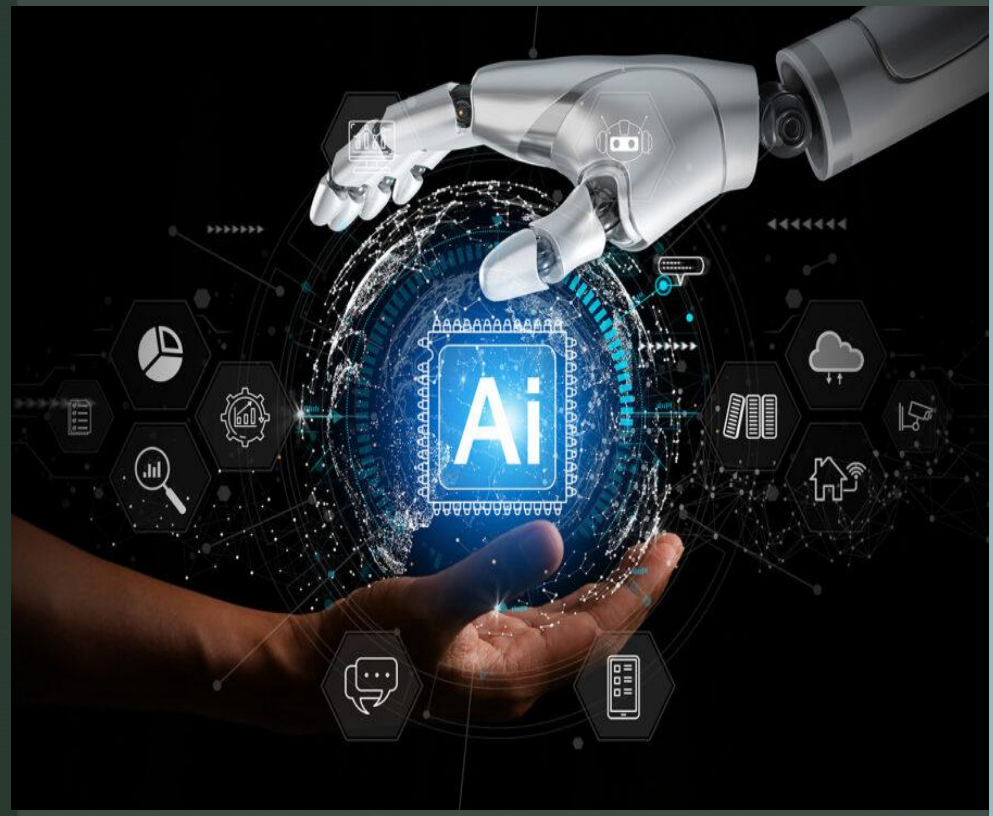
Maestría en
Ciberseguridad
y Ciberdefensa

Registro Calificado Res. 001140 del 03 de febrero de 2022, por 7 años.
Cód. SNIES 104695

“Inteligencia artificial aplicada a la protección de las infraestructuras críticas: oportunidades y riesgos”



TCRN EM Christian Vizcaino Villavicencio
Comandante del Grupo de Ciberdefensa de la Fuerza Terrestre

ING Lorena Mahecha Guzmán
Líder de Gobierno de Seguridad y Privacidad (sector financiero)

OBJETIVO

- Analizar la relevancia estratégica de las infraestructuras críticas y el papel de la Inteligencia Artificial en su protección, evaluando los principales riesgos y oportunidades que su implementación representa para la RESILIENCIA, la seguridad operativa y la toma de decisiones en entornos críticos

SUMARIO

Infraestructura crítica física / digital

Sistemas y activos, físicos o digitales, que proporcionan servicios esenciales cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".

Fuente: Ministerio de Telecomunicaciones del Ecuador (MINTEL, 2023); Banco Interamericano de Desarrollo (BID, 2023); CAF (2022).

Servicio esencial

Es el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Fuente: Metodología para catalogación de ICD - Colombia.

Fundamentación legal

Art.- 158 … Misión fundamental
Art. 313, … Sectores estratégicos

Art 43. De la protección de instalaciones e infraestructura

Mantener la protección de la infraestructura crítica, recursos y áreas estratégicas del Estado

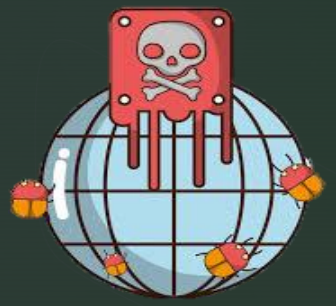
3

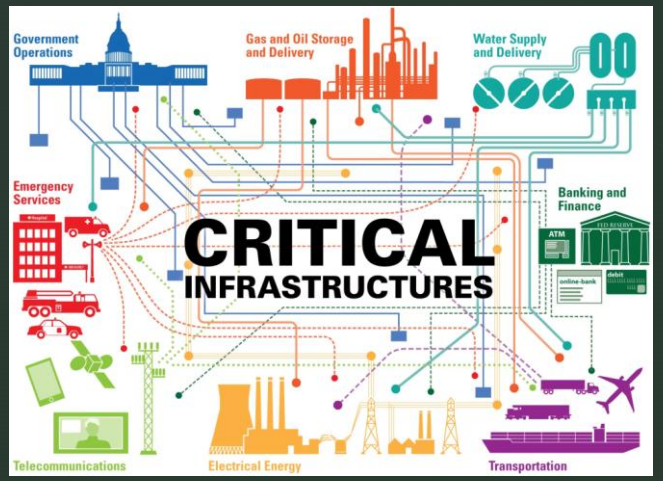
Protección de la Infraestructura Crítica de la Información y servicios esenciales

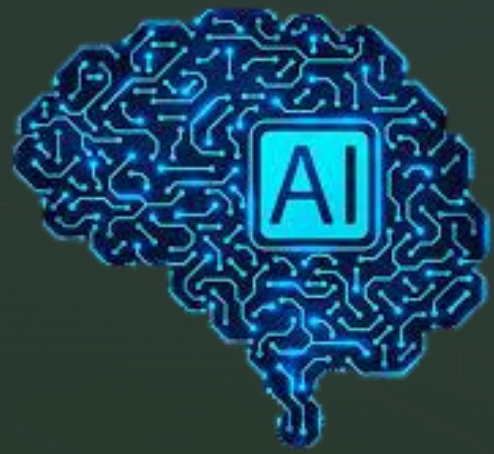
Defensa de la soberanía e integridad territorial - TNAC

Concepción estratégica de la Ciberdefensa: 5 Objetivos.

Importancia de proteger las infraestructuras críticas en la era de la Inteligencia Artificial







"Ciberataques a infraestructuras críticas aumentaron 200 % en América Latina desde 2020"

Fuente: Ministerio de Telecomunicaciones del Ecuador (MINTEL, 2023); Banco Interamericano de Desarrollo (BID, 2023); CAF (2022).

Metodología de puntaje ponderado de impacto

$$DIWS = (IP \times 0.3) + (ISN \times 0.25) + (CA \times 0.25) + (IE \times 0.2)$$

$$ICDE = \alpha.IP + \beta.\text{ISN} + \gamma.CA + \delta.IE$$

Factor	Peso (%)
Impacto Poblacional	α
Impacto a la seguridad nacional	β
Criticidad de Activos	γ
Económico	δ
Total	**100%**

Proceso Analítico Jerárquico **AHP**

$ICDE = > 40\%$ protegida con mayor urgencia

Fuente: Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) .

Situación actual del Ecuador frente a la protección de infraestructuras críticas

Avances institucionales

- Estrategia Nacional de Ciberseguridad (2022-2025) impulsada por el MINTEL.
- Colaboración con organismos internacionales: OEA-CSIRT Americas, FID .

Brechas y desafíos

Sin embargo, persisten brechas estructurales y tecnológicas:

- 70 % de déficit de profesionales en ciberseguridad OT (BID, 2023).
- 40 % de infraestructuras industriales operan con sistemas o protocolos obsoletos (CAF, 2022).
- Escasa adopción de normas ISA/IEC 62443 en sectores críticos.

"Ecuador avanza en su estrategia de ciberdefensa, pero proteger sus infraestructuras críticas exige inteligencia…Inteligencia Artificial."

ISA-95; ISA/IEC 62443; ISAGCA (2025); Diapositivas Ciberseguridad OT – Ecuador (2024).

De la automatización aislada a la infraestructura hiperconectada: el nuevo frente de riesgo

Ayer: Sistemas industriales aislados
Etapa 1

- Décadas 1980–2000: sistemas SCADA y PLC sin conexión a internet.
- Seguridad basada en aislamiento físico (air gap).
- Baja automatización, pero alta resiliencia a ataques externos.

Hoy: Convergencia IT/OT
Etapa 2

- Integración de redes industriales con redes corporativas (IT).
- Introducción de ERP, MES, y sistemas cloud.
- El perímetro desaparece; el ataque puede entrar por cualquier conexión.

Mañana: Infraestructura inteligente e hiperconectada
Etapa 3

- Ecosistemas IIoT (Industrial Internet of Things) y Edge Computing.
- Dispositivos inteligentes conectados a la nube y a 5G.
- IA para monitorear y responder a la velocidad de la máquina.

"Cada paso hacia la digitalización industrial aumenta la eficiencia...pero también amplía la superficie de ataque."

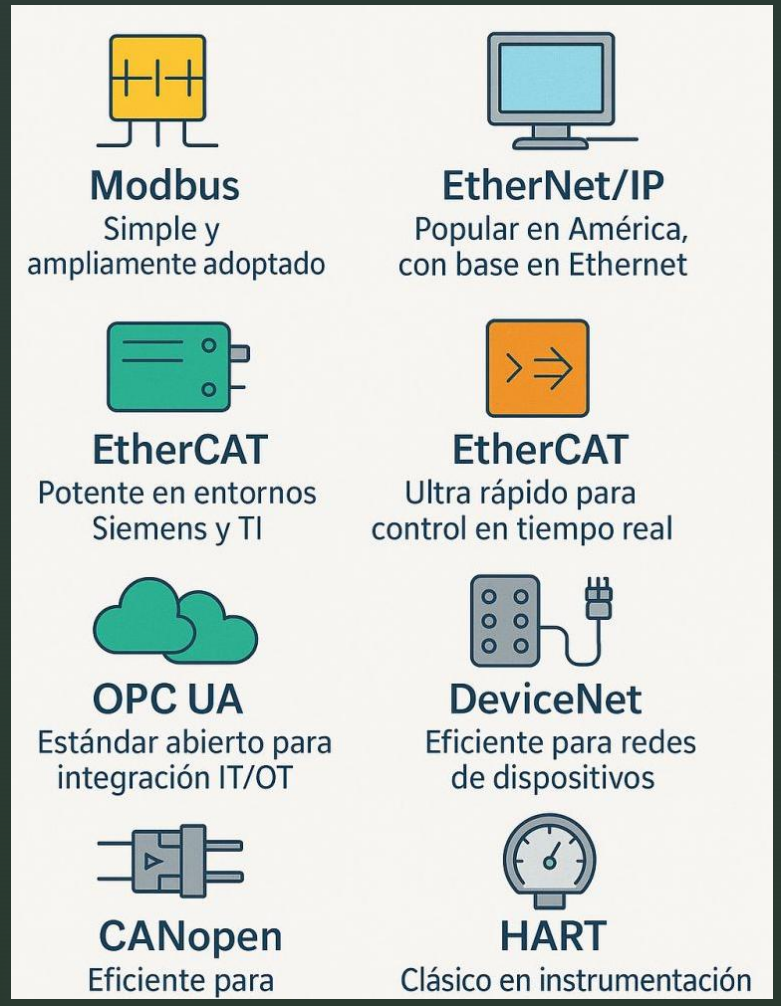
Fuente: Oltra – La Norma ISA 95; ISAGCA (2025); Banco Interamericano de Desarrollo (BID, 2023); CAF (2022).

Arquitectura OT: la columna vertebral de las infraestructuras críticas

"La seguridad de una infraestructura crítica comienza en su arquitectura"

ISA-95; ISA/IEC 62443; ISAGCA (2025); Diapositivas Ciberseguridad OT – Ecuador (2024).

Protocolos industriales y vulnerabilidades comunes



Los sistemas OT utilizan protocolos específicos que, en muchos casos, carecen de autenticación o cifrado:

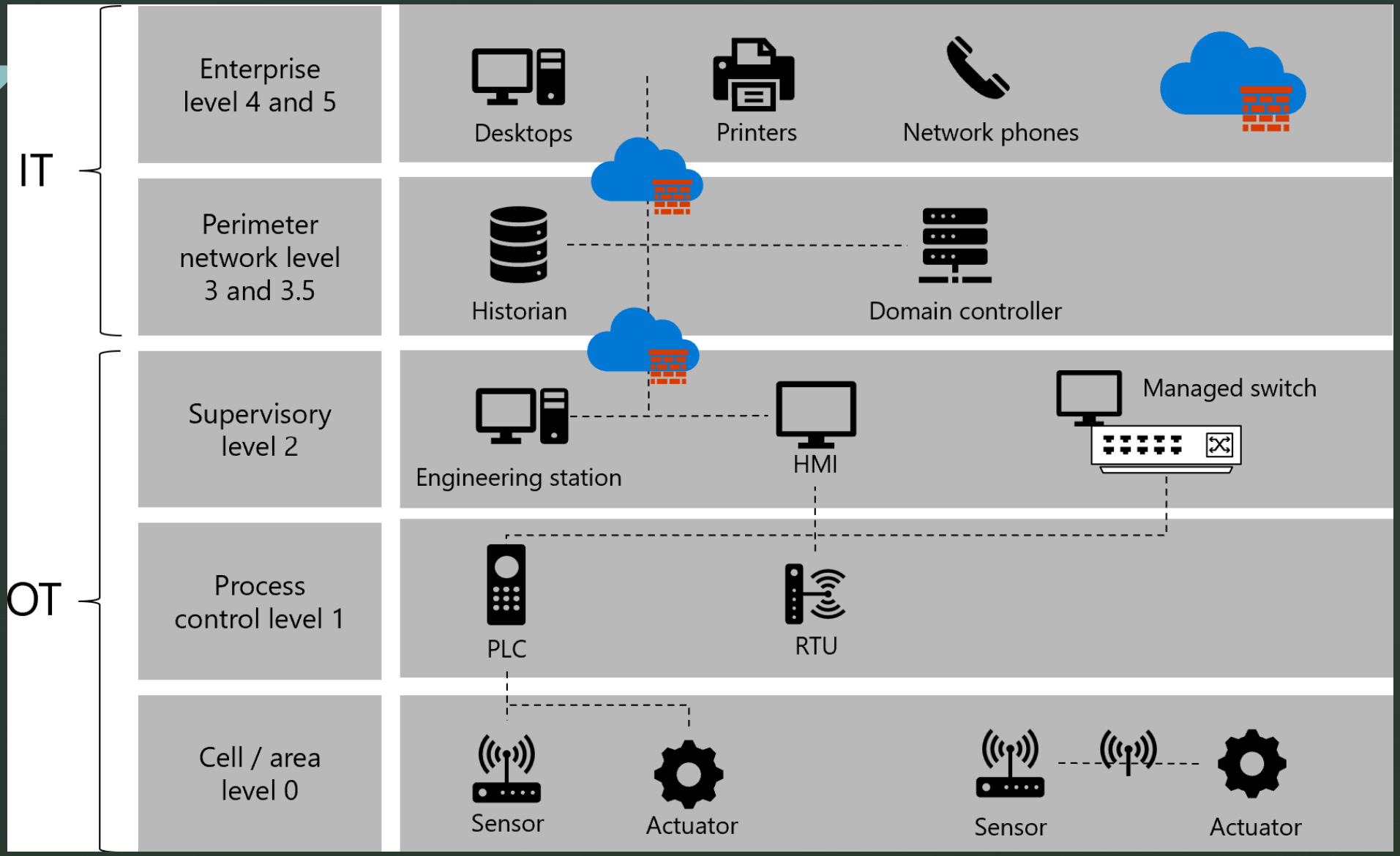
- Modbus TCP (puerto 502)
- Siemens S7Comm (puerto 102)
- DNP3 / IEC-104 / OPC UAEn

Ecuador, se han detectado dispositivos industriales expuestos públicamente en estos puertos, lo que evidencia la necesidad de segmentar y monitorear con IA.

"La seguridad de una infraestructura crítica comienza en su arquitectura"

ISA-95; ISA/IEC 62443; ISAGCA (2025); Diapositivas Ciberseguridad OT – Ecuador (2024).

Convergencia IT/OT



"La seguridad de una infraestructura crítica comienza en su arquitectura"

ISA-95; ISA/IEC 62443; ISAGCA (2025); Diapositivas Ciberseguridad OT – Ecuador (2024).

En ciberdefensa, la IA analiza millones de eventos en tiempo real, detectando comportamientos anómalos imposibles de percibir por un analista humano.

Tipo de IA	Aplicación práctica en defensa OT	Ejemplo
Machine Learning (ML)	Aprende patrones normales en redes industriales	Detecta tráfico anómalo en Modbus o DNP3
Deep Learning (DL)	Analiza señales complejas en múltiples capas	Identifica ataques multi-etapa o malware OT
IA Cognitiva	Interpreta contexto y lenguaje técnico	Correlaciona alertas y genera informes automáticos

Los sistemas OT generan millones de datos por segundo (tráfico de PLCs, sensores, logs SCADA).
Los métodos tradicionales no detectan ataques lentos o sutiles.

La IA permite:

- Detectar desviaciones mínimas en procesos industriales.
- Aprender del comportamiento normal de cada activo.
- Priorizar alertas reales y reducir falsos positivos.
- Automatizar respuestas seguras sin detener la operación.

"La IA no reemplaza al analista, lo convierte en un defensor con visión ampliada."

Fuente: Gartner (2023); Darktrace Industrial (2024); Banco Interamericano de Desarrollo (BID, 2023); CAF (2022); Grupo de Ciberdefensa FT (2025).

Cómo actúa la Inteligencia Artificial en la Ciberdefensa

En una red industrial ecuatoriana, la IA puede:

- Detectar anomalías en protocolos industriales (Modbus, S7Comm).
- Reconocer órdenes fuera de horario o comandos no habituales.
- Alertar antes de que se ejecute un cambio en un PLC o SCADA.

Todo sin interrumpir el proceso productivo.

Implementaciones reales de IA en ciberdefensa industrial muestran:

- Reducción del tiempo medio de detección (MTTD) hasta en 90 %.
- Reducción del tiempo medio de respuesta (MTTR) hasta en 85 %.
- Identificación de amenazas sin firma previa (zero-day).
- Aumento de eficiencia del analista hasta 4 veces (según Gartner, 2023).

“La defensa tradicional reacciona.La defensa con IA anticipa y neutraliza.”

Fuente: Gartner (2023); Darktrace Industrial (2024); CrowdStrike Falcon (2024)

Cómo la IA transforma la superficie de ataque

Oportunidades Defensivas

Detección y Respuesta Avanzada

Sistemas SIEM potenciados con machine learning pueden identificar patrones anómalos, correlacionar eventos complejos y reducir drásticamente el tiempo de detección de amenazas (de días/semanas a minutos/horas)

Mantenimiento Predictivo Inteligente

Modelos de IA analizan datos de sensores para predecir fallos antes de que ocurran, reduciendo ventanas de vulnerabilidad operativa y minimizando intervenciones humanas en entornos críticos

Análisis de Anomalías en Tiempo Real

Detección automatizada de comportamientos inusuales en redes OT/IT, tráfico de datos y comportamiento de usuarios, permitiendo respuesta inmediata ante desviaciones de líneas base establecidas

Nuevos Vectores de Riesgo

Envenenamiento de Datos

Atacantes pueden manipular datos de entrenamiento para corromper modelos de IA, introduciendo sesgos que generen decisiones erróneas en contextos críticos (data poisoning attacks)

Evasión y Manipulación de Modelos

Técnicas adversariales permiten engañar a sistemas de ML para que clasifiquen incorrectamente amenazas, evadan detección o generen falsos positivos que saturen equipos de respuesta

Automatización de Ataques con LLMs

Modelos de lenguaje grandes facilitan la creación automatizada de campañas de phishing sofisticadas, búsqueda acelerada de vulnerabilidades y generación de código malicioso polimórfico

Impacto en Decisiones OT

Cuando modelos de IA comprometidos controlan actuadores, válvulas o sistemas de control industrial, las consecuencias pueden incluir daño físico, interrupciones operativas graves y riesgos para seguridad humana

Fuente: Análisis de IBM Security sobre amenazas emergentes a sistemas de IA y reportes de laboratorios de defensa sobre uso ofensivo de machine learning

Oportunidades estratégicas para Ecuador en la protección inteligente de sus infraestructuras críticas

Fortalecimiento de capacidades nacionales

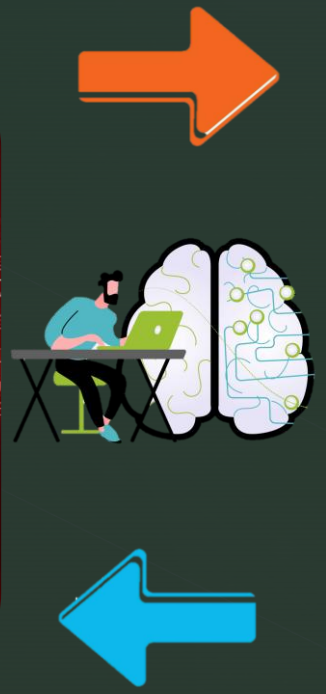
Talento humano y formación especializada

Cooperación internacional y alianzas estratégicas

Innovación tecnológica y soberanía digital

Fuente: MINTEL (2023); BID (2023); CAF (2022); ISAGCA (2025)

Riesgos y desafíos del uso de la Inteligencia Artificial en la defensa de infraestructuras críticas



La Inteligencia Artificial puede ser nuestro escudo…o nuestra vulnerabilidad más profunda, si no controlamos su propósito y sus límites.

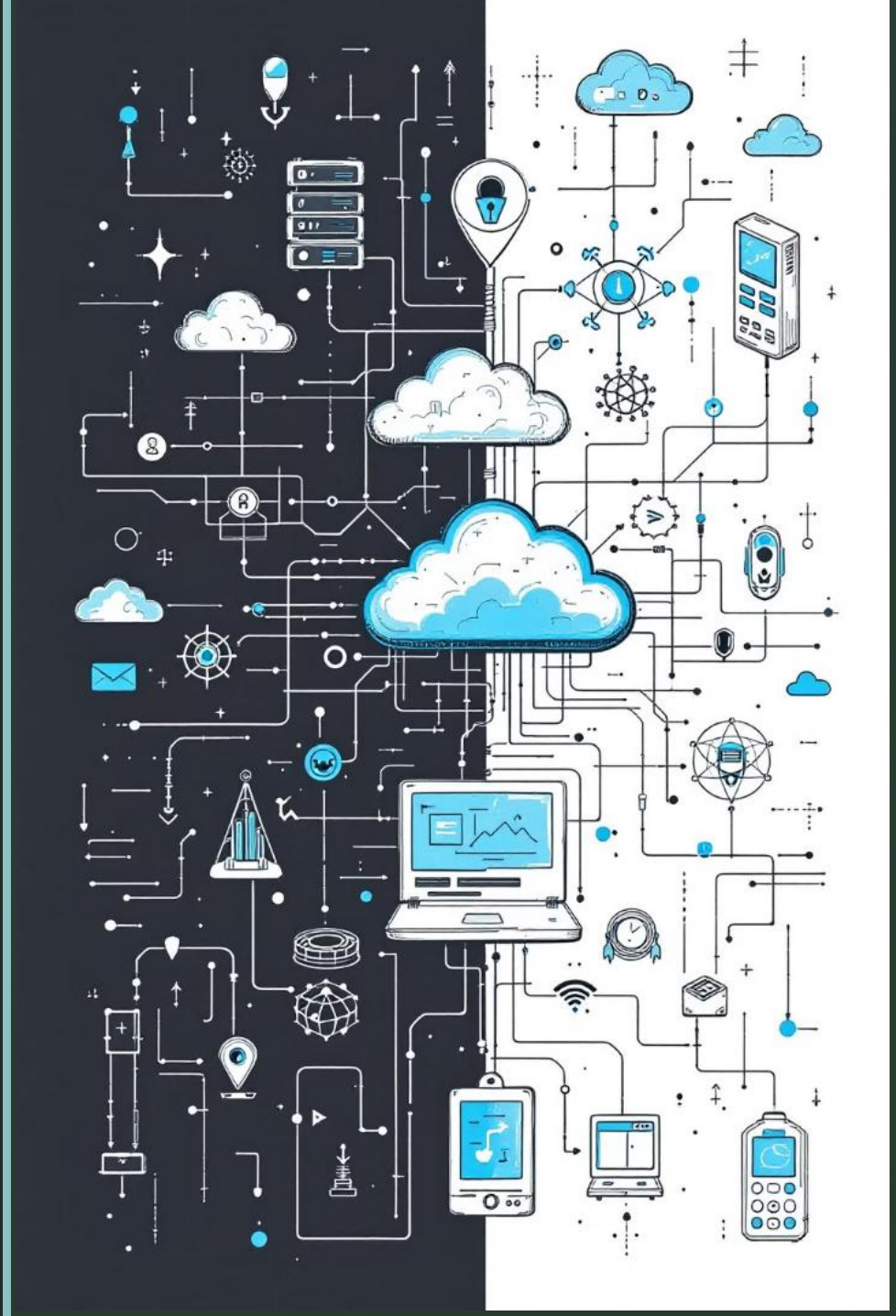
Fuente: ISAGCA (2025); Gartner (2024); ENISA (2023); BID (2023)

Marcos normativos y estándares internacionales aplicables a la protección inteligente de infraestructuras críticas

Norma / Marco	Enfoque	Aplicación en IA y OT
ISO/IEC 27001	Gestión de seguridad de la información	Crea políticas para integrar IA bajo control seguro.
ISO/IEC 27002	Controles de ciberseguridad	Define buenas prácticas para gestión de accesos y datos IA.
ISA/IEC 62443	Seguridad en sistemas de automatización industrial	Establece protección multinivel en entornos OT y SCADA.
NIST CSF (Cybersecurity Framework)	Gestión de riesgos cibernéticos	Alínea a lá IA al ciclo: Identificar, Proteger, Detectar, Responder y Recuperar.
ISAGCA 2025 Framework	Integración moderna entre ISO/IEC 27001 y 62443	Permite gobernar seguridad OT con IA, gestión de riesgos y auditoría continua.

Fuente: ISAGCA (2025); ISO/IEC 27001; ISA/IEC 62443; NIST Cybersecurity Framework (2023)

Conclusiones



“La defensa del Ecuador ya no se libra solo en tierra, mar y aire…también en el ciberespacio, donde la Inteligencia Artificial puede ser el nuevo escudo que garantice nuestra soberanía y seguridad nacional.”

GRACIAS