Conferencia Online - Comisión Técnica • Sistemas y TI. AIC - Comisión Técnica • Sistemas y TI, Buenos Aires, 2025.

Ciberresiliencia Inteligente: Aplicaciones de la IA en la Seguridad Digital.

Diego Sebastián Escobar.

Ciberresiliencia Inteligente: Aplicaciones de la IA en la Seguridad Digital

- Diego Sebastián Escobar

COMISIÓN TÉCNICA
SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

COMISIÓN TÉCNICA
SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

CONFERENCIA ONLINE

Ciberresiliencia Inteligente: Aplicaciones de la IA en la Seguridad Digital

Jueves • 31 de julio de 2025 • 12:00 (Hora de Panamá)

Diego Sebastián Escobar
Phd UBA. Sub Área Contabilidad
Magister
en Seguridad Informática (UBA)
Argentina - EXPOSICIÓN

Elsa Beatriz Suarez Kimura
Phd UBA. Área Contabilidad
Argentina - Mediación

Yvonne Luzette Huertas
Presidente de la CT de Sistemas y Tecnología de la Información
Puerto Rico - Mediación

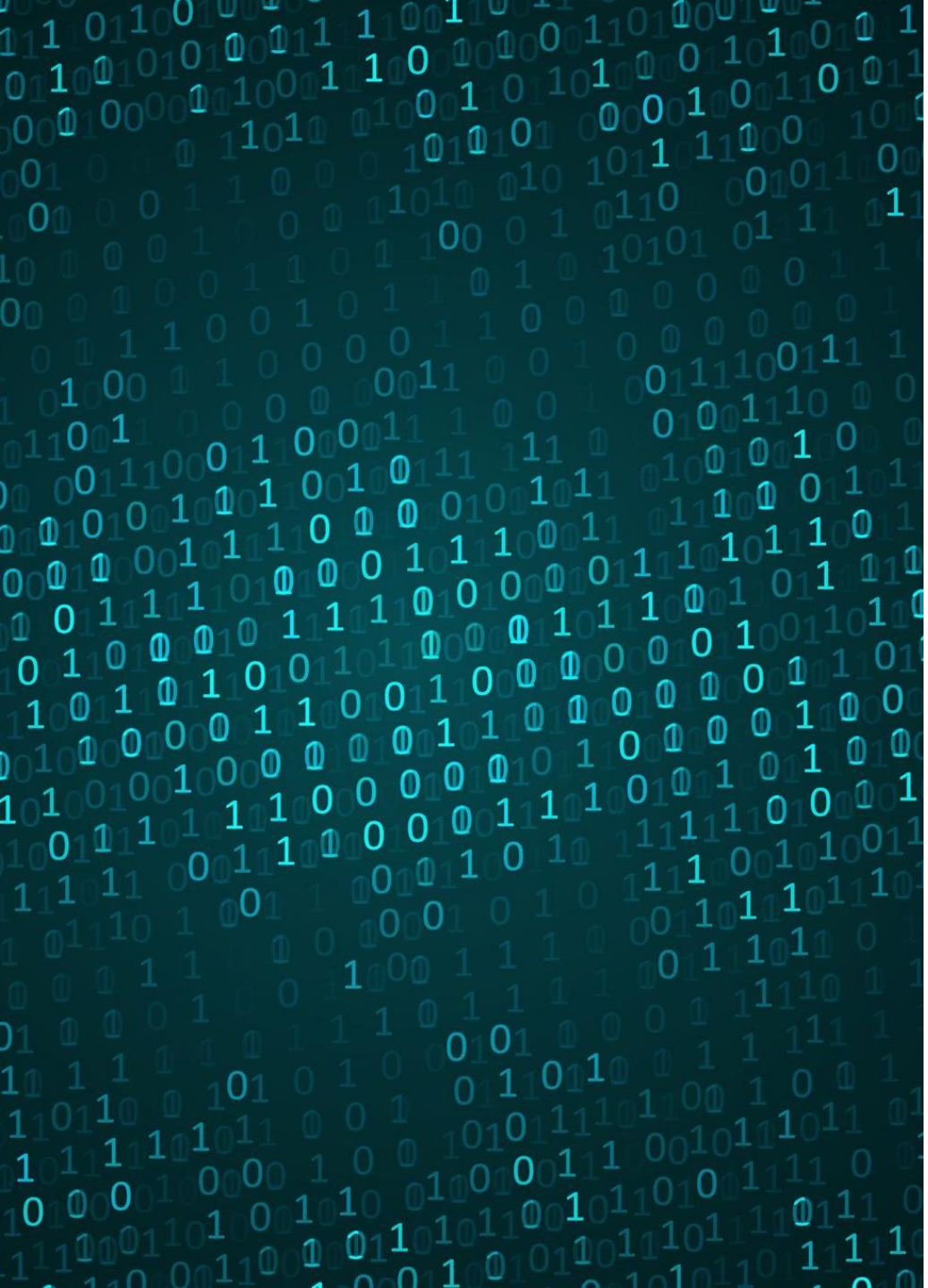
VER TAMBIÉN EN AIC YouTube

Aula virtual de AIC (ACCESO ZOOM)
https://us02web.zoom.us/webinar/register/WN_ggJcEPcjQASBuc-ENzeazA

AIC

Introducción a la temática

¿Estamos preparados para enfrentar la creciente amenaza de la guerra digital y los ciberataques globales?



Crecimiento de ciberataques

Los ciberataques están aumentando rápidamente, poniendo en riesgo la seguridad mundial y costos económicos gigantescos.

Impacto económico estimado

Se espera que los costos globales de los ciberataques superen los 10.5 billones de dólares anuales para 2025.

Agenda de la presentación

Desafíos de la ciberseguridad

Explora los retos actuales que enfrenta la ciberseguridad en entornos digitales modernos.

Inteligencia Artificial y aplicaciones

Define qué es la IA y sus diversas aplicaciones en distintos sectores, especialmente en seguridad.

IA en la seguridad de la información

Presenta casos prácticos donde la IA mejora la protección y gestión de la seguridad de la información.

Gestión y futuro de la IA

Analiza el rol de la IA en la gestión de incidentes, junto a desafíos y perspectivas futuras.

Panorama actual de la ciberseguridad

Evolución y sofisticación de los ataques

Crecimiento de ataques

El volumen de ataques cibernéticos ha aumentado de forma considerable en los últimos años, creando mayores desafíos.

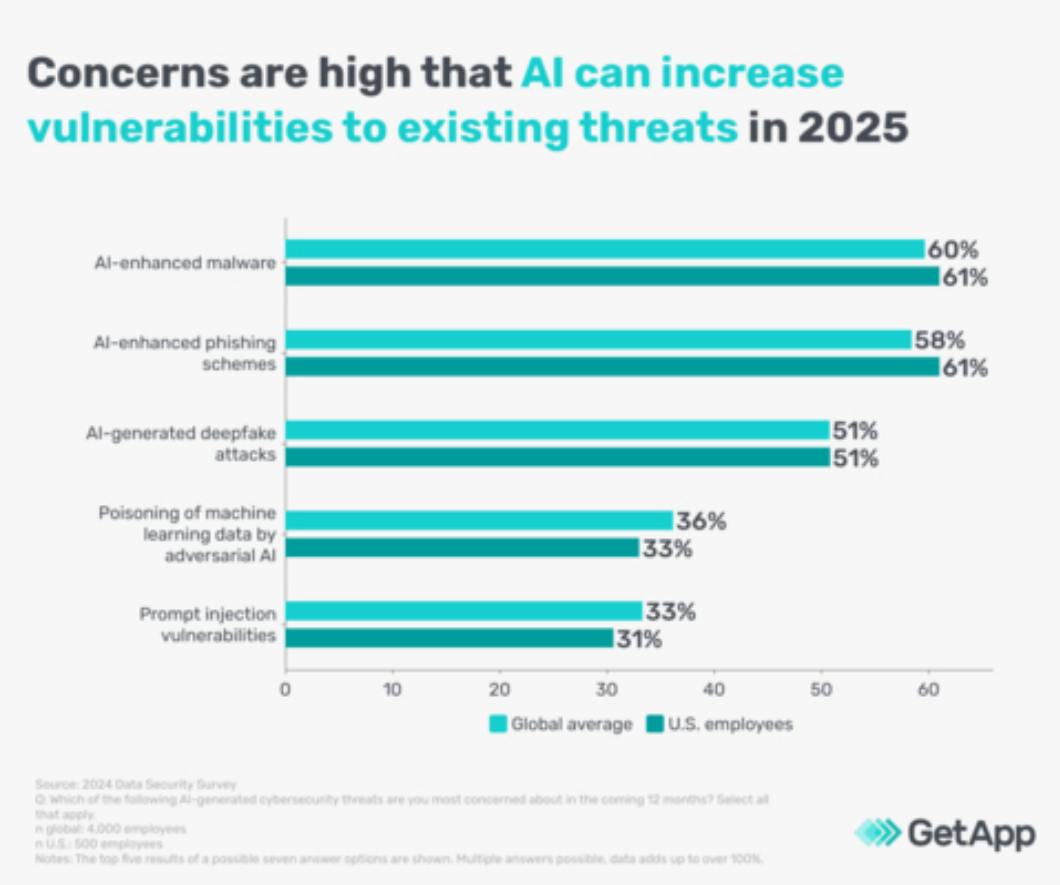
Mayor sofisticación

Los ataques son cada vez más sofisticados, utilizando técnicas avanzadas para evadir defensas y causar daños.

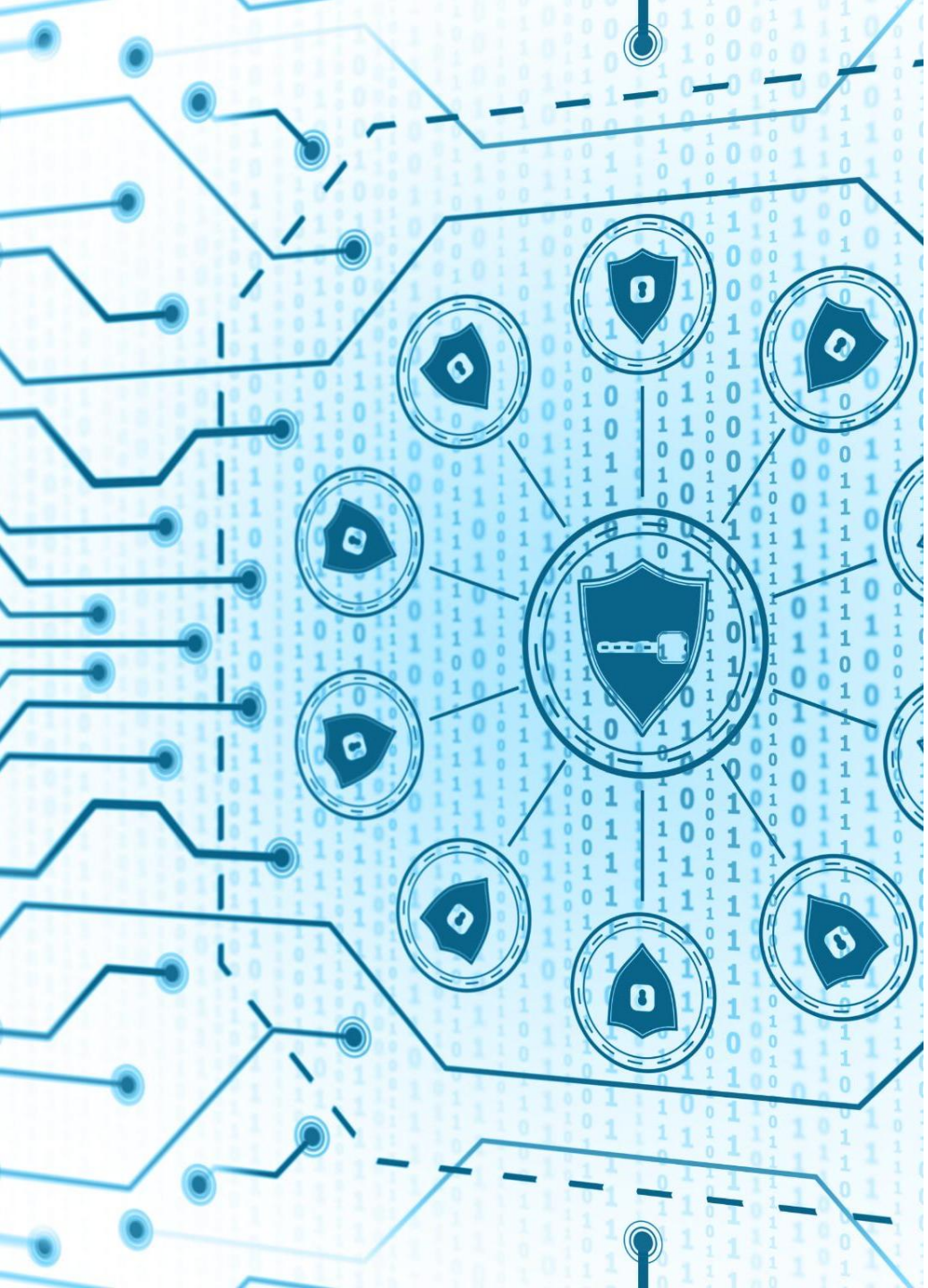
El phishing impulsado por IA está en aumento [¿Qué hacer?]

Orlaith Traynor

Una investigación revela que los ciberataques generados por IA son los ataques más temidos por los empleados de TI y los expertos en ciberseguridad en 2025.



Fuente: https://cybelangel.com/rise-ai-phishing/



Amenazas emergentes y limitaciones de métodos tradicionales

Amenazas de Día Cero

Los ataques de día cero representan vulnerabilidades desconocidas que explotan sistemas sin aviso previo, dificultando la defensa.

Malware Polimórfico

El malware polimórfico cambia su código para evadir detección, complicando la identificación con métodos tradicionales.

Limitaciones de los enfoques tradicionales

Obsolescencia de los antivirus y firewalls clásicos

Limitaciones de antivirus clásicos

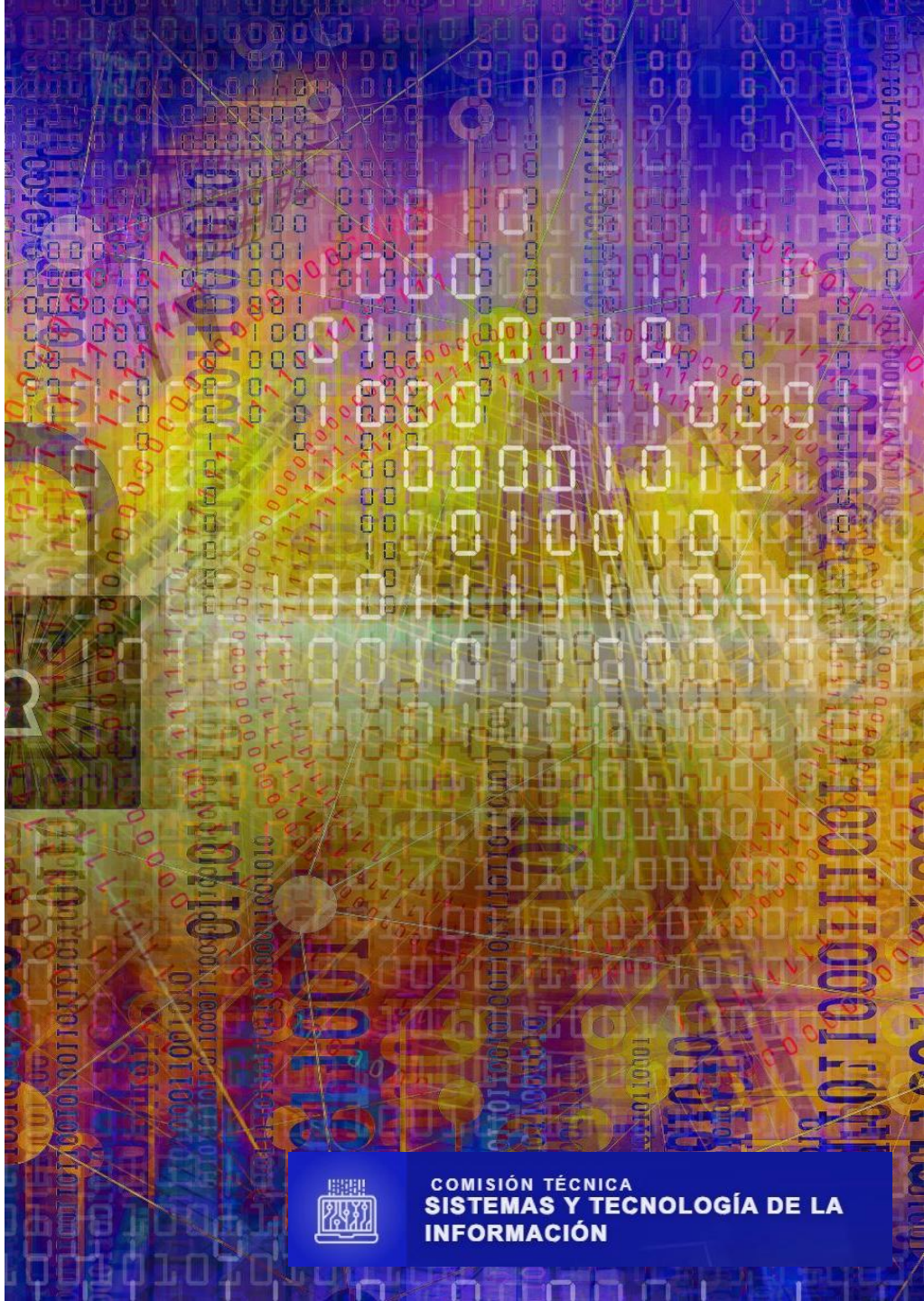
Los antivirus tradicionales usan reglas estáticas que no detectan amenazas nuevas o desconocidas.

Amenazas cibernéticas en evolución

Las amenazas digitales cambian constantemente, superando las defensas basadas en reglas fijas.

Necesidad de seguridad avanzada

Se requiere tecnología inteligente para proteger contra amenazas desconocidas y dinámicas.



Inteligencia Artificial en ciberseguridad: conceptos clave

COMISIÓN TÉCNICA
SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

Definición y tipos de IA aplicados a la seguridad

Machine Learning

Algoritmos que identifican y aprenden patrones a partir de grandes conjuntos de datos para mejorar decisiones de seguridad.

Deep Learning

Redes neuronales que analizan datos complejos para detectar amenazas avanzadas en sistemas de seguridad.

Aplicaciones prácticas de la IA en ciberseguridad

Casos de uso y ejemplos visuales

Detección de malware

Identificación precisa de malware mediante el análisis detallado de archivos sospechosos para proteger sistemas.

Análisis de comportamiento (UEBA)

Monitoreo y análisis de patrones normales para detectar actividades anómalas y posibles amenazas.

Prevención de phishing

Protección contra correos electrónicos fraudulentos mediante la detección y bloqueo de ataques de phishing.

Optimización de cifrado

Mejoras en la seguridad de datos mediante técnicas avanzadas de cifrado en la nube.

Análisis de vulnerabilidades

Escaneo exhaustivo de sistemas para identificar y corregir vulnerabilidades antes de que sean explotadas.

Ejemplo: Análisis de comportamiento UEBA

Concepto de UEBA

UEBA analiza patrones de comportamiento de usuarios y entidades para detectar anomalías en la seguridad.

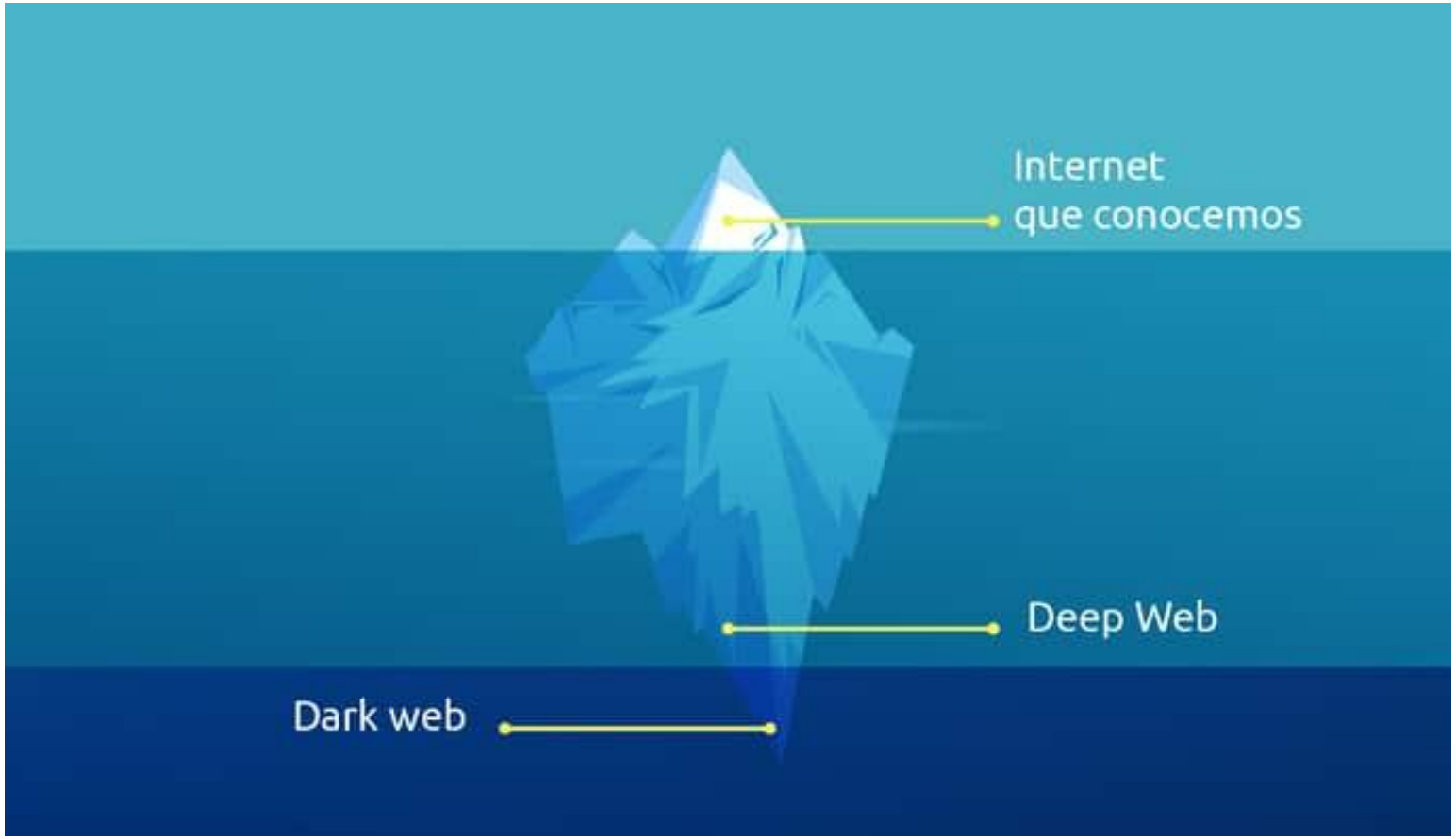
Comportamiento Normal

Ejemplo de comportamiento normal incluye horario laboral y ubicación habitual de acceso sin alertas.

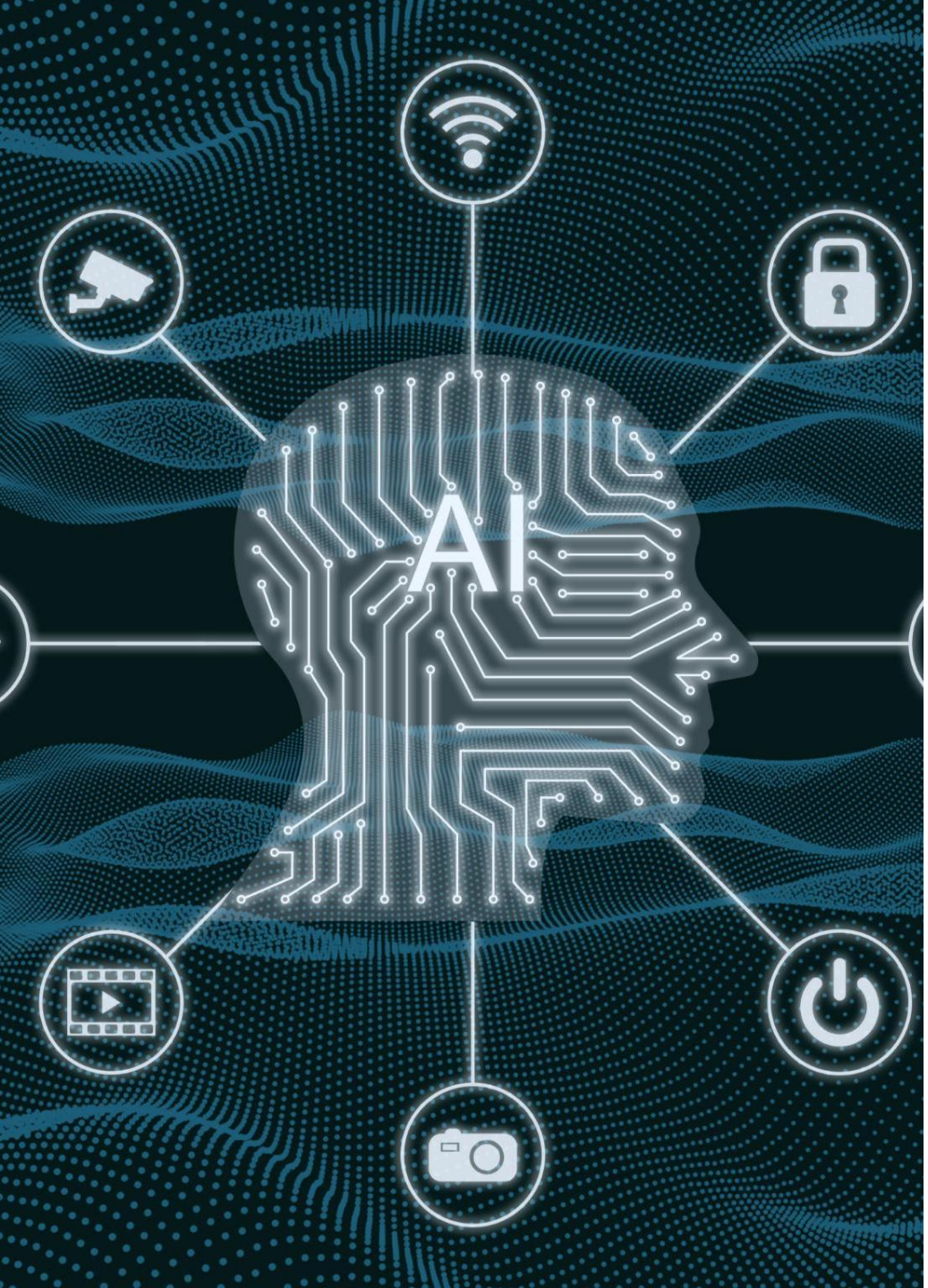
Alerta de Comportamiento Anómalo

Inicio de sesión inusual a las 3 a.m. desde un país nuevo genera alerta en el sistema UEBA.

Búsqueda y análisis de la información en la Deep y Dark Web



La IA en la gestión y respuesta a incidentes



Automatización y aceleración de la respuesta

Respuesta automatizada rápida

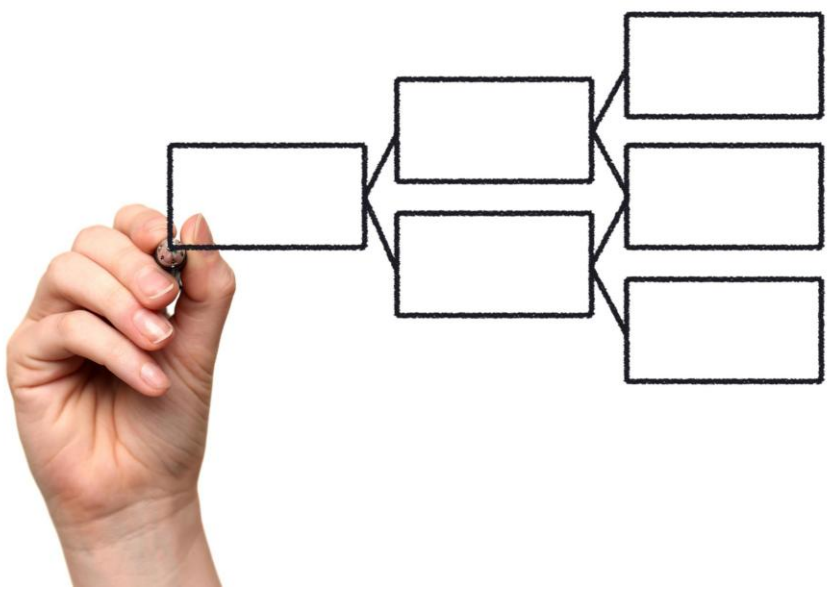
La IA permite respuestas automáticas inmediatas, reduciendo el tiempo de reacción de días a segundos.

Análisis forense asistido

La inteligencia artificial facilita un análisis forense eficiente, acelerando la investigación de incidentes.

Aprendizaje continuo

Los sistemas de IA aprenden constantemente de nuevos datos para mejorar la gestión y prevención de incidentes.



Aislamiento y mitigación automatizada de amenazas

Detección de Amenazas

La detección rápida de amenazas es esencial para iniciar respuestas automatizadas eficientes y minimizar riesgos.

Decisión Automatizada por IA

La inteligencia artificial evalúa la amenaza y decide el mejor curso de acción para su mitigación inmediata.

Aislamiento del Dispositivo

El dispositivo comprometido es aislado rápidamente para evitar la propagación de la amenaza en la red.

Bloqueo de IP Maliciosa

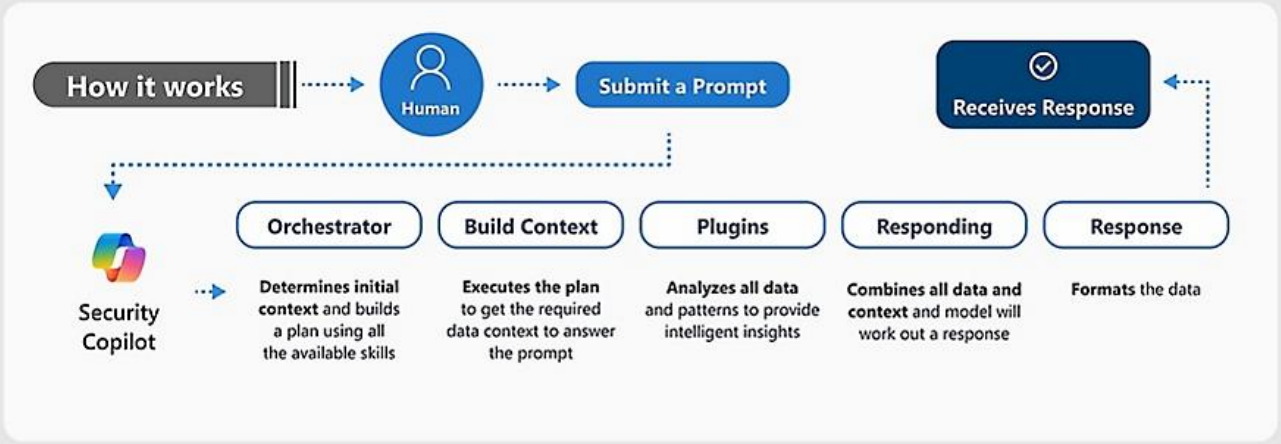
Se bloquea la dirección IP maliciosa para impedir accesos futuros y proteger la infraestructura.

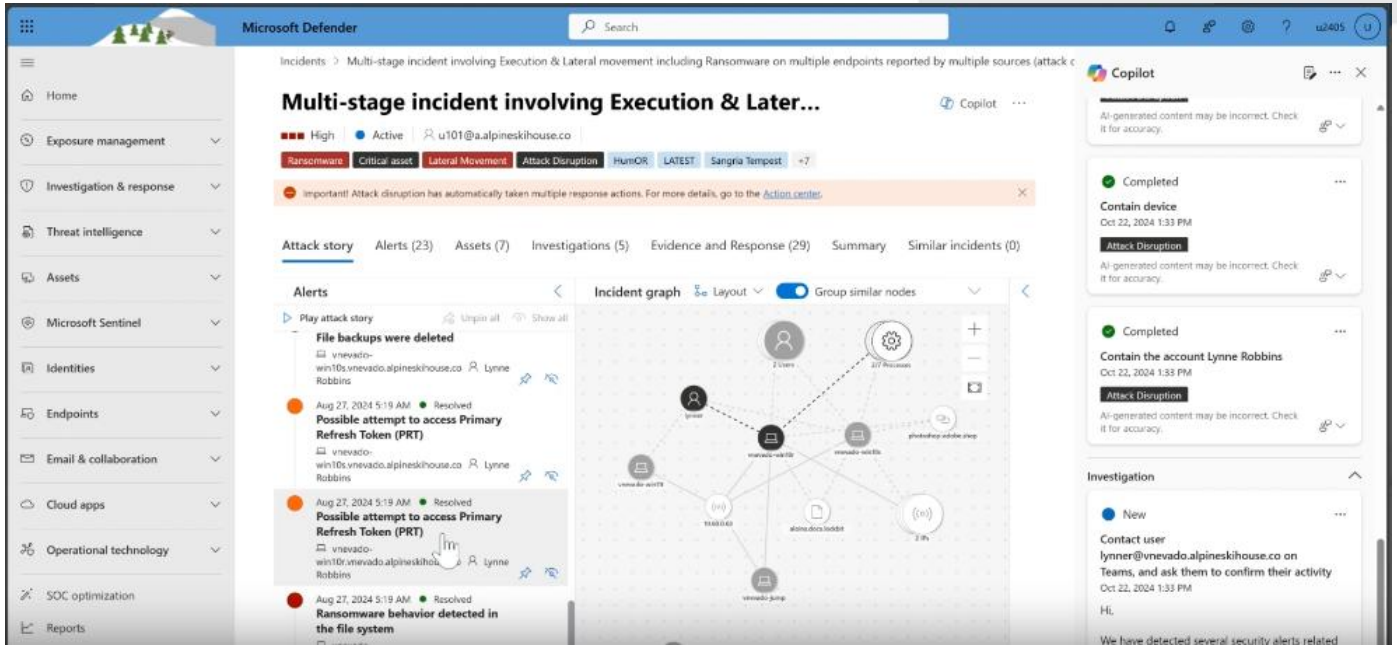
Ejemplo:

Security Copilot

Coverage and Capabilities

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI, while remaining compliant to responsible AI principles.





Desafíos, riesgos y futuro de la IA en ciberseguridad

Principales riesgos y dilemas éticos

IA Adversarial

La IA adversarial representa ataques que manipulan sistemas inteligentes generando resultados engañosos o maliciosos.

Falsos Positivos

Los falsos positivos ocurren cuando sistemas señalan alertas incorrectas que pueden causar desconfianza o errores de juicio.

Ética y Privacidad

El equilibrio entre ética y privacidad es vital para proteger datos personales y garantizar seguridad en la tecnología.

Visión de futuro y rol del experto humano

Ciberseguridad Autónoma

La ciberseguridad autónoma usa inteligencia artificial para proteger sistemas sin intervención constante.

Evolución del Rol Humano

El experto humano no desaparece, sino que su rol evoluciona para supervisar sistemas autónomos.

COMISIÓN TÉCNICA
SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

Conclusión

IA como Escudo de Seguridad

La inteligencia artificial proporciona defensas avanzadas para proteger sistemas y datos contra amenazas cibernéticas emergentes.

IA como Espada de Riesgo

El uso de IA también genera nuevos riesgos y vulnerabilidades que requieren vigilancia constante y manejo ético.

Responsabilidad y Conocimiento

Enfrentar los retos de la IA en ciberseguridad requiere un enfoque responsable basado en el conocimiento y la ética.

Muchas gracias

Bibliografía

COMISIÓN TÉCNICA
SISTEMAS Y TECNOLOGÍA DE LA INFORMACIÓN

- Escobar, D. S. (2025). Identificación de elementos para la elaboración de un marco conceptual no monetario de activos de información. Contabilidad y Auditoría, (61), 77-116.
- Escobar, D. S. (2024). Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA. In JORNADA DE INVESTIGACIÓN. UNIVERSIDAD DEL SALVADOR FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL.
- Escobar, D. S. (2024). Modelo capacitación y sensibilización en ciberseguridad para Contadores Públicos. In JORNADA DE INVESTIGACIÓN 2024. FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES-USAL.
- Escobar, D. S. (2023). CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO. In XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba.
- Escobar, D. S. (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. In XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE.
- Escobar, D. S. (2023). Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras. In XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE.
- Escobar, D. S. (2023). EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN EN LA FORMACIÓN PROFESIONAL DEL CONTADOR. In XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba.
- Escobar, D. S. (2023). La profesión contable ante los desafíos de la inteligencia artificial Chat GPT. In XXVI Congreso Nacional de Contabilidad. Colegio de Contadores del Paraguay.
- Escobar, D. S. (2022). Requisitos mínimos de concientización para usuarios de Canales Electrónicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-3), 1-8.
- Escobar, D. S. (2022). Identificación de estándares de seguridad de la información aplicables a los sistemas de información contable digitalizados. In XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO.
- Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria (Doctoral dissertation, Universidad de Buenos Aires (UBA)).
- Escobar, D. S. (2022). El rol del Contador en la era digital. In VI Jornadas de Orientación Vocacional. UBA.
- Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. In ECON 2022. UBA.
- Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. In XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO.
- Kimura, E. B. S., & Escobar, D. S. (2021). Gestión de la ciberseguridad en sistemas contables digitalizados. In Ciclo" Universidades Iberoamericanas Dialogan". UBA.
- Escobar, D. S. (2021). Mejores políticas para reducir los riesgos de alojar el sistema de información en la Nube. In ECON 2021. Facultad de Ciencias Económicas.
- Escobar, D. S. (2018). Replanteo en el análisis de las contingencias, oportunidades y amenazas de los desvíos en los Estados Financieros Prospectivos. Gestión Joven, (18), 11.