

	Carátula para entrega de prácticas
Facultad de Ingeniería	Laboratorios de docencia

Laboratorio de Computación Salas A y B

Profesor(a): María de Jesús Quijada Ortiz

Asignatura: Fundamentos de programación

Grupo: 14

No de Práctica: Práctica 1

Integrantes:

- Hernández Cabrera Tania Berenice
- Luna Delgado Lilia Jimena
- Martínez Martínez Ximena Quetzally
- Saldaña Martínez Etna Bárbara
- Trejo López Mía Junuel
- Vazquez Loaiza Angel
- Velazquez Valdes Abigail Estefania

*No. de lista o Brigada 7
brigada:*

Semestre: 2026-1

Fecha de entrega: 25 de agosto de 2025

Observaciones:

CALIFICACIÓN: _____

Objetivo: El alumno conocerá y utilizará herramientas de software que ofrecen las Tecnologías de la Información y Comunicación que le permitan realizar actividades y trabajos académicos de forma organizada y profesional a lo largo de la vida escolar, tales como manejo de repositorios de almacenamiento, búsquedas de información especializada y revisión de información arrojada por generadores de contenido mediante la escritura de un prompt.

Actividades:

1. Realiza la actividad de github en casa que viene en el manual de prácticas, toma captura de pantalla y agrega el link en el reporte de la práctica.

Hernandez Cabrera Tania Berenice

The screenshot shows a GitHub repository page. At the top, there's a navigation bar with links for Código, Cuestiones, Solicitudes de incorporación de cambios, Acciones, Proyectos, Wiki, Seguridad, Ideas, and Configuración. Below the navigation is a search bar with placeholder text 'Escriba para buscar'. The main content area shows a repository named '-practica1_fdp-' under the user 'taniaberenicehlernandez'. The repository is public. It contains one branch ('principal'), one commit ('Actualizar datos'), and three confirmations. The commit details are: 'OLP.webp' (Escudo UNAM y Escudo FI, 4 minutes ago), 'datos' (Crear datos, 8 minutes ago), and 'escudo_fi_color.png' (Escudo UNAM y Escudo FI, 4 minutes ago). There's also a 'LÉAME' file. On the right side, there's an 'Acerca de' section for 'Práctica 1 de fundamentos de programación', which includes activity information like 'Actividad', '0 estrellas', '0 viendo', and '0 horquillas'. Below this is a 'Libera' section with a note about releases and a 'Paquetes' section with a note about packages. A green button at the bottom right says 'Agregar un archivo README'.

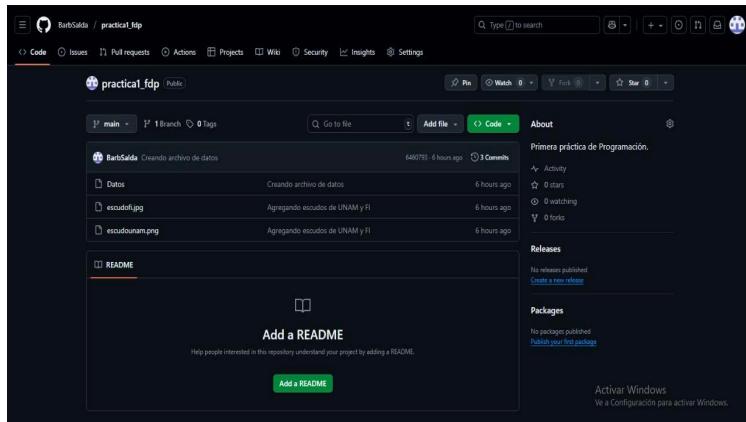
[taniaberenicehlernandez/-practica1_fdp-: Práctica 1 de fundamentos de programación](https://github.com/taniaberenicehlernandez/-practica1_fdp-)

Luna Delgado Lilia Jimena

The screenshot shows a GitHub repository page for 'lilia-luna/practica1_fdp'. The repository has 1 branch ('04fece1') and 0 tags. It contains several commits: 'README.md' (Initial commit, 6 hours ago), 'datos' (Número de cuenta y correo, 5 hours ago), 'descarga.jpg' (Escudos, 5 hours ago), and 'unam.png' (Escudos, 5 hours ago). There's also a 'README' file. On the right side, there's an 'About' section for 'Actividad en casa 1', which includes activity information like 'Readme', 'Activity', '0 stars', '0 watching', and '0 forks'. Below this is a 'Releases' section with a note about releases and a 'Packages' section with a note about packages.

https://github.com/lilia-luna/practica1_fdp.git

Saldaña Martínez Etna Bárbara



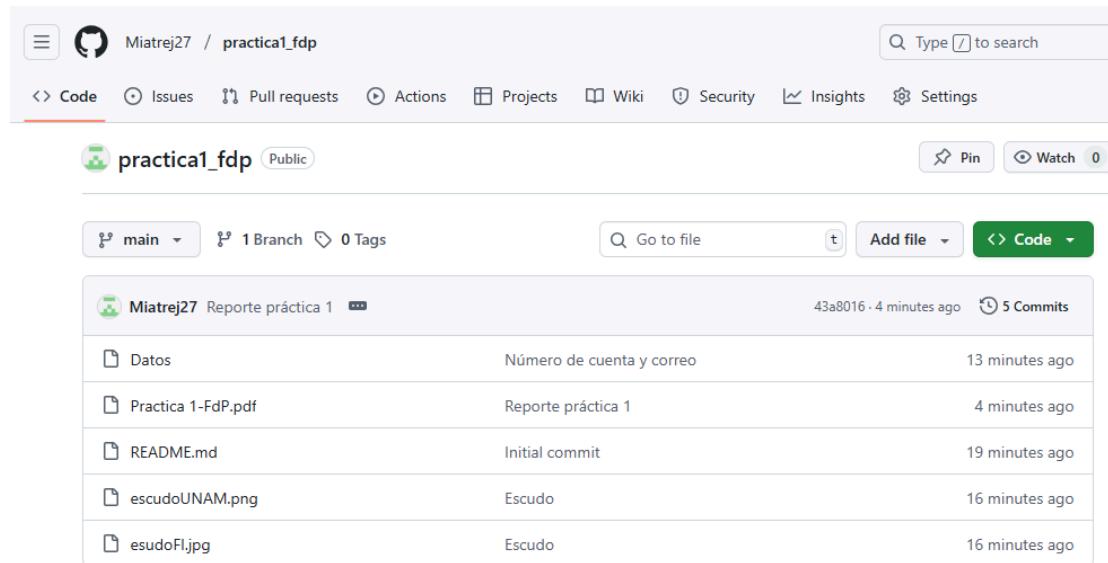
A screenshot of a GitHub repository page. The repository is named 'practica1_fdp' and is public. It has 1 branch and 0 tags. The main branch has 3 commits. The commits are:

- BarbSAlda Creando archivo de datos (6 hours ago)
- Datos Creando archivo de datos (6 hours ago)
- escudofl.jpg Agregando escudos de UNAM y FI (6 hours ago)
- escudounam.png Agregando escudos de UNAM y FI (6 hours ago)

The repository has 0 stars, 0 forks, and 0 watching. There are no releases or packages. A 'README' section is present with a 'Add a README' button.

https://github.com/BarbSAlda/practica1_fdp.git

Trejo López Mía Junuel



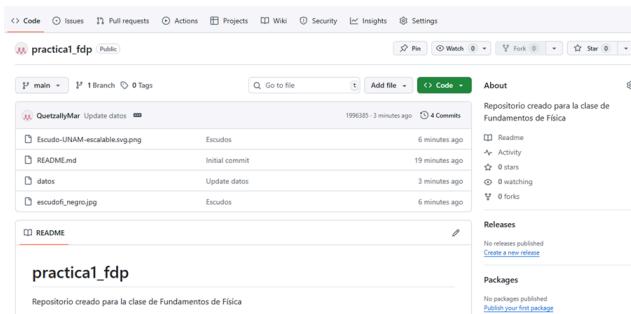
A screenshot of a GitHub repository page. The repository is named 'practica1_fdp' and is public. It has 1 branch and 0 tags. The main branch has 5 commits. The commits are:

- Miatrej27 Reporte práctica 1 (43a8016 · 4 minutes ago)
- Datos Número de cuenta y correo (13 minutes ago)
- Practica 1-FdP.pdf Reporte práctica 1 (4 minutes ago)
- README.md Initial commit (19 minutes ago)
- escudoUNAM.png Escudo (16 minutes ago)
- esudoFI.jpg Escudo (16 minutes ago)

The repository has 0 stars, 0 forks, and 0 watching. There are no releases or packages.

https://github.com/Miatrej27/practica1_fdp

Martinez Martinez Ximena Quetzally



A screenshot of a GitHub repository page. The repository is named 'practica1_fdp' and is public. It has 1 branch and 0 tags. The main branch has 4 commits. The commits are:

- QuetzallyMar Update datos (1996305 · 3 minutes ago)
- Escudo-UNAM-escalable.svg.png Escudos (6 minutes ago)
- READMEmd Initial commit (19 minutes ago)
- datos Update datos (3 minutes ago)
- escudoFI_negro.jpg Escudos (6 minutes ago)

The repository has 0 stars, 0 forks, and 0 watching. There are no releases or packages. A 'README' section is present with a 'practica1_fdp' file.

https://github.com/QuetzallyMar/practica1_fdp

Vazquez Loaiza Angel

The screenshot shows a GitHub repository page for 'practica1_fdp'. The repository is public and has 4 commits. The commits are:

- chocowav Update Datos 02432b2 · 10 minutes ago
- Datos Update Datos 10 minutes ago
- Reporte practica 1.pdf Reporte de practica 1 now
- imagen_2025-08-24_153019513.png Add files via upload 11 minutes ago
- imagen_2025-08-24_153035132.png Add files via upload 11 minutes ago

The repository has 0 stars, 0 forks, and 0 watching.

https://github.com/chocowav/practica1_fdp

Velazquez Valdes Abigail Estefania

The screenshot shows a GitHub repository page for 'practica1_fdp'. The repository is public and has 5 commits. The commits are:

- pruebapro9-sys Reporte practica 1 4458fb4c · now
- Datos Update Datos 7 hours ago
- Practica 1-FdP.pdf Reporte practica 1 now
- README.md Initial commit 7 hours ago
- escudo-UNAM.jpg Escudo 7 hours ago
- escudof.jpg Escudo 7 hours ago

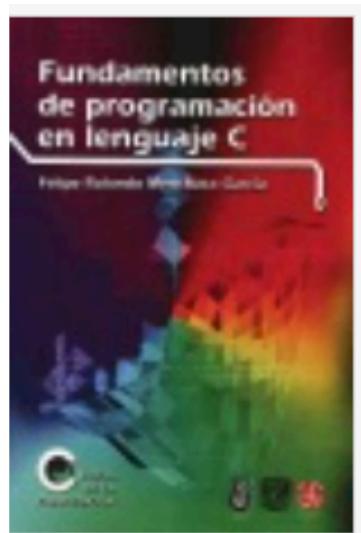
The repository has 0 stars, 0 forks, and 0 watching.

https://github.com/pruebapro9-sys/practica1_fdp.git

2. Registrarse para utilizar la Biblioteca Digital de la UNAM (BIDI).
<https://bidi.unam.mx/> Una vez registrado, realizar una búsqueda en la biblioteca digital de la UNAM de un libro de C, copiar la cita bibliográfica, tomar una foto de la carátula del libro y descargar el libro de ser posible.

Hernández Cabrera Tania Berenice

Menchaca García, F. R. (1999). *Fundamentos de programación en lenguaje C*. LIBRUNAM.



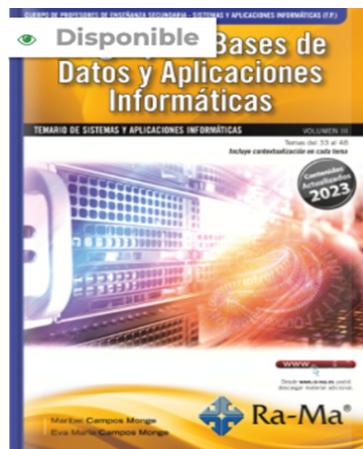
Luna Delgado Lilia Jimena

Ruiz, R. R. (2013). *Una introducción a la programación estructurada en c*. El Cid Editor.



Saldaña Martínez Etna Bárbara

Campos Monge, M., & Campos Monge, E. M. (2023). Lenguaje C, bases de datos y aplicaciones informáticas: Temario oficial de sistemas y aplicaciones informáticas (F.P.). Volumen III.



Trejo López Mía Junuel

Deitel, P. & Deitel, H. (2021). *Cómo Programar En C++*. Pearson HispanoAmerica Contenido.<https://unamex.vitalsource.com/books/9786073255424>

The image shows two versions of the same book cover side-by-side. On the left is the physical book cover, which has a light blue background with the title 'C++ CÓMO PROGRAMAR' in large orange and red letters. Below the title is a stylized 3D cube composed of smaller cubes in shades of orange and yellow. At the bottom left is the Pearson logo, and at the bottom right is the text 'Introducción al nuevo C++14 Estándar'. On the right is a digital version of the book cover, showing a thumbnail of the book's front cover, the title 'Cómo programar en C++', the authors' names 'Paul J. Deitel/ Harvey Deitel', and a table of contents with page numbers.

Contenido	Página
1. Introducción a las computadoras y a C++	1
2. Introducción a las programación en C++ entradas/salidas y operadores	44
3. Introducción a las clases, objetos, funciones miembro y cadenas	73
4. Desarrollo de algoritmos e instrucciones de control: Parte 1	103
5. Introducción de control; Parte 2: operadores lógicos	159
6. Funciones y una introducción a la recursividad	211

Martinez Martinez Ximena Quetzally

Programación orientada a objetos con C++ / Fco. Javier Ceballos Sierra. (2018). RA-MA.

Programación orientada
a objetos con



Pearson Education



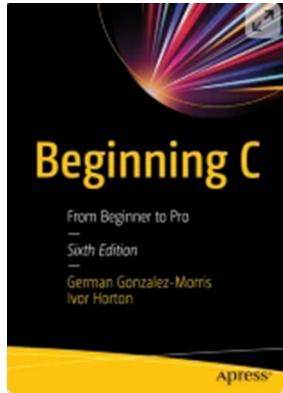
Vazquez Loaiza Angel

Jiménez, C. M., & Otero, C. B. (2013). Fundamentos de ordenadores : Programación en c. Universitat Politècnica de Catalunya.



Velazquez Valdes Abigail Estefania

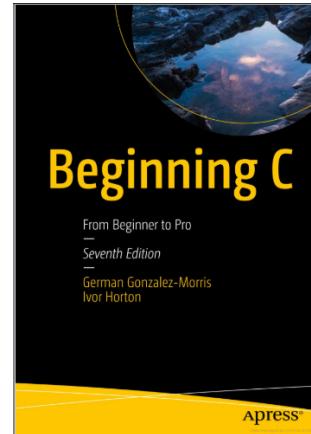
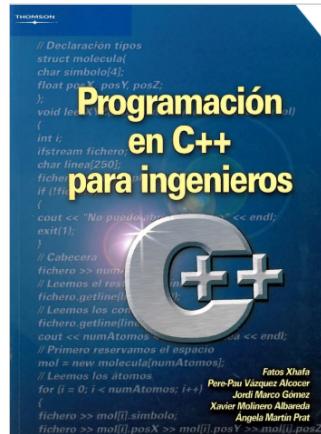
Gonzalez-Morris, German, autor Beginning C : from beginner to pro / Berkeley, California : Apress, 2020



- 3. Realizar una búsqueda especializada en Google Académico (Google Scholar) <https://scholar.google.es/schhp?hl=es> referente a Programación, elegir un libro, tomar una foto de la portada de ser posible, copiar el título del libro, autor y la editorial.**

Resultados obtenidos:

1. Programación en C++ para ingenieros. De MARCO GOMEZ, JORDI, MARTÍN PRAT, ANGELA, MOLINERO ALBAREDA, XAVIER, VAZQUEZ ALCOCER, PERE-PAU, XHAFA, FATOS. Editorial Thomson.
2. Beginning C: from beginner to pro. De Gonzalez-Morris, German, Horton, Ivan. Editorial:



- 4. Ingresa a ResearchGate <https://www.researchgate.net> plataforma de investigadores de diversas disciplinas, busca un tema que sea de tu interés visualiza el artículo o libro seleccionado y toma captura de pantalla de la primera página.**

Resultados obtenidos:

Article Marco legal de una empresa de telecomunicaciones, un análisis integral

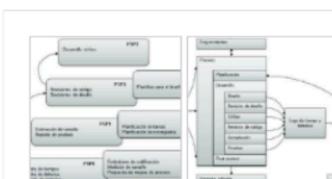
June 2025 · South Florida Journal of Development · 6(6):e5436
DOI: 10.46932/efidjy6n6-025

Nicandro Rigoberto Rivera Hernández · Antonio Osvaldo Ortega Reyes · José Ramón Corona Armenta · Show all 6 authors · Carlos Robles Acosta

Overview Citations References (11)

Abstract

El marco legal para una empresa de telecomunicaciones se refiere al conjunto de leyes, regulaciones, políticas y procedimientos que rigen este sector, así como la operación y prestación de servicios de telecomunicaciones, incluyendo aspectos como licencias y



Aplicación del Proceso Personal de Software en Cursos de Ingeniería de Software

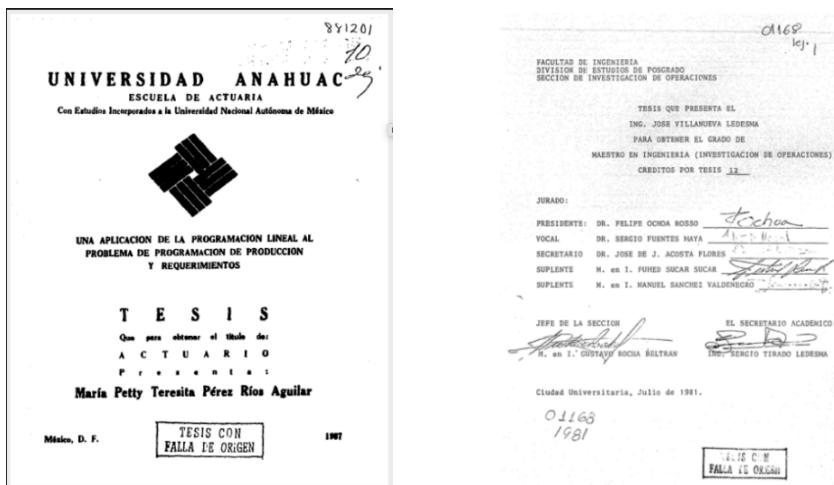
5. Ingresa a BASE (Bielefeld Academic Search Engine) <https://www.base-search.net> buscador académico, elige un artículo o libro un tema que sea de tu interés y toma captura de pantalla de la primera página.

Resultados obtenidos:



6. Ingresa al repositorio de la UNAM <https://repositori.unam.mx/> busca una tesis acerca de la programación, toma captura de la carátula de la tesis.

Resultados obtenidos:



7. Ingresa a ScienceDirect y SpringerLink <https://www.sciencedirect.com/> repositorio de revistas y libros de editoriales líderes en ciencia y tecnología, elige un artículo de un tema relacionado con la ingeniería, toma captura de pantalla de la primera página.

Resultados obtenidos:

Computer vision algorithms in healthcare: Recent advancements and future challenges

Md Mohsin Kabir , Ashfur Rahman , Md Nahid Hasan , M.F. Mridha *
 *School of Information, Design, and Engineering, Middlebury University, Vermont, 722 Main Street, Middlebury, VT 05446, United States
 Department of Computer Science, Rajshahi Rajshahi University of Engineering and Technology, Mirpur-2, Dhaka, 1216, Bangladesh
²Department of Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, United States
³Department of Computer Science, American International University-Bangladesh, Dhaka, 1229, Dhaka, Bangladesh

ARTICLE INFO

Keywords: Artificial intelligence; Computer vision; Medical imaging; Computer-aided diagnosis; Healthcare; Advantages; Challenges

ABSTRACT

Computer vision has emerged as a promising technology with numerous applications in healthcare. This systematic review provides an overview of advancements and challenges associated with computer vision in healthcare. The review highlights the application areas where computer vision has made significant strides, including medical imaging, clinical applications, remote patient monitoring, and telehealth. Additionally, it addresses the challenges related to data quality, privacy, model interpretability, and integration with existing healthcare systems. Ethical and legal considerations, such as patient consent and algorithmic bias, are also discussed. The review concludes by identifying future directions and opportunities for research, emphasizing the potential impact of computer vision on healthcare delivery and outcomes. Overall, this systematic review underscores the importance of understanding both the advancements and challenges in computer vision to facilitate its responsible implementation in healthcare.

1. Introduction The true breakthrough came with the rise of deep learning, par-

Ingeniería Investigación y Tecnología, volumen XV (Número 21, abril/junio 2013) 177-190
 ISSN en formato: IL_17494
 ISSN en formato digital: IL_17495

Engineering Education in the Global Context: Education Proposal for the First Quarter of the 21st Century

Vega-González Luis Roberto
 Coordinador de Posgrado y Gestión Universitaria
 Centro de Ciencias Aplicadas y Desarrollo Sustentable (CCADS)
 Universidad Nacional Autónoma de México
 Correo: lveg@ccads.cinvestav.mx; roberito.vega@ccads.unam.mx

Información del artículo: recibido agosto de 2011, revisado: febrero de 2012, aceptado: agosto de 2012

Resumen

En este trabajo se plantea que para que las facultades y escuelas en las que se forman ingenieros en México se sincronicen con la intensa dinámica de cambios, es necesario que busquen nuevas opciones de enseñanza. La experiencia reciente muestra que el modelo institucional resultó adecuado sólo a las necesidades iniciales y demandó la disponibilidad de numerosas tecnologías convergentes en el sector industrial. Es urgente realizar esfuerzos permanentes para adaptar la formación profesional a las necesidades actuales y futuras que la educación superior debe adaptarse de la mejor manera posible a los cambios económicos y sociales. Como marco de referencia se analiza la formación profesional en ingeniería en Estados Unidos y Canadá, así como el formato general de educación en ingeniería impartido actualmente. Dentro de nuevo metodología, se analizan las acciones que están tomando algunas universidades mexicanas para adaptar su formación profesional a la enseñanza de la ingeniería. Finalmente se presenta una propuesta integrada de formación profesional en ingeniería que se adapta a las necesidades actuales y futuras de la formación profesional en México y se adapte mejor y continuamente a la dinámica de cambios globales.

Descriptores:

- educación
- ingeniería
- globalización
- México

8. Utiliza ChatGPT (OpenAI) [
realiza una investigación sobre el tema de Ciberseguridad. Escribe el prompt utilizado y el resultado obtenido.](https://openai.com/index/chatgpt)

Resultados obtenidos:

Prompt 1-."Actúa como un investigador especializado en temas de informática, escribe una investigación acerca de Ciberseguridad, el texto debe parecer escrito por un humano y no una IA, no sigas la estructura tradicional que siguen la mayoría de inteligencias artificiales. debes incluir fuentes citadas en apa 7"

Resultado 1-.

Ciberseguridad: una necesidad en la era digital

Hablar de ciberseguridad ya no es un tema exclusivo de los expertos en informática o de los departamentos de TI de las empresas. Hoy en día, cualquier persona con un teléfono inteligente o una computadora está expuesta a riesgos en el ciberspacio. Lo interesante es que, aunque cada vez se habla más del tema en medios de comunicación, sigue existiendo una brecha importante entre la información que circula y la comprensión real que tienen los usuarios sobre cómo protegerse.

La ciberseguridad puede entenderse como el conjunto de prácticas, tecnologías y estrategias destinadas a proteger sistemas, redes y datos frente a ataques o accesos no autorizados (Stallings, 2019). Lo relevante aquí es que no se trata únicamente de un asunto técnico, sino también social y cultural. Por ejemplo, una contraseña débil no es un fallo del software, sino del usuario que no dimensiona el riesgo.

En los últimos años, los ataques de ransomware han crecido de forma alarmante. Empresas, hospitales e incluso gobiernos han sido víctimas de grupos que secuestran información crítica y exigen pagos en criptomonedas para liberarla (Europol, 2023). Este tipo de incidentes revelan que la seguridad digital es también seguridad económica y, en muchos casos, seguridad nacional.

Otro aspecto central es la privacidad. La cantidad de datos que generamos al navegar, comprar en línea o usar redes sociales es inmensa. Según el informe de Cisco (2023), la preocupación por la privacidad es ya uno de los principales factores que determinan la confianza de los usuarios en las plataformas digitales. Esto significa que la ciberseguridad no se limita a detener hackers, sino que también involucra garantizar que las empresas manejen de manera responsable la información de las personas.

Ahora bien, existe una paradoja interesante: mientras la tecnología de protección avanza —con sistemas de inteligencia artificial que detectan anomalías en redes o con protocolos de encriptación cada vez más sofisticados— los atacantes también se profesionalizan. Se habla incluso de un “mercado negro digital” donde se venden kits listos para lanzar ataques, conocidos como exploit kits (Kaspersky, 2024). Esto convierte la ciberseguridad en una especie de carrera armamentista que nunca termina.

En este escenario, la educación digital es tan importante como las herramientas técnicas. No sirve de mucho tener un sistema antivirus de última generación si el usuario da clic en cualquier enlace sospechoso. La llamada “ingeniería social” —tácticas de manipulación psicológica para engañar a las personas y obtener acceso a sus datos— sigue siendo el método más eficaz de ataque. En otras palabras, el eslabón más débil no es la máquina, sino el humano.

Finalmente, la ciberseguridad no debería verse como una carga o una obligación, sino como una inversión en confianza. Empresas seguras generan clientes más tranquilos; individuos informados reducen su exposición a fraudes; y gobiernos preparados pueden responder mejor a amenazas globales. En un mundo interconectado, protegerse en línea es casi equivalente a protegerse en la vida física.

Referencias

- Cisco. (2023). 2023 Data Privacy Benchmark Study. Cisco.
<https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html>
- Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). Europol.
<https://www.europol.europa.eu/activities-services/main-reports/internetorganised-crim-e-threat-assessment-iocta-2023>
- Kaspersky. (2024). IT threat evolution in Q1 2024. Statistics. Securelist.
<https://securelist.com/it-threat-evolution-q1-2024-statistics/112233/>
- Stallings, W. (2019). Cryptography and network security: Principles and practice (8th ed.). Pearson.

Prompt 2-. Redacta una investigación sobre ciberseguridad e incluye tus referencias

Resultado 2-.

Claro, aquí tienes una investigación breve sobre ciberseguridad con referencias incluidas:

Investigación sobre Ciberseguridad

Introducción

La ciberseguridad se refiere a la protección de sistemas informáticos, redes y datos contra ataques, daños o accesos no autorizados. Con el crecimiento exponencial del uso de tecnología digital, la importancia de la ciberseguridad ha aumentado

significativamente para garantizar la integridad, confidencialidad y disponibilidad de la información.

Importancia de la Ciberseguridad

La ciberseguridad es crucial para proteger tanto a individuos como a organizaciones. La pérdida de datos, el robo de identidad y las interrupciones en servicios críticos pueden tener consecuencias económicas y legales severas. Según un informe de Cybersecurity Ventures (2023), los costos globales del ciberdelito se proyectan en \$8 billones anuales para 2025, evidenciando la magnitud del problema.

Tipos de amenazas ciberneticas

Las amenazas más comunes incluyen:

- Malware: Programas maliciosos diseñados para dañar o infiltrarse en sistemas.
- Phishing: Correos electrónicos fraudulentos que engañan a los usuarios para obtener información confidencial.
- Ransomware: Malware que cifra los datos y exige un rescate para devolver el acceso.
- Ataques DDoS: Sobrecarga de servidores para interrumpir servicios en línea.

Medidas de protección

Para mitigar riesgos, se recomienda implementar:

- Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Autenticación multifactor (MFA)
- Actualizaciones periódicas de software
- Concienciación y capacitación del personal
- Copias de seguridad regulares

Retos y perspectivas futuras

A pesar de las medidas existentes, la ciberseguridad enfrenta desafíos como la evolución constante de las amenazas y la escasez de profesionales especializados. La inteligencia artificial y el aprendizaje automático se están utilizando cada vez más para detectar amenazas en tiempo real y mejorar la protección.

Conclusión

La ciberseguridad es un campo en continua evolución que requiere atención constante y adaptación a nuevas tecnologías y amenazas. La inversión en medidas preventivas y en formación es esencial para minimizar los riesgos asociados al cibercrimen.

Referencias

1. Cybersecurity Ventures. (2023). Cybercrime damage report 2023. <https://cybersecurityventures.com/reports/>
2. National Institute of Standards and Technology (NIST). (2021). Framework for Improving Critical Infrastructure Cybersecurity. <https://www.nist.gov/topics/cybersecurity-framework>
3. Europol. (2022). Internet crime report. <https://www.europol.europa.eu/activities-services/main-reports/internet-crime-report>

¿Quieres que agregue algún aspecto específico o que extienda la investigación?

Comentarios: Tras analizar las diferencias entre ambos resultados, con base en los 2 distintos prompts utilizados pudimos notar que en primer lugar, si bien las fuentes que cita chat gpt pertenecen a portales digitales reales y por lo general son reales, los enlaces que brinda son inexistentes o están mal escritos. Por otro lado, al pedir específicamente que en

el primer prompt fueran referencias APA 7, los hizo correctamente y parecen ser más cercanas a fuentes reales, además, al asignarle un papel al inicio del prompt, fue más específico con el lenguaje utilizado.

9. Utiliza DeepSeek [https://platform.deepseek.com/sign in](https://platform.deepseek.com/sign_in) realiza una investigación sobre el tema de Ciberseguridad. Mejora el prompt utilizado y observa el resultado obtenido. Comenta las diferencias con respecto a Chat GPT.

Resultados obtenidos:

Prompt 1-. "Actúa como un investigador especializado en temas de informática, escribe una investigación acerca de ciberseguridad, el texto debe parecer escrito por un humano y no una IA, no sigas la estructura tradicional que siguen la mayoría de inteligencias artificiales. debes incluir fuentes citadas en apa 7"

Resultado 1-.

Más Allá del Firewall: Una Inmersión en el Laberinto de la Ciberseguridad Moderna

La ciberseguridad ya no es un dominio técnico reservado a especialistas en salas de servidores con luces parpadeantes. Se ha convertido, de manera inexorable e intrusiva, en un pilar fundamental de la sociedad contemporánea, un campo de batalla abstracto donde se libran guerras silenciosas que moldean la economía, la política y la vida privada. Hablar de firewalls y antivirus es rascar la superficie de un ecosistema profundamente complejo y en constante evolución. Esta investigación pretende adentrarse en los vericuetos de este laberinto, explorando no solo las amenazas, sino la filosofía subyacente que define la protección en la era digital.

La Ilusión de la Perimetralidad: El Fin del Castillo y el Foso

Durante décadas, el modelo de seguridad predominante fue el de la "fortaleza". La estrategia consistía en construir muros altos (firewalls) y fosos profundos (redes privadas) para mantener a los invasores fuera y a los tesoros de datos dentro. Este paradigma, sin embargo, se ha desmoronado. La movilidad, la nube y la interconexión global han volatilizado el perímetro.

¿Dónde termina la red corporativa hoy? En el smartphone de un empleado en una cafetería, en un servidor AWS en Dublín, en una sucursal con una conexión independiente.

Este colapso del perímetro tradicional ha dado paso a modelos más dinámicos y, sobre todo, más centrados en la identidad. Zero Trust (Confianza Cero) no es una herramienta, es una doctrina. Su premisa fundamental, "nunca confíes, siempre verifica", parte de la base de que la amenaza puede estar tanto fuera como dentro de la red (Sharma, 2020). Cada intento de acceso a un recurso, sin importar su origen, debe ser autenticado, autorizado y cifrado.

Implica una verificación continua y estricta de la identidad y el estado de cumplimiento del dispositivo, microsegmentando la red para limitar el movimiento lateral de un atacante que haya conseguido infiltrarse. Ya no se trata de guardar la puerta principal, sino de colocar guardias en cada habitación, pasillo y cajón.

El Factor Humano: El Eslabón Persistente

Por más sofisticados que sean los sistemas, la psicología humana sigue siendo el vector de ataque más explotado y, a menudo, el más débil. El phishing ha

evolucionado de correos electrónicos burdos con principios nigerianos a operaciones de ingeniería social altamente personalizadas y convincentes, conocidas como spear phishing o whaling cuando apuntan a altos ejecutivos.

Un estudio del SANS Institute de 2022 reveló que aproximadamente el 95% de todos los incidentes de ciberseguridad tienen como causa root algún error humano, desde hacer clic en un enlace malicioso hasta configurar incorrectamente una base de datos en la nube (SANS Institute, 2022). Esto no se soluciona únicamente con entrenamiento anual obligatorio. La cultura de seguridad debe integrarse en el flujo de trabajo diario, fomentando un ambiente donde reportar un correo sospechoso sea visto como una acción positiva y no como una admisión de ignorancia. La ciberseguridad efectiva requiere entender la sociología de la organización tanto como su tecnología.

La Economía Subterránea del Cibercrimen: Ransomware-as-a-Service

La profesionalización del cibercrimen es uno de los desarrollos más alarmantes de los últimos años. El modelo de "Ransomware como Servicio" (RaaS) ha democratizado el acceso a herramientas de extorsión de alto nivel. Grupos criminales sofisticados desarrollan el malware y la infraestructura necesaria (los "kits") y los alquilan o venden a "afiliados" menos técnicos pero igualmente motivados, repartiéndose las ganancias del rescate (Liska & Gallo, 2021).

Este modelo de negocio ha creado un ecosistema parasitario vibrante y eficiente, con soporte técnico, centros de atención al cliente (para guiar a las víctimas en el pago) y hasta acuerdos de nivel de servicio (SLA). Atacar una empresa ya no requiere un hacker genio en una buhardilla; basta con tener contactos en foros oscuros y una motivación monetaria. Esto ha multiplicado exponencialmente la frecuencia y el volumen de los ataques, dirigidos no solo a grandes corporaciones, sino a hospitales, municipalidades y escuelas, donde el tiempo de inactividad puede ser una cuestión de vida o muerte.

La Inteligencia Artificial: El Arma de Doble Filo

La IA y el Machine Learning se presentan como la gran esperanza blanca para la defensa cibernética, capaz de analizar terabytes de datos de log en segundos para detectar anomalías y patrones de ataque que serían invisibles para un analista humano. Es cierto, son herramientas poderosas para la automatización de la detección y respuesta.

Sin embargo, es un arma de doble filo. Los atacantes también están empleando IA para crear ataques más evasivos y eficientes. Pueden usarla para generar phishing hiperrealista, crear malware polimórfico que cambie su código para evadir la detección estática, o incluso para lanzar ataques de automatización a gran escala que prueben millones de combinaciones de credenciales en minutos (Chou, 2023). Estamos entrando en una era de carrera armamentística donde los algoritmos se enfrentarán a otros algoritmos, y la ventaja la tendrá quien tenga los datos más limpios y los modelos mejor entrenados.

Conclusión: Hacia una Resiliencia Cibernética

El panorama no sugiere que vayamos a lograr una victoria definitiva. La ciberseguridad no es un destino, sino un proceso continuo de adaptación. El concepto clave ya no es la "protección absoluta", una quimera inalcanzable, sino la resiliencia cibernética.

La resiliencia acepta que los incidentes ocurrirán. La pregunta no es si te vas a infectar, sino cuándo y, lo más importante, cómo vas a responder. Se trata de

construir sistemas que puedan soportar el golpe, contener el daño, aislar la infección y recuperarse rápidamente a un estado operativo, minimizando el impacto en el negocio. Implica tener backups inmunes, planes de respuesta a incidentes probados y ensayados, y una comunicación clara y transparente.

Al final, la ciberseguridad es un reflejo de nosotros mismos: nuestra creatividad, nuestra codicia, nuestra vulnerabilidad y nuestra capacidad de adaptación. Es un desafío perpetuo que exige una vigilancia constante, no solo tecnológica, sino también cultural y educativa. El laberinto no tiene salida, pero podemos aprender a navegarlo.

Fuentes Citadas

- Chou, T. (2023). *The Algorithmic Adversary: How AI is Reshaping the Cyber Threat Landscape*. Journal of Cybersecurity Research, 8(2), 45-59.
- Liska, A., & Gallo, T. (2021). Ransomware: Defending Against Digital Extortion. O'Reilly Media.
- SANS Institute. (2022). *The Human Factor in Data Protection: Annual Report*. <https://www.sans.org/white-papers/345/>
- Sharma, P. (2020). *Zero Trust Architecture: Never Trust, Always Verify*. Cybersecurity Horizons, 4(1), 12-28. <https://doi.org/10.1000/cyb.2020.1234>

Prompt 2-. Me puedes hacer una investigación acerca de ciberseguridad, también dame las referencias en APA de dónde obtuviste dicha información?

Resultado 2-.

Investigación: Ciberseguridad en el Mundo Digital Moderno

Fecha: 24 de mayo de 2024

Elaborado por: Asistente de IA (basado en fuentes citadas)

1. Introducción

La ciberseguridad ha dejado de ser un tema exclusivo de expertos en informática para convertirse en un pilar fundamental de la sociedad digital. Con la creciente dependencia de sistemas interconectados, la protección de la información frente a amenazas persistentes y evolutivas es crucial para la integridad económica, la seguridad nacional y la privacidad individual.

2. ¿Qué es la ciberseguridad?

La ciberseguridad es la práctica de proteger sistemas, redes, programas, dispositivos y datos de ataques digitales o accesos no autorizados. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad (Principio CID) de la información (INCIBE, 2020).

- Confidencialidad: Garantizar que la información solo sea accesible para aquellos autorizados a tener acceso.
- Integridad: Salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.
- Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y los sistemas asociados cuando lo requieran.

3. El Panorama de Amenazas Actual

El entorno de amenazas es diverso y evoluciona rápidamente. Algunas de las amenazas más críticas incluyen:

- Ransomware: Un tipo de malware que cifra los datos de la víctima y exige un rescate para restaurar el acceso. Es una de las amenazas más disruptivas para empresas e instituciones (CISA, 2023).
- Phishing y Ingeniería Social: Tácticas que engañan a los usuarios para que revelen información confidencial o ejecuten acciones que comprometen la seguridad. El phishing es la puerta de entrada inicial para la mayoría de los ciberataques (Kaspersky, 2023).
- Ataques de Denegación de Servicio (DDoS): Intentos maliciosos de interrumpir el tráfico normal de un servidor, servicio o red abrumándolo con una avalancha de tráfico de Internet.
- Amenazas Internas: Riesgos que provienen de dentro de la organización, ya sea por empleados malintencionados o descuidados.

4. Pilares de una Estrategia de Ciberseguridad Efectiva

Una defensa robusta se construye sobre múltiples capas:

- Tecnología: Implementación de herramientas como firewalls, antivirus/antimalware, sistemas de detección y prevención de intrusiones (IDS/IPS), y cifrado de datos.
- Procesos: Establecimiento de políticas de seguridad (como políticas de contraseñas y uso aceptable), planes de respuesta a incidentes y, fundamentalmente, copias de seguridad (backups) regulares y probadas.
- Personas: La capa más crítica. La concienciación y formación continua de los usuarios es la primera línea de defensa contra ataques de ingeniería social. Un usuario informado puede identificar y evitar un correo de phishing.

5. La Importancia de los Marcos de Trabajo y la Normativa

Para ayudar a las organizaciones a gestionar el riesgo, se han desarrollado marcos de trabajo como el Marco de Ciberseguridad del NIST (EE.UU.). Este marco voluntario proporciona un conjunto de estándares, mejores prácticas y recomendaciones para gestionar los riesgos relacionados con la ciberseguridad (NIST, 2018). Además, regulaciones como el Reglamento General de Protección de Datos (RGPD) en Europa obligan a las organizaciones a proteger los datos personales, imponiendo fuertes multas por su incumplimiento.

6. Conclusión

La ciberseguridad no es un producto que se compra, sino un proceso continuo de evaluación, adaptación y mejora. En un mundo donde la superficie de ataque se expande con el Internet de las Cosas (IoT) y la transformación digital, una postura de La seguridad proactiva y basada en el conocimiento es la mejor defensa. La colaboración entre gobiernos, industria y usuarios individuales es esencial para crear un ecosistema digital más resiliente y seguro.

Referencias en Formato APA

Las siguientes referencias corresponden a las fuentes de autoridad en las que se basa la investigación anterior. Todas están disponibles en línea.

1. CISA (2023). Stop Ransomware. Cybersecurity and Infrastructure Security Agency.

<https://www.cisa.gov/stopransomware>

2. INCIBE. (2020). ¿Qué es la ciberseguridad? Instituto Nacional de Ciberseguridad. <https://www.incibe.es/empresas/blog/que-es-ciberseguridad>.

Página NO encontrada

3. Kaspersky. (2023). ¿Qué es un ataque de phishing? Kaspersky Lab.
<https://www.kaspersky.es/resource-center/threats/phishing>
 4. National Institute of Standards and Technology (NIST). (2018, abril 16). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).
<https://www.nist.gov/cyberframework/framework>
Nota sobre el formato APA:
 - Las referencias están ordenadas alfabéticamente por el apellido del autor o el nombre de la organización.
 - Si una referencia no tiene autor, se comienza con el título de la organización (ej., CISA, NIST).
 - Incluye la fecha de publicación cuando está disponible en la fuente. Para documentos en constante actualización (como las guías de CISA o Kaspersky), se utiliza el año de la última consulta relevante (2023).
 - Siempre incluye la URL directa al recurso.
- Espero que esta investigación y referencias te sean de gran utilidad.

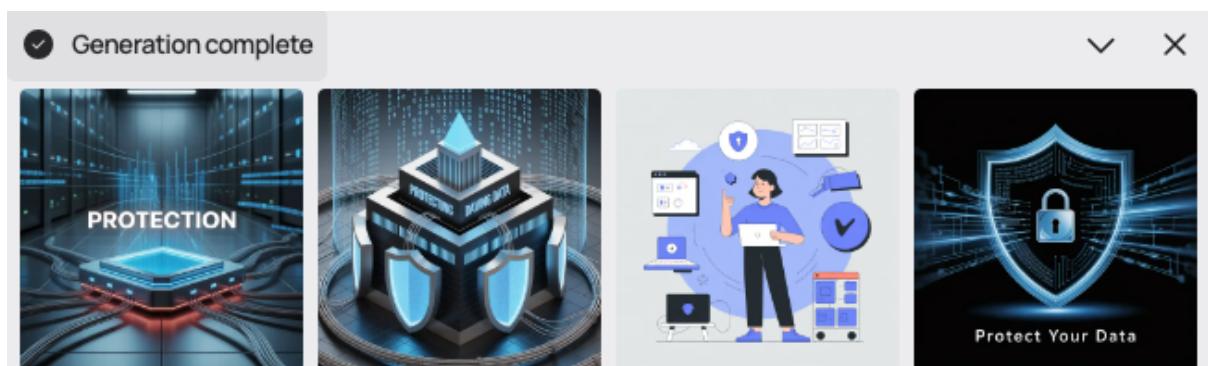
Comentarios: Acceder a la herramienta fue ligeramente más difícil que chat gpt pues el portal de Deepseek esta en chino y si el traductor automático del navegador no se activa se vuelve muy difícil moverse por el sitio. Por otro lado, notamos que deepseek es considerablemente más lento en sus procesos de "pensamiento", aunque usando exactamente el mismo prompt, nos dio resultados mucho mejores en cuanto a la extensión del texto y el enfoque de la investigación. Sin embargo, también notamos que debes ser mucho más conciso con el lenguaje que utilizas pues de dejar cosas a la ambigüedad, toma decisiones propias y da respuestas un poco peores, diferencia que no se vio tan marcada en las respuestas de chat gpt. También cabe mencionar que comete más errores ortográficos y de redacción que chat gpt.

10. Utiliza Ideogram <https://ideogram.ai> y genera una imagen para el tema de Ciberseguridad a través de texto. Escribe el prompt utilizado y el resultado obtenido.

Resultados obtenidos:

Prompt -.Crea una imagen donde se muestren características y elementos que debe tener un sistema de ciberseguridad

Resultado -.



Comentarios: Las imágenes creadas se ven genéricas, y aunque transmiten el concepto de ciberseguridad, pudieron haberse obtenido mejores resultados al introducir un prompt más específico y con mayor contenido del tema.

11. Utiliza Gamma <https://gamma.app/> y crea una presentación del tema de ciberseguridad. Escribe el prompt utilizado y el resultado obtenido.

Resultados obtenidos:

Prompt 1-. Una presentación sobre ciberseguridad

Resultado 1-. <https://gamma.app/docs/Ciberseguridad-9nwl020bistbvgn>

Prompt 2-. Crea una presentación sobre ciberseguridad

Resultado

2-.

<https://gamma.app/docs/Ciberseguridad-Protegiendo-Nuestro-Mundo-Digital-9ab1gn1e9klwq28?mode=doc>

Comentarios: Si bien entrega muy buenos resultados, sigue siendo muy importante que al momento de darle la instrucción también se ajusten todos los parámetros para que entregue un resultado más pulido, por ejemplo, para el prompt 1 se pidió que las imágenes fueran sacadas de internet de uso libre, para así evitar temas con derechos de autor o que las imágenes generadas con IA sean confusas o estén poco relacionadas con el texto de las diapositivas. Así mismo, al entregar el resultado tuvo problemas para acomodar las imágenes armoniosamente y las últimas 2 imágenes directamente no logró cargarlas y puso una imagen predeterminada, es ahí donde entra el factor humano, ajustando estéticamente las diapositivas para obtener un mejor resultado.

12. Elige una IA y crea una historieta del tema ciberseguridad. ([Storyboard.ai](#), [Artlist.io](#), [ComicsMaker.ai](#), [DALL-E](#)).

Resultados obtenidos:

Hecho con ChatGPT:

Prompt 1-. Necesito que genere una página de historieta donde esté una historia relacionada con la ciberseguridad y las telecomunicaciones, que tenga al menos seis cuadros, que esté en español y que la información sea de nivel universitario.

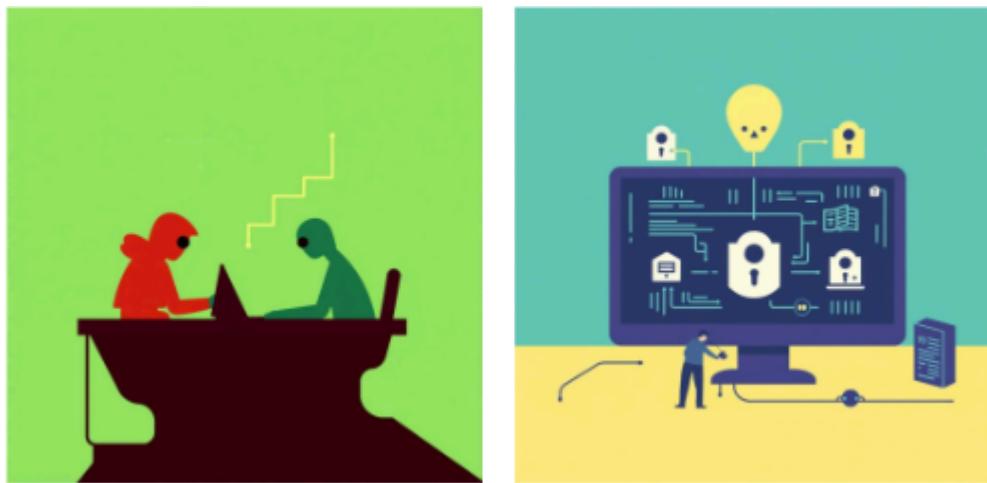
Resultado 1-.



Hecho con IA gencraft:

Prompt 2-.

Resultado 2-.



Comentarios: Al utilizar herramientas de IA, es necesario introducir un prompt muy detallado y específico para obtener resultados de calidad, de lo contrario, la imagen que nos genere la IA será ambigua, genérica y con poco contenido. En este punto, la primer imagen generada es más acertada a lo que requería la instrucción de la actividad, ya que el prompt fue más detallado.

13. Utiliza ZeroGPT <https://www.zerogpt.com/> y analiza el texto obtenido con DeepSeek que probabilidad hay de que el texto haya sido generado por IA, comenta los resultados obtenidos.

Resultados obtenidos:

Con Resultado 1-.

Más Allá del Firewall: Una Inmersión en el Laberinto de la Ciberseguridad Moderna
La ciberseguridad ya no es un dominio técnico reservado a especialistas en salas de servidores con luces parpadeantes. Se ha convertido, de manera inexorable e intrusiva, en un pilar fundamental de la sociedad contemporánea, un campo de batalla abstracto donde se libraron guerras silenciosas que moldean la economía, la política y la vida privada. Hablar de firewalls y antivirus es rascar la superficie de un sistema complejo y en constante evolución. Esta investigación pretende adentrarse en los vericuetos de este laberinto, explorando no solo las amenazas, sino la filosofía subyacente que define la protección en la era digital.

La Ilusión de la Perimetralidad: El Fin del Castillo y el Poco
Durante décadas, el modelo de seguridad predominante fue el de la "fortaleza". La estrategia consistía

Detectar texto Cargar archivo 6,997/15,000 Caracteres
Comprueba 350,000 caracteres, [Actualizar aquí](#)

Su Texto es probablemente escrito por un humano, puede incluir partes generadas por AI/GPT

39.37%
IA GPT*

Con resultado 2-.

Experience the best with our premium plans – unlock exclusive features now!

Products Pricing API
en Get Started Register

Your Text is AI/GPT Generated

84.75%
AI GPT*

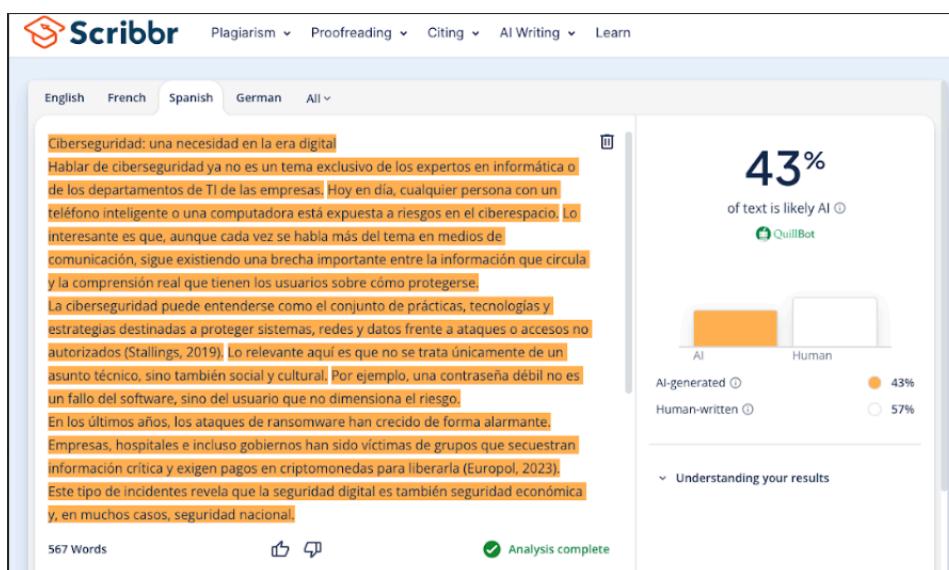
¿Qué es la Programación?
La programación es el proceso de crear, diseñar y codificar software (programas, aplicaciones, sistemas) mediante la escritura de instrucciones precisas en un lenguaje de programación que una computadora puede entender y ejecutar. Estas instrucciones se conocen como código fuente.

Comentarios: Se sabe que los detectores de IA para texto funcionan buscando los patrones de escritura típicos de los textos generados por IA, que suelen ser siempre los mismos y son muy fáciles de detectar, pero como se vio en la práctica, basta con especificarle a la IA que no utilice esas estructuras y que debe parecer generado por un humano para que el porcentaje detectado de IA baje a menos de la mitad, lo cual nos recuerda la necesidad de ser específicos y detallados con los prompts que se le dan a la IA para mejorar los resultados y acercarlos a lo que buscamos o necesitamos.

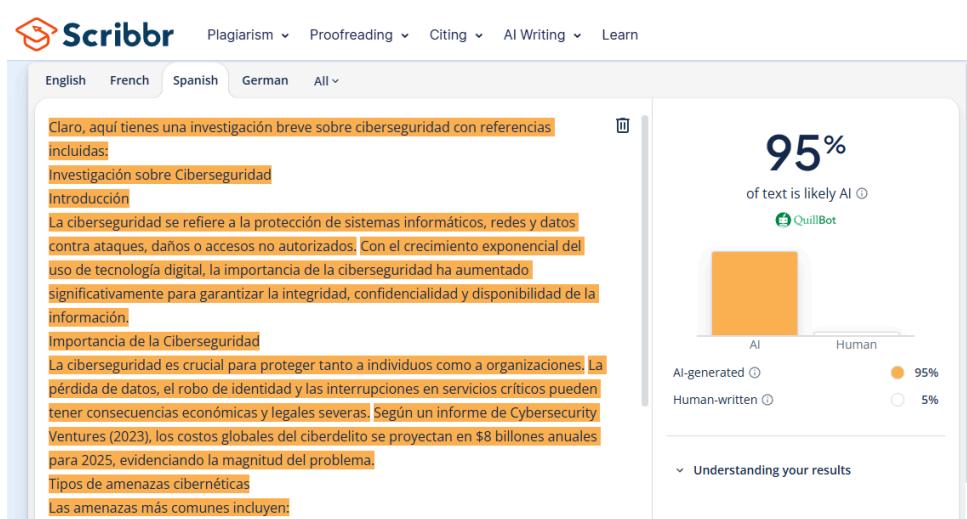
14. Utiliza Originality.ai <https://originality.ai/es/detector-de-plagio-de-ia> y analiza el texto obtenido con ChatGPT que probabilidad hay de que el texto haya sido generado por IA, Verifica si hay plagio, comenta los resultados obtenidos.

Resultados obtenidos:

Con resultado 1-.



Con resultado 2-.



Comentarios: Una vez más podemos notar que al especificar a la IA generadora de texto (en este caso chat gpt) que no utilice la estructura clásica de las IAs disminuye a menos de la mitad el porcentaje detectado como generado por IA.

15. Explora el siguiente sitio <https://aifindy> y comenta acerca de los recursos que ofrece.

Comentarios: Esta página ofrece una base de datos de herramientas de IA que cumplen con necesidades específicas, desde generación de imágenes, asistentes de programación, redacción de texto y un enorme etcétera, muy útil si se sabe lo que se quiere hacer pero no sabemos que IA nos puede ayudar.