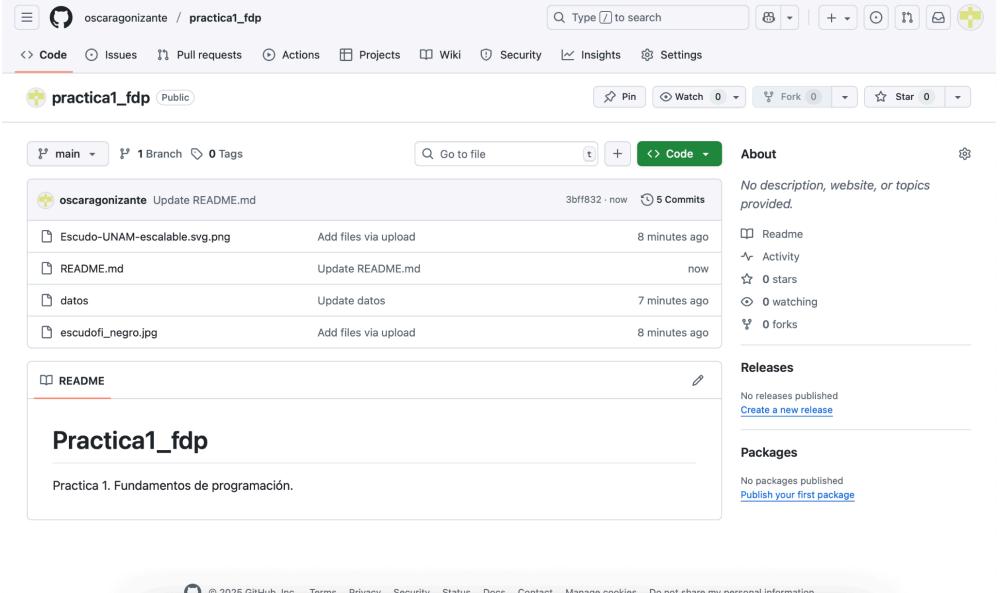


Actividad 1:

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

Agonizante Hernández Oscar:

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



A screenshot of a GitHub repository page for 'practica1_fdp'. The repository was created by 'oscaragonizante' and has 5 commits. The README file contains the text: 'Practica 1. Fundamentos de programación.'

Code | **Issues** | **Pull requests** | **Actions** | **Projects** | **Wiki** | **Security** | **Insights** | **Settings**

practica1_fdp (Public)

Code | **Issues** | **Pull requests** | **Actions** | **Projects** | **Wiki** | **Security** | **Insights** | **Settings**

oscaragonizante Update README.md 3bfff832 · now 5 Commits

Escudo-UNAM-escalable.svg.png Add files via upload 8 minutes ago

README.md Update README.md now

datos Update datos 7 minutes ago

escudof1_negro.jpg Add files via upload 8 minutes ago

About
No description, website, or topics provided.

Readme
Activity
0 stars
0 watching
0 forks

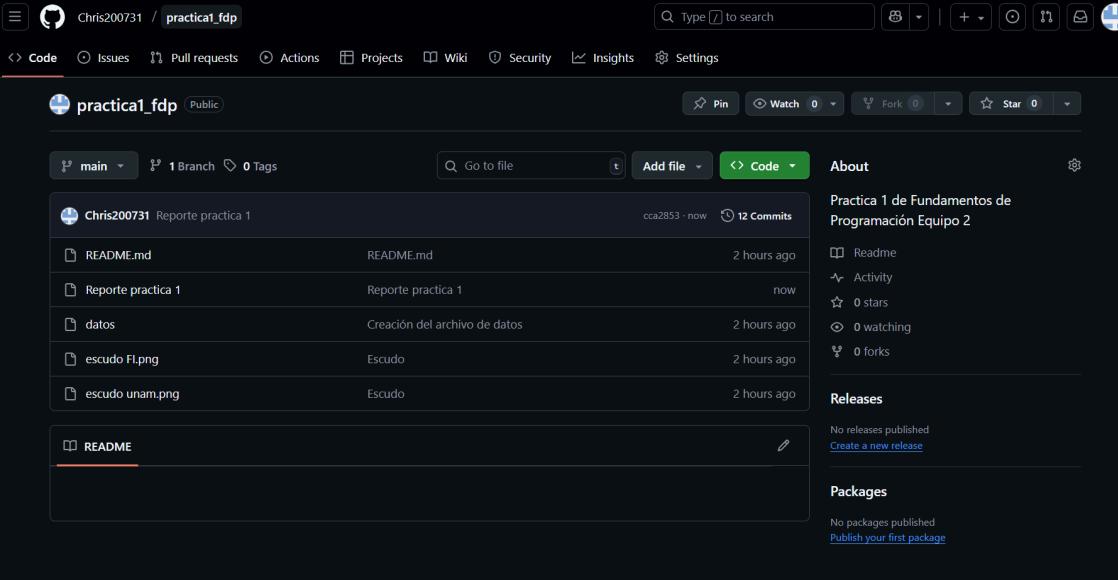
Releases
No releases published
[Create a new release](#)

Packages
No packages published
[Publish your first package](#)

© 2025 GitHub, Inc. [Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)

Cabrera Rivera Christian Fabian:

https://github.com/Chris200731/practica1_fdp.git



A screenshot of a GitHub repository page for 'practica1_fdp'. The repository was created by 'Chris200731' and has 12 commits. The README file contains the text: 'Practica 1 de Fundamentos de Programación Equipo 2'

Code | **Issues** | **Pull requests** | **Actions** | **Projects** | **Wiki** | **Security** | **Insights** | **Settings**

practica1_fdp (Public)

Code | **Issues** | **Pull requests** | **Actions** | **Projects** | **Wiki** | **Security** | **Insights** | **Settings**

Chris200731 Reporte practica 1 cca2853 · now 12 Commits

README.md README.md 2 hours ago

Reporte practica 1 Reporte practica 1 now

datos Creación del archivo de datos 2 hours ago

escudo F1.png Escudo 2 hours ago

escudo unam.png Escudo 2 hours ago

About
Practica 1 de Fundamentos de Programación Equipo 2

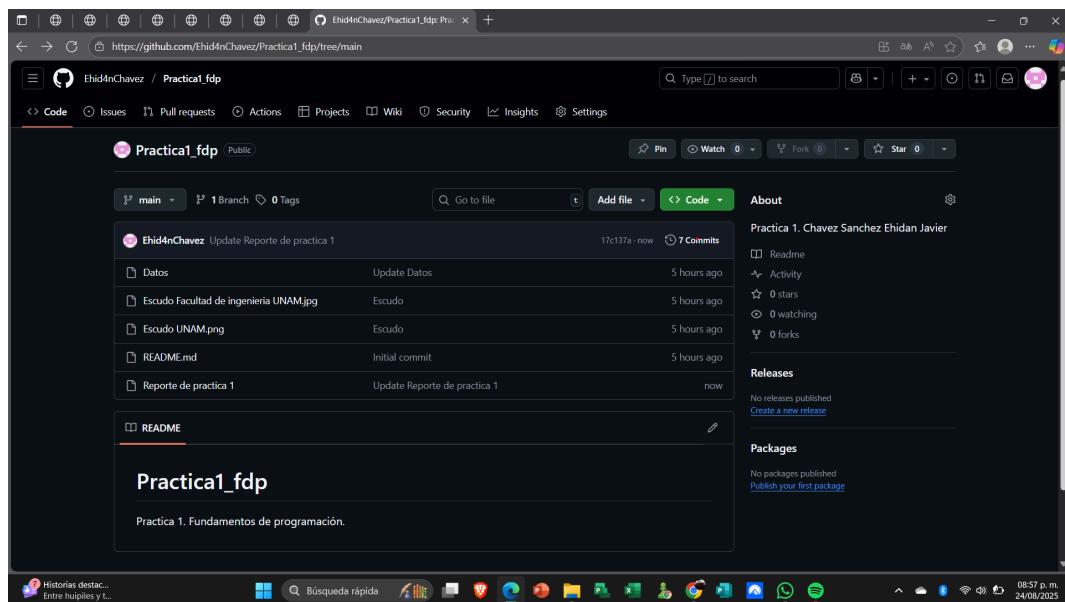
Readme
Activity
0 stars
0 watching
0 forks

Releases
No releases published
[Create a new release](#)

Packages
No packages published
[Publish your first package](#)

Chávez Sánchez Ehidan Javier:

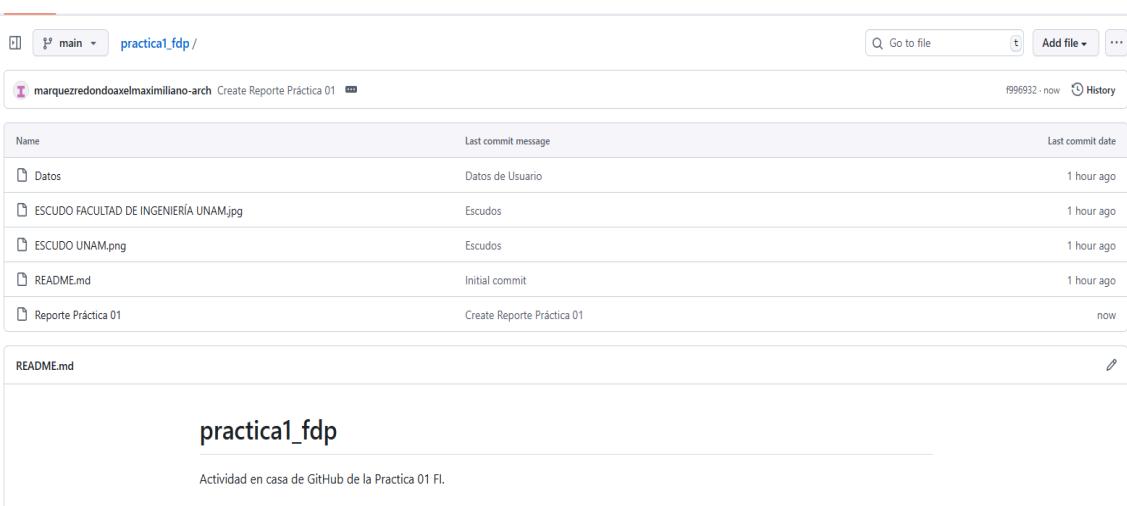
[Ehid4nChavez/Practica1_fdp: Practica 1. Chavez Sanchez Ehidan Javier](https://github.com/Ehid4nChavez/Practica1_fdp)



A screenshot of a GitHub repository page. The repository name is "Practica1_fdp" and it is public. The main branch is "main". There is 1 branch and 0 tags. The README file contains the text "Practica1_fdp" and "Practica 1. Fundamentos de programación.". The commit history shows 7 commits from "Ehid4nChavez" with messages like "Update Reporte de practica 1", "Update Datos", and "Initial commit". The repository has 0 stars, 0 forks, and 0 watching.

Marquez Redondo Axel Maximiliano:

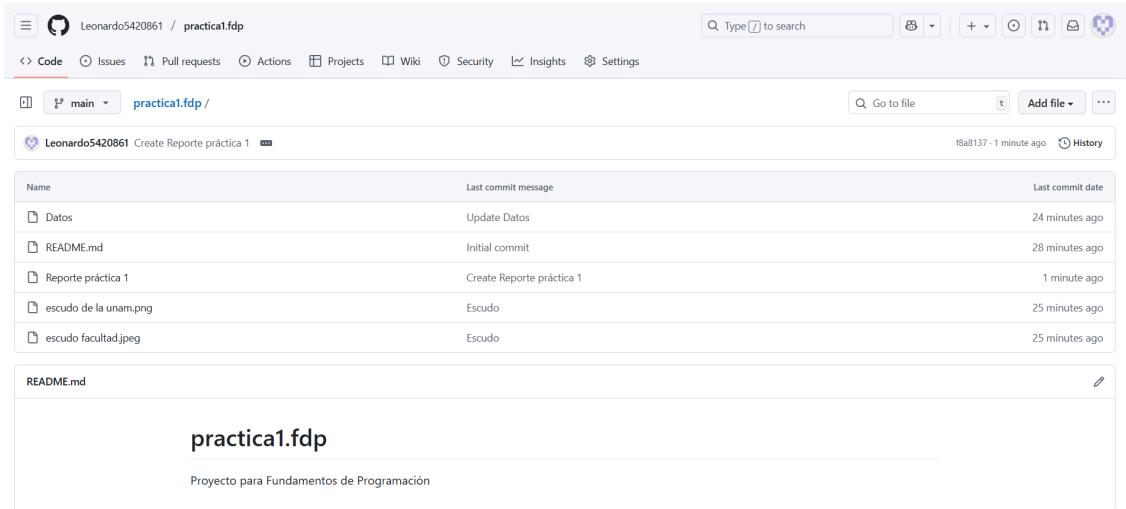
https://github.com/marquezredondoaxelmaximiliano-arch/practica1_fdp/tree/f9969322d7290ebd274ecb4a6638f1f90e8b7aab



A screenshot of a GitHub repository page. The repository name is "practica1_fdp" and it is private. The main branch is "main". There is 1 branch and 0 tags. The README file contains the text "practica1_fdp" and "Actividad en casa de GitHub de la Practica 01 Fl.". The commit history shows 7 commits from "marquezredondoaxelmaximiliano-arch" with messages like "Create Reporte Práctica 01", "Datos de Usuario", and "Initial commit". The repository has 0 stars, 0 forks, and 0 watching.

Martínez Gutierrez Leonardo:

<https://github.com/Leonardo5420861/practica1.fdp>

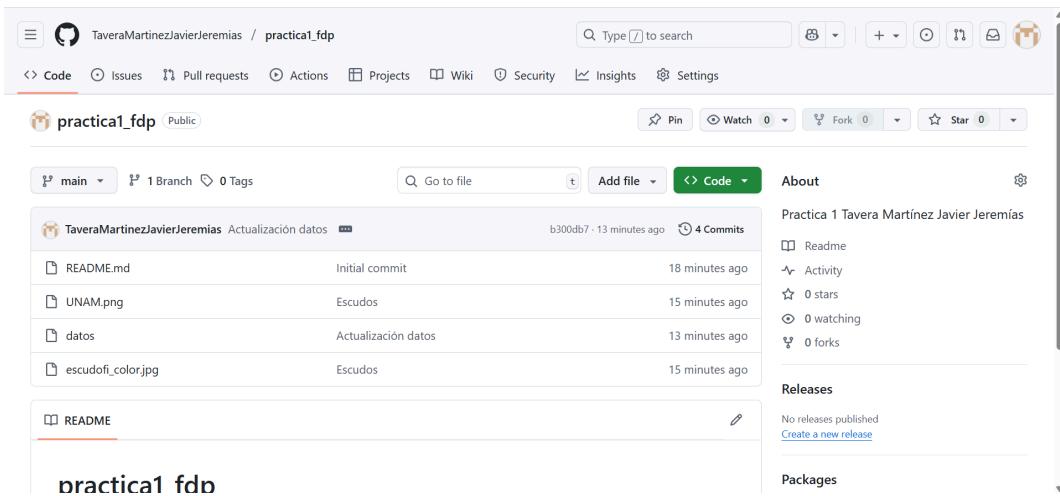


A screenshot of a GitHub repository page. The repository name is "practica1.fdp". The main branch is "main". There is one commit from "Leonardo5420861" titled "Create Reporte práctica 1". The commit message is "Last commit message". The commit was made 1 minute ago. The repository contains files: "Datos", "README.md", "Reporte práctica 1", "escudo de la unam.png", and "escudo facultad.jpeg". The README.md file contains the following content:

```
practica1.fdp  
Proyecto para Fundamentos de Programación
```

Tavera Martínez Javier Jeremías:

https://github.com/TaveraMartinezJavierJeremias/practica1_fdp



A screenshot of a GitHub repository page. The repository name is "practica1_fdp". The main branch is "main". There are four commits from "TaveraMartinezJavierJeremias" with the following details:

| File | Message | Time Ago |
|--------------------|---------------------|----------------|
| README.md | Initial commit | 18 minutes ago |
| UNAM.png | Escudos | 15 minutes ago |
| datos | Actualización datos | 13 minutes ago |
| escudof1_color.jpg | Escudos | 15 minutes ago |

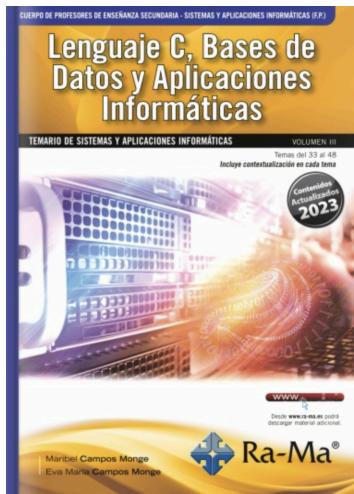
The repository has 0 stars, 0 forks, and 0 releases. The README file contains the following content:

```
practica1 fdp
```

Actividad 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.

Agonizante Hernández Oscar:



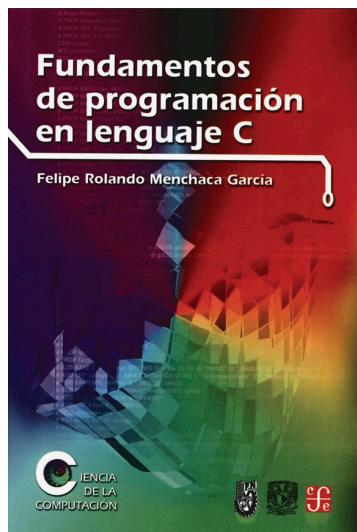
Cita bibliográfica: Campos Monge, Maribel, autor Lenguaje C, bases de datos y aplicaciones informáticas : temario oficial de sistemas y aplicaciones informáticas (F.P.). Paracuellos de Jarama, Madrid : Ra-Ma, [2023]

Cabrera Rivera Christian Fabian:



Cita bibliográfica: Barba Salvador, Antonio, autor Aprende C# programando juegos / Madrid : Dextra, [2024].

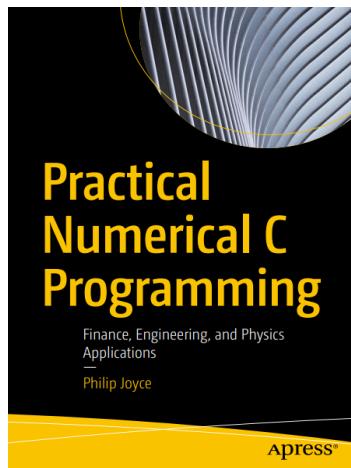
Chavez Sanchez Ehidan Javier:



Cita bibliográfica: Menchaca, García, Felipe Rolando. Fundamentos de programación en Lenguaje C, Instituto Politécnico Nacional, 2010. ProQuest Ebook Central,

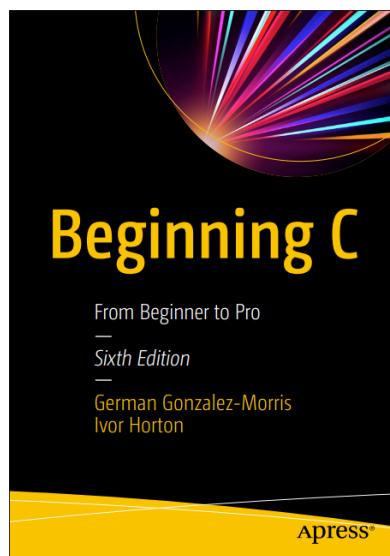
<https://ebookcentral.proquest.com/lib/bibliodgbsp/detail.action?docID=3188133>.

Marquez Redondo Axel Maximiliano:



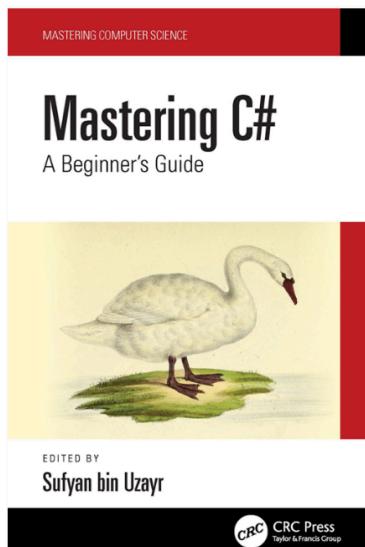
Cita bibliográfica: Joyce, Philip, autor Practical numerical C programming: finance, engineering, and physics applications / Berkeley, California : Apress, [2020]

Martínez Gutiérrez Leonardo:



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

Tavera Martínez Javier Jeremías:



Cita bibliográfica: Mastering C# : a beginner's guide / Boca Raton, Florida : CRC Press, 2022

Actividad 3:

Realizar una búsqueda especializada en Google Académico (GoogleScholar) <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.

Título: PROGRAMACIÓN

Autor: IES José Luis GUTIÉRREZ

**IES
José Luis
GUTIÉRREZ**

PROGRAMACIÓN

DOCUMENTOS DE BASE:

- *ORDEN EDU 362/2015, de 4 de mayo, por la que se establece el currículo y se regula la implantación, evaluación y desarrollo de la Educación Secundaria Obligatoria en Castilla y León.*
- *REAL DECRETO 1105/2014, de 29 de diciembre, por el que se establecen el currículo básico de la Educación Secundaria Obligatoria y del Bachillerato.*
- *ORDEN ECD/65/2015, de 21 de enero, por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato.*

CURSO: 2021 / 2022

ETAPA: Educación Secundaria Obligatoria (ESO)

CURSO: 4º

MATERIA: Educación Física

PROFESOR: David Gutiérrez Rodríguez

Actividad 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.



Revista Digital de Tecnologías Informáticas y Sistemas
<https://doi.org/10.61530/redtis.vol8.n1.2024>

PARADIGMA DE LA PROGRAMACION ORIENTADA A OBJETOS (POO)

Lucio Guadalupe Quirino Rodríguez¹, Eduardo Alfonso Huerta Mora², Asia Cecilia Carrasco Valenzuela³, Héctor Luis López López⁴

¹Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán (MÉXICO)

²Universidad Autónoma de Sinaloa, Facultad de Ingeniería y Tecnología de Mazatlán (MÉXICO)

³Universidad Autónoma de Sinaloa, Preparatoria Rubén Jaramillo (MÉXICO)

Resumen

El estudio “paradigma de programación orientada a objetos”, tuvo como objetivo principal el detectar el nivel de aprendizaje de los alumnos que cursan la materia de paradigma orientada a objetos POO, se utilizó la metodología hibrida, cuantitativa-cualitativa para analizar los datos recabados de una muestra de 65 estudiantes de la carrera de ingeniería de software de la universidad autónoma de occidente, unidad regional sur. Se aplicó un cuestionario de 10 ítems de tipo linkert, para evaluar cada una de las características de la POO, abstracción, polimorfismo, encapsulación y herencia. También se entrevistó por medio de un cuestionario de preguntas abiertas a cada docente sobre la experiencia que tiene sobre los recursos didáctico utilizados para la instrucción de la materia. Los resultados que se obtuvieron indican que más del 50% de los estudiantes no entienden el paradigma de la POO, solo el 28% si lo entiende y lo aplica para solucionar problemas reales y el 22% entiende los conceptos, pero no los saben aplicar a cada situación problemática que se les presenta. Se recomiendan algunas estrategias didácticas de aprendizaje tales como aprendizaje basado en proyectos, descomposición de problemas, etc. Lo cual reducirá el número de reprobados en esta materia y entenderán el paradigma orientado a objetos.

Palabras clave: Aprendizaje, educación, enseñanza, objeto, paradigma, programación.

Abstract

The study “Object-Oriented Programming Paradigm” aims to detect the level of learning among students enrolled in the Object-Oriented Programming (OOP) course. A hybrid quantitative-qualitative methodology is used to analyze data collected from a sample of 65 software engineering students from the Autonomous University of the West, Southern Regional Unit. A questionnaire with 10 items was administered to evaluate each of the characteristics of OOP: abstraction, polymorphism, encapsulation, and inheritance. Additionally, each instructor was interviewed using an open-ended questionnaire about their experiences with the educational resources used to teach this subject. The results indicate that more than 50% of the students do not understand the OOP paradigm, only 28% understand and apply it to solve real-world problems, and 22% understand the concepts but do not know how to apply them to different problem situations they encounter. Several educational strategies are recommended such as project-based learning, problem

Actividad 5:

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

Resumen: Estudiar los videojuegos implica clasificarlos de alguna manera. Pero construir criterios de clasificación que no sean los que prescriben la industria de los videojuegos o las formas conocidas de censura social (p.e., videojuegos apropiados para niños y videojuegos para adultos) entraña varias dificultades, dado lo diversos y crecientemente variados. En la literatura contemporánea es posible encontrar interesantes iniciativas orientadas a proponer algún tipo de clasificación que sea pertinente a la investigación en psicología y ciencias afines. Este artículo ofrece una propuesta de clasificación de los videojuegos atendiendo al talante y naturaleza de las tareas implicadas en los videojuegos (más abiertas o más cerradas), y sugiere una alternativa a la clasificación propuesta por Juul (2002 y 2007), que distingue entre videojuegos con metas obligatorias, metas opcionales y sin metas. Para sugerir una propuesta distinta a la de Juul, se ha apelado a categorías y distinciones establecidas por Pierre Levy (1999) para definir el estatuto de lo virtual.

PALABRAS-CLAVE: videojuegos, tarea dinámica, cognición situada, resolución de problemas.

74

I

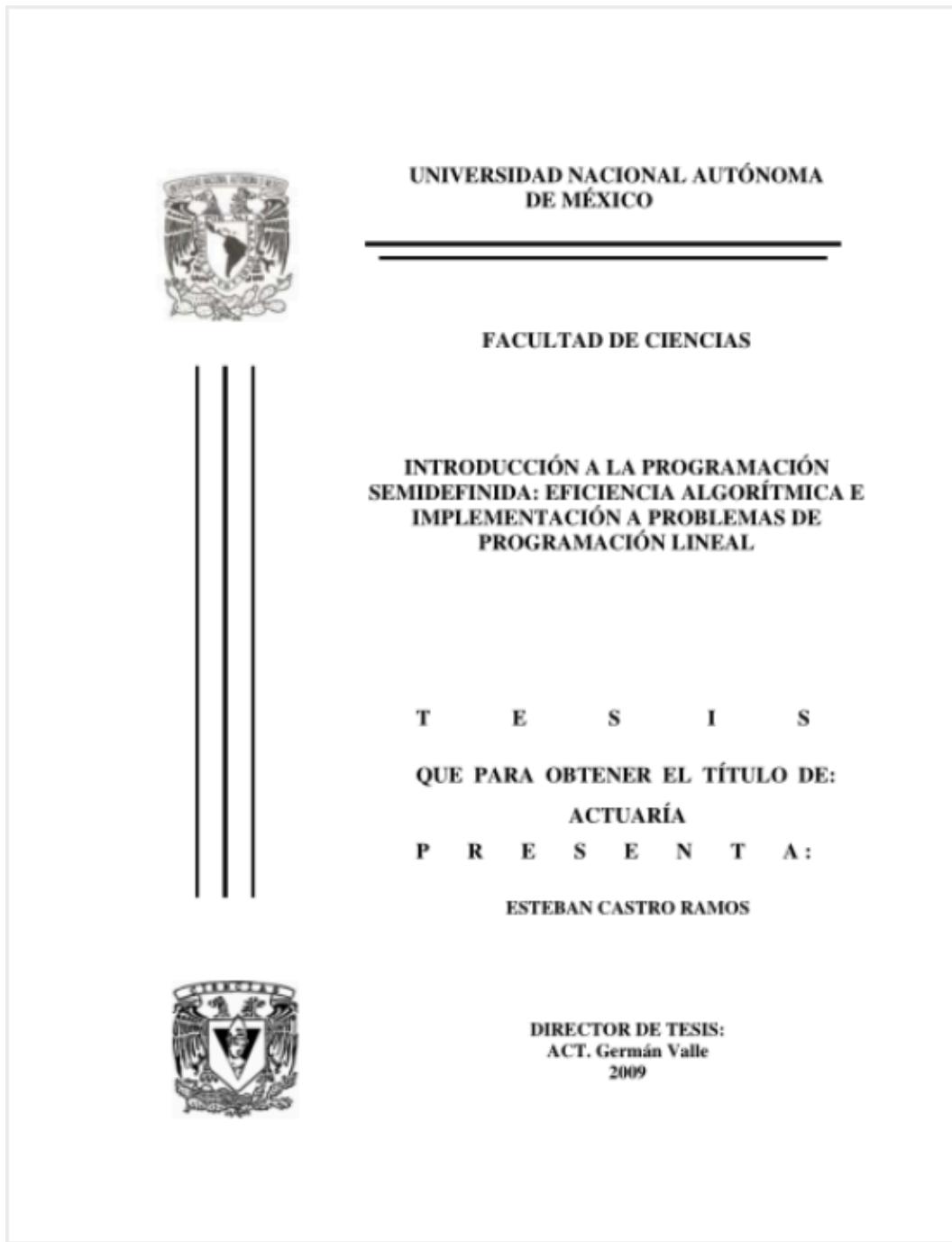
ntentar avanzar en una comprensión del lugar que ocupan los videojuegos en la vida de los niños ha sido una preocupación para investigadores y estudiosos del fenómeno en todo el mundo y en Colombia. En Estados Unidos, los estudios sobre videojuegos se han desarrollado de manera sostenida desde la década de 1980. Desde sus inicios, dos vertientes claras dominaron el campo: por un lado, aquella que versaba sobre las posibles aplicaciones y derivas de los videojuegos en la educación escolar y el desarrollo cognitivo de los niños; y por otro lado, aquella que indagaba sobre los efectos y peligros de los videojuegos en la conducta (Gentile, 2005). En

Estados Unidos, estos estudios han comprometido no sólo una variopinta gama de iniciativas de investigación en universidades, sino también ingentes esfuerzos públicos y gubernamentales orientados a estudiar, examinar y realizar diagnósticos referidos al consumo de videojuegos, formular recomendaciones y trazar políticas para regular su uso entre la población infantil y adolescente.

En Colombia la incorporación de consolas y videojuegos en los hogares y en espacios comerciales de acceso público ha sido un fenómeno significativo y creciente desde hace al menos dos décadas. En la actualidad es el segundo mercado de consolas y videojuegos en América Latina, después de México y por encima de Brasil y Chile. Sin embargo, sólo desde hace cinco años se iniciaron estudios serios sobre penetración y tiempo de exposición y uso de los videojuegos dentro los hogares y en diferentes cohortes generacionales o grupos de edad. Gracias a una iniciativa del Ministerio de Cultura, y a través del Departamento Administrativo Nacional de Estadísticas (DANE), la entidad encargada de dar cuenta de las estadísticas oficiales en el país, en la actualidad se cuenta con algunos datos generales sobre la presencia de los

Actividad 6:

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



Actividad 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.

Educación Química (2017) 28, 196–201



educación Química
www.educacionquimica.info

REFLEXIÓN

Los paradigmas de la ingeniería química: las nuevas fronteras

Reynerio Álvarez-Borroto*, Ullrich Stahl, Elvia V. Cabrera-Maldonado y Marco V. Rosero-Espín

Facultad de Ingeniería Química, Universidad Central del Ecuador, Quito, Ecuador

Recibido el 3 de febrero de 2017; aceptado el 16 de mayo de 2017
Disponible en Internet el 16 de junio de 2017

PALABRAS CLAVE
Paradigma;
Ingeniería química;
Nuevas fronteras;
Educación

KEYWORDS
Paradigm;
Chemical
Engineering;
New frontiers;
Education

Resumen James Wei, profesor del «Department of Chemical Engineering-MIT» empleó el concepto de paradigma en 1988, introducido por T. Kuhn, para caracterizar las etapas evolutivas de la ingeniería química. Wei identificó 3 períodos: el preparadigmático, un primer paradigma que lo relaciona con la publicación del texto *Principles of Chemical Engineering*, y un segundo paradigma asociado al texto: *Transport Phenomena*, de Bird, Stewart and Lightfoot, en 1960. Los paradigmas de Wei son reduccionistas y limitados y deben ser ampliados y actualizados. En el presente trabajo se identifican 3 etapas: el preparadigmático, el paradigma de las operaciones unitarias, y el paradigma de la ciencia de la ingeniería química. Se hace referencia a las nuevas fronteras de la ingeniería química y a la necesidad de incluir nuevas disciplinas académicas y nuevas técnicas de enseñanza-aprendizaje.
© 2017 Universidad Nacional Autónoma de México, Facultad de Química. Este es un artículo Open Access bajo la licencia CC BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

The paradigms of Chemical Engineering: The new frontiers

Abstract James Wei, a professor at the Department of Chemical Engineering-MIT, used the paradigm concept in 1988, introduced by T. Kuhn, to characterize the steps of evolution of the Chemical Engineering. Wei identified three periods: the pre-paradigmatic, a first paradigm which he relates to the publication of the text 'Principles of Chemical Engineering', and a second paradigm associated with the text: 'Transport Phenomena', by Bird, Stewart and Lightfoot, in 1960. Wei's paradigms are reductionistic as well as limited and need to be expanded and

* Autor para correspondencia.
Correo electrónico: reynerioalvarez2011@gmail.com (R. Álvarez-Borroto).
La revisión por pares es responsabilidad de la Universidad Nacional Autónoma de México.
<http://dx.doi.org/10.1016/j.eq.2017.05.002>
0187-893X/© 2017 Universidad Nacional Autónoma de México, Facultad de Química. Este es un artículo Open Access bajo la licencia CC BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1



2



3



4



Actividad 8:

Utiliza ChatGPT (OpenAI)

realiza una investigación sobre el tema de ciberseguridad. Escribe el prompt utilizado y el resultado obtenido.

1-Prompt utilizado: “Realizame una investigación referente a la ciberseguridad”. Al ejecutarlo, me desglosa la siguiente información:

1. Definición de Ciberseguridad

La ciberseguridad se refiere al conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas informáticos, redes, programas y datos de ataques, daños o accesos no autorizados. Su principal objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, tanto en entornos digitales como en el uso de sistemas tecnológicos.

2. Importancia de la Ciberseguridad

En un mundo cada vez más digitalizado, la ciberseguridad es fundamental para proteger la privacidad de los usuarios, la integridad de los datos y la continuidad de las operaciones. Las amenazas cibernéticas han evolucionado con el tiempo y se han vuelto más sofisticadas, por lo que es esencial contar con mecanismos de defensa eficaces para mitigar los riesgos.

Consecuencias de la falta de ciberseguridad

- Robo de datos: Información personal, financiera o empresarial puede ser robada, lo que lleva a fraudes y violación de la privacidad.
- Ataques a infraestructuras críticas: Empresas y gobiernos que dependen de sistemas informáticos para operaciones críticas pueden ser blanco de ciberataques que paralizan actividades vitales.
- Pérdida económica: Las empresas pueden perder dinero debido a los costos de recuperación tras un ataque, multas por no cumplir con normativas de protección de datos y la pérdida de reputación.
- Cibercrimen: Los ataques pueden ser usados para extorsionar a víctimas mediante ransomware o el robo de identidad.

3. Tipos Comunes de Amenazas Cibernéticas

Las amenazas cibernéticas son diversas y evolucionan rápidamente. Algunos de los tipos más comunes incluyen:

- **Malware:** Software malicioso diseñado para dañar o explotar computadoras y redes. Ejemplos incluyen virus, gusanos, spyware y ransomware.
- **Phishing:** Técnica utilizada para obtener información sensible (como contraseñas o detalles bancarios) a través de mensajes fraudulentos que parecen provenir de fuentes confiables.
- **Ataques de denegación de servicio (DDoS):** Los atacantes sobrecargan los servidores de una red con tráfico masivo para interrumpir su funcionamiento.
- **Exploits de vulnerabilidades:** Ataques que explotan fallas en el software o hardware de un sistema.
- **Ransomware:** Un tipo de malware que bloquea el acceso a los archivos o sistemas de una víctima, exigiendo un pago para liberarlos.

4. Estrategias y Herramientas de Defensa en Ciberseguridad

Para proteger los sistemas, es necesario implementar diversas estrategias y tecnologías:

- **Firewalls:** Actúan como una barrera entre una red interna y externa, bloqueando accesos no autorizados.
- **Antivirus y Antimalware:** Software que detecta y elimina programas maliciosos.
- **Encriptación:** El proceso de codificar información para que solo las partes autorizadas puedan acceder a ella.
- **Autenticación multifactor (MFA):** Técnica que requiere más de un método de verificación para acceder a un sistema.
- **Monitoreo y auditoría de redes:** Herramientas que permiten observar el tráfico de la red para identificar comportamientos anómalos.
- **Parcheo de software:** Actualización periódica de sistemas y programas para corregir vulnerabilidades conocidas.

5. Tendencias en Ciberseguridad

Algunas de las tendencias que están moldeando el futuro de la ciberseguridad son:

- Inteligencia Artificial y Aprendizaje Automático: El uso de IA ayuda a detectar y mitigar amenazas en tiempo real, identificando patrones anómalos y mejorando las respuestas ante incidentes.
- Ciberseguridad en la nube: A medida que más empresas adoptan servicios en la nube, la protección de los datos almacenados y procesados en la nube se vuelve una prioridad.
- Zero Trust: Un enfoque en el que no se confía en ningún usuario o dispositivo, incluso si están dentro de la red corporativa, y se verifica continuamente.
- Privacidad de los datos: La protección de la información personal de los usuarios es un tema cada vez más importante, especialmente con regulaciones como el GDPR.

6. Normativas y Regulaciones en Ciberseguridad

Las normativas legales están tomando un papel crucial en la implementación de medidas de ciberseguridad. Algunas de las más relevantes incluyen:

- Reglamento General de Protección de Datos (GDPR): Un conjunto de leyes que rige la protección de los datos personales de los ciudadanos de la UE.
- Ley Cybersecurity Act: Ley en EE. UU. que establece requisitos de seguridad para las infraestructuras críticas del país.
- Ley de Protección de Datos Personales (LFPDPPP): En México, regula el tratamiento de datos personales para garantizar su privacidad y protección.

7. Desafíos Actuales en Ciberseguridad

- Escasez de profesionales capacitados: La demanda de expertos en ciberseguridad sigue superando la oferta, lo que hace más difícil la implementación de soluciones de seguridad eficaces.
- Evolución rápida de las amenazas: Los atacantes desarrollan nuevas técnicas y herramientas con frecuencia, lo que hace que las defensas tradicionales sean insuficientes.
- Ciberseguridad en el Internet de las Cosas (IoT): Con el crecimiento de dispositivos conectados, la seguridad en estos dispositivos es cada vez más crítica.

8. Futuro de la Ciberseguridad

El futuro de la ciberseguridad se centrará en la adaptación continua ante las amenazas emergentes. Las inversiones en inteligencia artificial, la automatización de procesos de defensa y la colaboración global en el intercambio de información sobre amenazas serán claves para proteger mejor la infraestructura digital.

2- La información desglosada es muy buena y concisa, pero no cumplió satisfactoriamente con el formato adecuado de investigación, ya que no me arrojo las fuentes consultadas, por consiguiente tuve que mejorar el prompt de la siguiente manera “dame tus fuentes utilizadas” con lo que me dio a conocer la siguiente información.

Instituciones de ciberseguridad: Organizaciones como el Centro Nacional de Ciberseguridad (en varios países), Cybersecurity and Infrastructure Security Agency (CISA), y la European Union Agency for Cybersecurity (ENISA), que proporcionan informes, recomendaciones y directrices sobre ciberseguridad.

Regulaciones y leyes: Directrices y leyes como el GDPR (Reglamento General de Protección de Datos de la Unión Europea), la Ley de Ciberseguridad de EE. UU., y la LFPDPPP (Ley Federal de Protección de Datos Personales en México).

Publicaciones y reportes de empresas de ciberseguridad: Como Symantec, Kaspersky, McAfee, Trend Micro, y otros informes de análisis de amenazas de empresas especializadas, como los informes anuales de Verizon sobre violaciones de datos.

Artículos en blogs especializados: Sitios como DarkReading, Krebs on Security, y CSO Online, que publican regularmente sobre tendencias de ciberseguridad, incidentes recientes y mejores prácticas.

Investigaciones académicas: Muchas universidades y centros de investigación (por ejemplo, Carnegie Mellon, MIT, Stanford) publican estudios sobre ciberseguridad, vulnerabilidades y nuevas amenazas.

3- De igual forma si cumplió con la función de darme las fuentes de consulta, tras la verificación de las fuentes, todas son correctas y verídicas, es decir, la información viene de autores reales y no es inventada, pero falto un prompt más para brindarme las bibliografías de manera adecuada en formato APA; ya que no cumplió de nuevo con el formato de investigación adecuado.

El prompt utilizado fue: “Las necesito en formato APA, como un trabajo de investigación adecuado y profesional”, con lo que por fin concluyó la investigación de forma adecuada y precisa desglosando lo siguiente.

Referencias en formato APA

1. CISA (Cybersecurity and Infrastructure Security Agency)
CISA. (n.d.). *Cybersecurity & Infrastructure Security Agency*. Recuperado el 22 de agosto de 2025, de <https://www.cisa.gov>
2. ENISA (European Union Agency for Cybersecurity)
European Union Agency for Cybersecurity (ENISA). (n.d.). *ENISA – European Union Agency for Cybersecurity*. Recuperado el 22 de agosto de 2025, de <https://www.enisa.europa.eu>
3. GDPR (Reglamento General de Protección de Datos)
GDPR-info. (n.d.). *General Data Protection Regulation (GDPR) Compliance Guidelines*. Recuperado el 22 de agosto de 2025, de <https://gdpr-info.eu>
4. Verizon Data Breach Investigations Report (DBIR)
Verizon. (2025). *2025 Data Breach Investigations Report*. Recuperado el 22 de agosto de 2025, de <https://www.verizon.com/business/resources/reports/dbir>
5. Krebs on Security
Krebs, B. (n.d.). *Krebs on Security*. Recuperado el 22 de agosto de 2025, de <https://krebsonsecurity.com>
6. DarkReading
DarkReading. (n.d.). *Dark Reading - Cybersecurity News*. Recuperado el 22 de agosto de 2025, de <https://www.darkreading.com>

4- Así concluyó la ayuda con la inteligencia artificial “Chat GPT” con varios errores para formar un trabajo profesional, pero tras varios intentos y formular nuevos prompts logró darnos unos buenos resultados más eficientes y útiles.

Actividad 9:

Utiliza DeepSeek <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 ChatGPT.

Prompt utilizado: Genera una investigación referente al tema de ciberseguridad con las siguientes características: Introducción, historia, características, usos, temas relacionados y fuentes.

Resultado Obtenido:

Investigación: Ciberseguridad en la Era Digital

Autor: Asistente de Investigación

Fecha: 26 de octubre de 2023

Introducción

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. En un mundo cada vez más interconectado, donde la información es un activo crítico para individuos, empresas y gobiernos, la ciberseguridad ha dejado de ser una preocupación técnica para convertirse en una necesidad estratégica global. Su objetivo fundamental es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo los sistemas y datos contra accesos no autorizados, ciberataques y daños.

Historia de la Ciberseguridad

La evolución de la ciberseguridad está intrínsecamente ligada al desarrollo de la informática y las redes.

•Década de 1970 - Los inicios: Con la creación de ARPANET (predecesora de Internet), surgieron las primeras preocupaciones por la seguridad. El primer caso documentado de un "gusano" informático fue Creeper (1971), un programa experimental que se replicaba a sí mismo. Como contramedida, se creó Reaper, el primer programa antivirus de la historia.

•Década de 1980 - La popularización del malware: La llegada de las PC hizo que los virus se volvieran más comunes. El Brain (1986), considerado el primer virus para IBM PC, marcó el inicio de una nueva era de amenazas. Este período también vio nacer los primeros Firewalls para filtrar el tráfico de red.

- Década de 1990 - La explosión de Internet y el comercio electrónico: La popularización de Internet abrió un vasto nuevo campo para los ciberdelincuentes. Aparecieron virus más dañinos como Melissa y I Love You. La necesidad de proteger las transacciones financieras en línea impulsó el desarrollo de protocolos de cifrado como SSL (Secure Sockets Layer).
- Década de 2000 - La profesionalización del cibercrimen: Los ataques se volvieron más sofisticados y con motivaciones económicas. Surgieron botnets, ransomware incipiente y el phishing se popularizó. Incidentes masivos como el gusano SQL Slammer (2003) demostraron la vulnerabilidad global.
- Década de 2010 a la actualidad - La era de los APT y la guerra cibernética: Los ataques son ahora realizados por grupos organizados y estados-nación. Se popularizan los Advanced Persistent Threats (APT), campañas de espionaje complejas y de larga duración. El ransomware se convierte en una epidemia global (ej. WannaCry, 2017). La aparición del Internet de las Cosas (IoT) expande la superficie de ataque. La Inteligencia Artificial (IA) comienza a ser utilizada tanto para defender como para atacar.

Características Principales de la Ciberseguridad

La ciberseguridad efectiva se basa en varios pilares fundamentales:

1. Confidencialidad: Garantizar que la información solo sea accesible para aquellas personas autorizadas a tener acceso a ella.
2. Integridad: Proteger la exactitud y totalidad de la información y los métodos de procesamiento. Implica que los datos no sean alterados de manera no autorizada.
3. Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y a los recursos asociados cuando así lo requieran.
4. Autenticación: Verificar la identidad de un usuario, proceso o dispositivo, a menudo como un prerequisito para permitir el acceso a los recursos del sistema.
5. No repudio: Garantizar que una parte involucrada en una comunicación no pueda negar la autenticidad de su firma en un documento o el envío o recepción de un mensaje.
6. Defensa en Profundidad (DiD): Estrategia que emplea múltiples capas de seguridad para proteger la información. Si una capa falla, otra previene el acceso.

Usos y Aplicaciones

La ciberseguridad tiene un amplio espectro de aplicaciones en distintos sectores:

- Sector Financiero: Protección contra fraudes en banca online, secuestro de transacciones (man-in-the-browser) y defensa de infraestructuras críticas.
- Sector Salud (Healthtech): Protección de historiales médicos confidenciales (PHI) y de dispositivos médicos conectados (marcapasos, bombas de insulina) que podrían ser hackeados.
- Infraestructuras Críticas: Seguridad de sistemas SCADA/ICS que controlan centrales eléctricas, redes de agua, transporte y sistemas de comunicación.
- Gobierno y Defensa: Protección de información clasificada, defensa contra ciberataques de estados-nación y asegurar la integridad de procesos electorales.
- Empresas de todos los tamaños: Protección de secretos comerciales, propiedad intelectual, datos de clientes y continuidad del negocio mediante planes de recuperación ante desastres.
- Usuarios Individuales: Protección de la identidad digital, privacidad en redes sociales, seguridad en transacciones online y protección de dispositivos personales (PC, smartphone, IoT del hogar).

Temas Relacionados

La ciberseguridad es un campo interdisciplinario que se intersecta con varias áreas cruciales:

- Privacidad Digital: Derecho a controlar cómo se recopila, utiliza y comparte la información personal. Regulaciones como el GDPR en Europa o la LGPD en Brasil están directamente relacionadas.
- Ciberinteligencia (Cyber Intelligence): Recopilación y análisis de información sobre amenazas, actores y tácticas para anticipar y prevenir ataques.
- Forense Digital: Análisis posterior a un incidente de seguridad para determinar las causas, recopilar evidencias y entender el alcance del daño.
- Hacking Ético (Penetration Testing): Práctica de probar los sistemas informáticos de una organización de forma autorizada para descubrir vulnerabilidades antes de que un atacante malintencionado lo haga.
- Concientización en Seguridad: Factor humano como la primera línea de defensa. La formación para identificar correos de phishing y seguir buenas prácticas de higiene digital es fundamental.
- Seguridad en la Nube (Cloud Security): Conjunto de políticas, tecnologías y controles para proteger datos, aplicaciones e infraestructuras en entornos cloud.

- Seguridad de Aplicaciones (AppSec): Proceso de desarrollar, agregar y probar funciones de seguridad en las aplicaciones para prevenir vulnerabilidades contra amenazas.

Fuentes y Referencias

1.Institucionales:

- NIST (National Institute of Standards and Technology) - Cybersecurity Framework: <https://www.nist.gov/cyberframework> (Marco de referencia globalmente aceptado).
- ENISA (European Union Agency for Cybersecurity): <https://www.enisa.europa.eu/> (Informes y guías sobre tendencias y regulaciones en la UE).
- ISC² (International Information System Security Certification Consortium): <https://www.isc2.org/> (Organización líder en certificaciones y recursos educativos).
- CISA (Cybersecurity and Infrastructure Security Agency - USA): <https://www.cisa.gov/> (Alertas y consejos sobre ciberseguridad).

2.Libros:

- "The Art of Invisibility" por Kevin Mitnick.
- "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers" por Andy Greenberg.
- "This Is How They Tell Me the World Ends: The Cyberweapons Arms Race" por Nicole Perlroth.

3.Publicaciones y Medios:

- Krebs on Security: <https://krebsonsecurity.com/> (Blog de investigación periodística sobre ciberseguridad).
- The Hacker News: <https://thehackernews.com/> (Sitio web de noticias sobre vulnerabilidades y ciberataques).
- Dark Reading: <https://www.darkreading.com/> (Portal de noticias e información para profesionales de la seguridad).

Diferencias con ChatGPT:

La información obtenida es realmente satisfactoria cumpliendo en su totalidad con el prompt propuesto, a diferencia de ChatGPT que no realizó una investigación tan extensa, aunque en esta ocasión se mejoraron las instrucciones dadas (prompt) ChatGPT de cualquier manera no cumple de una forma tan satisfactoria, teniendo que indagar más en lo que pides sin cumplirlo en su totalidad. De igual forma acerca de las referencias bibliográficas en formato APA, DeepSeek las cita sin ningún problema aunque no especifiques el formato, por otro lado con ChatGPT tienes que generar varias especificaciones para que lo cumpla.

Es decir que DeepSeek formula una mejor investigación más extensa, cita de mejor manera las referencias y cumple mejor las instrucciones dadas.

Actividad 10:

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

Prompt utilizado: Crea una imagen del tema de ciberseguridad donde aparezca un hacker.

Imágenes Obtenidas:



Actividad 11:

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

Prompt utilizado: Crea una presentación sobre ciberseguridad dirigida a estudiantes de la Facultad de Ingeniería de la UNAM. con los siguientes puntos:
-Introducción a la ciberseguridad. -amenazas comunes. -impacto de ciberataques.
-cómo prevenir ataques. -futuro de la ciberseguridad.

Ciberseguridad: Protegiendo Nuestro Mundo Digital



¿Qué es la Ciberseguridad?

La ciberseguridad es la disciplina que se encarga de proteger los sistemas, redes y datos contra ataques digitales, garantizando la confidencialidad, integridad y disponibilidad de la información. Es un pilar fundamental en nuestra era digital.



Made with GAMMA

Amenazas Comunes en el Mundo Digital



Made with GAMMA

Impacto Real de los Ciberataques

En 2024, el costo global del cibercrimen superó los **\$8 billones de dólares**. En México, empresas han sufrido pérdidas millonarias y robo de datos sensibles.

Casos Emblemáticos en México:

- **Pemex:** Ataque de ransomware en 2019 que afectó sus sistemas críticos.
- **CFE:** También sufrió un ataque en 2019, comprometiendo sus operaciones.
- **Bancos:** Incidentes de fraude y acceso no autorizado a sistemas.



Estos ataques no solo generan pérdidas económicas, sino que también afectan la privacidad, la confianza en los servicios digitales y pueden paralizar operaciones esenciales.

Made with GAMMA

Cómo Prevenir Ataques: Buenas Prácticas

- **Contraseñas Robustas y Gestores**

Utiliza combinaciones complejas de letras, números y símbolos. Un gestor de contraseñas te ayudará a administrarlas de forma segura.

- **Actualizaciones Constantes**

Mantén tu sistema operativo, aplicaciones y navegadores siempre actualizados para corregir vulnerabilidades conocidas.

- **Autenticación Multifactor (MFA)**

Activa MFA en todas tus cuentas importantes para añadir una capa extra de seguridad.

- **Detección de Sospechas**

Sé escéptico con enlaces o archivos desconocidos. Verifica siempre al remitente antes de hacer clic o descargar.

- **Copias de Seguridad (Backups)**

Realiza copias de seguridad periódicas de tu información crucial y guárdalas en un lugar seguro.

Made with **GAMMA**

Herramientas y Tecnologías Clave



Antivirus y Antimalware

Programas esenciales para detectar y eliminar software malicioso en tus dispositivos.



Firewalls y Sistemas IDS/IPS

Protegen tu red monitoreando el tráfico y bloqueando accesos no autorizados.



Cifrado de Datos

Transforma tu información para que sea ilegible para personas no autorizadas, protegiendo su confidencialidad.



Redes Privadas Virtuales (VPN)

Crean una conexión segura y cifrada a través de una red pública, ideal para proteger tu privacidad.



Monitoreo y Respuesta

Sistemas que detectan actividades sospechosas y permiten una respuesta rápida ante incidentes de seguridad.

Made with **GAMMA**

El Factor Humano: La Primera Línea de Defensa

Aunque la tecnología es vital, la **mayoría de los ataques exitosos explotan errores humanos**. Por ello, el eslabón más fuerte o más débil en ciberseguridad eres tú.

¡Tu Responsabilidad es Clave!

- **Capacitación Constante:** Mantente informado sobre las nuevas amenazas y las mejores prácticas de seguridad.
- **Cultura de Seguridad:** Reporta cualquier incidente o sospecha, por pequeña que parezca, sin miedo a represalias.

Ejemplo: La UNAM ha implementado campañas internas de concientización para sus estudiantes y personal, enfocándose en la identificación de phishing y la importancia de contraseñas seguras.



El Futuro de la Ciberseguridad

Inteligencia Artificial (IA) y Machine Learning

La IA será fundamental para detectar y responder a amenazas en tiempo real, automatizando procesos y prediciendo ataques.

Regulaciones Globales y Estándares

Se espera una mayor armonización de leyes y normativas a nivel internacional para proteger la privacidad y los datos.

Seguridad en la Nube e IoT

A medida que más datos y dispositivos se conectan, la protección de la nube y del Internet de las Cosas (IoT) será crucial.

Crecimiento de Oportunidades Profesionales

La demanda de expertos en ciberseguridad seguirá en aumento, creando un campo laboral prometedor para ingenieros.

Casos de Éxito y Aprendizajes en México



México está avanzando en ciberseguridad con iniciativas notables:

- **Cursos Especializados:** La UNAM ha lanzado el "Curso de Ciberseguridad para No Informáticos" para ampliar el alcance del conocimiento.
- **Clubes Estudiantiles:** En la UNAM y otras universidades, los clubes fomentan habilidades prácticas y la investigación en el campo.
- **Colaboración Estratégica:** La unión entre la academia, el gobierno y el sector privado es clave para fortalecer la infraestructura de seguridad digital del país.

Conclusión: Tu Rol en la Ciberseguridad

La ciberseguridad es responsabilidad de todos.



Como futuros ingenieros, tienen un papel crucial:

- **Adopta hábitos seguros:** Practica y promueve la ciberhigiene en tu vida diaria.
- **Mantente informado:** El mundo digital evoluciona, y tú también debes hacerlo.
- **Diseña para la seguridad:** Desde tu disciplina, integra la seguridad desde el inicio en cada sistema o producto que desarrolles.

¡Protejamos juntos nuestro futuro digital en la UNAM y más allá!

Bibliografía y Recursos Adicionales

Para profundizar en los temas de ciberseguridad, te recomendamos consultar las siguientes fuentes y recursos:

- "Estadísticas de Ciberseguridad en México 2023." PricewaterhouseCoopers (PwC) México. (Informe anual de la industria)
- "Guía de Buenas Prácticas en Ciberseguridad para PyMES." Asociación Mexicana de Internet (AMIPCI). (Recurso sectorial)
- "Ciberseguridad: Un Enfoque Integral para el Mundo Digital." Dr. Alonso Ramírez, UNAM. (Publicación académica)
- "Reporte de Amenazas de ESET Latinoamérica 2023." ESET. (Análisis de tendencias y riesgos)
- "Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)." Gobierno de México. (Portal oficial de seguridad)



Actividad 12:

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





Actividad 13:

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

La investigación en ciberseguridad fue elaborada utilizando la herramienta DeepSeek y posteriormente evaluada con el verificador ZeroGPT, el cual determinó un 85.28% de probabilidad de haber sido generada mediante inteligencia artificial.

1. Producción con DeepSeek: El empleo de esta herramienta permitió estructurar un documento con un alto nivel de coherencia, orden y desarrollo técnico. Sin embargo, su uso intensivo también incrementa la posibilidad de que el texto presente patrones propios de redacción automática, reduciendo la percepción de originalidad y aportación personal.
2. Evaluación de ZeroGPT (85.28% IA): El porcentaje obtenido indica que el trabajo muestra una fuerte tendencia hacia la autoría automatizada, aunque no en su totalidad. Esto sugiere que probablemente hubo una combinación entre contenido generado por IA y cierto grado de intervención humana, ya sea en la edición, adaptación o incorporación de ideas propias.

Actividad 14:

Utiliza [Originality.ai](https://originality.ai/) y analiza el texto obtenido con Chat GPT que probabilidad hay de que el texto haya sido generado por IA, verifica si hay plagio, comenta los resultados obtenidos. Utilizar la página just done para comprobar el uso de ia. Scribbr AI Detector.

Resultado de plagio y si el texto fue generado por IA:

La investigación fue sometida a dos verificadores digitales con el fin de evaluar su autenticidad y originalidad. Los resultados obtenidos fueron los siguientes:

1. **Just Done reportó un 92% de plagio:** Este porcentaje es sumamente elevado y refleja que la mayoría del contenido proviene de fuentes externas sin una adecuada reestructuración o citación. En un contexto académico, este nivel de coincidencia resulta inaceptable, ya que compromete la validez del trabajo y pone en duda la autoría intelectual.
2. **Quillbot determinó un 99% de probabilidad de generación mediante inteligencia artificial:** Este valor sugiere que el texto presenta patrones de redacción característicos de sistemas automatizados, lo cual indica que gran parte del contenido fue generado o modificado con ayuda de IA.

Actividad 15:

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

La página de aifindy me parece bastante interesante porque junta en un solo lugar muchos recursos de inteligencia artificial. Lo que más me llamó la atención es que todo está organizado por categorías, lo que hace más fácil encontrar lo que buscas sin perder tanto tiempo. No es como otras páginas que son un relajo, aquí todo se siente más claro y directo.

Algo que me gusta es que te da una idea de cuántas opciones existen y de lo mucho que la IA se está usando en diferentes áreas. Al ver todo junto te das cuenta de que no es solo para cosas complicadas, sino que realmente puede ser útil en la vida diaria o en la escuela.

En general, pienso que aifindy es como un espacio donde puedes conocer rápido lo que hay disponible sin necesidad de estar investigando tanto. Me parece práctico, accesible y sobre todo una buena manera de aprovechar lo que la tecnología está ofreciendo ahora.