UN EXPERTO OPINA
JORGE MERCHÁN
CEDIA

WALTER FUERTES
ESPE

VTIC DESDE CEDIA
Boletín de Vigilancia Tecnológica e Inteligencia Competitiva;
Innovando en el Sector de la Ciberseguridad

OPORTUNIDADES, EVENTOS Y FONDOS
Información relevante sobre innovación y transferencia tecnológica

CONNECT Noticias

MARKETT

cedia

LA PRIMERA REVISTA ECUATORIANA DE VIGILANCIA Y TRANSFERENCIA TECNOLÓGICA PARA LA INNOVACIÓN

Nº 15

ISSN 2806-5816 Edición Nº15 JUNIO 2024

VTIC INNOVANDO EN EL SECTOR DE LA CIBERSEGURIDAD

connect

www.cedia.edu.ec

cedia

in ▶ X f ⓘ ⟶ @CediaEc

TICEC 2024

LOJA-ECUADOR

16 - 18 OCT

X f @CongresoTICEC

ORGANIZAN: cedia · UTPL

ticec2024.cedia.edu.ec

cedia.edu.ec

LOJA - ECUADOR 16 - 18 OCT · LOJA - ECUADOR 16 - 18 OCT · LOJA - ECUADOR 16 - 18 OCT · LOJA - ECUADOR 16 - 18 OCT · LOJA - ECUADOR 16 - 18 OCT

cedia

connect

Nº 15
JUNIO 2024

LA PRIMERA REVISTA ECUATORIANA DE VIGILANCIA Y TRANSFERENCIA TECNOLÓGICA PARA LA INNOVACIÓN

REVISTA INTERACTIVA

Navegue por el contenido ampliado de nuestra revista y solicite información al hacer clic en estos símbolos

STAFF

DIRECCIÓN EJECUTIVA
Juan Pablo Carvallo, PhD.

REDACCIÓN Y ESTUDIOS DE VIGILANCIA
Gabriela Valarezo Álvarez
Gisselle Soto Minchalo
Francisco Álvarez Arévalo
Aníbal Macas Villagómez
Esteban Arcos Salamea

DISEÑO Y DIAGRAMACIÓN
Paúl Arévalo García
Samantha Romero Sánchez

ARTÍCULO DE OPINIÓN
Jorge Merchán Lima
Walter Fuertes Díaz

ASESORES TÉCNICOS
Xavier Tintin Gavilanes
Denys Flores Armas
Francisco Reinoso Delgado
Sofía Gómez Illescas

OPORTUNIDADES, BECAS Y FONDOS
Gabriela Valarezo Álvarez
Gisselle Soto Minchalo

FOTOGRAFÍA
CEDIA | Cortesía | Stock

EDICIÓN
Laura Malache Silva
EDITORIAL CEDIA

INFORMACIÓN
innovacion@cedia.org.ec

EDITORIAL

CARLOS GUZMÁN JARAMILLO

Director de Desarrollo de Productos y Servicios CEDIA

Estimados lectores:

En un mundo cada vez más interconectado, la ciberseguridad se ha posicionado en el centro de nuestra atención, planteando desafíos únicos y oportunidades sin precedentes. Como parte de los esfuerzos de CEDIA en promover la vigilancia tecnológica e inteligencia competitiva, nuestra revista Connect se enorgullece en presentar su 15ª edición, dedicada a "Innovando en el sector de la ciberseguridad".

Desde el inicio de la era digital, hemos sido testigos de cómo la tecnología ha transformado todos los aspectos de nuestra sociedad. Sin embargo, este progreso también ha traído consigo una creciente ola de amenazas cibernéticas que ponen en riesgo nuestra seguridad, privacidad y bienestar económico. La innovación en el ámbito de la ciberseguridad no solo es crucial para la defensa contra ataques maliciosos, sino que también ofrece la oportunidad de un futuro más seguro y resiliente.

En la actualidad, enfrentamos desafíos sin precedentes en el mundo digital. El aumento exponencial en el volumen y sofisticación de los ataques cibernéticos exige una evolución constante en nuestras estrategias de defensa y prevención. La ciberseguridad ya no es una opción, sino una obligación para proteger nuestra infraestructura crítica, datos personales y secretos empresariales. En esta edición, exploramos cómo la innovación y la colaboración son fundamentales para adelantarnos a los ciberdelincuentes.

Este año, Connect celebra su quinto aniversario, un hito que nos llena de orgullo y gratitud hacia nuestra comunidad lectora y nuestros colaboradores. En este tiempo, hemos sido testigos de la creciente importancia de la ciberseguridad en el escenario nacional e internacional, destacando su relevancia en la protección de la integridad y privacidad de los datos en un mundo cada vez más digitalizado.

La temática principal de esta edición, "Innovando en el sector de la ciberseguridad", se centra en las últimas tendencias y desarrollos que están moldeando el futuro de este campo. Desde la inteligencia artificial hasta la criptografía cuántica, pasando por la seguridad de la información y la protección de infraestructuras críticas, abordamos cómo estas innovaciones están fortaleciendo nuestras defensas contra las amenazas cibernéticas.

Concluimos esta edición con una invitación a la reflexión y la acción. La ciberseguridad es un viaje colectivo que requiere la participación activa de individuos, empresas y gobiernos. Te invitamos a sumergirte en las páginas de esta edición de Connect, a inspirarte con las historias de innovación y colaboración, y a ser parte de la solución en la construcción de un ciberespacio más seguro para todos.

VTIC desde CEDIA

El desarrollo acelerado y la integración, cada vez mayor, de las Tecnologías de la Información y la Comunicación (TIC) en nuestra vida cotidiana plantean nuevos desafíos en cuanto a la protección de datos, procesos y actividades. En este contexto, se destaca la importancia de la ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de la información. El potencial emergente de estas tecnologías requiere un enfoque estratégico, donde la vigilancia tecnológica, académica, comercial y competitiva proporciona información crucial sobre su estado actual y sus perspectivas futuras, facilitando así la toma de decisiones empresariales.

Siguiendo esta premisa, las autoridades regulatorias en Ecuador han implementado políticas y estrategias destinadas a resguardar la seguridad del usuario en el entorno digital. A su vez, en CEDIA se ofrecen una serie de servicios que incluyen monitorización continua, inteligencia de amenazas, detección, respuesta y recuperación de incidentes de seguridad, en estricto cumplimiento de la normativa regulatoria ecuatoriana. Además, la temática de esta edición busca crear conciencia sobre la importancia de contar con esquemas de seguridad cibernética sólidos tanto en el ámbito académico como en el sector público y privado.

Dada la amplia gama de aspectos abordados por la ciberseguridad, esta edición analiza el estado académico y tecnológico según los principales enfoques de aplicación, que incluyen personas, hardware, software, redes y estrategias. El exhaustivo proceso de monitoreo proporciona información crucial sobre el ecosistema de Investigación, Desarrollo e Innovación (I+D+i) en ciberseguridad. Además, la sección de vigilancia comercial y competitiva ofrece información estratégica sobre los mercados y su relación con el ámbito académico.

Los datos recopilados no solo ofrecen una visión detallada del entorno comercial, tecnológico y académico, sino también identifican actores clave y oportunidades para fomentar nuevas investigaciones y desarrollos. Esto contribuye al progreso científico, la sostenibilidad y la innovación en Ecuador. La iniciativa de CEDIA no solo impulsa la investigación científica de alta calidad, sino también facilita la colaboración entre empresas y universidades para generar proyectos con un fuerte impacto socioeconómico. Además, resalta la importancia de la ciberseguridad y las consecuencias de las vulnerabilidades en el entorno digital.

INNOVANDO EN EL SECTOR DE LA CIBERSEGURIDAD

La digitalización avanza rápidamente en la sociedad moderna, gracias a las innovadoras tecnologías que promueven la interconexión global. Las Tecnologías de la Información y la Comunicación (TIC) se han tornado esenciales en la vida diaria, abarcando una gran variedad de servicios: financieros, salud, transporte, energía y más. En este contexto, la ciberseguridad se ha tornado en un elemento crucial de la sociedad para salvaguardar los sistemas económicos, políticos, académicos, y para resguardar la privacidad de los datos personales[1].

La ciberseguridad evolucionó para promover prácticas digitales seguras, gestionar riesgos y responder a incidentes. Además, impulsa la innovación tecnológica mediante el desarrollo de soluciones avanzadas, como la inteligencia artificial y el aprendizaje automático, para combatir las amenazas cibernéticas cruciales. A pesar de que se han logrado avances significativos, persisten desafíos como la adaptación a las tácticas cambiantes de los ciberdelincuentes, la protección de la privacidad digital y la necesidad de estándares internacionales. Abordar estos problemas requiere un enfoque integral que considere aspectos tecnológicos, éticos, legales y sociales[2].

Esta entrega de la revista CONNECT ofrece al lector el abordaje de la ciberseguridad desde varias aristas: vigilancia tecnológica, académica, comercial y del entorno. Esta información permite analizar la situación actual y las perspectivas de la ciberseguridad a nivel regional y global, e informar sobre investigación, tendencias del mercado y regulaciones relevantes. Así, se presentan los últimos avances científicos y tecnológicos sobre ciberseguridad y se presentan oportunidades para fortalecer la protección digital, mitigar riesgos y desarrollar nuevas soluciones. Todo esto orienta a la toma de decisiones estratégicas de seguridad cibernética y, así, contribuir al avance de la investigación, desarrollo e innovación.

REVISA LA INFOGRAFÍA

CONTENIDO AMPLIADO

REVISA EL INFORME COMPLETO

[1]Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

[2]Süzen, A. A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. International Journal of Computer Network and Information Security, 12(1), 1–12. https://doi.org/10.5815/ijcnis.2020.01.01

TENDENCIAS TECNOLÓGICAS DEL SECTOR

La ciberseguridad se define como el conjunto de tecnologías y procesos diseñados para proteger computadores, redes, programas y datos contra ataques, daños o accesos no autorizados. En el año 2023, a nivel mundial, se evidenció un aumento significativo en los riesgos y ataques a la ciberseguridad. Los efectos de estos ataques se dividen en impacto digital (20%); impacto económico (18%); impacto social, en la reputación o impacto psicológico (5% cada uno) e incidentes físicos (1%)[1–3].

El entorno de la seguridad informática abarca varios aspectos que van desde la concienciación individual hasta la implementación de políticas y estrategias administrativas. Es así como se han determinado que las tendencias actuales de ciberseguridad pueden categorizarse desde cinco enfoques distintos, sin alinearse a ninguna categorización convencional:

Individuos

En ciberseguridad, un individuo es cualquier persona considerada un activo por el dominio de gestión. Este enfoque se centra en la conciencientización, conocimiento y comportamiento de individuos al equiparlos con herramientas y conocimientos de protección en ciberseguridad[4,5].

Hardware

Son los componentes físicos materiales de un sistema, como cámaras de seguridad o infraestructura industrial. Los ciberataques, en este sentido, se enfocan en ataques mediante dispositivos USB, el espionaje mediante hardware y las vulnerabilidades en los chips[5,6].

Software

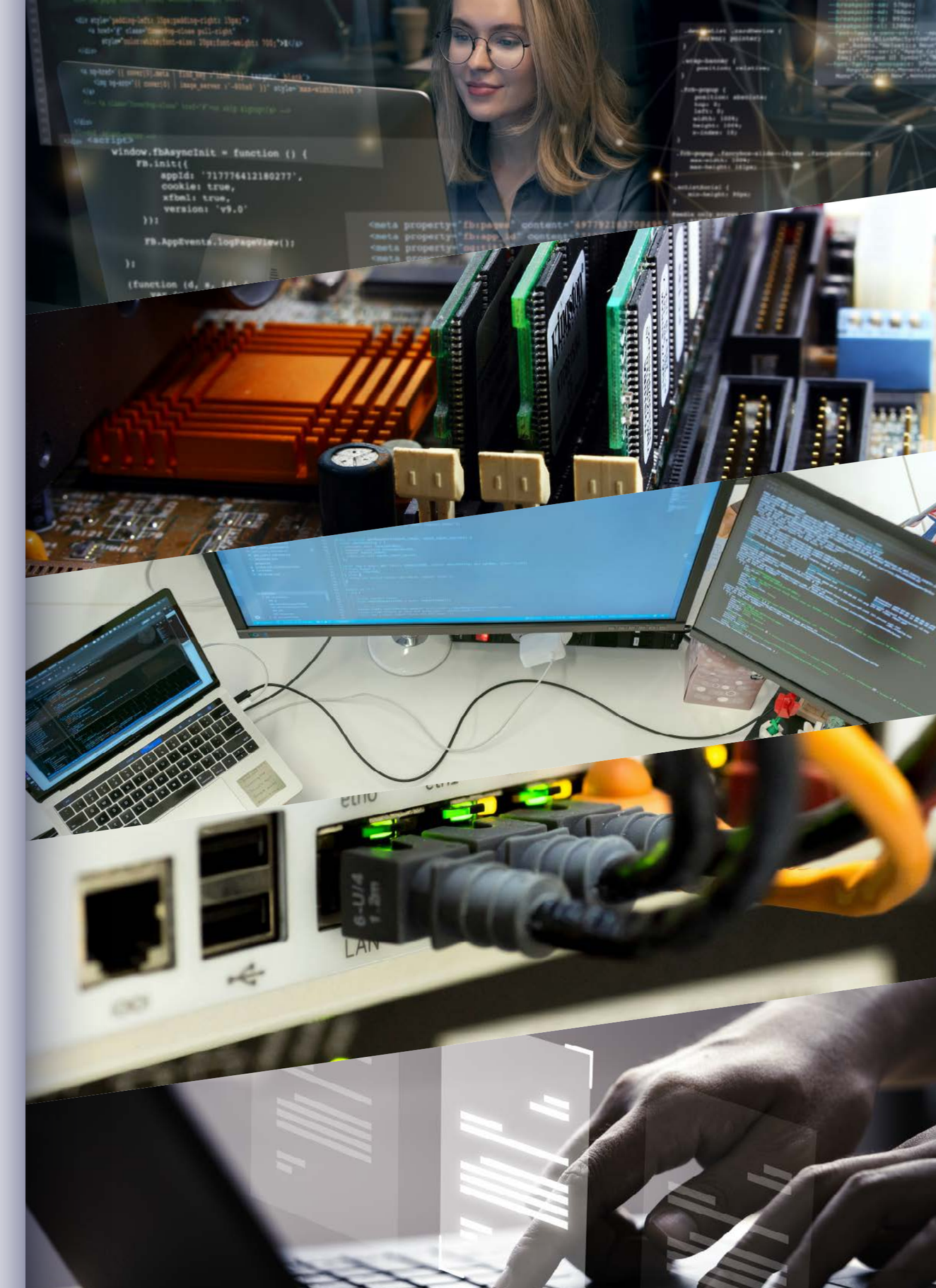
Se refiere a los programas informáticos y datos asociados que pueden escribirse o modificarse y cuyas debilidades pueden ser explotadas por cualquier atacante para comprometer la seguridad, afectando por ejemplo a sistemas de almacenamiento de información[5,6].

Network

Se refiere a ataques destinados a sistemas o información en redes conectados con o sin cables[5,7].

Estrategias de protección

Hace referencia a medidas y acciones planificadas para prevenir, detectar, responder y recuperarse de ataques cibernéticos. Ejemplos de estrategias pueden ser: identificación de vulnerabilidades, gestión de riesgos, la implementación de políticas de seguridad y la gobernanza de la ciberseguridad[5,8].



[1]IBM. (2024). Informe Coste de la vulneración de datos, 2023.
[2]ENISA. (2024). SINGLE PROGRAMMING DOCUMENT 2024-2026. https://doi.org/10.2824/338913
[3]Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00318-5
[4]Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. In Computer Science Review (Bd. 40). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2021.100361
[5]NICCS. (2024). A Glossary of Common Cybersecurity Words and Phrases. https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-s
[6]Arredondo-Méndez, V. H., Para-González, L., Mascaraque-Ramírez, C., & Domínguez, M. (2021). The 4.0 industry technologies and their impact in the continuous improvement and the organizational results: An empirical approach. Sustainability (Switzerland), 13(17). https://doi.org/10.3390/su13179965
[7]Lavorgna, A., & Antonopoulos, G. A. (2022). Criminal markets and networks in Cyberspace. Trends in Organized Crime, 25(2), 145–150. https://doi.org/10.1007/s12117-022-09450-5
[8]Süzen, A. A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. International Journal of Computer Network and Information Security, 12(1), 1–12. https://doi.org/10.5815/ijcnis.2020.01.01

VIGILANCIA TECNOLÓGICA

EVOLUCIÓN DEL DESARROLLO TECNOLÓGICO

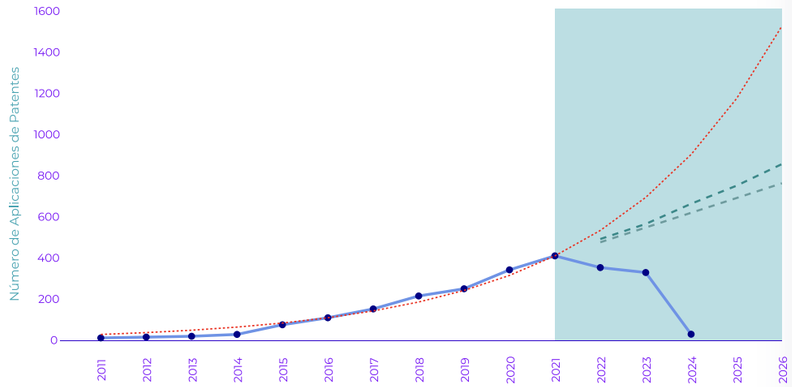
2385 SOLICITUDES DE PATENTES EN EL PERIODO 2012 A 2022 (10 AÑOS)*.

355 SOLICITUDES DE PATENTES SOLAMENTE EN EL 2022.

66 PATENTES EMITIDAS SOLAMENTE EN EL 2022.

*El tiempo promedio del otorgamiento de patentes es de 2.4 años.
Por lo tanto, las tendencias en aplicaciones y aprobaciones se reflejan hasta 2022.

Evolución y pronóstico de aplicaciones de patentes sobre ciberseguridad por año



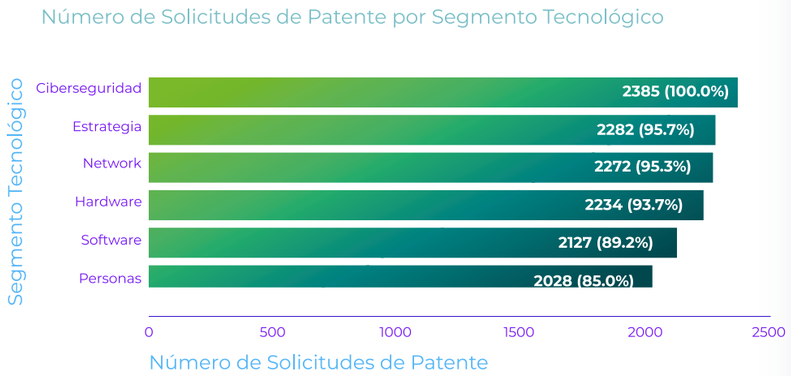
Aplicaciones de patente por año
Pronóstico ETS
Pronóstico ARIMA
Proyección CAGR

El número de aplicaciones de patentes ha variado con una Tasa de Crecimiento Anual Compuesta (CAGR) de 29.99% para el periodo 2016-2021, sin incluir 2022. Este gráfico muestra el número de aplicaciones de patentes por año, junto con los pronósticos utilizando los modelos ETS, ARIMA y su CAGR.

Se pronostica una tendencia de crecimiento sostenido en la aplicación de patentes en los próximos años, demostrando que el estado de la tecnología se encuentra en periodo de crecimiento o, en otras palabras, que anticipa un crecimiento de mercado.

Fuente: PatSnap.

Estado tecnológico por segmento tecnológico



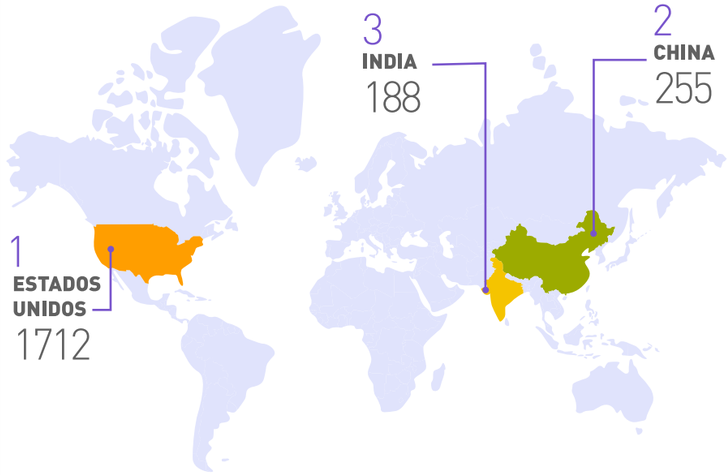
Los resultados son indicativos de la naturaleza holística de la ciberseguridad, dado que las patentes encontradas son una combinación de tendencias. Por ejemplo, una patente en ciberseguridad aplicada a hardware puede involucrar otras tendencias del panorama de defensa cibernética, como software, network, entre otros. Los ataques cibernéticos pueden comprometer datos personales y corporativos sensibles, interrumpir el comercio, todo el funcionamiento de una institución y, en casos extremos, comprometer la integridad de un país[1]. Por ello, son tan potentes los esfuerzos desde distintas perspectivas para mantener un sistema de ciberseguridad robusto y eficiente.

Fuente: PatSnap.

Ranking de países desarrolladores

En la producción de patentes relacionadas con ciberseguridad, Estados Unidos se posiciona como el líder, con una notable concentración de innovaciones en este campo. Esto nos indica que su jurisdicción ofrece ventajas en protección intelectual y existe creciente interés en la investigación e inversión. Le siguen China e India, con una creciente contribución al panorama de desarrollo tecnológico de seguridad digital.

NÚMERO DE PATENTES SOBRE CIBERSEGURIDAD POR PAÍS



*Ecuador no registra patentes relacionadas con ciberseguridad, de acuerdo con la búsqueda.

[1]Lavorgna, A., & Antonopoulos, G. A. (2022). Criminal markets and networks in Cyberspace. Trends in Organized Crime, 25(2), 145–150. https://doi.org/10.1007/s12117-022-09450-5

Fuente: PatSnap.

Estimaciones de valores de patentes relacionadas con la ciberseguridad

El análisis de alrededor de 80 indicadores permite estimar el valor de las patentes en el mercado; para las innovaciones en ciberseguridad se determinó que alrededor de la mitad las patentes tienen un valor menor a $300 000. Con respecto a los demás segmentos, la valorización es similar en todos con mayor porcentaje de patentes con un valor sobre los $3 millones en los segmentos de ciberseguridad enfocada en personas y en software.

SEGMENTO	PORCENTAJE DE PATENTES	VALOR ESTIMADO DEL MERCADO
CIBERSEGURIDAD ENFOCADA EN PERSONAS	42,25	$1 - $30K
	44,91	$30K - $300K
	4,15	$300K - $600K
	6,57	$600K - $3M
	2,11	>$3M
CIBERSEGURIDAD ENFOCADA EN HARDWARE	45,17	$1 - $30K
	42,79	$30K - $300K
	3,99	$300K - $600K
	6,16	$600K - $3M
	1,89	>$3M
CIBERSEGURIDAD ENFOCADA EN SOFTWARE	43,29	$1 - $30K
	43,89	$30K - $300K
	4,28	$300K - $600K
	6,53	$600K - $3M
	2,03	>$3M
CIBERSEGURIDAD ENFOCADA EN NETWORK	46,03	$1 - $30K
	42,20	$30K - $300K
	3,90	$300K - $600K
	6,02	$600K - $3M
	1,85	>$3M
CIBERSEGURIDAD ENFOCADA EN ESTRATEGIAS	46,46	$1 - $30K
	41,83	$30K - $300K
	3,88	$300K - $600K
	5,99	$600K - $3M
	1,84	>$3M

Fuente: PatSnap.

Las organizaciones con los principales portafolios de patentes son de procedencia estadounidense. Sin embargo, se evidencia un proceso de globalización en la innovación en ciberseguridad, pues otros países ya cuentan con un entorno de innovación robusto.

El año de solicitud de la primera patente revela una interesante dualidad en la composición de las empresas. Empresas relativamente jóvenes, con menos de 10 años, han logrado destacarse entre las más prominentes en seguridad digital. En contraste, se mencionan compañías centenarias, inicialmente dedicadas a otros ámbitos, que también han incursionado exitosamente en ciberseguridad.

NÚMERO DE APLICACIONES DE PATENTES SOBRE CIBERSEGURIDAD POR PAÍS

Compañía	Procedencia	Número de Aplicaciones de Patentes	Año de la primera aplicación*
QOMPLX INC	Estados Unidos	168	2015
MICROSOFT TECH LICENSING LLC	Estados Unidos	41	1984
DARKTRACE HLDG LTD	Reino Unido	37	2017
PROOFPOINT INC	Estados Unidos	37	1997
CHITKARA UNIV	India	34	2014
THE BOEING CO	Estados Unidos	32	1922
BLUEST METTLE SOLUTIONS PTE LTD	India	32	2022
HONEYWELL INT INC	Estados Unidos	30	1914
INT BUSINESS MASCH CORP	Estados Unidos	30	1917
SAUDI ARABIAN OIL CO	Emiratos Árabes Unidos	26	1983

* Año en el que la empresa aplicó su primera patente, en cualquier ámbito tecnológico.

Fuente: PatSnap.

VIGILANCIA ACADÉMICA

EVOLUCIÓN EN EL TIEMPO

29854

PUBLICACIONES CIENTÍFICAS RELACIONADAS CON LA CIBERSEGURIDAD EN EL PERIODO 2013 A 2023 (10 AÑOS).

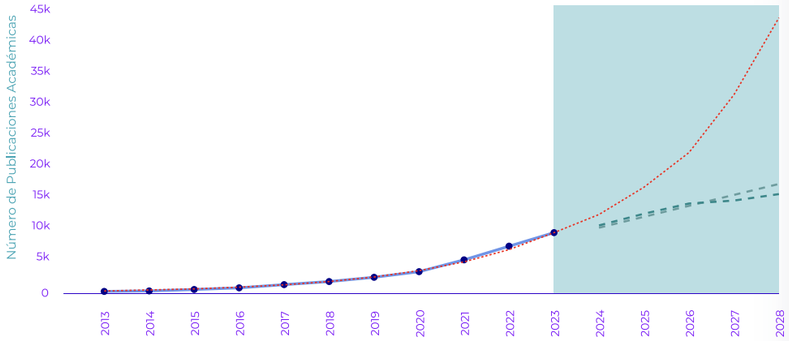
8324

PUBLICACIONES CIENTÍFICAS EN 2023 SOBRE CIBERSEGURIDAD.

38.93%

TASA DE CRECIMIENTO PROMEDIO ANUAL EN EL NÚMERO DE PUBLICACIONES CIENTÍFICAS SOBRE CIBERSEGURIDAD EN LA ÚLTIMA DÉCADA.

Evolución y pronóstico de publicaciones académicas sobre ciberseguridad por año



El número de publicaciones académicas ha variado con una Tasa de Crecimiento Anual Compuesta (CAGR) de 38.93% para el periodo 2018-2023, sin incluir 2024. Este gráfico muestra el número de aplicaciones de publicaciones académicas por año, junto con los pronósticos utilizando los modelos ETS, ARIMA y su CAGR.

Fuente: SCOPUS.

La tendencia ascendente en la cantidad de investigación en ciberseguridad va de la mano con el comportamiento en el otorgamiento de patentes en la industria. La academia no solo sirve como un catalizador de conocimiento, sino que también desempeña un papel esencial en la generación de ideas y descubrimientos que, a su vez, influyen en la actividad patentadora de la industria.

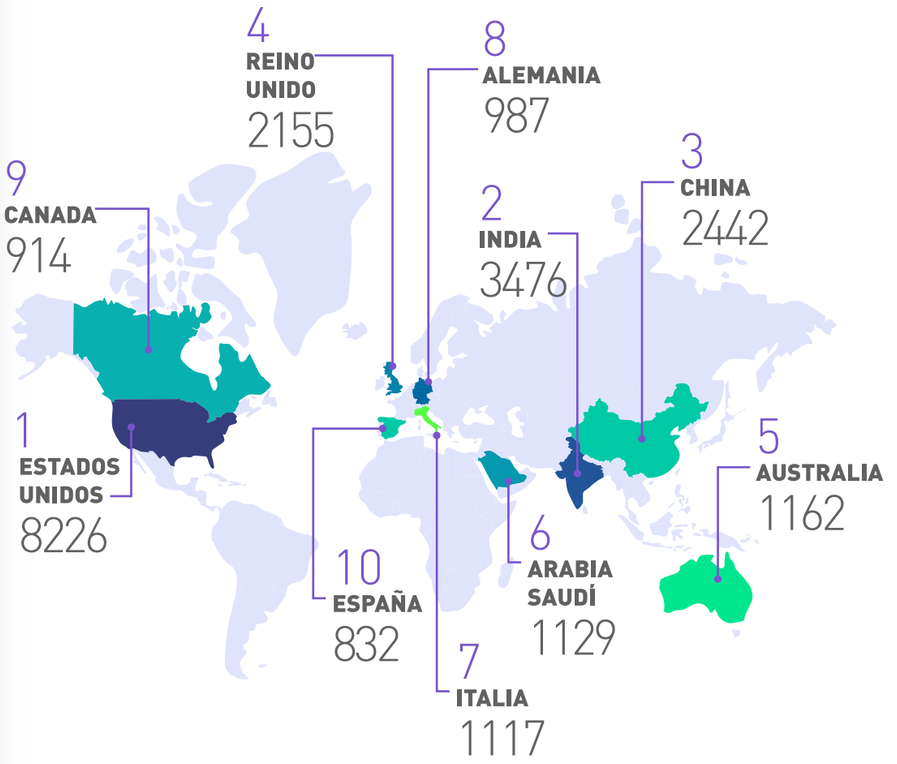
Estado de la academia según segmentos

En contraste con la vigilancia tecnológica, la segmentación de publicaciones científicas sí presenta marcadas disparidades, posiblemente causadas porque los investigadores y generadores de conocimiento suelen dirigirse inicialmente a empresas para vender y patentar innovaciones en lugar de publicarlas.

SEGMENTO	# DE PUBLICS ACADÉMICAS
CIBERSEGURIDAD ENFOCADA EN PERSONAS	1922
CIBERSEGURIDAD ENFOCADA EN HARDWARE	16118
CIBERSEGURIDAD ENFOCADA EN SOFTWARE	6901
CIBERSEGURIDAD ENFOCADA EN NETWORK	2134
CIBERSEGURIDAD ENFOCADA EN ESTRATEGIAS	24173

Fuente: SCOPUS.

Ranking de países con el mayor número de publicaciones en torno a la ciberseguridad



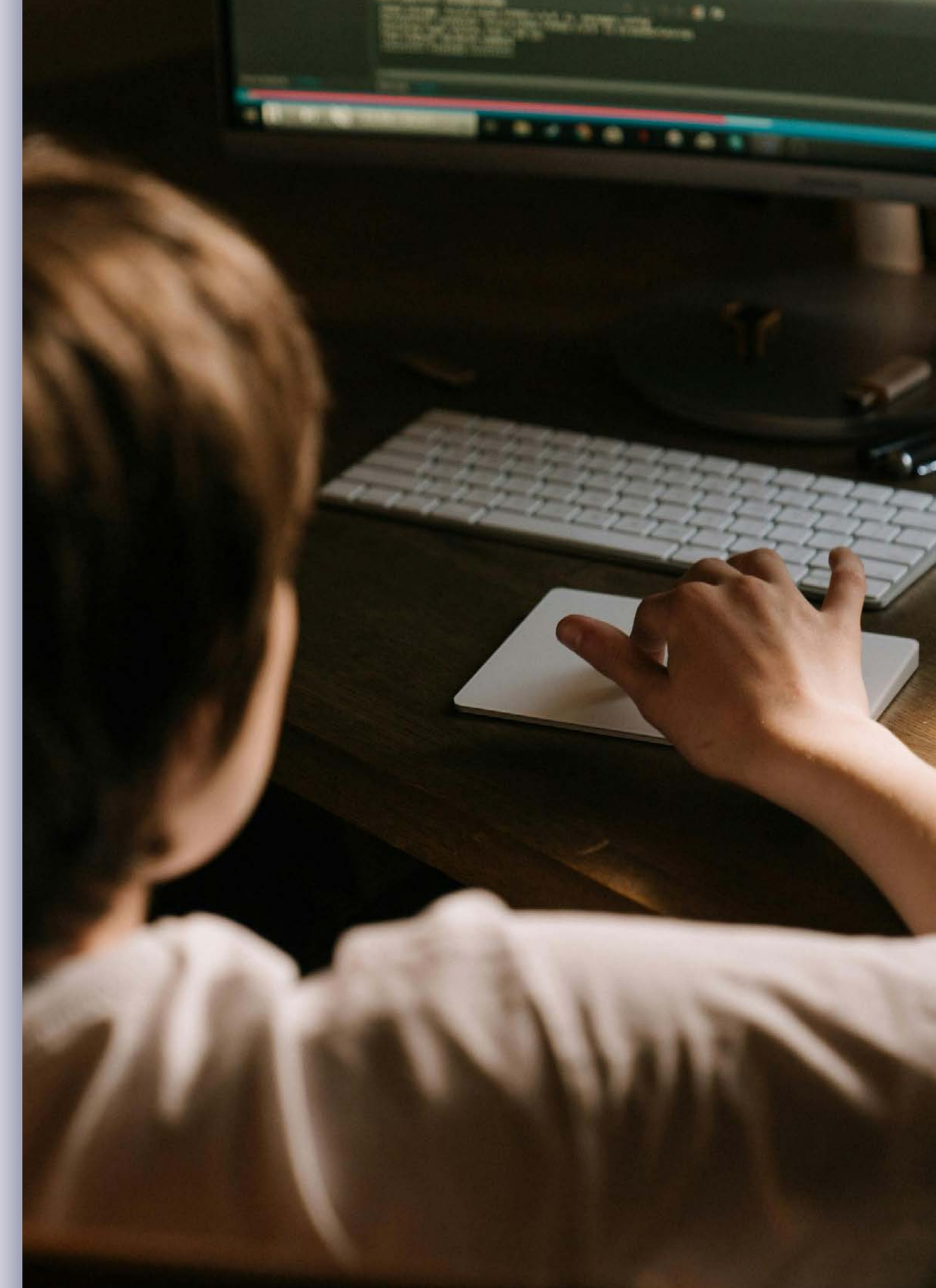
Al igual que la distribución geográfica de patentes en ciberseguridad, la mayor parte de investigación académica se está realizando en Estados Unidos. A diferencia de la vigilancia tecnológica, el segundo país con mayor producción científica es India y el tercero es China. Este fenómeno se correlaciona con el aumento en la innovación en India, ejemplificando cómo el crecimiento en la investigación impulsa la generación de patentes.

Fuente: SCOPUS.

Distribución de la Producción Científica de la ciberseguridad por Área de Conocimiento

Las ciencias de la computación y la ingeniería abarcan el 56.9% de las publicaciones en ciberseguridad y el restante 43.1% refleja la naturaleza holística de este campo; incluye una amplia gama de disciplinas que van desde la ciencia de la decisión hasta las ciencias sociales y la medicina. La investigación en ciberseguridad tiene enfoques interdisciplinarios que incorporan aspectos sociales, éticos y humanos para abordar eficazmente los desafíos emergentes en este ámbito.

Fuente: SCOPUS.



VIGILANCIA COMERCIAL Y COMPETITIVA

TAMAÑO DEL MERCADO

$174.7

miles de millones de dólares en 2024[1]

TASA DE CRECIMIENTO ANUAL COMPUESTA

8.1%

durante el periodo 2020-2024[1]

COSTO DE PÉRDIDAS ECONÓMICAS POR CIBERATAQUES

8000

millones de dólares en 2024[2]

En 2023, a nivel global el

95%

de los ataques a la ciberseguridad costaron a las organizaciones afectadas entre

1 y 2,25

millones de dólares por cada uno[3].

[1]IDC. (2023, November). Top 10 Worldwide IT Industry 2024 Predictions: Mastering AI Everywhere. https://blogs.idc.com/2023/11/01/top-10-worldwide-it-industry-2024-predictions-mastering-ai-everywhere/
[2]CriticalStart. (2023, December). 2024 Cybersecurity Predictions: Navigating the Evolving Threat Landscape. https://www.criticalstart.com/2024-cybersecurity-predictions-navigating-the-evolving-threat-landscape/
[3]Verizon. (2024, January). 2023 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Compañías relevantes a nivel mundial

Compañía	País	Descripción
intel Security	EEUU	Diseña, fabrica y comercializa plataformas informáticas, de redes y de comunicación en todo el mundo. Mediante McAfee ofrece varios productos para el análisis avanzado de amenazas, cifrado de datos, seguridad de endpoints y seguridad de bases de datos.
CISCO	EEUU	Diseña y comercializa amplias líneas de productos enfocados en desarrollar y conectar redes en todo el mundo, integrando soluciones de ciberseguridad avanzadas.
IBM	EEUU	Ofrece una amplia gama de productos y servicios de tecnología de la información (TI) a empresas, gobiernos e individuos de todo el mundo. Opera en ciberseguridad a través de la división IBM Security.
LOCKHEED MARTIN	EEUU	Empresa aeroespacial, de defensa y seguridad global dedicada a dar soluciones militares avanzadas a gobiernos de todo el mundo. La compañía brinda soluciones de ciberseguridad al Departamento de Defensa de los Estados Unidos y sus aliados.
Hewlett Packard Enterprise	EEUU	Ofrece soluciones tecnológicas a empresas comerciales y del sector público, proporciona soluciones de seguridad de aplicaciones que cubren todo el ciclo de vida del desarrollo de software, realiza escaneos de seguridad profundos y comprobaciones en tiempo real para monitorear cualquier presencia maliciosa.

Fuente: NASDAQ. (2024, January). 2024 Cybersecurity Predictions. https://www.nasdaq.com/articles/ai-ransomware-and-election-security-2024-cybersecurity-predictions.

Compañías relevantes en América Latina

Compañía	País	Descripción
Telefónica Tech	Colombia	Ofrece servicios informáticos incluyendo soluciones de ciberseguridad. Identifican riesgos de ciberseguridad del negocio y diseñan un plan estratégico de seguridad que incluya la implementación, gestión y respuesta; además del cumplimiento de la normativa legal permitente.
	Brasil	La compañía Livetech da Bahia, Industria e Comercio S.A. proporciona servicios y productos, incluyendo infraestructura de banda ancha, cámaras de vigilancia, sistemas de control de acceso, ciberseguridad, centro de datos, automatización y generadores de energía solar.
cedia	Ecuador	Provee internet académico de alta conectividad y velocidad que une a las Instituciones de Educación Superior (IES) miembros a nivel mundial. Provee los servicios del SOC- CSIRT de CEDIA que maneja la seguridad de toda la red mediante un avanzado monitoreo y respuesta a ataques cibernéticos. Además, brinda asesoría y capacitación sobre seguridad informática para blindar a las instituciones de las distintas amenazas cibernéticas.

VIGILANCIA DEL ENTORNO

NORMATIVAS REGULATORIAS DE LA CIBERSEGURIDAD EN ECUADOR

1. Constitución de la República del Ecuador.
2. Ley Orgánica de Telecomunicaciones.
3. Ley Orgánica de Protección de Datos Personales.
4. Ley Orgánica para la Transformación Digital y Audiovisual.
5. Acuerdo Ministerial 006-2021 - Política de Ciberseguridad.
6. Estrategia Nacional de Ciberseguridad del Ecuador.
7. ISO 27001 Seguridad de la Información acuerdo Nro. Mintel-Mintel-2024-0003-Esquema Gubernamental de Seguridad de la Información.
8. ISO/IEC 27002:2022-Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.
9. Código Orgánico Integral Penal.

Políticas y reglamentos en Ecuador

Constitución de la República del Ecuador (2008)

• Derecho a una comunicación libre, acceso a las TIC, derecho a la protección de datos personales.
• Determina acciones para acceder a su información personal, alojada en archivos o base de datos de instituciones públicas o privadas.
• Genera facultades que van desde el acceso, modificación hasta la eliminación de información.

Ley Orgánica de Protección de Datos Personales

• Identifica los tipos de datos personales que una organización maneja para contrastar si el tratamiento cumple con lo determinado de los derechos y deberes de los prestadores de servicios y usuarios.

Ley Orgánica para la Transformación Digital y Audiovisual

• Promueve la economía digital global, para las instituciones públicas, empresas privadas y la sociedad.
• Fortalece el uso efectivo y eficiente de las plataformas, las tecnologías digitales, las redes y servicios digitales.
• Busca impulsar la economía y competencias digitales necesarias para el empleo, educación, salud y productividad.

006-2021 Política de Ciberseguridad

• La primera política de ciberseguridad en el país busca fortalecer capacidades para identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad.

Esquema Gubernamental de Seguridad de la Información

• Mecanismo para implementar el Sistema de Gestión de Seguridad de la Información.
• Medidas orientadas a proteger la información, indistintamente del formato en el que se encuentre, contra cualquier amenaza.

UN EXPERTO OPINA

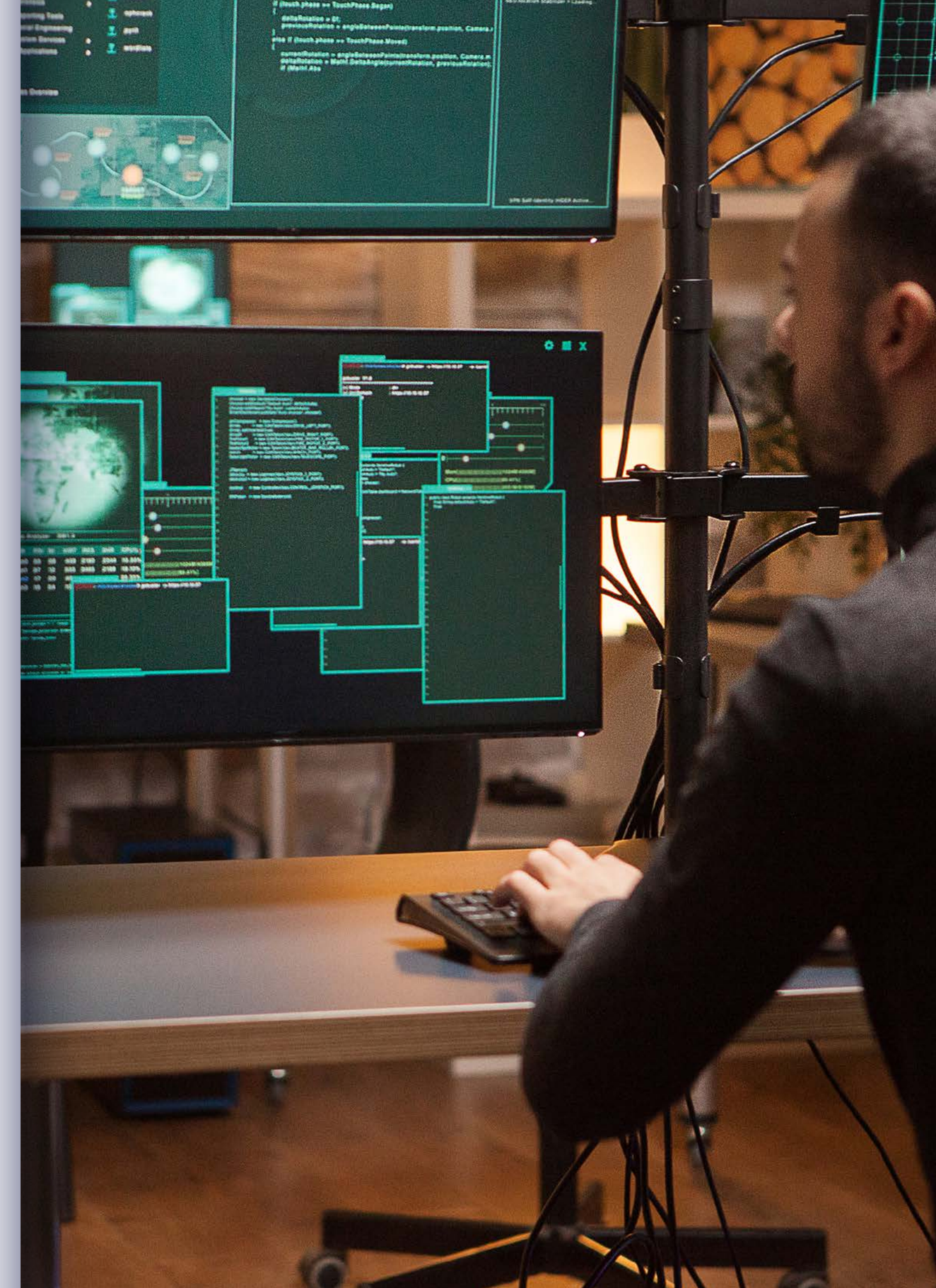
JORGE MERCHÁN LIMA

Gerente de Seguridad de la Información
CEDIA

FORTALECIENDO LA CIBERSEGURIDAD CON ESTRATEGIAS PROACTIVAS E INNOVADORAS

Un vistazo a la evolución y futuro de la ciberseguridad desde una perspectiva SOC-CSIRT

En la constante batalla contra las amenazas cibernéticas, América Latina y el Caribe han atestiguado una evolución significativa en la forma en que se aborda la ciberseguridad. Los Centros de Operaciones de Seguridad (SOC) y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) han sido pilares fundamentales en esta transformación, adaptándose y evolucionando hasta convertirse en entidades proactivas y, eventualmente, predictivas. Este artículo explora la trayectoria de estos centros, sus avances tecnológicos, los desafíos que enfrentan y las proyecciones hacia un futuro más seguro en el ciberespacio, con un enfoque especial en la situación de Ecuador; destacando los beneficios del SOC-CSIRT de CEDIA.



Historia

El concepto de un equipo de respuesta a incidentes de seguridad informática se materializó por primera vez con la creación del Computer Emergency Response Team (CERT) en Estados Unidos, en 1988, tras el incidente del gusano Morris. Este equipo, ahora conocido como CERT Division del Software Engineering Institute (SEI) en Carnegie Mellon University, se estableció con el enfoque de estudiar y contrarrestar las vulnerabilidades de seguridad en redes de computadoras.

En América Latina, Brasil fue el primero en establecer un equipo de respuesta a incidentes de seguridad con la creación del CERT.br, en 1997, gestionando incidentes y promoviendo la concienciación sobre seguridad informática. En Ecuador, el ECU-CERT se estableció oficialmente en 2015 para proteger infraestructuras críticas nacionales y mejorar la seguridad informática en el país.

El concepto moderno de SOC comenzó a desarrollarse en Estados Unidos en la década de 1990, enfocándose en monitorear y proteger infraestructuras de TI contra ciberamenazas, gestionar incidentes de seguridad en tiempo real y asegurar la continuidad de operaciones.

De la reacción a la predicción: La evolución de los SOC y CSIRT

Los SOC y CSIRT han evolucionado de roles reactivos a adoptar estrategias proactivas y predictivas. Utilizan inteligencia de amenazas cibernéticas (CTI) para anticiparse a los ataques mediante el conocimiento del comportamiento del adversario y las técnicas utilizadas. Esto permite una detección más precisa y una respuesta más efectiva.

A diferencia de los CSIRT, que responden a incidentes, los SOC se dedican a la vigilancia continua y la gestión de la seguridad de la información en tiempo real. Juegan un papel crucial en la protección de los activos organizacionales mediante la identificación, análisis y respuesta oportuna a las amenazas cibernéticas. Proporcionan servicios adicionales como la identificación de vulnerabilidades, gestión de inventarios, inteligencia de amenazas y mitigación de riesgos potenciales.

Innovación Tecnológica y el Camino hacia la Automatización

La integración de tecnologías avanzadas, como la inteligencia artificial (IA) y el aprendizaje automático, ha marcado una nueva era para los SOC y CSIRT en América Latina y el Caribe. Según MarketsandMarkets, se prevé un crecimiento anual de IA en ciberseguridad del 23.3% hasta 2026. Estas herramientas han revolucionado la capacidad de análisis de datos en tiempo real, permitiendo la detección de patrones anómalos y la identificación temprana de amenazas emergentes. La colaboración interinstitucional y el intercambio de inteligencia sobre amenazas son esenciales para una defensa cibernética efectiva[1].

Desafíos persistentes y la realidad Actual

América Latina enfrenta desafíos significativos en ciberseguridad, especialmente la escasez de talento especializado. Se proyecta que, para 2024, la región necesitará alrededor de 10 millones de expertos en ciberseguridad. Actualmente, hay un déficit considerable de profesionales capacitados para gestionar y responder a incidentes de seguridad, agravado por la rápida evolución y sofisticación de las amenazas cibernéticas. En 2023, América Latina y el Caribe experimentaron un aumento significativo en la actividad cibercriminal, con incrementos notables en ataques de phishing, ransomware y troyanos bancarios. Según Kaspersky, los ataques de phishing aumentaron un 617%, mientras que los troyanos bancarios vieron un aumento del 50%, equivalente a cinco ataques por minuto en la región[2].

El gasto en servicios de ciberseguridad en América Latina alcanzó los $3,600 millones en 2023, un aumento del 11.1% respecto a 2022, según IDC. Brasil lidera en intentos de phishing con 134 millones de intentos registrados, seguido por México, Ecuador, Perú y Colombia. El uso de malware en ataques ha sido considerablemente alto, con un 78% de los ataques involucrando algún tipo de malware, como spyware y troyanos bancarios[2].

Ecuador: Un caso de estudio en la región

Ecuador ha mostrado un firme compromiso con el fortalecimiento de sus SOC y CSIRT, buscando no solo responder a las amenazas actuales sino también anticiparse a los desafíos futuros. Sin embargo, enfrenta el reto de formar y retener a profesionales de ciberseguridad calificados. En 2023, Ecuador registró más de 12 millones de ciberataques, con adware, troyanos bancarios y spyware siendo los principales tipos de ataques.

Según un informe de ISACA, el 48% de las organizaciones reportaron un aumento en los ciberataques en 2023. Aunque preocupante, esta cifra representa el menor incremento en los últimos seis años, indicando una leve estabilización en el crecimiento de incidentes cibernéticos.

Hacia un futuro más seguro

Según un informe de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), el número de SOC y CSIRT en la región ha aumentado significativamente. En 2022, más del 60% de los países en América Latina y el Caribe tenían al menos un CSIRT operativo, un aumento del 40% en comparación con cinco años atrás.

Un informe de IBM indicó que el uso de tecnologías avanzadas ha reducido el tiempo de detección y respuesta a incidentes en un 50% en algunas organizaciones de la región. Además, la automatización de procesos en SOC ha permitido un manejo más eficiente de los incidentes, reduciendo la carga de trabajo manual y mejorando la precisión en la respuesta.

El desarrollo de talento en ciberseguridad es un desafío continuo. Un estudio de (ISC)² en 2023 reveló que América Latina necesita aproximadamente 600,000 profesionales adicionales en ciberseguridad para cubrir la demanda actual. En Ecuador, la colaboración entre el sector público y privado ha sido crucial para fortalecer la ciberseguridad. El SOC-CSIRT de CEDIA (Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia) es un ejemplo destacado de esta colaboración, proporcionando soporte y recursos para mejorar la seguridad de las instituciones educativas y de investigación en el país.

Beneficios del SOC-CSIRT de CEDIA

Soporte Especializado: Ofrece acompañamiento especializado y colaborativo en la respuesta y manejo de incidentes de seguridad, asegurando una rápida recuperación y minimización de daños, comprometidos con la integridad, confidencialidad y disponibilidad mediante la cooperación interinstitucional.

Concienciación y Capacitación: CEDIA se enfoca en empoderar a individuos y organizaciones con el conocimiento y las habilidades necesarias para defenderse contra las amenazas cibernéticas, reconociendo que la tecnología por sí sola no es suficiente para garantizar la ciberseguridad.

Gestión Proactiva/Predictiva de Riesgos: El SOC-CSIRT de CEDIA se especializa en la vigilancia continua de amenazas cibernéticas y la verificación de actualizaciones y parches de seguridad, permitiendo una gestión de riesgos informáticos integral y anticipada.

Cumplimiento Normativo: Se compromete a fortalecer el cumplimiento de leyes y normativas nacionales e internacionales en ciberseguridad, lo que refuerza la confianza y la seguridad legal de las entidades asociadas, con el objetivo de mitigar el impacto en reputación, financiero, normativo y de infraestructura.

Conclusión

La evolución de los SOC y CSIRT en América Latina y el Caribe ha sido fundamental para enfrentar las amenazas cibernéticas. Estos centros han pasado de roles reactivos a adoptar estrategias proactivas y predictivas, aprovechando la inteligencia artificial y el aprendizaje automático para mejorar la detección y respuesta a incidentes. A pesar de los avances tecnológicos, la región enfrenta una escasez significativa de talento especializado, necesitando alrededor de 10 millones de expertos para 2024. En 2023, los ataques de phishing y troyanos bancarios aumentaron considerablemente, en parte debido al uso de IA. La colaboración entre el sector público, privado y la Academia ha sido esencial para fortalecer la ciberseguridad, que proporciona soporte y recursos indispensables. Finalmente, es crucial que la innovación tecnológica esté acompañada del desarrollo de talento y una cultura robusta de seguridad para enfrentar los desafíos futuros.

[1]El impacto de la IA en la ciberseguridad: ataques avanzados y defensas mejoradas (computerhoy.com).
[2]Panorama cibernético 2023: América Latina bajo asedio de los criminales por aumento de ataques - Infobae.

UN EXPERTO OPINA

WALTER FUERTES DÍAZ

Profesor-Investigador
Departamento de Ciencias de la Computación
ESPE

DETECCIÓN Y PREVENCIÓN DE CIBERCRIMEN

Una solución basada en Inteligencia Artificial y Psicología Cognitiva

Actualmente, la Inteligencia Artificial (IA) vinculada con la Psicología Cognitiva promete varios beneficios y desafíos para la prevención y mitigación del cibercrimen. Esta combinación aprovecha la capacidad analítica de la IA junto con la comprensión de los procesos cognitivos para mejorar la detección de amenazas cibernéticas.

En la actualidad, la academia y la industria han demostrado que las soluciones para el cibercrimen no se enfocan sólo en mecanismos técnicos (Ciberseguridad) [3]. Implica también comprender y abordar el comportamiento humano, es decir, discernir las acciones, reacciones y respuestas de las personas frente a diversas situaciones, estímulos y entornos (Psicología Cognitiva).

En este ensayo se explora cómo la combinación de la IA y la Psicología Cognitiva puede mejorar la capacidad de mitigación a las amenazas cibernéticas. Para lograrlo se analizan tanto los fundamentos teóricos, las aplicaciones prácticas y los desafíos de esta integración, con el fin de proporcionar los fundamentos para el desarrollo de soluciones de ciberseguridad en la lucha contra el cibercrimen.

El cibercrimen puede ocasionar graves consecuencias que van desde pérdidas financieras, violación de la privacidad, hasta la posible afectación a la soberanía nacional. Conforme avanza la tecnología, los criminales cibernéticos mejoran sus estrategias, aumentando tanto la sofisticación como la frecuencia de los ataques [1] [2]. Frente a esta situación, se hace evidente la urgencia de investigar enfoques que trasciendan las soluciones convencionales en el campo de la ciberseguridad.

En respuesta a este desafío, surge como una estrategia el aprovechar el poder de la IA [3], junto con una comprensión de los procesos cognitivos humanos involucrados en las acciones delictivas en línea, para desarrollar soluciones en contra del cibercrimen [4] . Para entender mejor el contexto, a continuación se definen estos elementos:

El cibercrimen engloba a toda actividad ilícita realizada a través de las Tics mediante el uso de computadoras y dispositivos electrónicos en su conexión con el ciberespacio [5]. Esto incluye el robo de datos personales o credenciales financieras, el fraude en línea, la distribución de malware, el secuestro de información (ransomware), el phishing o estafa mediante transacciones bancarias, los ataques a aplicaciones web, y a infraestructuras críticas del Estado, así como otros tipos de actividades criminales que aprovechan las debilidades en sistemas informáticos y redes.

Según la norma ISO/IEC 27032:2012, la ciberseguridad se define como la preservación de la información en el ciberespacio [6], es decir, es la responsable de la seguridad de información en las redes de datos, de telecomunicaciones, de telefonía celular y de las infraestructuras de misión crítica de los Estados.

De acuerdo con la UNESCO, la IA se refiere a sistemas con la capacidad de imitar o replicar algunas de las funciones cognitivas asociadas con la inteligencia humana [7] e incluyen algoritmos de aprendizaje automático, redes neuronales, procesamiento del lenguaje natural y otras técnicas que les permiten aprender de datos, reconocer patrones, tomar decisiones y resolver problemas.

Por su parte, la Psicología Cognitiva, según la Asociación de Ciencias Psicológicas (APS), estudia los procesos mentales como la adquisición de conocimientos, la percepción, la memoria, el razonamiento y la toma de decisiones. Su objetivo es comprender cómo la mente humana procesa información, organiza pensamientos, almacena y recupera remembranzas, y utiliza estos procesos para resolver problemas [8].

Ahora, entrando en materia, en relación con las técnicas de aplicación de IA para combatir el cibercrimen, se emplean diversos algoritmos de Aprendizaje Automático (ML). Entre ellos se destacan: Redes Neuronales Artificiales (ANN), Máquinas de Vectores de Soporte (SVM), Árboles de Decisión (DT), Bosques Aleatorios (RF) y de Aprendizaje Profundo (DL). Además, se utilizan el Procesamiento del Lenguaje Natural (NLP) y el Aprendizaje Automático no Supervisado, como el clustering y la detección de anomalías, para identificar comportamientos sospechosos en el tráfico de red o registros de eventos [9].

En relación con la psicología cognitiva para combatir el cibercrimen, los algoritmos no se emplean directamente en comparación con los de ML. En su lugar, se incorporan modelos, técnicas y tácticas en el diseño e

implementación de soluciones de Ciberseguridad. Estos incluyen el modelado del comportamiento humano para comprender la interacción de los usuarios con los sistemas informáticos y su susceptibilidad a la Ingeniería Social. También abarcan el análisis de riesgos y la toma de decisiones, identificando sesgos cognitivos y desarrollando estrategias para mitigar su impacto. Además, se consideran las tácticas de ingeniería social y manipulación psicológica utilizadas por los ciberdelincuentes [10][11].

En cuanto a las soluciones para combatir el cibercrimen, se pueden citar: Inteligencia de amenazas avanzadas, por su capacidad de analizar grandes volúmenes de datos para identificar patrones de comportamiento anómalos que puedan indicar actividades delictivas en línea. Al combinar este análisis con las motivaciones y comportamientos de los delincuentes, es posible mejorar la detección temprana de amenazas avanzadas. Prevención del fraude, al desarrollar modelos predictivos que identifiquen transacciones financieras sospechosas o actividades fraudulentas en línea. Autenticación de usuarios, al analizar patrones del comportamiento del usuario y combinarlos con las señales de engaño y manipulación en la interacción humana, se desarrollarían sistemas de autenticación más robustos y seguros [12].

Por otro lado, las aplicaciones existentes incluyen la prevención de ataques de Ingeniería Social, como el phishing y el ransomware, mediante el entrenamiento empleando algoritmos de ML para identificar correos electrónicos infectados y otros intentos de suplantación de identidad [13]. También mejora la autenticación biométrica, utilizando IA para desarrollar sistemas que emplean rasgos físicos únicos como huellas dactilares, reconocimiento facial o patrones de voz. Además, la IA se utiliza en el análisis de sentimientos en redes sociales para detectar conversaciones o actividades sospechosas para identificar tendencias y comportamientos delictivos.

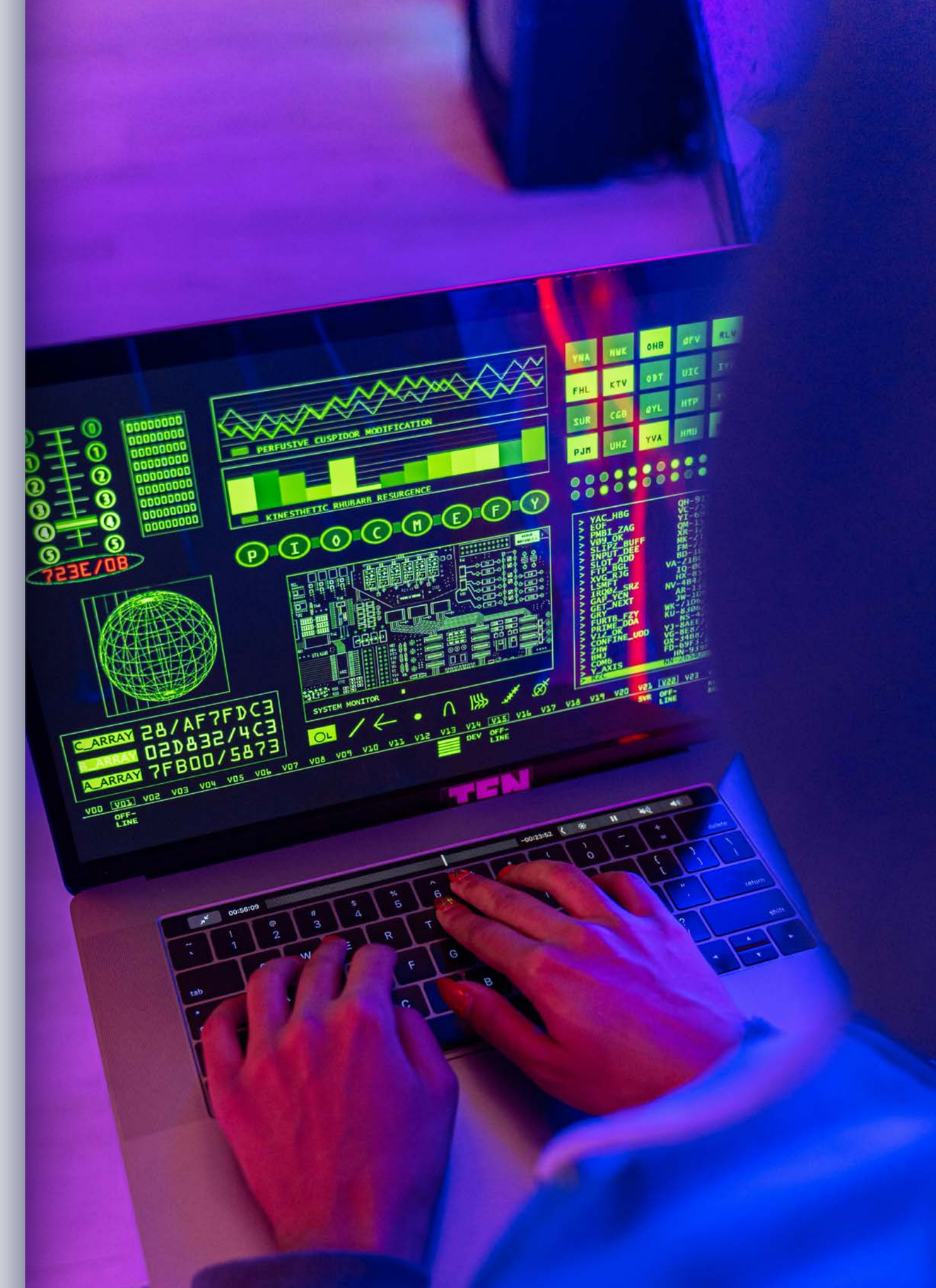
En cuanto a los desafíos y líneas de investigación futuras de la aplicación de la IA y la psicología cognitiva en la ciberseguridad, se siguen desarrollando [14][15][16]. Sin embargo, aún enfrenta retos que incluyen preocupaciones éticas y de privacidad, así como la necesidad de generar una cultura de ciberseguridad, concienciación y entrenamiento del personal [17].

En resumen, esta combinación proporciona un enfoque integral para detectar y mitigar las amenazas cibernéticas. Es decir, al aprovechar el poder de la IA y la comprensión de la mente humana, se pueden desarrollar soluciones más efectivas para proteger sistemas, datos y usuarios contra las crecientes amenazas en el ciberespacio. Además, es muy importante promover una cultura de ciberseguridad, concienciación y capacitación del personal en seguridad de la información, así como la inversión en mecanismos de protección y software especializado a favor de los usuarios y las empresas.

Conclusión

Esta integración en la lucha contra el cibercrimen permite desarrollar soluciones reales para proteger sistemas de información, datos y usuarios, promoviendo la seguridad en un entorno digital dinámico. Aunque los avances en esta área están generando soluciones sofisticadas para combatir amenazas cibernéticas, la implementación de una cultura de ciberseguridad, la concientización del personal y la inversión en mecanismos de protección siguen siendo esenciales para prevenir y mitigar ataques a la ciberseguridad.

[1] https://repositorio.espe.edu.ec/handle/21000/36481.
[2] DOI: https://doi.org/10.1016/j.comnet.2022.109032
[3] DOI: https://doi.org/10.3390/electronics11111692
[4] DOI: https://doi.org/10.1007/978-981-16-6309-3_4
[5] DOI: https://doi.org/10.1186/s13731-019-0105-z
[6] DOI: https://ieeexplore.ieee.org/document/10326028
[7] DOI: https://doi.org/10.1016/j.caeo.2024.100159.
[8] DOI: https://doi.org/10.1007/978-3-031-28073-3_59
[9] DOI: https://doi.org/10.3390/app13095275
[10] DOI: https://doi.org/10.3390/electronics12194007.
[11] DOI: https://doi.org/10.1007/978-3-031-24985-3_28
[12] DOI: https://doi.org/10.1007/978-3-031-03884-6_28.
[13] DOI: https://doi.org/10.1007/978-3-031-03884-6_26
[14] DOI: https://ieeexplore.ieee.org/document/9514039
[15] DOI: https://doi.org/10.1007/978-3-030-60467-7_24
[16] DOI: https://ieeexplore.ieee.org/document/8845626
[17]DOI:https://ieeexplore.ieee.org/abstract/document/10487329

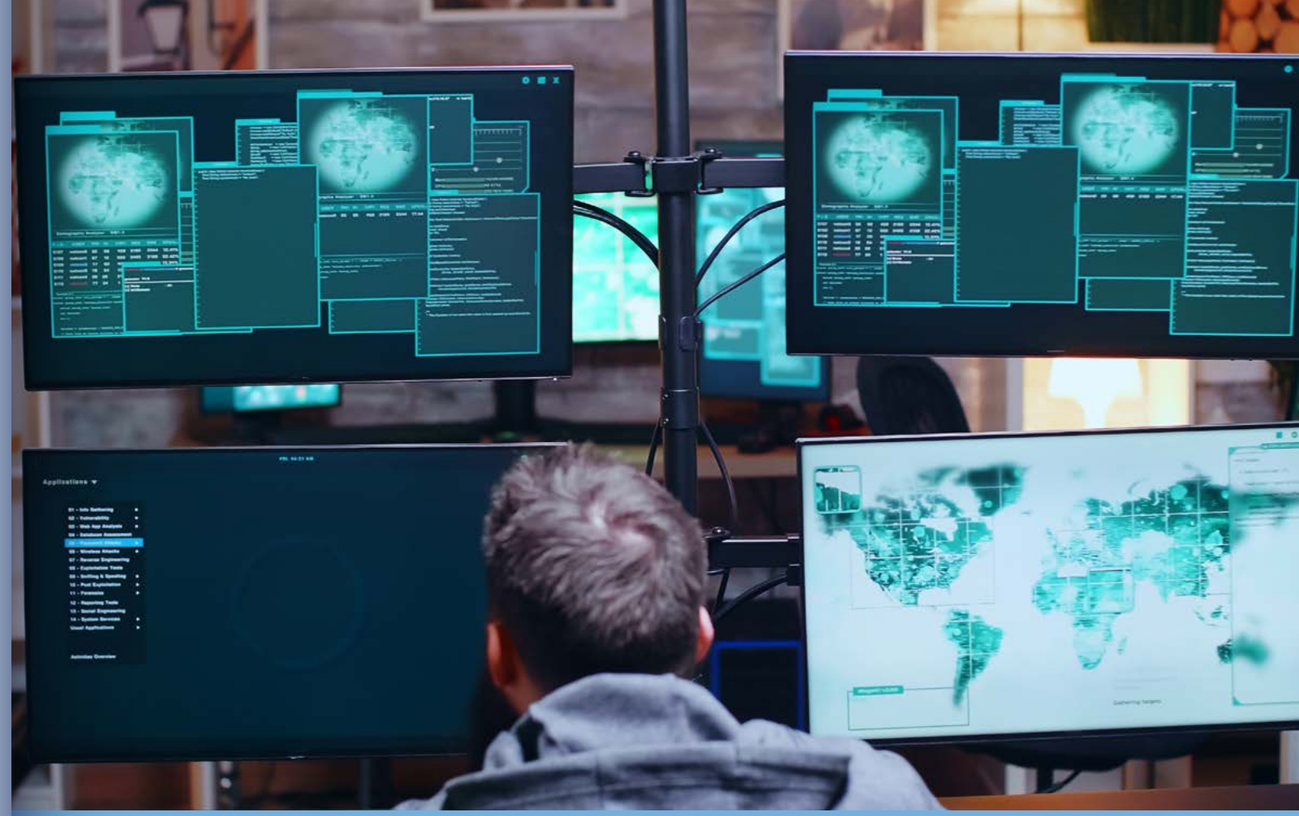


CEDIA participó en el encuentro anual de Erasmus+ en Bruselas, donde se promovieron alianzas para aprovechar las oportunidades del programa. Se capacitó a los Puntos Focales Nacionales (ENFPs) en asistencia técnica para aumentar la participación de los países en el programa. Workshops, charlas y networking generaron dinámicas de articulación entre regiones como África, Asia-Pacífico, América y Medio Oriente, propiciando un diálogo sobre la cooperación internacional en educación superior, centrándose en planes de acción para promover la participación y aumentar las tasas de financiamiento.

CEDIA transferirá estos conocimientos a las Instituciones de Educación Superior (IES) del país, brindándoles asistencia técnica en programas de financiamiento para investigación. Se busca fomentar la colaboración académica a través de la cooperación internacional, con la meta final de incrementar los indicadores de vinculación e internacionalización de las IES en Ecuador. Con estos encuentros, CEDIA reafirma su compromiso con la excelencia académica y la internacionalización de la educación superior en Ecuador.

CONTENIDO AMPLIADO

CEDIA participó en la reunión anual del programa Erasmus+



CEDIA incorporó un Centro de Operaciones de Seguridad (SOC).

En reunión ordinaria de Asamblea General, de fecha 05 de abril del 2024, se dio a conocer la mejora del servicio de ciberseguridad CSIRT, que forma parte del paquete de Red Avanzada ofrecido por CEDIA, incorporando las capacidades de un Centro de Operaciones de Seguridad (SOC). El valor añadido constituye una operación integral de seguridad informática que proporciona una defensa proactiva y en tiempo real contra las amenazas digitales. Al consolidar herramientas de monitoreo, análisis y respuesta, el SOC detecta y responde de manera ágil a las intrusiones y eventos de seguridad, protegiendo así los activos críticos y la integridad de los datos.

Esta iniciativa subraya el sólido compromiso de CEDIA para atender las necesidades emergentes de nuestros miembros. Este servicio reformulado ofrecerá un respaldo esencial para cumplir con diversas normativas y estándares críticos, como la Ley Orgánica de Protección de Datos Personales, el Esquema Gubernamental de Seguridad de la Información, las Normas de Control Interno de la Contraloría General del Estado y la norma ISO 27001, entre otros requisitos relevantes.

RETO CEDIA CIBERSEGURIDAD

CEDIA busca impulsar el desarrollo y capacidades de los estudiantes, a través de la implementación de procesos de innovación que propicien la vinculación Academia-Empresa. CEDIA reconocerá un premio económico al equipo que presente la solución más exitosa y destacada al reto de desarrollo del Sistema de Colaboración de Ciberseguridad para la Comunidad Educativa.

Se realizarán jornadas de capacitación para que los interesados puedan completar los formularios de postulación correctamente, además a los ganadores se les realizara seguimiento de apoyo para la implementacion del proyecto. Un comité de conformado por el equipo de CEDIA y una organización internacional evaluará las postulaciones en función de los componentes solicitados en el formulario de postulación.

Postulaciones abiertas hasta el 15 de julio de 2024.

CONTENIDO AMPLIADO

Por quinto año consecutivo, CEDIA organiza la Semana de la Propiedad Intelectual y esta vez lo hace junto a la Pontificia Universidad Católica del Ecuador- PUCE y el Servicio Nacional de Derechos Intelectuales – SENADI. El evento se desarrolló de manera híbrida, en las instalaciones de la PUCE y en la plataforma virtual ZOOM by CEDIA los días 24 y 25 de abril.

En el marco de esta celebración, se realizarán en paralelo los siguientes sub-eventos:

- Feria Nacional de Invenciones Académicas, es el evento anual más importante del Ecuador dedicado exclusivamente a las invenciones.
- Charlas Magistrales.
- TrendLab - Medicina de Precisión.

Participaron 165 asistentes, y contó con 15 conferencias impartidas por expertos de Colombia, Perú, España, Argentina y Ecuador. Entre los temas que se abordaron en esta edición estuvieron: Inteligencia Artificial generativa: Implicaciones y desafíos para la propiedad intelectual; la titularidad del Derecho de Autor en el Código Ingenios: Aciertos y desaciertos; la Propiedad intelectual y la innovación en el marco universitario.

CONTENIDO AMPLIADO

V EDICIÓN DE LA SEMANA DE LA PROPIEDAD INTELECTUAL

OPORTUNIDADES, FERIAS Y EVENTOS

Eventos anuales del BID

El Banco Interamericano de Desarrollo-BID lanza varios eventos, cursos en línea, conferencias y retos que abordan desde temáticas financieras hasta propuestas en innovación, políticas públicas, medio ambiente y sustentabilidad.

CONTENIDO AMPLIADO

Hacktivity NOW+NEXT: 21TH Edition

El mayor festival de seguridad informática de Europa central y oriental será el espacio donde se intercambiará información acerca de las últimas tendencias en ciberseguridad.

Budapest, Hungría
Del 17 al 18 de diciembre de 2024.

CONTENIDO AMPLIADO

CS4CA LATAM – Cumbre Latinoamericana de Ciberseguridad para Activos Críticos

Esta conferencia tiene como temática principal la ciberseguridad en Latinoamérica, con un enfoque especial en la ciberresiliencia.

São Paulo, Brasil
Del 26 al 27 de noviembre de 2024.

CONTENIDO AMPLIADO

Asociación Interamericana de la Propiedad Intelectual

ASIPI ofrece seminarios gratuitos sobe diferentes temas relacionadas con Propiedad Intelectual (PI), también ofrece varios cursos de markenting vinculados a PI, investigación y Propiedad Intelectual.

CONTENIDO AMPLIADO

Academia de Innovación por PatSnap

PatSnap ofrece una serie de cursos en diferentes ámbitos como: vigilancia tecnológica, innovación, propiedad intelectual para la investigación, y desarrollo y negociación. Además, diversos seminarios web y podcast.

CONTENIDO AMPLIADO

Webinars de la OMPI

La OMPI ofrece seminarios web gratuitos sobre diferentes temas relacionados con Propiedad Intelectual (PI), entre ellos: gestión de la PI, manejo de marcas, gestión de bases de datos, software, cesión de derechos, litigios y licenciamientos, entre otros. Estos eventos se realizan en diferentes horarios y son actualizados constantemente.

CONTENIDO AMPLIADO

AWS re:Invent

Las conferencias propuestas por Amazon Web Services (AWS) son espacios destinados al aprendizaje en la computación de la nube, siendo el evento de mayor concentración de expertos en la nube.

Las Vegas, Estados Unidos
Del 2 al 6 de diciembre de 2024.

CONTENIDO AMPLIADO

International Security Expo

Esta feria es el punto de encuentro de la industria de la ciberseguridad a nivel mundial. Se reúnen a los expertos y líderes en diferentes campos de aplicación.

Londres, Reino Unido
Del 24 al 25 de septiembre de 2024.

CONTENIDO AMPLIADO

Cyber Security & Cloud Expo

Este evento cubre aspectos variados de la ciberprotección y la innovación en este campo, como son: detección de amenazas, conflictos cibernéticos globales, gestión de riesgos, ciber-crímen, entre otros temas.

Amsterdam, Países Bajos
Del 1 al 2 de octubre de 2024.

CONTENIDO AMPLIADO

FONDOS Y RETOS

GLOBAL INNOVATION FUND

Es un fondo de inversión sin fines de lucro con sede en Londres. Apoya proyectos con soluciones innovadoras que provengan de empresas con fines de lucro, organizaciones sin fines de lucro, investigadores y agencias gubernamentales para maximizar su impacto y generar un cambio significativo. Sin plazos ni rondas de financiación.

CONTENIDO AMPLIADO

PAI - programa de asistencia a inventores

A través de abogados probono, el Servicio Nacional de Derechos Intelectuales (SENADI) colabora, sin costo, en el trámite de patentes de inventores independientes. PAI ECUADOR vincula a los inventores con abogados de patentes que estén dispuestos a brindar asesoramiento jurídico gratuito sobre cómo presentar una solicitud de patente para proteger sus invenciones.

CONTENIDO AMPLIADO

FONDO AVANTE — CEDIA

El objetivo es financiar programas de capacitación que promuevan el desarrollo de habilidades y formación de talento humano, en las áreas de conocimiento de interés de las instituciones miembros de CEDIA.

CONTENIDO AMPLIADO

FONDO I+D+i Institutos

Tiene como objetivo el financiamiento de proyectos de procesos de mentoría y de investigación científica y aplicada, desarrollo tecnológico e innovación, propuestos por los institutos miembros de CEDIA, específicamente institutos tecnológicos, y que contribuyan con el desarrollo del país.

CONTENIDO AMPLIADO

FONDO I+D+i

Busca financiar proyectos de investigación científica y aplicada, desarrollo tecnológico e innovación, propuestos por instituciones miembros de CEDIA y que contribuyan con el desarrollo del país, poniendo a disposición de las instituciones participantes los recursos administrativos y tecnológicos que CEDIA tiene disponibles.

CONTENIDO AMPLIADO

FINANCIACIÓN

BID Lab ofrece una amplia gama de productos de financiamiento que pueden combinarse para brindar un mejor apoyo a quienes lo necesitan, el objetivo es cerrar las brechas de financiamiento clave para empresas innovadoras y empresas que impulsan la inclusión y el cambio sistémico en América Latina y el Caribe.

CONTENIDO AMPLIADO

FONDO DIVULGA — CEDIA

Fondo que financia la difusión del trabajo científico realizado por investigadores e inventores pertenecientes a instituciones miembros de CEDIA en eventos científicos de alto impacto a nivel mundial.

CONTENIDO AMPLIADO

KICKSTARTER
Empieza tu proyecto

Kickstarter está diseñado para proyectos creativos en las siguientes categorías: Arte, Cómic, Artesanía, Danza, Diseño, Moda, Cine y vídeo, Comida, Juegos, Periodismo, Música, Fotografía, Publicaciones, Tecnología y Teatro.

CONTENIDO AMPLIADO

FONDO UNO A UNO — CEDIA

El objetivo es cofinanciar propuestas de colaboración Academia – Empresa, en la cual un miembro de CEDIA propone resolver una problemática de una empresa pública o privada a través de la transferencia de conocimiento y/o tecnología.

CONTENIDO AMPLIADO

BECAS

Para realizar estudios de pregrado, posgrado (tanto maestrías como doctorados), así como cursos de corta duración, recomendamos revisar permanentemente las siguientes páginas web.

CONACYT

CONTENIDO AMPLIADO

ERASMUS MUNDUS

CONTENIDO AMPLIADO

FULBRIGHT ECUADOR

CONTENIDO AMPLIADO

FUNDACIÓN CAROLINA

CONTENIDO AMPLIADO

IILA ORGANIZZAZIONE INTERNAZIONALE ITALO-LATINO AMERICANA

CONTENIDO AMPLIADO

OEA

CONTENIDO AMPLIADO

Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

CONTENIDO AMPLIADO

FOR WOMEN IN SCIENCE

CONTENIDO AMPLIADO

Becas del DAAD para Maestrías y Doctorados

CONTENIDO AMPLIADO

WORLD SCHOLARSHIP FORUM

Dirigido a fortalecer las capacidades empresariales del sector agroalimentario para incrementar las exportaciones de productos orgánicos hacia el mercado de la Unión Europea y la Asociación Europea de Libre Comercio (EFTA), con énfasis en el mercado suizo.

CONTENIDO AMPLIADO

BECAS SIN FRONTERAS

La plataforma reúne información de más de 1500 convocatorias de becas. Una buena parte de ellas son becas internacionales ofrecidas por gobiernos, fundaciones, universidades y otro tipo de instituciones, tanto públicas como privadas.

CONTENIDO AMPLIADO

FUNIBER

Ofrece un programa de becas internacionales para estudiar maestrías, especializaciones, doctorados y licenciaturas a distancia (online) y presenciales con titulación universitaria. Las becas son limitadas y dependen de la asignación de las universidades en convenio.

CONTENIDO AMPLIADO

UNIR

La Universidad Internacional de La Rioja mantiene un firme compromiso con el fomento y la expansión de la educación en Ecuador. Por este motivo, promueve acuerdos de colaboración con algunas de las más prestigiosas instituciones de fomento educativo.

CONTENIDO AMPLIADO

SANTANDER BECAS

Un programa regulado por el Banco Santander, S. A con el objetivo de otorgar becas a quienes quieran estudiar en universidades de Argentina, Brasil, Chile, Colombia, España, México, Perú, Portugal, Puerto Rico y Uruguay.

CONTENIDO AMPLIADO

EIFFEL EXCELLENCE

Es el programa de becas de excelencia del Ministerio de Asuntos Exteriores del Gobierno francés. Permite a los estudiantes extranjeros acceder a un posgrado o doctorado con todos los gastos cubiertos hasta cuatro años, en áreas de ciencias, ingeniería, economía, administración, derecho y ciencias políticas.

CONTENIDO AMPLIADO

STUDY IN HOLLAND

Esta beca ofrece ayuda a todos los estudiantes internacionales fuera del espacio europeo que quieran postular a una licenciatura o maestría en los Países Bajos. Está financiada por el Ministerio holandés de Educación, Cultura y Ciencia, además de varias universidades holandesas de investigación y ciencias aplicadas.

CONTENIDO AMPLIADO

THE TRANSFER INSTITUTE

Es una startup irlandesa que ofrece certificaciones, cursos y herramientas basadas en innovación tecnológica y ciencia con el fin de apoyar a profesionales a validar su conocimiento y experiencia en el área.

CONTENIDO AMPLIADO

MAASTRICHT UNIVERSITY

Holland-High Potential Scholarship destinará 24 becas completas para el año académico 2022-2023, dirigidas a personas interesadas en realizar sus estudios de maestría en diferentes ramas académicas por un período máximo de dos años.

CONTENIDO AMPLIADO

LECTURAS DE INTERÉS

Guía de Ciberseguridad para PyMEs

Este documento es una guía completa para proteger a PyMEs de ataques cibernéticos. Describe las amenazas actuales, cómo evaluar riesgos y las medidas de seguridad que se pueden tomar. También ofrece recursos para capacitación y asistencia técnica en caso de un ataque.

Agencia de Desarrollo Internacional de los Estados Unidos (USAID)
2020

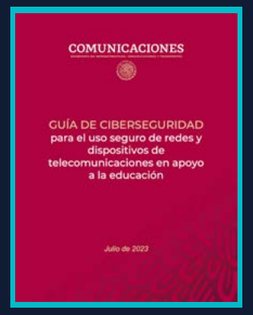
CONTENIDO AMPLIADO

Global Cybersecurity Outlook 2024

Este informe destaca la necesidad de la ciberresiliencia de las organizaciones a nivel mundial. Dentro de los puntos clave está el aumento de las ciberamenazas con tácticas cada vez más sofisticadas, la necesidad de una colaboración global para abordar nuevos desafíos y la disparidad en la preparación cibernética de las organizaciones.

World Economic Forum
2024

CONTENIDO AMPLIADO



Guía de Ciberseguridad

Esta guía busca proteger a la comunidad educativa de los riesgos en el mundo digital. Ofrece recomendaciones generales y específicas para estudiantes, docentes, padres y personal administrativo. Su objetivo es concientizar sobre la importancia de la ciberseguridad, brindar herramientas y promover una cultura de seguridad en el ámbito educativo.

Secretaría de Infraestructura, Comunicaciones y Transportes
2023

CONTENIDO AMPLIADO

Ciberseguridad Industrial

El documento analiza la importancia de proteger los sistemas de control industrial contra las amenazas cibernéticas. Se destaca la importancia de la supervisión y detección de anomalías para identificar comportamientos inusuales y prevenir ataques.

CISCO
2021

CONTENIDO AMPLIADO

MARKETT

SU MEJOR ALIADO EN TRANSFERENCIA Y COMERCIALIZACIÓN TECNOLÓGICA

Un espacio para la difusión de resultados de investigación y desarrollo con potencial de transferencia y de interés para la sociedad.

Limitaciones de MARKETT

MARKETT facilita el contacto inicial entre compradores y vendedores de resultados de investigación y desarrollo que cuentan con derechos de propiedad intelectual. Las posibles negociaciones, así como las ventas, se llevan a cabo fuera de línea y no se concluyen en MARKETT.

Lea los términos y condiciones para usar IP Marketplace aquí.

CONTENIDO AMPLIADO

UCUENCA

ACTIVIDAD ANTICONVULSIVA DEL ACEITE DE CÚRCUMA

PATENTE DE INVENCIÓN

Referencia: Patent No. 2729138 (Patente Comunidad Europea),
Patent No. 9,782,361 (Patente Estados Unidos),
Patent No. 6090867 (Patente Japón)

Problema / Oportunidad

La epilepsia farmacorresistente es aquella que no se controla con los medicamentos actualmente disponibles. Por ello es necesario y urgente la identificación de nuevos compuestos con capacidad anticonvulsiva que además ofrezcan seguridad y mínimo riesgo asociado a su administración crónica.

Producto / Solución

La cúrcuma se utiliza en Asia como alimento desde hace siglos, sin efectos adversos. El aceite de cúrcuma tiene compuestos capaces de controlar convulsiones sin efectos secundarios, convirtiéndolo en un interesante candidato para el tratamiento farmacológico de la epilepsia.

PARA
+ INFO
ESCRÍBENOS

CONNÉCTATE
CON NOSOTROS

¿Eres uno de esos lectores inquietos que requiere más información, profundizar en algunos temas de interés personal en cuanto a tecnología o simplemente deseas compartir tu opinión?

AYÚDANOS A MEJORAR

Si tienes una idea o sugerencia para mejorar nuestra revista, no dudes en escribirnos; tus inquietudes serán respondidas de inmediato y, a su vez, las compartiremos con nuestros lectores.

FÁBRICA DE IDEAS Y CONEXIONES

Si quieres generar propuestas de I+D para una industria u organización académica, si necesitas el apoyo de personal especializado para poner en marcha tu I+D, o si buscas lanzar tu propuesta de innovación, escríbenos y te vincularemos a nuestra RED.

INVITACIÓN PRÓXIMA EDICIÓN

Si estás interesado en formar parte de nuestras próximas ediciones con tu empresa, o si eres un experto en la materia, contáctate con nosotros y únete a nuestro equipo.

PARA + INFO ESCRÍBENOS

cedia

@CediaEc

SOC CSIRT CEDIA

Evolucionamos. Potenciamos

tu ciberseguridad

reduciendo

riesgos digitales.

CONOCE MÁS EN:

soccsirt.cedia.edu.ec

cedia.edu.ec

cedia

www.cedia.edu.ec
info@cedia.org.ec
(+593) 7 407 9300
CEDIAec

Por un Ecuador
que investiga e innova
con niveles de clase mundial
conectando a los mejores.

connect

LA PRIMERA REVISTA ECUATORIANA DE VIGILANCIA Y
TRANSFERENCIA TECNOLÓGICA PARA LA INNOVACIÓN