfico de red, entre muchas otras.
- Beneficios: Mayor precisión en detección de threats en tiempo real.

¿Qué es Deep Learning?



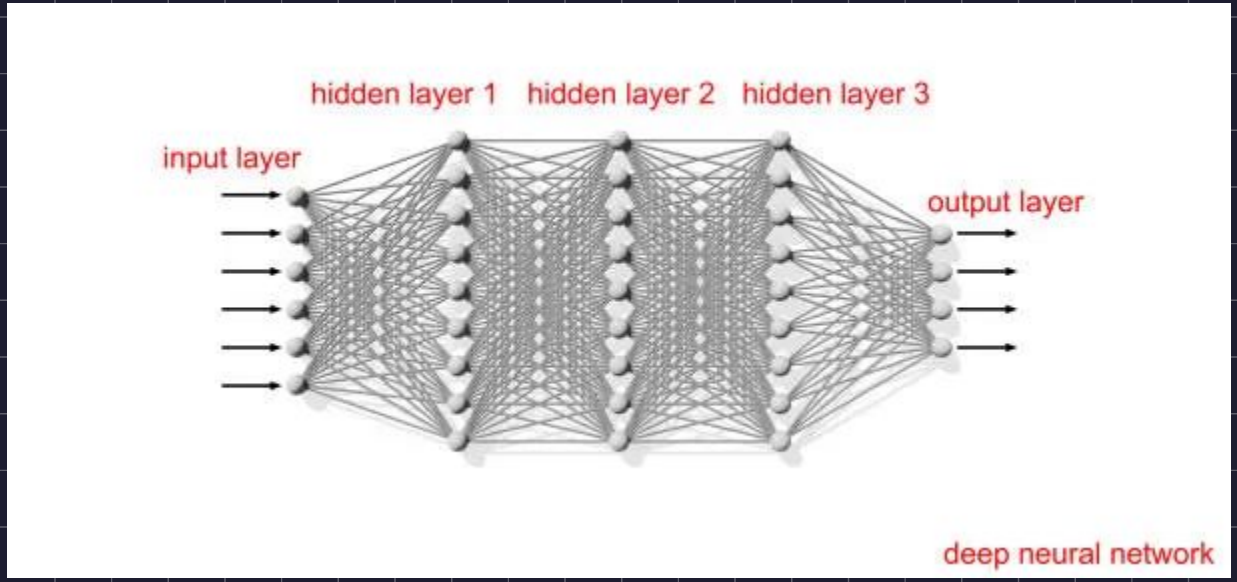
keep coding

Redes Neuronales Básicas

- Estructura: Capas de entrada, ocultas y salida, con pesos que se ajustan durante entrenamiento.
- Proceso: Datos entran, se procesan con activaciones (e.g., ReLU), y salen predicciones.
- En cyber: Detecta anomalías en comportamiento de usuarios (UBA).

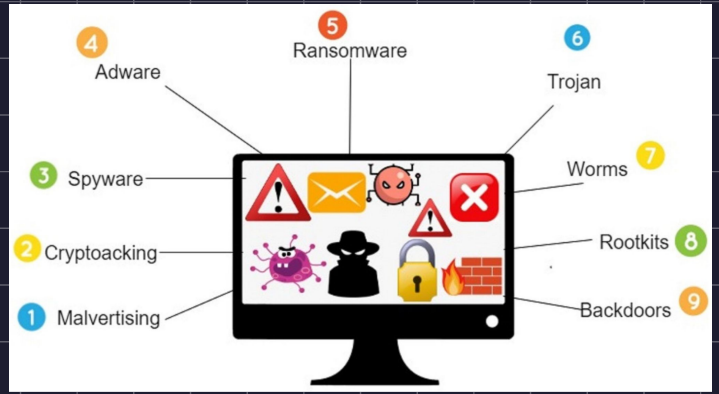
keep coding

Redes Neuronales



DL en Ciberseguridad

- Aplicaciones: Detección de malware (analizando binarios como imágenes), predicción de breaches.
- Herramientas: TensorFlow o PyTorch para modelos personalizados.
- Caso real: Sistemas como Darktrace usan DL para alertas autónomas.
- Ventaja: Maneja big data de IoT y cloud security.



Desafíos de DL en Cyber

- Overfitting y generalización pobre: Modelos que memorizan datos de entrenamiento pero fallan ante variaciones reales en threats, abriendo especializaciones en técnicas de regularización y validación cruzada avanzada.

- Ataques adversariales: Manipulación de inputs por parte de atacantes para evadir detección, destacando ramas como IA robusta y defensas adversariales en ciberseguridad.

keep coding

Desafíos de DL en Cyber

- Calidad e imbalance de datos: Datasets incompletos, ruidosos o desbalanceados que reducen la precisión, ideal para especializarse en ingeniería de datos, augmentation y aprendizaje semi-supervisado.

- Falta de explicabilidad: Modelos "caja negra" que dificultan entender decisiones, sugiriendo áreas como XAI (eXplainable AI) y auditoría de modelos en entornos regulados.

Desafíos de DL en Cyber

- Complejidad y escasez de talento: Requiere expertos para implementación y tuning, con oportunidades en formación en ML para cyber y roles híbridos como DevSecOps con IA.

- Alto consumo de recursos y costos: Entrenamiento intensivo en cómputo y energía, promoviendo especializaciones en optimización de modelos, edge AI y computación eficiente para seguridad.

keep coding

Introducción a Computer Vision

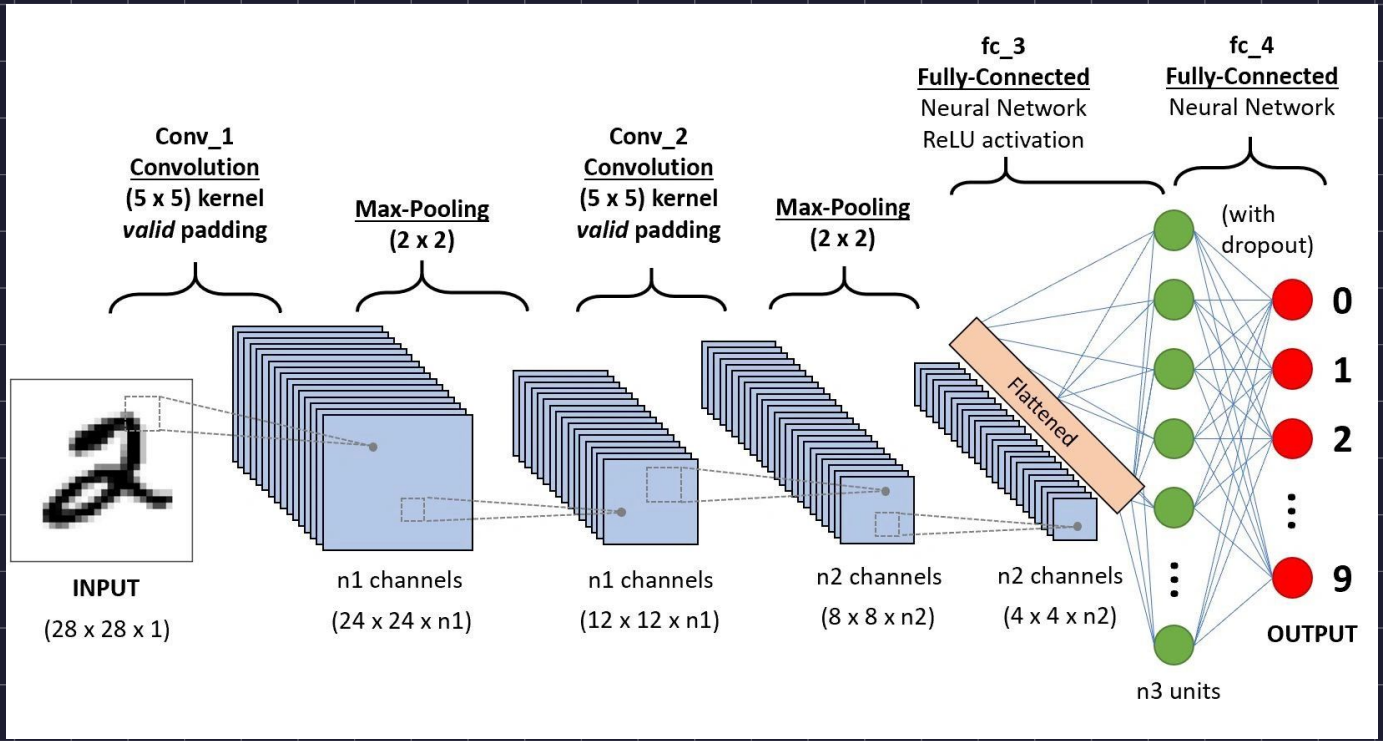
- CV permite a las máquinas "ver" e interpretar imágenes/vídeos.
- Basado en DL: Extrae features como bordes, formas.
- En cyber: Analiza capturas de pantalla para detectar phishing visual o deepfakes.
- Herramientas gratuitas: OpenCV para prototipos rápidos.

Introducción a Computer Vision
Redes Convolucionales (CNNs)

- Arquitectura: Capas de convolución, pooling y fully connected.
- Función: Detecta patrones locales en imágenes (e.g., filtros para texturas). Replica el funcionamiento del cortex cerebral.
- Ejemplo: Clasificar imágenes de malware (e.g., visualizando ejecutables como grayscale).
- Fácil de usar: Modelos pre-entrenados en Hugging Face (el github de ML).
- Y mucho más

keep coding

CNNs



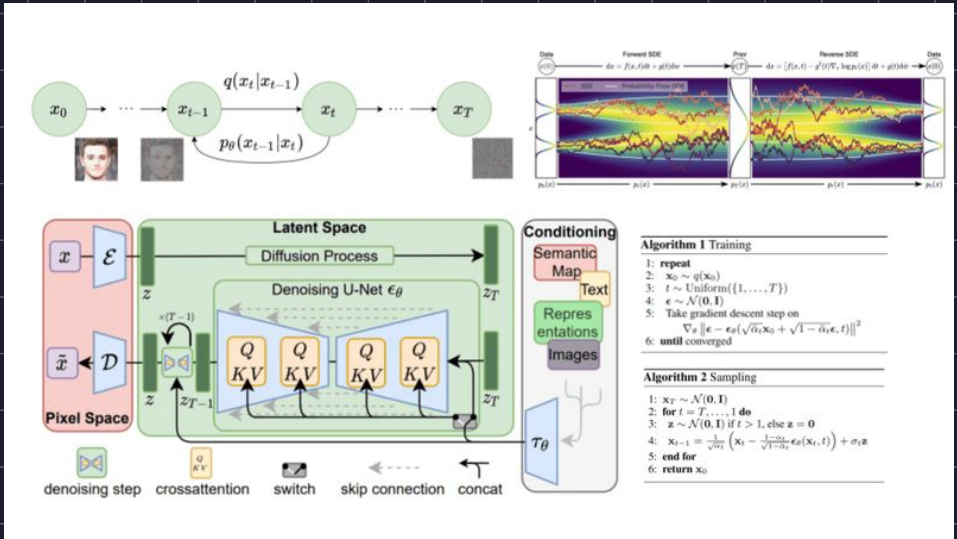
keep coding

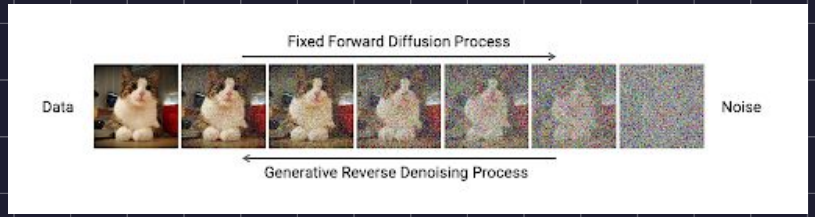
Introducción a Computer Vision
Modelos de Difusión

- Proceso forward (difusión): Se agrega ruido Gaussiano gradual a una imagen hasta convertirla en ruido puro, simulando una cadena de Markov para modelar la distribución de datos.
- Proceso reverse (denoising): Una red neuronal (e.g., U-Net) aprende a predecir y eliminar el ruido paso a paso, reconstruyendo la imagen original desde el ruido.
- Entrenamiento: Minimiza la diferencia entre ruido predicho y real, permitiendo generar nuevas imágenes de alta calidad en CV.

keep coding

Modelos de Difusión





keep coding

Computer Vision en Ciberseguridad

keep coding

Computer Vision en Ciberseguridad

- Reconocimiento facial para control de acceso seguro: Identifica individuos en entornos físicos, abriendo especializaciones en biometría y sistemas de autenticación híbrida físico-digital.

- Detección de intrusiones en tiempo real: Analiza videos para identificar amenazas en vigilancia, destacando ramas como AI en sistemas de seguridad perimetral y monitoreo automatizado.

keep coding

Computer Vision en Ciberseguridad

- Prevención de ingeniería social: Detecta comportamientos anómalos en espacios físicos, ideal para especializarse en detección de anomalías y fusión de CV con ciberseguridad conductual.

- Identificación de deepfakes y fraudes visuales: Verifica autenticidad en videos o imágenes para combatir estafas, sugiriendo áreas como IA generativa defensiva y verificación de medios digitales. Generación y detección de imágenes realistas con los modelos de difusión.

keep coding

Computer Vision en Ciberseguridad

- Detección de objetos prohibidos: Como armas en vigilancia, promoviendo especializaciones en object detection y pose estimation para seguridad pública y empresarial.

- Tendencias 2025: Integración multimodal (CV + audio) para threat detection avanzada, con oportunidades en edge computing y AI para ciberseguridad física.

Desafíos de CV en Cyber

- Iluminación variable y oclusiones en imágenes reales.
- Privacidad: Manejo ético de datos biométricos.
- Soluciones: Transfer learning de modelos como ResNet.

Introducción a LLMs

- LLMs son modelos de lenguaje grandes basados en transformers (e.g., GPT, BERT, Llama).
- Capacidades: Generan texto, resumen, clasifican, automatizan.
- En cyber: Analizan logs o emails para threats, automatizan pentesting o análisis de vulnerabilidades.
- Acceso fácil: APIs como Hugging Face o ChatGPT/Grok.

keep coding

Arquitectura de Transformers

- Componentes: Attention mechanisms, encoders/decoders.
- Ventaja: Resuelve el vanishing problem. Maneja secuencias largas aumentando el contexto (e.g., hilos de correos completos).

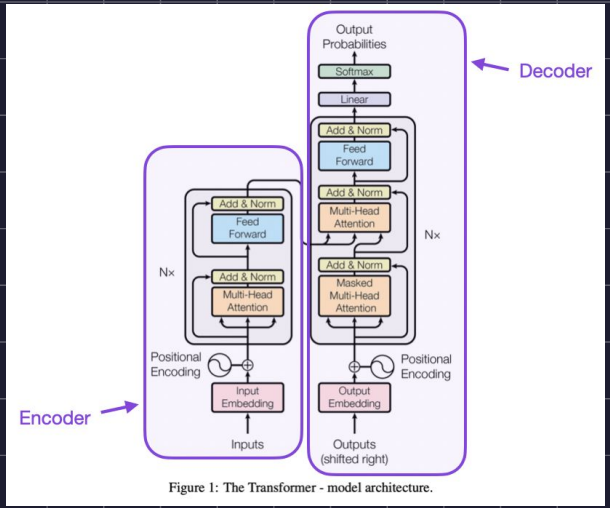


Figure 1: The Transformer - model architecture.

LLMs en Defensa Cyber

- Detección de amenazas y phishing: Analizan patrones en correos y logs para identificar estafas automatizadas, abriendo especializaciones en procesamiento de lenguaje natural y detección en tiempo real.

- Análisis de vulnerabilidades y malware: Evalúan código y hardware para detectar debilidades, ideal para especializarse en inteligencia de amenazas y análisis forense digital.

LLMs en Defensa Cyber

- Automatización de respuestas e informes: Generan alertas y resúmenes de incidentes, destacando ramas como respuesta autónoma a incidentes y DevSecOps con AI.

- Inteligencia de amenazas y detección de anomalías: Identifican patrones tempranos en redes, sugiriendo áreas como user behavior analytics y machine learning predictivo.

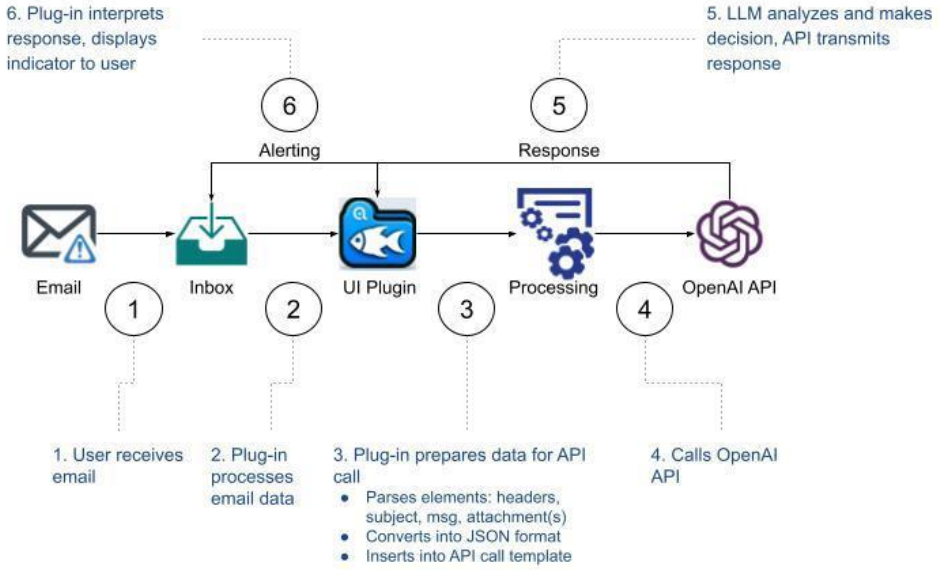
LLMs en Defensa Cyber

- Simulación de ataques y entrenamiento defensivo: Crean escenarios para probar defensas, promoviendo especializaciones en red teaming y simulación basada en AI.

- Tendencias 2025: Integración en plataformas nativas LLM para email y cloud security, con oportunidades en AI ethics y escalabilidad en entornos empresariales.

LLMs en Defensa Cyber, ejemplo

Process Flow



LLMs en Ataques y Desafíos

- Ataques de inyección de prompts: Manipulación de entradas para generar outputs maliciosos, destacando ramas como safeguards de AI y testing de vulnerabilidades en LLMs.

- Fuga de datos y privacidad: Exposición de información sensible durante entrenamiento o uso, ideal para especializarse en data governance y encriptación diferencial.

keep coding

LLMs en Ataques y Desafíos

- Envenenamiento de modelos: Alteración de datasets para sesgar predicciones, sugiriendo áreas como supply chain security y detección de poisoning en ML.

- Generación de contenido malicioso: Creación de phishing o malware automatizado por atacantes, abriendo oportunidades en monitoreo de AI generativa y ethical hacking.

LLMs en Ataques y Desafíos

- Hallucinations y bias: Producción de información falsa o discriminadora en detección de threats, promoviendo especializaciones en explainable AI y fairness auditing.

- Alto costo y escalabilidad: Recursos intensivos para implementación segura, con campos en optimización de LLMs y edge computing para cyberdefensa.

keep coding

Integración de DL, CV y LLMs

- Sistemas híbridos para detección multimodal: Combinan CV para analizar imágenes/deepfakes, LLMs para texto/logs y DL para predicciones en threats, abriendo especializaciones en fusión de datos y AI integrada.

- Automatización en threat intelligence: DL procesa big data, CV verifica visuales y LLMs generan informes, ideal para ramas como SOC automation y real-time analytics.

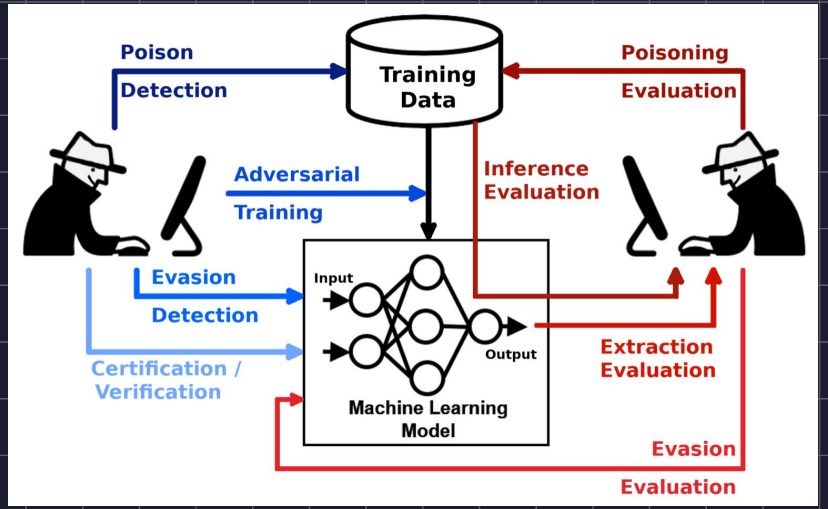
Integración de DL, CV y LLMs

- Defensa contra ataques adversariales: Uso conjunto para robustez, como CV+DL para anomalías visuales y LLMs para contexto textual, destacando áreas en adversarial training y cyber resilience.

- Aplicaciones en cloud y IoT security: Integración para monitoreo distribuido, sugiriendo especializaciones en edge AI y secure AI frameworks.

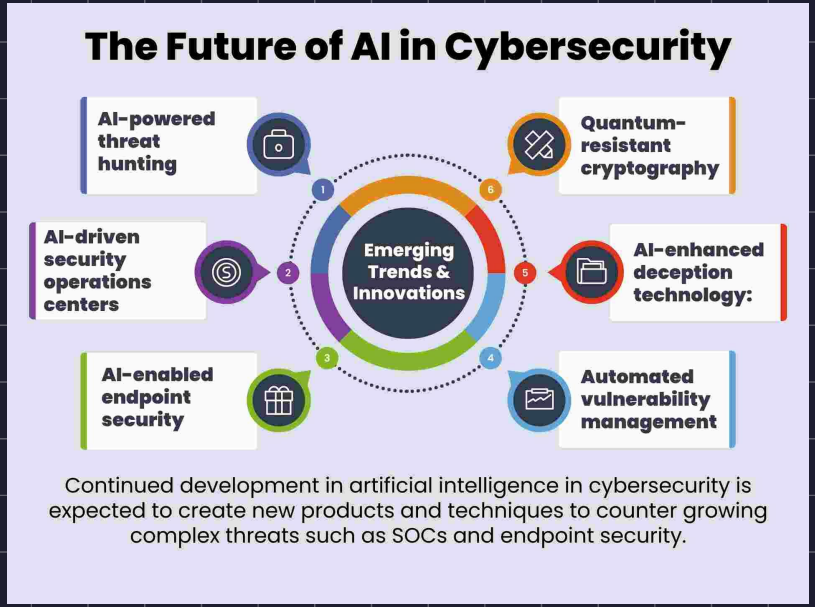
Integración de DL, CV y LLMs

- Herramientas open source: Frameworks como TensorFlow para DL, OpenCV para CV y Hugging Face para LLMs, con oportunidades en DevSecOps y prototipado híbrido.



Tendencias Futuras en 2025+

- AI generativa para simular ataques.
- Quantum-resistant DL en cyber.
- Ética: Bias y privacidad en modelos.



www.keepcoding.io cursos@keepcoding.io (+34) 916 33 1779

Cuerpo de texto

Título sección

Texto extra

Título sección

Texto extra

Cuerpo de texto

keep coding

Título solo

Cuerpo de texto

keep coding

Título combinado

Cuerpo de texto

keep coding

Título Largo

keep coding

TÍTULO APARTADO ESPECÍFICO

TÍTULO APARTADO ESPECÍFICO

Ejemplo Bootcamp Web

Proyecto Final Web

Ejemplo Bootcamp Ciber

Proyecto Final Ciber

Cuerpo de texto (si aplica)

Título elementos

Elemento 1

Cuerpo

Elemento 2

Cuerpo

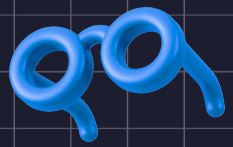
Elemento 3

Cuerpo

Título elementos V2

Elemento 1	Elemento 2	Elemento 3
Cuerpo	Cuerpo	Cuerpo

www.keepcoding.io cursos@keepcoding.io (+34) 916 33 1779













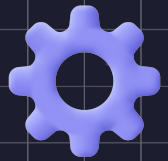


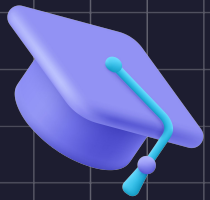
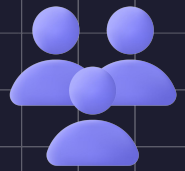
keep coding





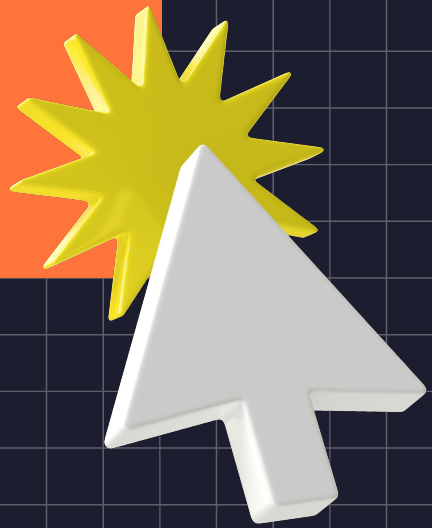


*Slide de ejemplo de aplicación del emoji

Módulo Fundamentos



keep coding

Cuerpo de texto

Título sección

Texto extra