ENTHEC

WHITEPAPER

Inteligencias Artificiales autónomas:

Su impacto en la ciberseguridad

kartos

ÍNDICE

Introducción 02

Qué son las Inteligencias Artificiales Autónomas 03

Ventajas de las IA Autónomas 04

Amenazas emergentes para la ciberseguridad 05

Tecnologías y estrategias de defensa 06

Desafíos éticos y regulatorios 07

Recomendaciones para empresas y entidades públicas 08

Conclusiones 09

INTRODUCCIÓN

Durante la última década, las organizaciones han dependido de soluciones basadas en reglas, automatizaciones limitadas y sistemas de análisis asistido para defender infraestructuras cada vez más complejas. Sin embargo, la llegada de las **inteligencias artificiales y, en especial, las autónomas (IAA)** marca un punto de inflexión histórico: estamos pasando de herramientas reactivas y dependientes de una supervisión continua a entidades capaces de razonar, aprender, coordinar acciones, tomar decisiones en tiempo real y ejecutar estrategias defensivas de manera proactiva.

Las IAs autónomas están emergiendo gracias a avances en modelos multimodales, planificación secuencial, orquestación de herramientas, acceso en tiempo real a datos operativos y mecanismos de adaptación continua. Estas capacidades permiten que un **agente autónomo** no solo detecte anomalías, sino que también comprenda patrones complejos, correlacione eventos distribuidos, anticipe comportamientos maliciosos, despliegue contramedidas y aprenda de cada interacción.

Sin embargo, el mismo progreso que potencia la defensa también impulsa la sofisticación del adversario. Las IAs autónomas pueden ser utilizadas por actores maliciosos para lanzar campañas de intrusión coordinadas, explotar vulnerabilidades de forma automática, generar malware polimórfico o ejecutar operaciones complejas a una velocidad incompatible con las capacidades humanas. Este escenario inaugura un **nuevo paradigma de conflicto digital entre agentes inteligentes**, donde la ventaja dependerá de la capacidad de desplegar, supervisar y controlar de forma segura sistemas autónomos resilientes.

Ante este panorama, las preguntas sobre gobernanza, seguridad, transparencia y control se vuelven críticas. ¿Cómo garantizamos que una IA autónoma actúe de forma alineada con las políticas de seguridad? ¿Cómo prevenimos la manipulación, el secuestro o la explotación de agentes defensivos? ¿Qué salvaguardas son necesarias para evitar decisiones erróneas o desproporcionadas en sistemas que operan de forma continua? Además, la autonomía exige **nuevos marcos** de auditabilidad, trazabilidad y validación de comportamientos, especialmente cuando estas IAs participan en la protección de infraestructuras críticas, de cadenas de valor globales o de servicios esenciales.

Este documento tiene como objetivo ofrecer una visión clara y estratégica del **impacto previsible de las IAs autónomas en la ciberseguridad**, analizando tanto su potencial transformador como los riesgos y responsabilidades que conllevan. En un escenario en el que tanto defensores como atacantes operarán con inteligencia autónoma, comprender esta transformación resulta imprescindible. El futuro de la ciberseguridad dependerá de nuestra capacidad colectiva para aprovechar este poder tecnológico sin perder el control sobre él.

QUÉ SON LAS INTELIGENCIAS ARTIFICIALES AUTÓNOMAS

Las inteligencias artificiales autónomas (IAA) representan una evolución de los sistemas de IA tradicionales. Mientras que la mayoría de modelos de inteligencia artificial actuales requieren de supervisión humana constante para entrenarse, configurarse y aplicarse en contextos concretos, las IAA están diseñadas para **operar de manera independiente**, con capacidad de:

- **Aprender y adaptarse** a partir de la experiencia y del entorno sin intervención externa continua.
- **Tomar decisiones en tiempo real** basadas en objetivos definidos y no únicamente en instrucciones preprogramadas.
- **Ejecutar acciones de forma automática,** optimizando recursos y corrigiendo errores sin esperar supervisión.

En esencia, las IAA son sistemas con **capacidad de autogestión**, capaces de establecer estrategias de respuesta y de coordinar múltiples tareas en entornos complejos. Esto las convierte en una tecnología particularmente relevante para escenarios donde la **velocidad de reacción y la adaptabilidad** son factores críticos, como ocurre en la ciberseguridad.

La aparición de las IAA no es un fenómeno aislado, sino el resultado de una **trayectoria tecnológica acumulativa:**

IA clásica (décadas de 1950–1990):	IA basada en datos (2000–2010):	IA generativa y de gran escala (2018–2025):	IA autónoma (presente y futuro):
centrada en sistemas expertos, reglas lógicas y algoritmos deterministas.	centrada en sistemas expertos, reglas lógicas y algoritmos deterministas.	con los modelos fundacionales y de lenguaje, capaces de generar texto, imágenes, código y de realizar razonamientos complejos.	sistemas capaces de integrar varias de estas capacidades, gestionarse de forma independiente y ejecutar acciones de valor estratégico sin depender de un control humano constante.

Hoy en día, la convergencia de infraestructuras en la nube, cómputo de alto rendimiento, sensores distribuidos y avances en modelos multimodales ha abierto la puerta a sistemas capaces de operar como agentes autónomos. Estos agentes no solo responden a comandos, sino que también pueden **definir metas intermedias, coordinar recursos y anticipar riesgos.**

Diferencias entre IA tradicional e IA autónoma

En el campo de la ciberseguridad, este contexto se traduce en un cambio de paradigma: pasar de soluciones reactivas a **defensas proactivas y autoajustables,** con el potencial de **neutralizar amenazas antes de que escalen.**

ASPECTO	IA TRADICIONAL	IA AUTONOMA
Dependencia humana	Requiere supervisión constante y configuración manual.	Funciona con mínima supervisión, tomando decisiones propias.
Capacidad de adaptación	Limitada a escenarios previstos en el entrenamiento.	Se adapta a entornos cambiantes en tiempo real.
Toma de decisiones	Basada en patrones aprendidos o reglas predefinidas.	Integra análisis, planificación y ejecución de acciones en ciclos continuos.
Gestión de errores	Necesita ajustes humanos para corregir fallos.	Detecta, corrige y optimiza su desempeño de manera autónoma.
Escalabilidad	Difícil de escalar sin rediseño ni reentrenamiento.	Puede desplegarse en múltiples entornos coordinando tareas de forma distribuida.
Aplicación en seguridad	Detección puntual de anomalías o amenazas.	Respuesta dinámica, proactiva y coordinada frente a ciberataques complejos.

Las **IAA no sustituyen a la IA tradicional,** sino que la amplían y superan, ofreciendo un nivel de autonomía que resulta decisivo para ámbitos donde el **tiempo de respuesta y la resiliencia** son factores diferenciales, como la protección de infraestructuras digitales críticas.

VENTAJAS DE LAS IA AUTÓNOMAS

Las **Inteligencias Artificiales Autónomas (IAA)** no solo representan un avance tecnológico, sino también una oportunidad estratégica para múltiples sectores. Su capacidad de operar sin supervisión constante, adaptarse a entornos dinámicos y ejecutar acciones proactivas abre la puerta a un modelo de **automatización inteligente y resiliente**, con un impacto directo en la seguridad, la productividad y la competitividad.

AUTOMATIZACIÓN AVANZADA DE PROCESOS

A diferencia de la automatización clásica, basada en scripts o flujos predefinidos, las IAA son capaces de:

- **Orquestar procesos complejos** en entornos cambiantes, ajustando la secuencia de tareas según las circunstancias.
- **Reducir la intervención humana en actividades repetitivas**, minimizar errores y liberar talento para funciones de mayor valor estratégico.
- **Gestionar incidentes y excepciones** de manera autónoma, sin necesidad de reglas explícitas para cada escenario posible.

En ciberseguridad, esto se traduce en la capacidad de monitorizar redes, detectar anomalías, mitigar ataques y documentar incidentes de forma integral, sin depender de la intervención continua de analistas humanos.

TOMA DE DECISIONES EN TIEMPO REAL

El rasgo distintivo de las IAA es su capacidad para **procesar información, evaluar riesgos y actuar de inmediato:**

- **Velocidad de reacción:** permiten responder en milisegundos frente a ciberataques, lo que supera ampliamente las capacidades humanas.
- **Evaluación contextual:** no se limitan a aplicar patrones estáticos, sino que consideran múltiples variables del entorno antes de actuar.
- **Resiliencia adaptativa:** si una estrategia falla, la IAA puede reajustar automáticamente su curso de acción, manteniendo la continuidad operativa.

Este enfoque convierte a las IAA en aliadas clave para infraestructuras críticas, donde una decisión tardía puede significar la interrupción de servicios esenciales.

APLICACIONES EN SECTORES CLAVE

Las ventajas de las IAA no se limitan al ámbito de la ciberseguridad. Su impacto abarca múltiples sectores estratégicos:

- **Industria:** optimización de cadenas de suministro, mantenimiento predictivo de maquinaria y reducción de los tiempos de inactividad.
- **Salud:** diagnóstico asistido en tiempo real, gestión autónoma de datos clínicos y soporte en cirugías robóticas de alta precisión.
- **Defensa y seguridad nacional:** despliegue de sistemas autónomos para la vigilancia, la ciberdefensa y el análisis de inteligencia operativa.
- **Finanzas:** detección automática de fraudes, análisis de riesgos dinámicos y optimización de carteras de inversión.
- **Transporte y logística:** gestión de flotas autónomas, rutas optimizadas y respuesta inmediata ante interrupciones en el flujo logístico.

En todos estos sectores, las IAA representan un salto cualitativo hacia **operaciones más seguras, ágiles y rentables.**

IMPACTO ECONÓMICO Y DE EFICIENCIA

El despliegue de IAA tiene un efecto directo en los indicadores económicos y de eficiencia:

- **Reducción de costes operativos:** al minimizar los errores humanos y automatizar tareas de alto volumen.
- **Incremento de la productividad:** gracias a la ejecución paralela y continua de procesos, sin limitaciones de horario ni de fatiga.
- **Escalabilidad empresarial:** permiten ampliar operaciones a gran escala sin necesidad de multiplicar la fuerza laboral.
- **Nuevos modelos de negocio:** impulsan la creación de servicios basados en la autonomía (por ejemplo, cybersecurity-as-a-service con respuesta automática en tiempo real).

En términos macroeconómicos, la adopción de IAA acelerará la competitividad de los países y de las organizaciones que las implementen, marcando una brecha con quienes no las adoptan.

AMENAZAS EMERGENTES PARA LA CIBERSEGURIDAD

El mismo potencial que hace de las inteligencias artificiales autónomas (IAA) una herramienta poderosa para la defensa también puede ser aprovechado por actores maliciosos. Las IAA introducen un nuevo nivel de **sofisticación, velocidad y autonomía** en los ataques, lo que plantea un panorama de amenazas radicalmente diferente al que se conocía hasta ahora.

CIBERATAQUES AUTÓNOMOS: VELOCIDAD, ESCALA Y ADAPTABILIDAD

Los **ciberataques autónomos** constituyen uno de los mayores riesgos emergentes. Una IAA maliciosa puede:

- **Ejecutar ataques en milisegundos**, superando cualquier capacidad humana de respuesta.
- **Escalar operaciones automáticamente**, lanzando miles de intentos de intrusión en paralelo contra múltiples objetivos.
- **Adaptar tácticas en tiempo real**, modificando los patrones de ataque según las defensas que encuentre.

Esto supone pasar de ataques puntuales y predefinidos a **campañas dinámicas autogestionables y autoajustables**, con un potencial disruptivo masivo para organizaciones y estados.

INGENIERÍA SOCIAL AUTOMATIZADA Y SUPLANTACIÓN INTELIGENTE

Las IAA también potencian la **ingeniería social**, uno de los vectores más efectivos en la ciberseguridad:

- **Creación de mensajes personalizados** basados en el análisis en tiempo real de perfiles digitales.
- **Suplantación de identidad convincente**, con voces e imágenes sintéticas indistinguibles de las reales.
- **Interacciones sostenidas** en chats, llamadas o correos electrónicos que simulan el comportamiento humano con gran credibilidad.

Esto eleva el riesgo de **phishing avanzado, fraudes y manipulación psicológica**, incluso entre usuarios con un alto nivel de formación en seguridad.

GENERACIÓN DE DESINFORMACIÓN Y MANIPULACIÓN A ESCALA

Las IAA son capaces de producir y difundir **contenidos falsos o manipulados** de forma masiva y coordinada:

- **Producción automatizada** de textos, imágenes, audios y vídeos falsificados (deepfakes).
- **Gestión de ejércitos de bots autónomos**, capaces de propagar narrativas específicas en redes sociales.
- **Ajuste dinámico de mensajes**, adaptándolos en tiempo real a audiencias y contextos culturales.

La **desinformación a escala** puede desestabilizar sociedades, erosionar la confianza en instituciones y afectar directamente a la seguridad nacional y económica.

RIESGOS PARA INFRAESTRUCTURAS CRÍTICAS Y SISTEMAS CONECTADOS

Las IAA también incrementan las amenazas contra **infraestructuras críticas** y sistemas industriales (ICS/SCADA):

- **Ataques coordinados a sistemas energéticos, de transporte o de comunicaciones,** capaces de provocar interrupciones masivas.
- **Exploración autónoma de vulnerabilidades** en entornos operativos altamente conectados.
- **Persistencia encubierta,** con agentes maliciosos que aprenden y se adaptan para permanecer invisibles en sistemas críticos.

El impacto potencial abarca desde apagones eléctricos o interrupciones de los servicios sanitarios hasta la paralización de cadenas logísticas internacionales.

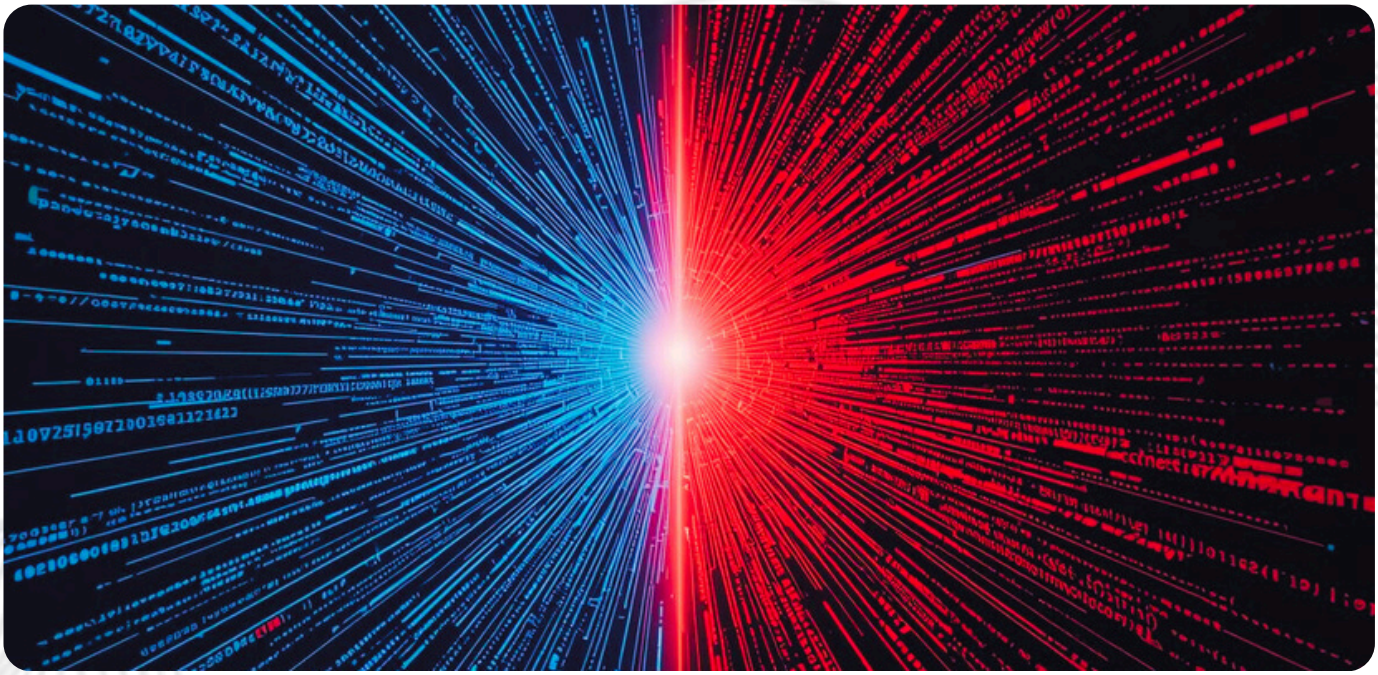
AMENAZAS A LA PRIVACIDAD PERSONAL Y AL ESPIONAJE CORPORATIVO

Finalmente, las IAA introducen riesgos significativos en el ámbito de la privacidad y el espionaje:

- **Recolección masiva y autónoma de datos personales,** combinando múltiples fuentes digitales para elaborar perfiles completos.
- **Explotación de vulnerabilidades en comunicaciones privadas,** incluidas debilidades de cifrado o errores humanos.
- **Espionaje corporativo avanzado,** donde agentes autónomos acceden, clasifican y extraen información sensible sin ser detectados.

Este tipo de amenazas puede comprometer tanto la seguridad individual como la ventaja competitiva de las organizaciones y los estados.

En conjunto, las IAA maliciosas representan un salto cualitativo en la amenaza cibernética: no se trata únicamente de una mayor capacidad técnica, sino de inteligencia y autonomía ofensivas, lo que desafía los modelos de defensa actuales y exige nuevas estrategias de protección.



TECNOLOGÍAS Y ESTRATEGIAS DE DEFENSA

La irrupción de las **Inteligencias Artificiales Autónomas (IAA)** como posibles amenazas ha impulsado el desarrollo de **nuevas defensas adaptativas**. Las estrategias actuales combinan inteligencia artificial, marcos de seguridad avanzados y enfoques de gobernanza para mantener la confianza en entornos cada vez más automatizados.

Ciberdefensa basada en IA: detección y respuesta autónoma

Los sistemas de ciberdefensa basados en IAA representan un cambio de paradigma frente a la seguridad tradicional:

Detección proactiva	Análisis en tiempo real de tráfico, de los registros y de los comportamientos anómalos.
Respuesta autónoma	Ejecución inmediata de medidas de contención (aislar nodos, cerrar accesos, activar respaldos).
Aprendizaje continuo	Adaptación de estrategias defensivas a medida que cambian las tácticas de los atacantes.

Ejemplo práctico: una red corporativa detecta actividad sospechosa en un servidor crítico. La IAA no solo genera la alerta, sino que también aísla el servidor, despliega una réplica en la nube y mantiene la continuidad operativa en cuestión de segundos.

Modelos de IA explicable y gobernanza algorítmica

Para que las IAA sean confiables, deben ser **transparentes y auditables**. Aquí surge la importancia de la **IA explicable (XAI)** y de la gobernanza algorítmica:

Explicabilidad	Los sistemas deben justificar sus decisiones de forma comprensible para humanos, especialmente en incidentes críticos.

Supervisión humana

Aunque las IAA actúen de forma autónoma, debe existir un mecanismo de validación y control.

Gobernanza algorítmica

Establecimiento de políticas que regulen el entrenamiento, el despliegue y la supervisión de los modelos autónomos.

Esto no solo refuerza la **confianza de los usuarios,** sino que también facilita la **conformidad con las normativas legales y éticas.**

Seguridad Zero Trust aplicada a entornos con IA

El principio de **Zero Trust** ("nunca confiar, siempre verificar") cobra una dimensión crítica en entornos con IAA:

Autenticación y autorización continua

Incluso entre agentes autónomos, cada transacción debe verificarse en tiempo real.

Microsegmentación

Limitar el alcance de accesos, de manera que una posible intrusión autónoma no comprometa toda la red.

Monitoreo constante

Aplicar análisis en tiempo real para validar comportamientos y detectar desviaciones.

Ejemplo práctico: en una empresa con múltiples IAA colaborando en la gestión de datos, un agente solo puede acceder a los recursos estrictamente necesarios para su tarea, lo que reduce drásticamente la superficie de ataque.

Red teams autónomos y simulación de amenazas IA

Las organizaciones están empezando a emplear **red teams autónomos:** IAA que simulan ataques sofisticados para probar defensas en condiciones reales.

Automatización de pruebas de penetración — Los sistemas simulan ataques avanzados a gran escala.

Evolución adaptativa — Los red teams aprenden de las defensas y adaptan sus tácticas en tiempo real.

Refuerzo defensivo — Permite a las organizaciones identificar vulnerabilidades antes de que los atacantes reales las detecten.

Ejemplo práctico: un banco despliega un red team autónomo que simula intentos de fraude en su infraestructura digital. Los agentes adaptan sus tácticas según las respuestas defensivas, lo que les permite ajustar la seguridad antes de una intrusión real.

Normativas y marcos regulatorios emergentes

El avance de las IAA exige **marcos regulatorios y normativos sólidos** que garanticen un uso responsable:

Unión Europea — El AI Act establece categorías de riesgo y requisitos de transparencia para los sistemas autónomos.

Estados Unidos — Iniciativas de NIST sobre IA responsable y ciberseguridad autónoma.

Ámbito internacional — Necesidad de tratados multilaterales para evitar el uso ofensivo de IAA en conflictos cibernéticos.

Además de las leyes, se impulsan **estándares industriales** (ISO/IEC, ENISA, IEEE) que promueven buenas prácticas en seguridad, auditoría y trazabilidad de los algoritmos.

DESAFÍOS ÉTICOS Y REGULATORIOS

La adopción de **inteligencias artificiales autónomas (IAA)** en ciberseguridad abre oportunidades inéditas, pero también plantea dilemas éticos y regulatorios complejos. Estos desafíos no solo afectan al ámbito tecnológico, sino también a la gobernanza, la seguridad internacional y la confianza pública.

Normativas y marcos regulatorios emergentes

Uno de los principales retos es **determinar quién asume la responsabilidad** cuando una IAA toma una decisión que acarrea consecuencias negativas.

- Si un sistema autónomo bloquea un servicio crítico de manera errónea, ¿es responsable el desarrollador, el proveedor de servicios o la entidad que lo desplegó?
- La falta de un marco claro puede generar vacíos legales y ralentizar la adopción de estas tecnologías.

> *Hipótesis de estudio: Si una IAA en un Security Operations Center decide aislar automáticamente un servidor crítico debido a una falsa alarma, lo que provoca la interrupción de servicios públicos, la responsabilidad puede recaer en múltiples actores, lo que subraya la necesidad de reglas claras de atribución de responsabilidad.*

Transparencia y trazabilidad de las acciones de IA

La explicabilidad y la trazabilidad son requisitos clave para garantizar la confianza en los sistemas autónomos.

- Muchas IAA funcionan como "cajas negras", lo que dificulta auditar cómo llegaron a una decisión.
- Sin trazabilidad, resulta imposible verificar si una acción fue legítima o si fue producto de una manipulación externa.

> *Hipótesis de estudio: En el sector financiero, una IAA que bloquee transacciones por considerarlas sospechosas debe generar registros claros y auditables, de manera que tanto clientes como reguladores puedan revisar las decisiones.*

Riesgo de escalada en conflictos cibernéticos automatizados

El uso de IAA en operaciones ofensivas plantea riesgos de escalada no intencionada en conflictos digitales.

- Un ataque autónomo que responda automáticamente ante una amenaza percibida podría desencadenar represalias desproporcionadas.
- La ausencia de supervisión humana incrementa el riesgo de que se inicien "guerras de algoritmos", en las que los sistemas actúan sin coordinación ni un control político adecuado.

Hipótesis de estudio: Una IAA de defensa que detecta un ciberataque masivo en una red eléctrica podría, sin intervención humana, lanzar un contraataque automático contra las infraestructuras del atacante. Este escenario podría escalar un conflicto regional a un incidente internacional.

RECOMENDACIONES PARA EMPRESAS Y ENTIDADES PÚBLICAS

La incorporación de **inteligencias artificiales autónomas (IAA)** en los entornos de ciberseguridad exige no solo inversión tecnológica, sino también ajustes estratégicos, organizativos y culturales. Este capítulo ofrece un conjunto de recomendaciones prácticas para guiar a organizaciones públicas y privadas hacia una adopción segura y efectiva.

Evaluación de riesgos en entornos con IA

- **Mapeo de riesgos emergentes:** antes de desplegar IAA, las organizaciones deben identificar posibles escenarios de ataque en los que estas tecnologías puedan ser explotadas.
- **Análisis de dependencia tecnológica:** evaluar el grado de exposición al fallo o al compromiso del sistema autónomo.
- **Simulación de escenarios adversos:** realizar ejercicios de red teaming para medir la resiliencia de la organización frente a amenazas potenciadas por la IA.

Fortalecimiento de capacidades SOC con IA

- **Integración de IA en el SOC:** los centros de operaciones de seguridad deben evolucionar hacia SOC cognitivos, donde las IAA procesen grandes volúmenes de alertas en tiempo real.
- **Priorización inteligente de incidentes:** los sistemas autónomos pueden reducir la saturación de alertas y centrar al equipo humano en las amenazas críticas.
- **Colaboración humano–máquina:** las IAA deben actuar como asistentes estratégicos, no como sustitutas completas, para potenciar la toma de decisiones humanas.

Capacitación y concienciación en nuevas amenazas autónomas

- **Programas de formación especializados:** tanto empleados técnicos como personal no técnico deben entender qué son las amenazas autónomas y cómo reconocerlas.
- **Concienciación en ingeniería social avanzada:** preparar a usuarios para detectar ataques generados por IA, como correos hiperpersonalizados o deepfakes en llamadas de voz.

- **Entrenamiento continuo:** los programas de capacitación deben actualizarse en paralelo a la evolución de las capacidades ofensivas de las IAA.

Políticas internas de adopción segura de IA

- **Marco de gobernanza interno:** definir políticas claras sobre qué procesos pueden ser automatizados y bajo qué controles de supervisión.
- **Principio de mínima autonomía:** delegar funciones críticas de forma gradual, con niveles de autonomía escalonados según el riesgo.
- **Auditoría y trazabilidad:** mantener registros verificables de las decisiones tomadas por la IAA para fines regulatorios y de cumplimiento.
- **Ética y transparencia:** garantizar que la adopción de IAA respete los principios de privacidad, no discriminación y protección de derechos.

CONCLUSIONES

La irrupción de las **inteligencias artificiales autónomas (IAA)** representa un punto de inflexión en el ámbito de la ciberseguridad. A lo largo de este documento se ha evidenciado que estas tecnologías poseen un **doble filo**: por un lado, ofrecen capacidades sin precedentes para la defensa digital, la detección temprana de amenazas y la automatización de respuestas; por otro, introducen **riesgos emergentes** que van desde ciberataques autónomos hasta dilemas éticos y regulatorios aún no resueltos.

En el plano **técnico**, las IAA destacan por su potencial de mejorar la eficiencia operativa, reducir los tiempos de respuesta y anticipar amenazas en entornos de gran complejidad. Sin embargo, también se convierten en herramientas que pueden ser explotadas para generar desinformación, ejecutar ataques a escala masiva o comprometer infraestructuras críticas, con una velocidad difícil de contrarrestar con medios humanos tradicionales.

Desde una perspectiva **estratégica**, la adopción de estas tecnologías exige que tanto empresas como entidades públicas avancen en tres frentes prioritarios:

1. **Gobernanza y responsabilidad:** definir marcos claros para la atribución de decisiones y la rendición de cuentas.
2. **Transparencia y explicabilidad:** garantizar que las acciones de las IAA sean auditables y comprensibles.
3. **Cooperación internacional y normativa:** establecer estándares comunes que equilibren la innovación y la seguridad.

De cara al **futuro inmediato**, se prevé un escenario en el que las IAA se consolidarán como aliadas indispensables en la defensa digital. No obstante, su éxito dependerá de la capacidad de los actores implicados, sector público, sector privado, organismos internacionales y sociedad civil, para diseñar una adopción responsable que maximice los beneficios y minimice los riesgos.

En definitiva, las IAA no deben verse únicamente como herramientas tecnológicas, sino como **catalizadores de un cambio estructural** en la forma en que entendemos la ciberseguridad. Su impacto trascenderá el plano operativo para convertirse en un elemento clave de la **confianza digital, la estabilidad geopolítica y la resiliencia de nuestras sociedades.**

WHITEPAPER

kartos©

Kartos Corporate Threat Watchbots: Gestión Continua de la Exposición a Amenazas (CTEM)

Monitorización automatizada, continua y en tiempo real de la exposición a amenazas de la organización, orientada a criterios de ciberseguridad y de negocio.

SUPERFICIE EXTERNA DE ATAQUE

Localización de la información y las vulnerabilidades abiertas y expuestas de la Compañía en Internet, la Deep Web, Dark Web y las Redes Sociales: Campañas de phishing, fraude y estafa; CVEs; salud de DNS; contraseñas y credenciales filtradas; documentacióny bases de datos filtradas y expuestas.

PROTECCIÓN DEL RIESGO DIGITAL

Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar acabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la Compañía. Protección de marca, dominio y subdominios. Protección de correo electrónico corporativo. Protección contra ransomware. Seguridad web y eliminación de amenazas.

RIESGO DE TERCEROS

Control en tiempo real del riesgo de terceros. Datos objetivos sobre amenazas en curso relacionadas con la cadena de valor. Visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo no intrusivo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos de terceros.

COMPLIANCE

Monitorización de cumplimiento legal corporativo y de terceros basado en datos objetivos tomados en tiempo real. ISO 27001. PCI - DSS. ENS. RGPD. Justificación de cumplimiento de exigencias legales y normativas para asociaciones, fusiones y adquisiciones, auditorías, certificaciones y contratos con la administración

SCORING DE CIBERSEGURIDAD

Permite que la información sobre seguridad salga del despacho del CISO y se presente de manera sencilla a personas que deben participar en la gestión de la seguridad sin tener formación técnica. Scoring de ciberseguridad propio y de terceros para asociaciones, auditorías, fusiones, adquisiciones y contratos con la administración.

Análisis de 11 vectores

- **Algoritmos**
- **Certificados**
- **Servicios / IoT / VoIP**
- **Salud de DNS / Phishing**
- **Gestión de Parches**
- **Reputación IP**
- **Seguridad Web**
- **Seguridad e-mail**
- **Filtración de Documentos**
- **Filtración de Credenciales**
- **Redes Sociales**

- **Capa de IA** que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.
- **Herramienta estrictamente no intrusiva.** La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las organizaciones, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.
- Única plataforma que analiza las conversaciones en **redes sociales desde la perspectiva de detección de amenazas y ataques**, más allá de la relativa a reputación y branding.
- **Funcionamiento continuo 365x24x7**, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real.
- **Máxima sencillez de uso.** No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.
- Monitorización automatizada, objetiva y continúa de los **riesgos causados por las terceras partes** que pertenecen a la Superficie de Ataque Externa de la organización.

Conoce más sobre nuestras licencias.
Prueba de forma gratuita nuestra herramienta.
Empieza a usar Kartos y a extender la estrategia de ciberseguridad corporativa.

→ hello@enthec.com

Enthec Solutions es una compañía tecnológica española que desarrolla software de ciberseguridad para la protección de organizaciones y personas.Enthec Solutions se ha consolidado como una de las Deep Tech con soluciones de Cibervigilancia más innovadoras y eficaces gracias al éxito de su plataforma **Kartos Corporate Threat Watchbots**, que proporciona a las organizaciones Ciberseguridad, Ciberinteligencia, Cyberscoring, Compliance y Capacidades de Gestión del Riesgo de Terceros, y a su innnovadora plataforma **Qondar Personal Threat Watchbots** para la protección online individual de las personas relevantes de la organización.

www.enthec.com