**Título:**

**Evaluación de la cultura digital en Panamá y propuesta de un modelo de asistente para concientizar sobre navegación segura en internet.**

Contenido

[Resumen 2](#_Toc140438698)

[Introducción 2](#_Toc140438699)

[Formulación de hipótesis y objetivos 3](#_Toc140438700)

[Palabras clave: 3](#_Toc140438701)

[Marco teórico 3](#_Toc140438702)

[Cultura, sociedad y conciencia digital. 3](#_Toc140438703)

[Cultura digital y ciberseguridad en Panamá 4](#_Toc140438704)

[Delitos informáticos en Panamá y leyes 5](#_Toc140438705)

[Revisión de la literatura 5](#_Toc140438706)

[Procesamiento del lenguaje natural 5](#_Toc140438707)

[Asistentes digitales, inteligencia artificial y bigdata. 5](#_Toc140438708)

[Modelos y herramientas existentes para generar conversaciones fluidas 6](#_Toc140438709)

[Estudios relacionados 6](#_Toc140438710)

[Objetivos del proyecto: 7](#_Toc140438711)

[Objetivo general: 7](#_Toc140438712)

[Objetivos específicos: 7](#_Toc140438713)

[Materiales, métodos y metodología 7](#_Toc140438714)

[Materiales y métodos para la recolección de datos y análisis de la población. 7](#_Toc140438715)

[Metodología y materiales para el desarrollo y configuración del modelo GPT. 7](#_Toc140438716)

[Creación de conjunto de datos de entrenamiento y Adaptación de modelo nanoGPT 8](#_Toc140438717)

[Configuración de los parámetros de entrenamiento del código y entrenamiento 11](#_Toc140438718)

[Resultados y discusión 19](#_Toc140438719)

[Resultados 19](#_Toc140438720)

[Discusión 19](#_Toc140438721)

[Oportunidades de desarrollo del prototipo 24](#_Toc140438722)

[Conclusión 24](#_Toc140438723)

[Referencias 24](#_Toc140438724)

# Resumen

En este proyecto se investiga sobre el nivel de conciencia digital en una muestra de 76 personas seleccionadas con muestreo aleatorio simple, la población reconoce la importancia del conocimiento sobre navegación segura y métodos que garanticen la triada de la seguridad informática. Los resultados muestran que el 34,2% de la población considera tener conocimientos básicos de seguridad informática el 69.3%, no ha experimentado ningún incidente de seguridad aparente. Según los resultados, la propuesta de un modelo de asistente de lenguaje autorregresivo especializado en brindar recomendaciones prácticas de seguridad y navegación segura respalda positivamente la propuesta de un modelo GPT.

Abstract

# Introducción

La sociedad actual, está completamente digitalizada, pero carece de conciencia digital que permite disminuir los riesgos: La falta de conocimiento relacionado con las tendencias actuales del Internet de las Cosas (IoT), las plataformas cloud, los servicios en la nube, las redes sociales y el uso de aplicaciones Fintech. (De este modo se atraen a los ciberdelincuentes para aprovecharse y ampliar su *modus operandi)*. Aun así, toman ventaja de la información personal publicada en redes sociales, además de que utilizan ataques para intervenir y captar datos que pueden utilizar en contra de la víctima para sacar beneficio. Aun cuando son desplegadas y adoptadas estás tecnologías se requiere de un personal consiente como: primeria línea de defensa ante ataques; ya que los sistemas por si solos a pesar de contar con mecanismos de tecnologías preventivas y para la detección (son los usuarios los cuales manipulan, configuran y utilizan las tecnologías).

A fin de cuentas, las consultas masivas a servicios web, a través de la red hacen que todo usuario conectado sea vulnerable; Cabe aclarar que si no somos consciente de las amenazas o métodos adecuados en Internet para contrarrestar: los ataques cibernéticos, mitigar riesgos o daños causado por las amenazas de Internet. Siendo así necesario para la sociedad en general que los desarrollos e implementaciones de tecnologías se orienten a innovaciones inclusivas que mejoran el bienestar social. Algo que siempre será un reto para países menos desarrollados en el ámbito cultural tecnológico es: crear brechas de conocimiento que provocan afectaciones en la seguridad personal, social, empresarial y nacional. Como lo menciona [1], casos como: el ciberacoso, el fraude, suplantación de identidad, filtración de datos y perdidas, infiltración en sistemas críticos pueden generar caos social (por lo que es necesario educar desde temprano sobre seguridad cibernética). Otros autores que han realizado investigaciones sobre conciencia digital han identificado las áreas de estudio que tienen un bajo nivel de conocimiento sobre malwares, técnicas de phishing, ataques de fuerza bruta y uso de contraseñas inseguras.[2]

El creciente uso de los medios digitales, en diversas áreas cotidianas de la vida, ha hecho que los ciudadanos estén más conectados a lo que sucede en su entorno. Estos utilizan tecnologías para comunicarse por múltiples medios sociales, controlar remotamente equipos, maquinarias y realizar transacciones. Este nuevo ecosistema digital, donde concurren las interacciones sociales, contiene una creciente ola de riesgos que pueden moldear el comportamiento en masa, influir, manipular y provocar daños (con ataques en el ecosistema digital en la llamada nueva ciudadanía digital). [3][4]

Es por esto por lo que esta investigación busca conocer el nivel de conciencia sobre riesgos cibernéticos en un grupo focal; Y plantear una propuesta a través de un prototipo de asistencia, por lenguaje natural a través de texto, por medio de un modelo GPT (de manera que se adopté y se ajusté a una pequeña escala a temas que apoyen a la concientización sobre seguridad informática y navegación segura en internet).

# Formulación de hipótesis y objetivos

1. En Panamá existe conciencia sobre los riesgos y vulnerabilidades en el ciberespacio.
2. Mediante un modelo GPT entrenado con un dataset se puede dar un mejor enfoque para concientizar y comunicar las amenazas y brindar recomendaciones de mitigación.
3. ¿Un asistente puede concienciar sobre la seguridad digital y sobre la importancia de la seguridad y del uso de técnicas que permitan aplicar buenas ‘prácticas de navegación en la sociedad informática en los medios electrónicos digitales?

# Palabras clave:

Asistente digital, Seguridad Informática, Modelo GPT, Cultura de seguridad digital, concientizar.

# Marco teórico

## Cultura, sociedad y conciencia digital.

A medida que la sociedad y las ciudades pasan a un enfoque inteligente, donde todo está digitalizado; Aumentan más los desafíos de seguridad protección y privacidad, existen correlaciones entre las ciudades interconectadas, la economía digital, la sociedad y los impactos negativos de gran alcance por falta de conciencia, cultura digital y una gestión integral entre los elementos que interactúan en la dinámica social. Pese a que se abordan las ciberamenazas no solo deben utilizarse enfoques de aspectos técnicos, sino también como componentes sociales que son necesarios capacitar.[5] Distintas ciudades en el mundo utilizan medidores inteligentes, cámaras de vigilancia por internet, pagos de servicios públicos, redes wifi-nacionales esto logra una conectividad y alcance mayor de acceso a internet. (Toda la información generada en la sociedad está siendo digitalizada). [6] [7]

La ciudadanía digital es la adopción del uso de sistemas de información y tecnológico para la sociedad, a través de los cuales realizan transacciones diarias con su entorno. Esto permite que todos los ciudadanos puedan consumir y utilizar los servicios públicos a través de medios digitales.[8] De manera que se puede llevar a través de comunidades en internet en donde el individuo adquiere una identidad, derechos, obligaciones que hacen que su participación a través de esta sea válida para la interacción social con su entorno de forma libre.[8]

La conciencia digital es el punto de partida para una cultura digital sólida, diversos estudios demuestran que la capacitación sobre la seguridad informática es una excelente manera de comunicar y concientizar a la población sobre las amenazas digitales. En el estudio realizado por [9], Se muestra que a través de la investigación de un grupo de niños y jóvenes a los cuales se les proporcionó información sobre las amenazas en internet, casos de estudio e historias. Otros estudios demuestran como las empresas adoptan este sistema de capacitaciones para asegurar la infraestructura y sus activos para garantizar la continuidad y cultura empresarial digital logrando mitigar las amenazas cibernéticas con este enfoque. [10], [11]

Al igual que una empresa, los países deben buscar proteger a los ciudadanos, los programas educativos, las implementaciones curriculares de tecnología permiten hacer que las generaciones venideras se conviertan en buenos ciudadanos digitales y usuarios de internet. Es complicado lograr esto en la práctica ya que, cada generación, grupo social, puede ser visto desde diferentes ángulos con respecto a el ámbito tecnológico, este aspecto generacional y profundización de internet en las generaciones venideras pueden hacerlas más propensas a engaños, perdida de sus datos y renuncia a su información con tal de aprovechar los beneficios de los servicios que utilizan.[12]

## Cultura digital y ciberseguridad en Panamá

En la investigación de [8], se indaga sobre el ciudadano panameño en aspectos de brechas digitales e informática educativa. En la investigación se realizó un proceso exploratorio para ver la adopción y cotidianidad de uso de tecnologías sobre materia digital. En Panamá se tiene un alcance de la red nacional de internet que permite cerrar brechas, pero aún existen retos para romper las desigualdades de acceso y participación a través de la red, algo se deslumbró con la pandemia como lo menciona[13] en la educación, en el acceso a la información por medios digitales obligados por la pandemia. Muchas de las instituciones han transformado sus servicios a enfoques digitales que permiten el rápido acceso a sus ciudadanos. Plataformas como Panamá Digital y muchas otras implementaciones a nivel educativo han aumentado la forma en que la sociedad interactúa con las instituciones educativas, financieras etc. Los retos de las brechas sociales y las capacidades relacionadas para crear conciencia digital entre diversas culturas internas, grupos sociales dificultan la capacitación a nivel de País para mitigar problemas y afectaciones a ciudadanos con carentes conocimientos que acceden a estas plataformas de instituciones públicas. Según [8], el ciudadano digital debe poseer educación en tecnología, estándares de conducta en medios electrónicos, participación electrónica, responsabilidad, libertades e inclusión, conciencia digital sobre los riesgos. Este conjunto de capacidades del ciudadano digital hace que este posea capacidad para actuar con conciencia y libertad siendo responsabilidad sobre los medios digitales, este espacio de sociedad virtual y cultura permite que los ciudadanos mantengan estándares de conducta y conciencia que permite la paz social resultado del buen el uso de la tecnología.

Por otro lado, según la AIG, en Panamá no se escapa de los ciberataques, en el 2021 se registraron en el País más de 3.2 millones de intentos, durante la pandemia las cifras aumentaron por el trabajo remoto, las clases en línea, pagos a empresas a través de medios virtuales etc. Estas cifras colocan a Panamá en el top 10. Si las empresas, personas y el gobierno no implementan medidas y una cultura de ciberseguridad estos ataques pueden generar alteración en la vida cotidiana y en la sociedad.[14]

## Delitos informáticos en Panamá y leyes

En Panamá existen leyes que determinan claramente los delitos cibernéticos como se menciona en el TITULO VIII del Código Penal sobre los delitos contra la seguridad jurídica de los medios electrónicos. En él se mencionan los delitos contra la seguridad informática y otros cuatro artículos,289,290,291 y 292.

Estas leyes apoyan las garantías constitucionales o legales en Panamá y penalizan o sancionan a aquellos que ejecuten actos delictivos por medios electrónicos o tecnológicos. Sin embargo, la sociedad no tiene cultura de denuncia cuando se es víctima de estos actos delictivos y las leyes actuales no persiguen estos delitos verdaderamente. [15]

# Revisión de la literatura

## Procesamiento del lenguaje natural

El procesamiento del lenguaje natural es un subconjunto de técnicas utilizadas para generar algoritmos de inteligencia artificial que se acerquen a las capacidades humanas de texto y voz. Existen una terminología para comprender los algoritmos, estos utilizan procesos matemáticos para codificar y decodificar las entradas, en el proceso se crean tokens, unidades lingüísticas del texto de entrada. Según [16], esta técnica de procesamiento puede aplicarse a análisis de sentimiento para comprender las respuestas de usuarios y orientados en la asistencia personal. Esta técnica de IA trabaja sobre redes neuronales.

## Asistentes digitales, inteligencia artificial y bigdata.

En los últimos años hemos visto como la disciplina de la IA aplicada ha incrementado sus casos de uso y beneficiado a múltiples sectores haciendo que se mejore la capacidad de análisis y procesamiento dando resultados simulados a capacidades humanas.[17] Este trabaja sobre macrodatos (BigData) y potencia de hardware permitiendo encontrar patrones en la entrada y estimar probabilísticamente un resultado.[18]

Los asistentes virtuales con IA es uno de estos casos de uso en donde se aplica tecnología de procesamiento de lenguaje natural; esta técnica permite que un equipo computacional pueda analizar e interpretar el idioma humano a través de algoritmos que permiten realizar procesos para comprender las estructuras textuales. Los asistentes digitales se han implementado en muchas industrias, empresas públicas y privadas establecer conversaciones con las personas. Estos asistentes a diferencia con los chatbots son capaces de comprender la entrada del usuario y responder bajo el contexto de la pregunta de forma natural. La inteligencia artificial ha empoderado a estos asistentes haciéndolos más robustos y fuertes para mantener la interacción. [19]

Los modelos transformadores generativos pre-entrenados(GPT) utilizan técnicas de aprendizaje profundo, procesamiento del lenguaje natural con redes neuronales para la creación de texto, imágenes, voz, análisis, clasificación y muchas aplicaciones más. Cuando son utilizados para la generación de texto estos se basan en conocimientos que adquieren durante el entrenamiento con grandes cantidades de datos lingüísticos. Durante el proceso de codificar las entradas de texto (encoder) en un vector, separan la oración en llamados tokens los cuales son palabras en entran a la red neuronal que tiene asignada los pesos, cada peso asignado son la cantidad de “perillas con las que juega la red neuronal para probabilísticamente en el procesamiento encontrar las palabras más adecuadas para cuando se inicia el proceso de decodificación(decoder) que es la que permite centrarse en partes de la entrada para dar los tokens mas probables. Estos modelos pueden utilizar mecanismos para recibir paralelamente oraciones y crear representaciones matemáticas complejas para que el decoder estime múltiples salidas.[20]

## Modelos y herramientas existentes para generar conversaciones fluidas

El creciente uso de los modelos de lenguaje natural ha mejorado y dado muchas aplicaciones prácticas de procesamiento del leguaje natural. Estos modelos requieren un corpus de texto de entrenamiento seguido de ajustes que permitan ajustar el modelo para responder y realizar tareas específicas, el modelo GPT-3 tiene 175 mil millones de parámetros y fue entrenado con un amplio contenido de texto web, esta puede accederse mediante la API para crear soluciones integradas en aplicaciones. [21]

## Estudios relacionados

La inteligencia artificial y sus subramas proponen aplicaciones que pueden ser orientarse a soluciones para generar más inclusión social y desarrollo cultura de un país. En el estudio de

Actualmente no hay estudios que basen modelos de asistentes orientados en la asistencia a la educación sobre ciberseguridad y conciencia digital. Los estudios relacionados se basan en modelos orientados a asistentes comerciales como el realizado por[22], que implemento un sistema web basado en plataforma DialogFLow que trabaja con el modelo BERT para interpretar el texto, consistió en un asistente web para apoyo a la atención al cliente a través de una interfaz web. El estudio muestra una arquitectura de cliente servidor que permite a través de una interfaz interactuar con el cliente final para responder preguntas relacionadas al comercio. El estudio muestra como el modelo de DialogFlow permite utilizar los algoritmos de NPL para responder a preguntas no establecidas previamente, al estar utilizando modelos NPL se puede interpretar la pregunta del usuario y que el modelo responda con base a el conjunto de datos con el que fue entrenado.

# Objetivos del proyecto:

## Objetivo general:

Evaluar el nivel de conciencia digital en Panamá mediante la propuesta de un prototipo de asistente digital basado en un modelo GPT, entrenado con datos sobre seguridad informática.

## Objetivos específicos:

1. Construir del conjunto de datos de entrenamiento relacionado a vulnerabilidades comunes, consejos de mitigación y de buenas prácticas de navegación y uso de medios digitales.
2. Ajustar un modelo GPT mediante la utilización del conjunto de datos para asistir con respuestas relevantes sobre seguridad informática, consejos de mitigación de vulnerabilidades, buenas prácticas de navegación.
3. Entrenar el modelo GPT, utilizando un conjunto de datos optimizados, relacionados a los riesgos de la navegación en Internet.

# Materiales, métodos y metodología

## Materiales y métodos para la recolección de datos y análisis de la población.

Se realizó un muestreo aleatorio simple, aplicándose en el distrito de David, Chiriquí. Para la selección de la muestra se consideró un subconjunto de la población finita de 96321 habitantes. Dato identificado en las estadísticas del INEC.[23]. Por lo tanto, tenemos una muestra con un margen de error del 10% como rango para reflejar la variación de los resultados de la población general, un nivel de confianza del 95% para reflejar las actitudes más precisamente. Al calcular el tamaño de la muestra se obtiene el tamaño de 96 participantes que serán seleccionados aleatoriamente. Las preguntas se orientaron conocer el nivel de conciencia digital y medios de acceso a la red.

Se busca evaluar el nivel de conocimiento sobre “el uso cotidiano de internet y seguridad en el ciberespacio” en una población aleatorio con que preguntas están ponderadas de manera que se pueda identificar las variaciones nivel de estas están relacionadas a el uso cotidiano de internet, dispositivos usados y sitios frecuentados lugares o medios de acceso, reconocimiento de la importancia, así como incidentes de seguridad en caso de haber tenido.

Los datos recopilados se analizarán con estadística descriptiva y permitirán validar o desechar la primera hipótesis. Para la escala de medición se aplican niveles de ponderación a cada pregunta relacionada a prácticas de seguridad online, en donde 1 es falta de conciencia y métodos de navegación segura, 2 uso medio de métodos seguros y conciencia media, 3 conocimiento de los riesgos y uso de mecanismos de seguridad.

## Metodología y materiales para el desarrollo y configuración del modelo GPT.

Luego de la aplicación de la encuesta se realiza la recopilación de un conjunto de datos sobre buenas prácticas de navegación, consejos clasificados y etiquetados por categoría de amenazas en la web que luego son procesados para crear subconjuntos de entrenamiento y validación.

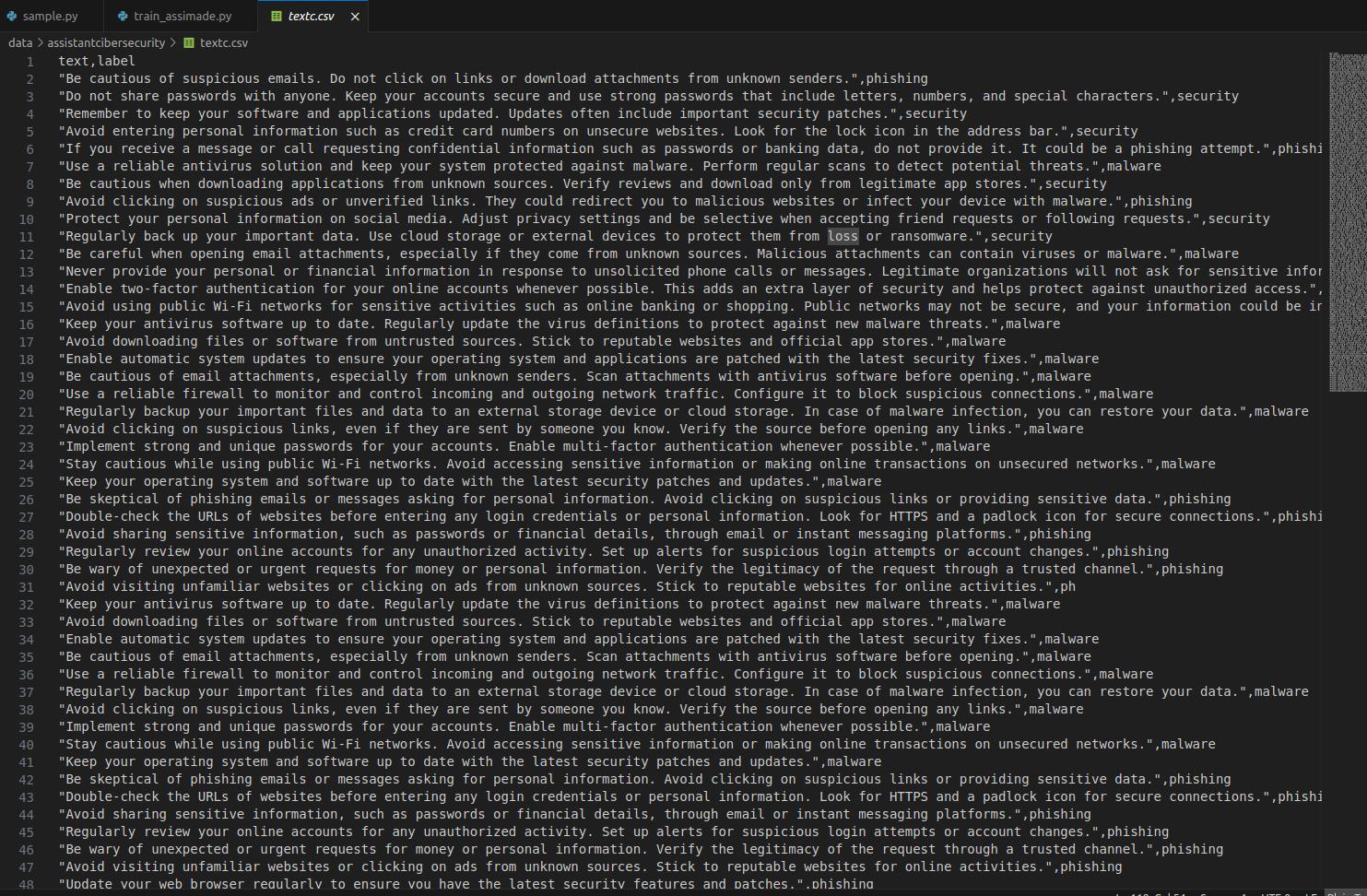
Para la construcción del modelo se utiliza el framework NanoGPT, esta es una solución a pequeña escala que permite reproducir modelos GPT simples y complejos entrenamientos con pocas líneas de código. [24]

Para ello se realizan las etapas siguientes:

* Creación del conjunto de datos etiquetados
* Carga y preparación del conjunto de datos nanoGPT
* Entrenamiento
* Pruebas del modelo

### Creación de conjunto de datos de entrenamiento y Adaptación de modelo nanoGPT

Para la propuesta del prototipo objeto de esta investigación se plantea la creación de un conjunto de datos a partir de textos clasificados por categoría de amenazas en internet y de medios digitales. Para ello se tiene una columna de texto plano en formato CSV con contenido sobre la recomendación y una etiqueta de clasificación de la recomendación. Esta columna es procesada por la librería pandas que permite cargar los datos en un dataframe o estructura de datos para el posterior procesamiento.[24]



Conjunto de datos

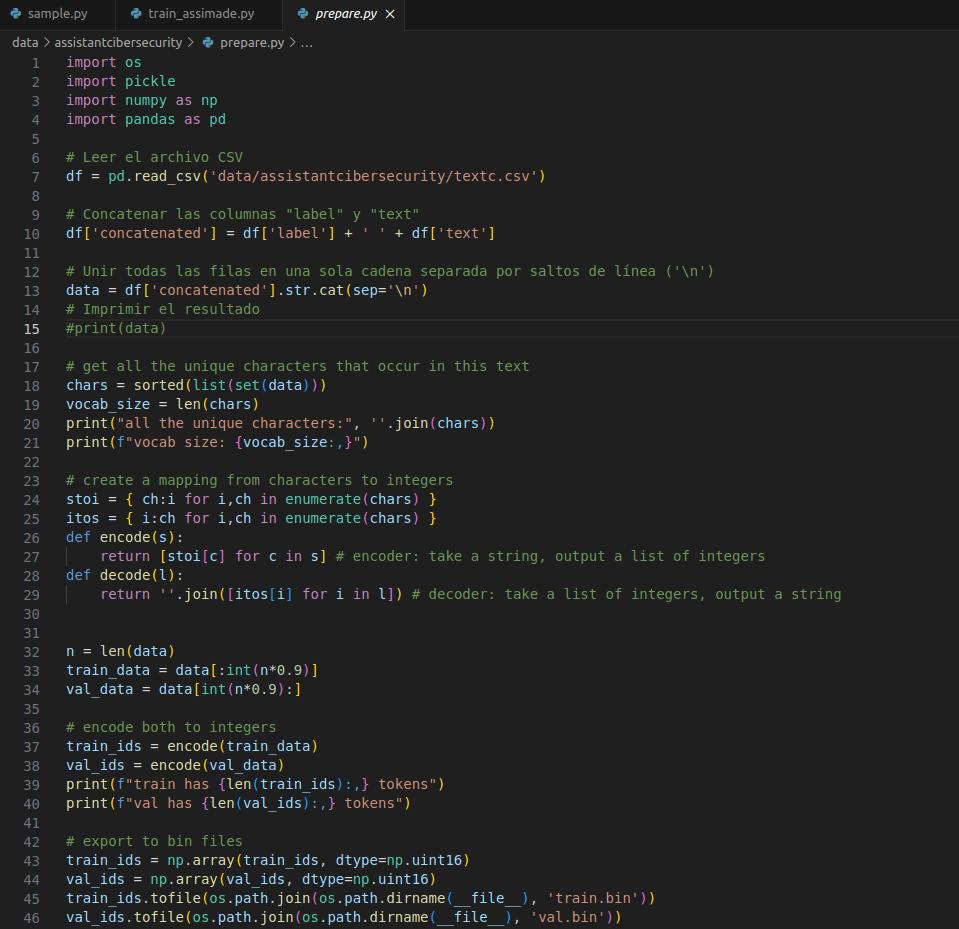


Figura n: Configuración para extraer el conjunto de datos en un dataframe y preparacion de los datos.

El cada registro del conjunto de datos posee una etiqueta que permite que el modelo pueda identificar la categoría de clasificación de datos de clasificados. Para ello se realiza una selectiva escogencia de datos verdaderos y consistentes.[25]

Este conjunto luego se carga para la tokenización, proceso que permite dividir las cadenas en piezas basadas en patrones específicos.[26] El entrenamiento con NanoGPT creamos las carpetas que albergan el dataset en formato CSV, luego se procesa para el entrenamiento. Este procesamiento crea ficheros de validación, entrenamiento y un metamodelo de apoyo .mkt realizando la ejecuciòn del comando python3 train.py config/train\_assistmade.py luego se realiza el entrenamietno con el comando python3 train.py config/train\_assimade.py. El resultado es un fichero .pt que contiene el modelo entrenado el cual se ejecuta posteriormente el cual es ejecutado con el comando con el comando python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start=”prompt” que se muestra en la figura (Configuraciones y parámetros de entrenamiento que crea los directorios de salida para el modelo entrenado).

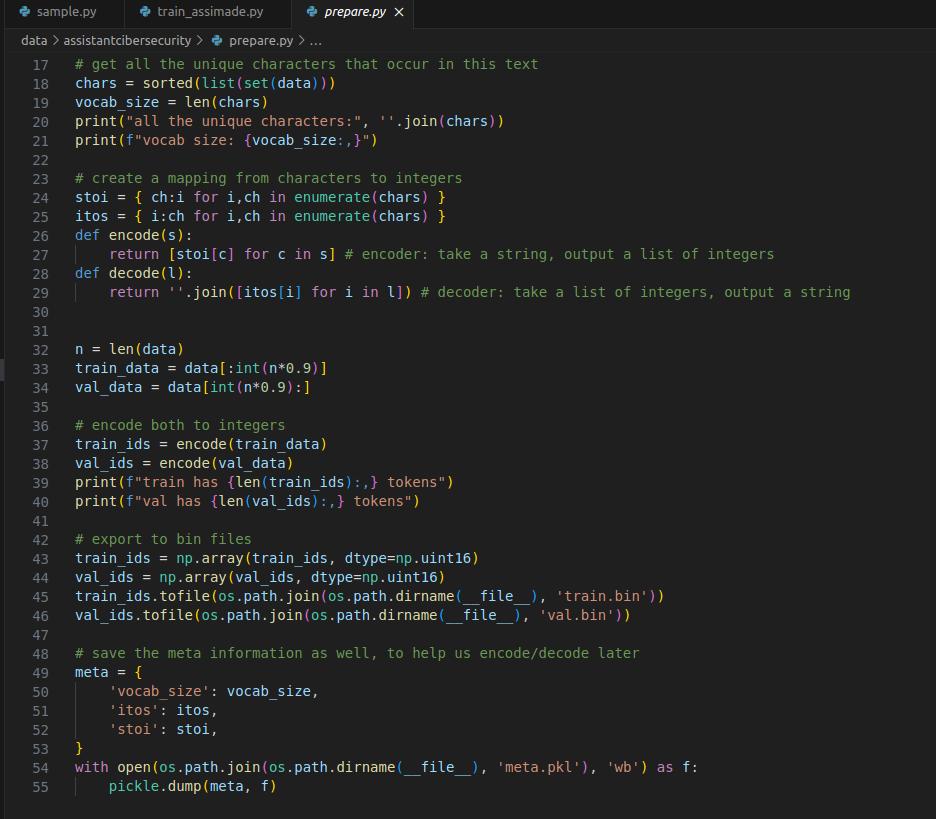


Figura n: Proceso de mapeo y tokenización para crear binarios de entrenamiento, validación y el metamodelo.

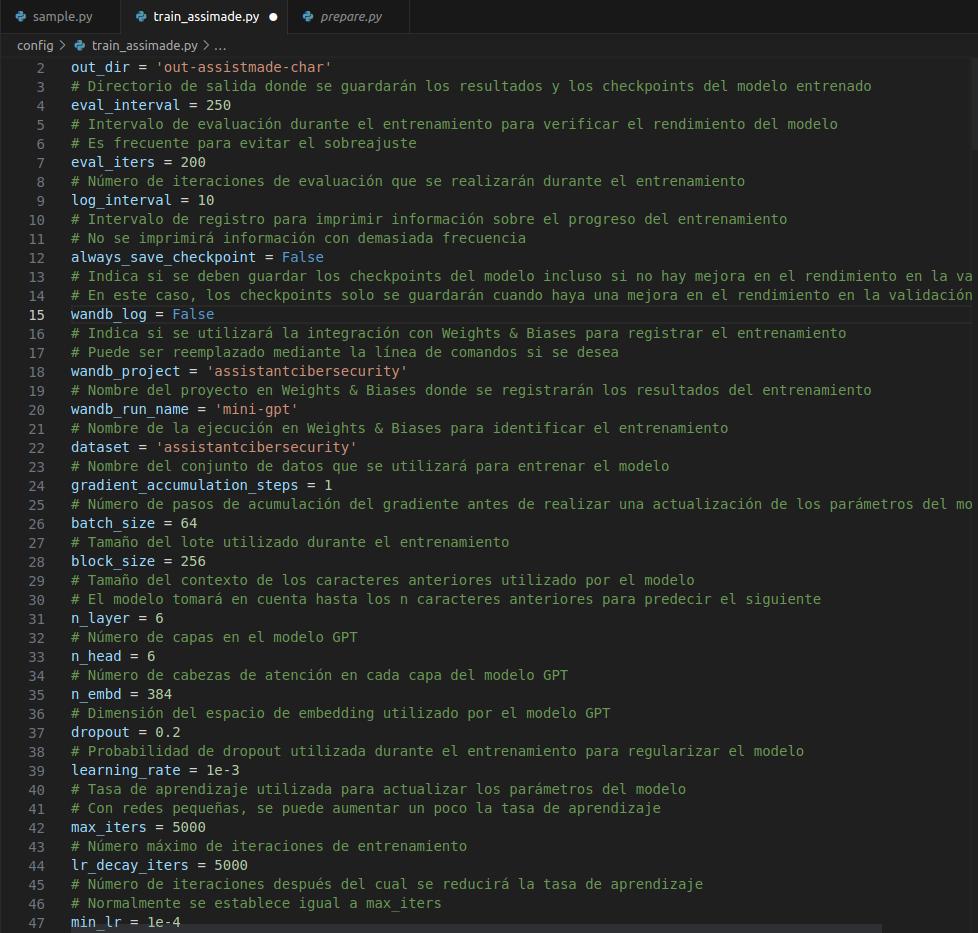


Figura n: Configuraciones y parámetros de entrenamiento que crea los directorios de salida para el modelo entrenado y posteriores usos.

## Configuración de los parámetros de entrenamiento del código y entrenamiento

Posteriormente se configuran los parámetros del código para entrenar con los datos un modelo sobre nanoGPT con ciclos de entrenamiento.

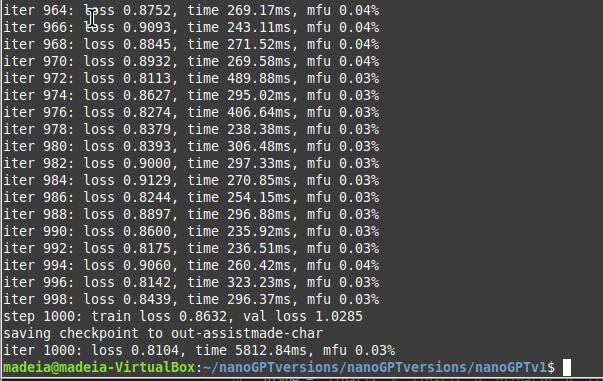
configuraciones actualizadas junto con los objetivos específicos para cada una y los puntos de comparación que puedes utilizar para crear una tabla en tu investigación:

**Configuración 1:**

python

* python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=50 --log\_interval=5 --block\_size=128 --batch\_size=64 --n\_layer=4 --n\_head=4 --n\_embd=128 --max\_iters=1000 --lr\_decay\_iters=1000 --dropout=0.2

python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=20 --log\_interval=1 --block\_size=64 --batch\_size=12 --n\_layer=8 --n\_head=8 --n\_embd=128 --max\_iters=1000 --lr\_decay\_iters=1000 --dropout=0.2



* Objetivo: Ejecutar el entrenamiento de manera más rápida al reducir el número máximo de iteraciones y ajustar otros parámetros.
* Explicación: Esta configuración aumenta el número de capas (n\_layer) y cabezas de atención (n\_head) a 4 para proporcionar una capacidad de representación más alta. El tamaño del lote (batch\_size) se incrementa a 64 para aprovechar mejor los recursos de la CPU. Se reduce el número máximo de iteraciones (max\_iters) a 1000 para acelerar el entrenamiento. El número de iteraciones para reducir la tasa de aprendizaje (lr\_decay\_iters) se establece en 1000. Se mantiene un tamaño de bloque (block\_size) de 128 y una dimensión del espacio de embedding (n\_embd) de 512 para mantener una representación adecuada del texto. La probabilidad de dropout (dropout) se establece en 0.2 para regularizar el modelo durante el entrenamiento

Pruebas del modelo:

Num\_samples = 1

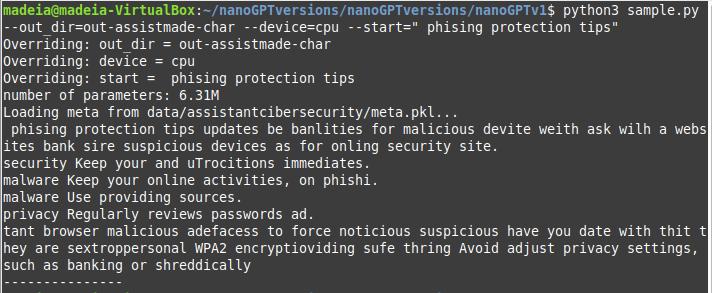
Temperatura = 1.2

Top\_k = 100

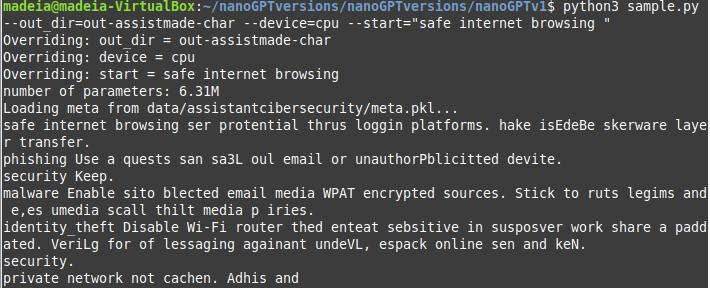
Max\_new\_tokens = 500

python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start=" phising protection tips"

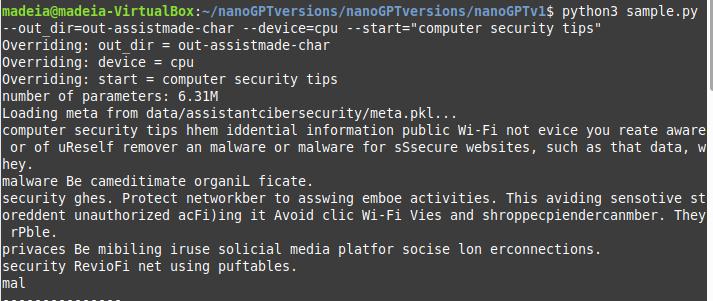
Resultados:



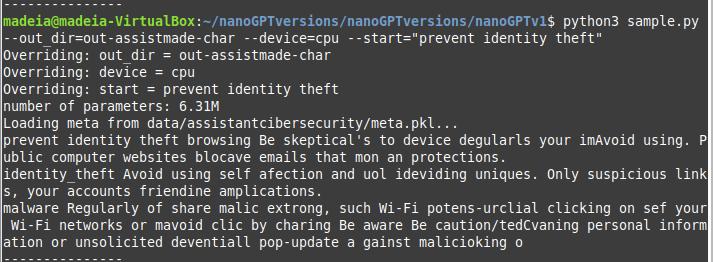
python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="safe internet browsing "



python3 sample.py –out-dir=out-assistmade-char --device=cpu --start="computer security tips"



python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="prevent identity theft"



**Configuración 2:**

python

python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=50 --log\_interval=5 --block\_size=128 --batch\_size=32 --n\_layer=4 --n\_head=4 --n\_embd=256 --max\_iters=3000 --lr\_decay\_iters=3000 --dropout=0.1

python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=50 --log\_interval=5 --block\_size=128 --batch\_size=32 --n\_layer=4 --n\_head=4 --n\_embd=256 --max\_iters=3000 --lr\_decay\_iters=3000 --dropout=0.1

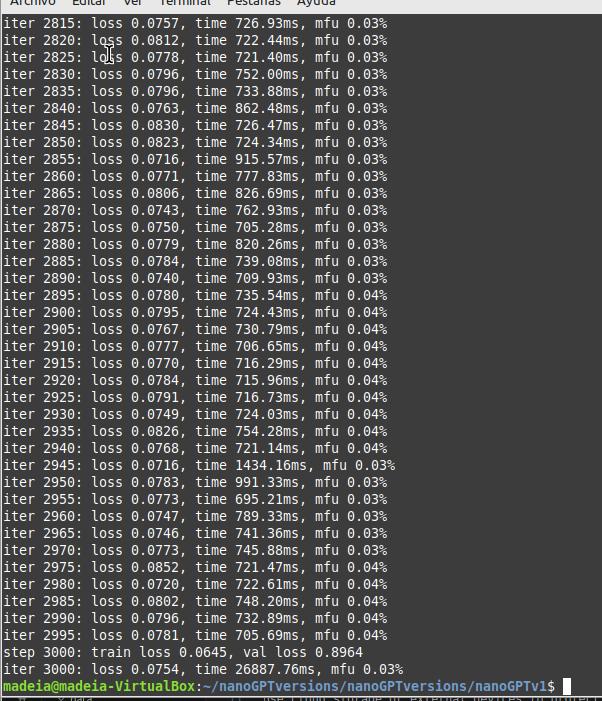
* Objetivo: Evaluar las respuestas del modelo entrenado con las configuraciones establecidas.
* Explicación: Esta configuración se centra en entrenar un modelo con la configuración de parámetros para tareas de clasificación en el conjunto de datos de seguridad que permitan acercar. Se utiliza un tamaño de bloque más pequeño (block\_size) para limitar el contexto de los caracteres anteriores. Se reduce el número de capas (n\_layer) y cabezas de atención (n\_head) para disminuir la complejidad del modelo. El tamaño del lote (batch\_size) también se reduce para adaptarse a recursos limitados.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente



Configuraciones de ejecucion del prompt:

# -----------------------------------------------------------------------------

start = "\n" # o "" u otros. También se puede especificar un archivo, por ejemplo: "FILE:prompt.txt"

# Texto de inicio para la generación de texto. Puede ser un string directo o especificar un archivo que contenga el texto de inicio.

num\_samples = 1 # número de muestras a generar

# Número de muestras de texto que se generarán

max\_new\_tokens = 500 # número de tokens generados en cada muestra

# Número máximo de tokens que se generarán en cada muestra de texto

temperature = 1.2 # 1.0 = sin cambios, < 1.0 = menos aleatorio, > 1.0 = más aleatorio en las predicciones

# Parámetro de temperatura que controla la aleatoriedad en la generación de texto.

# Un valor mayor hace que las predicciones sean más aleatorias, mientras que un valor menor hace que sean más deterministas.

top\_k = 100 # retiene solo los top\_k tokens más probables, los demás tienen una probabilidad de 0

# Número de tokens más probables que se mantendrán durante la generación de texto.

# Los tokens con probabilidad más baja se eliminarán de las opciones posibles.

seed = random.randint(1, 25348973256)

# Semilla utilizada para la generación de números aleatorios. Permite reproducir resultados.

# -----------------------------------------------------------------------------

Pruebas del modelo:

Prueba 1:

Tok\_k = 1

Temperatura = 10

Ma\_new\_tokens = 500:

Texto

Descripción generada automáticamente

Prueba 2:

Temperatura = 0.8

Top\_k = 10

Max\_new\_tokens = 500

python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="safe internet browsing"

Texto

Descripción generada automáticamente

Prueba n

Num\_samples = 1

Temperatura = 1.2

Top\_k = 100

Max\_new\_tokens = 500

Prompt = python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start=" phising protection tips"

Prompt = python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="safe internet browsing "

Prompt = python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="computer security tips"

Prompt = python3 sample.py --out\_dir=out-assistmade-char --device=cpu --start="prevent identity theft"

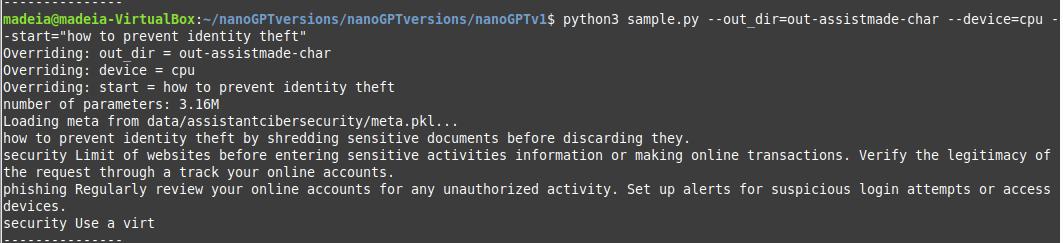
Texto

Descripción generada automáticamente

U,{98861f5e-5066-4a1f-923c-aa79937dc81c}{64},3.125,3.125

Texto

Descripción generada automáticamente



Prueba n :

num\_samples = 1

max\_new\_tokens = 500

temperature = 1.1

Texto

Descripción generada automáticamente

Comparaciones

* Puntos de comparación para la tabla:
* Rendimiento del modelo en el conjunto de datos de seguridad, medido en métricas como precisión, recall y F1-score.
* Eficiencia computacional, que puede evaluarse en términos de tiempo de entrenamiento y uso de recursos (CPU, memoria).
* Capacidad de generalización del modelo, evaluada mediante la precisión en un conjunto de datos de prueba o validación independiente.
* Estabilidad del modelo, verificando si hay fluctuaciones significativas en el rendimiento en diferentes ejecuciones.
* Tamaño y complejidad del modelo, expresados en términos de número de parámetros y requisitos de almacenamiento.

Resultados

Creación de conjunto de entrenamiento

Configuración del modelo nanoGPT.

Aplicación de entrenamiento al modelo

Entrenamiento

Prototipado final para usuario

Validación del prototipo

Interfaz de usuario

Usabilidad y respuestas acertadas

# Resultados y discusión

## Resultados

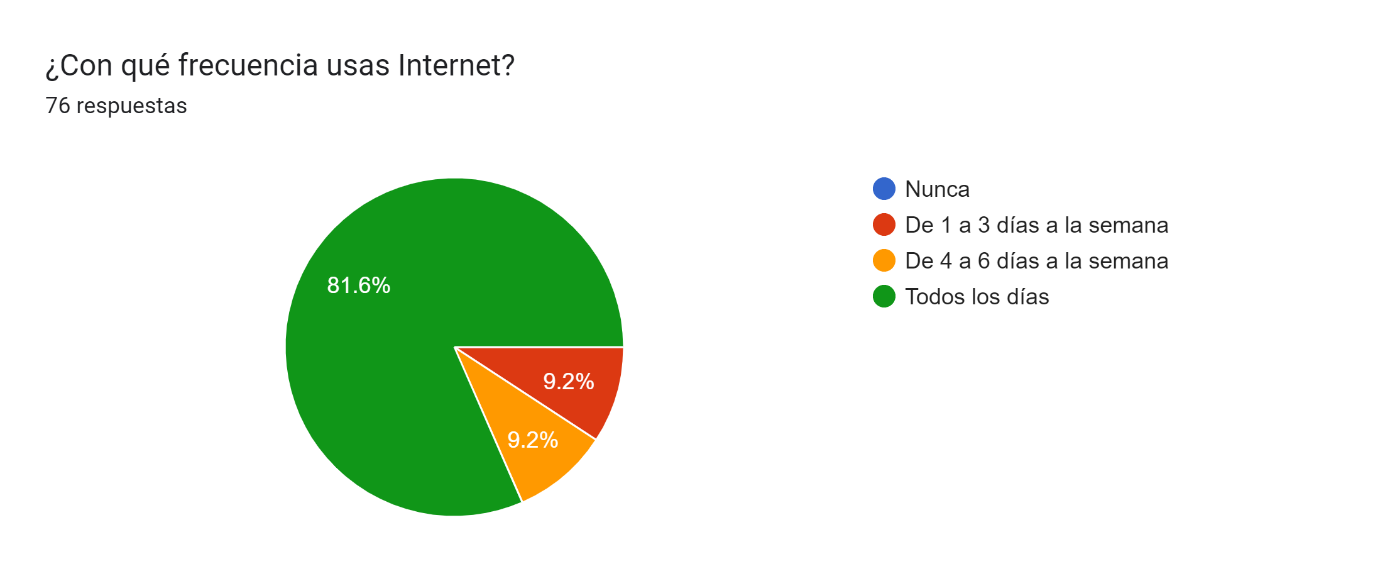
Limitantes

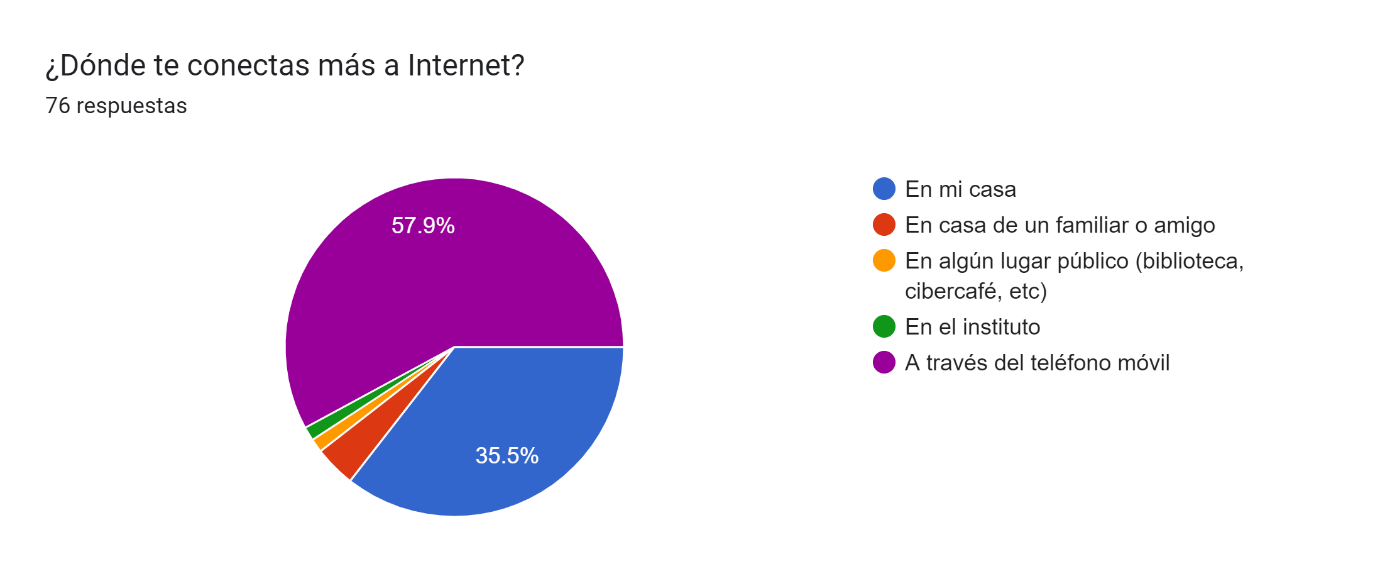
## Discusión

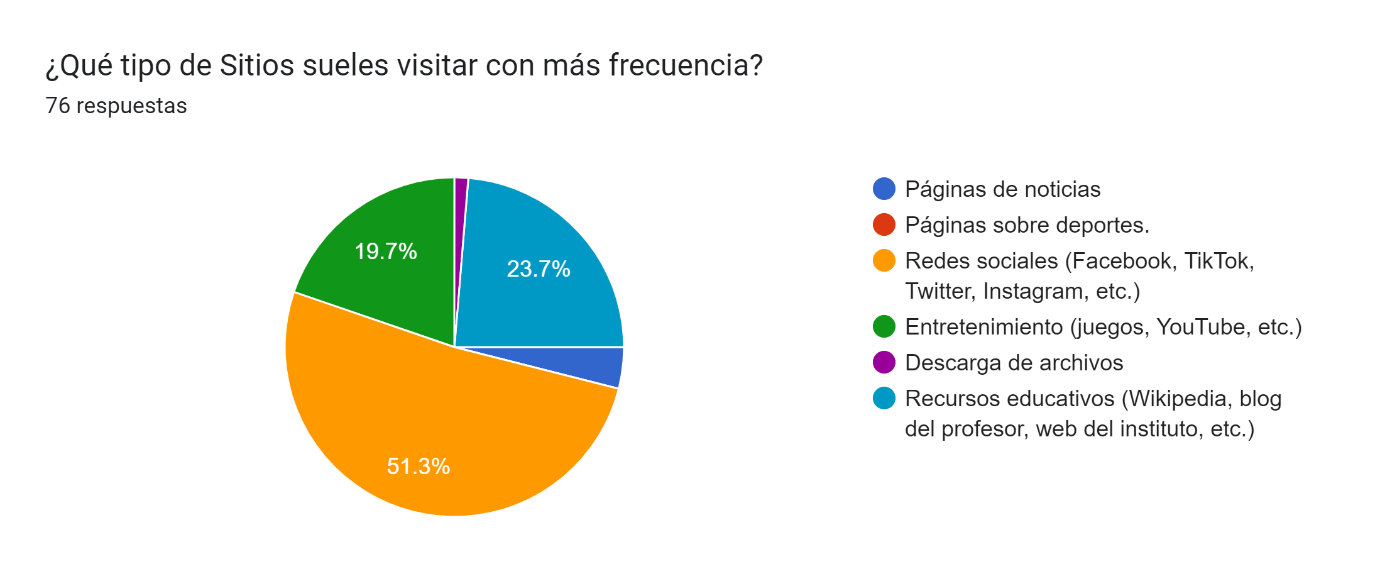
Graficas de entrenamiento

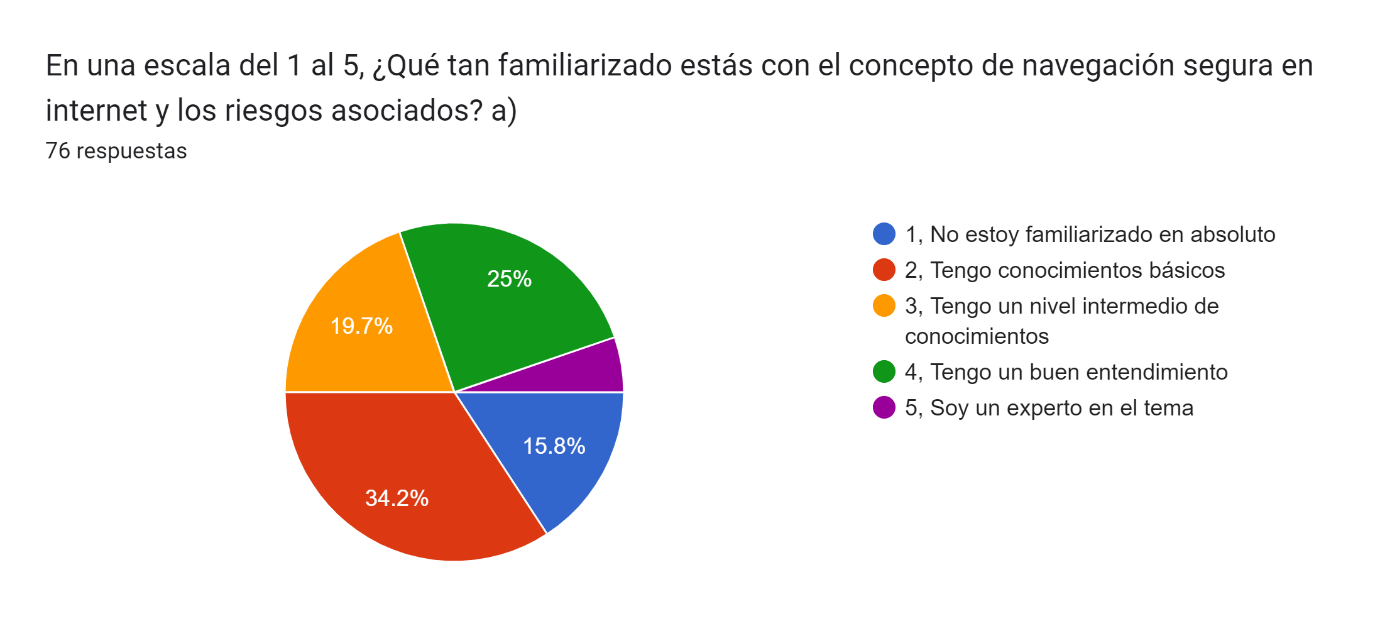
Gráfico de las respuestas de Formularios. Título de la pregunta: Ingrese su Edad
. Número de respuestas: 76 respuestas.

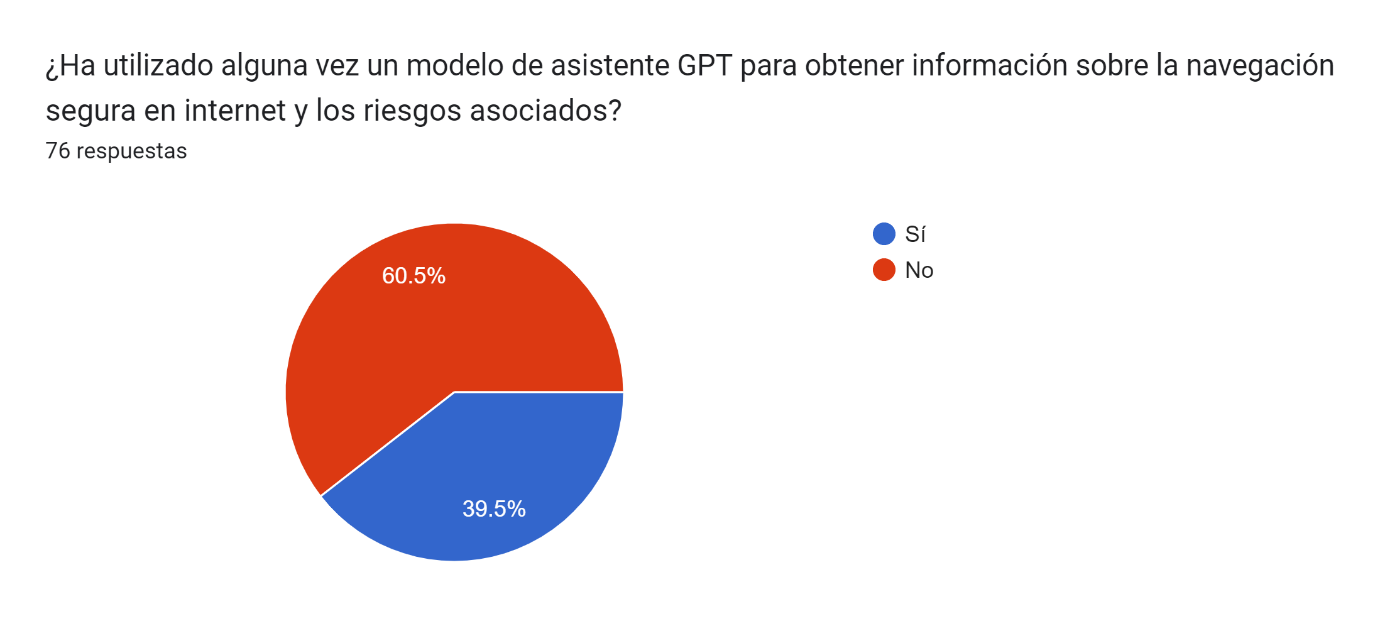
Gráfico de las respuestas de Formularios. Título de la pregunta: Nivel de escolaridad
. Número de respuestas: 76 respuestas.

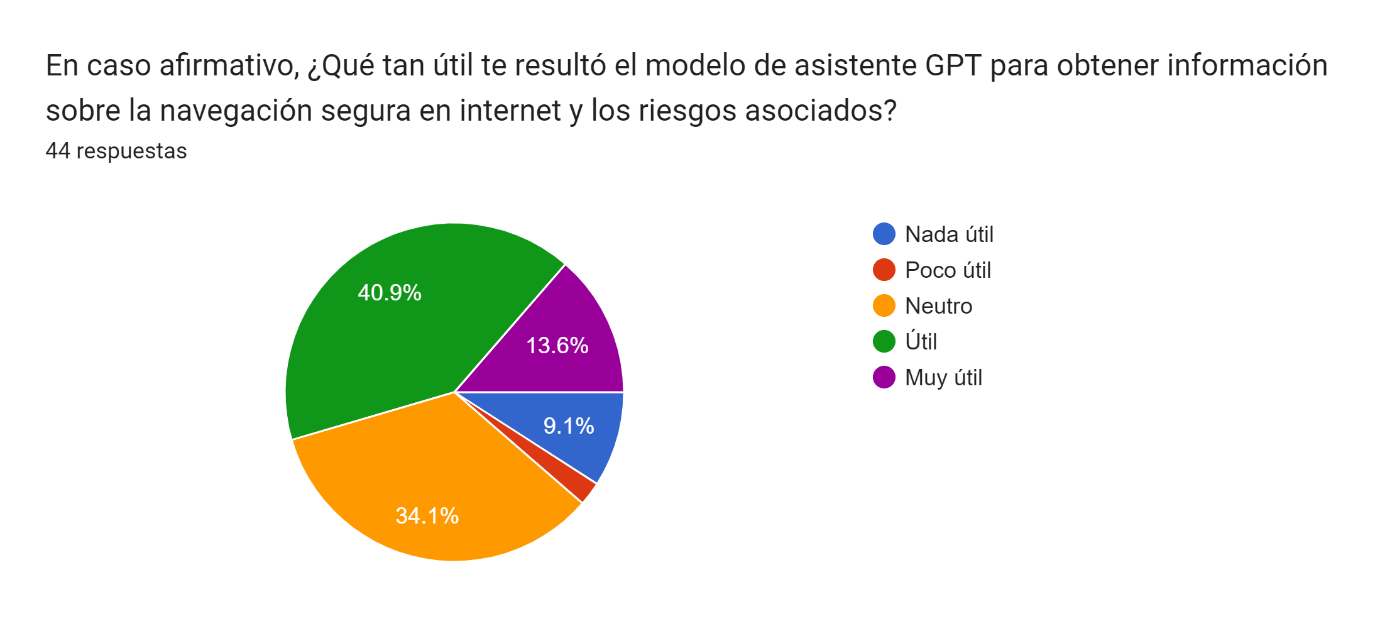


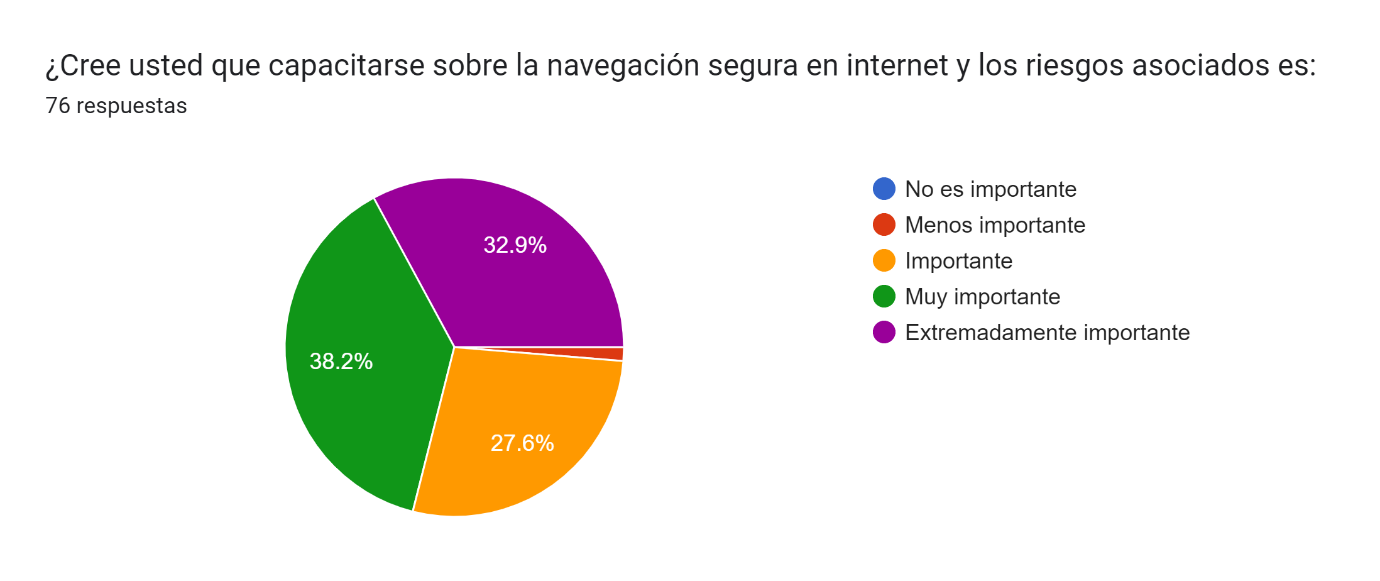


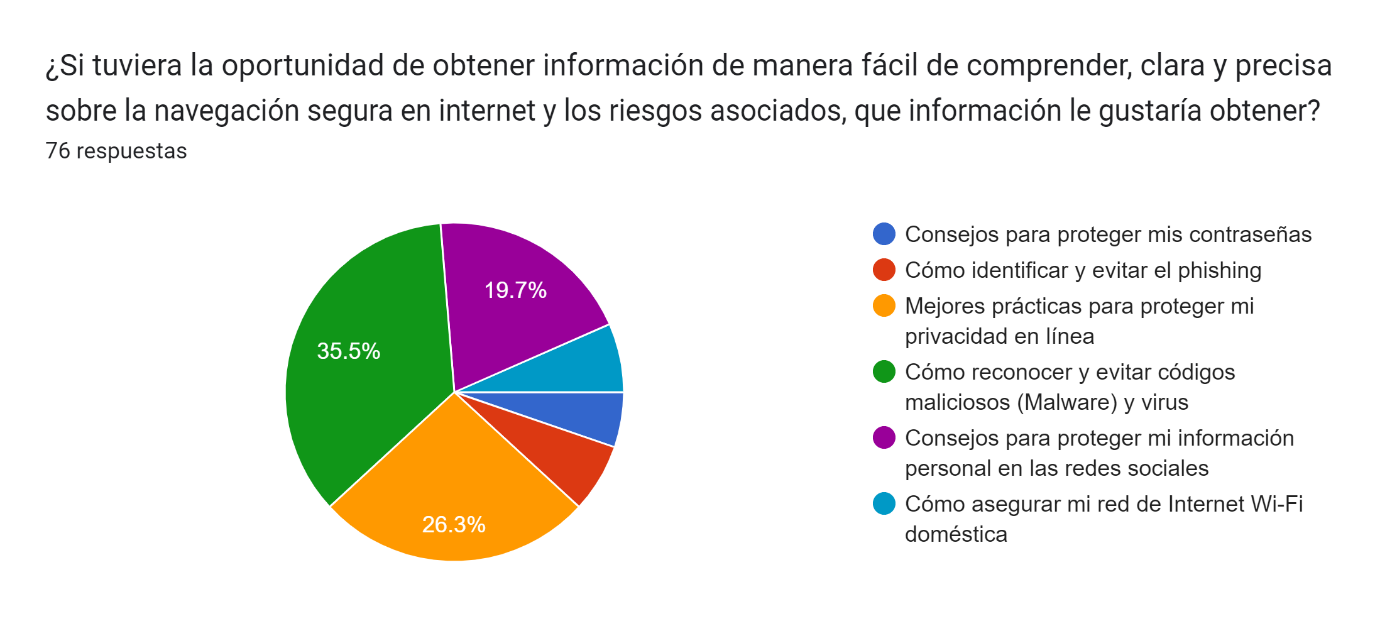






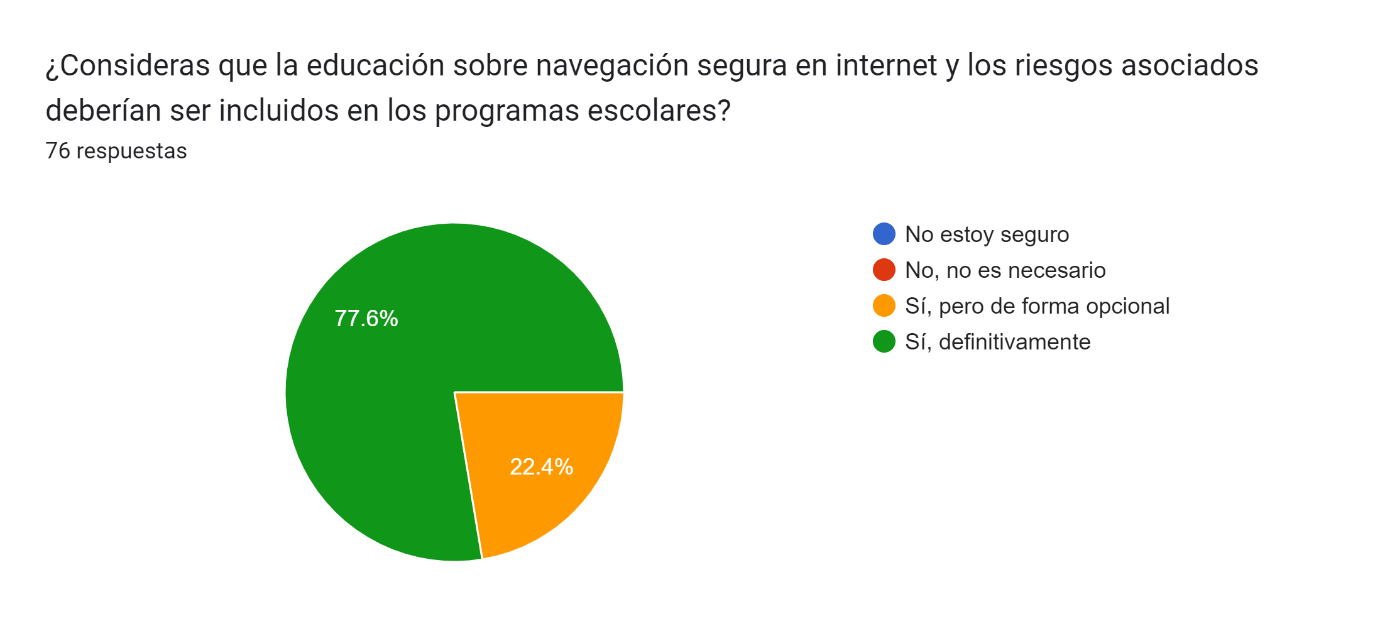


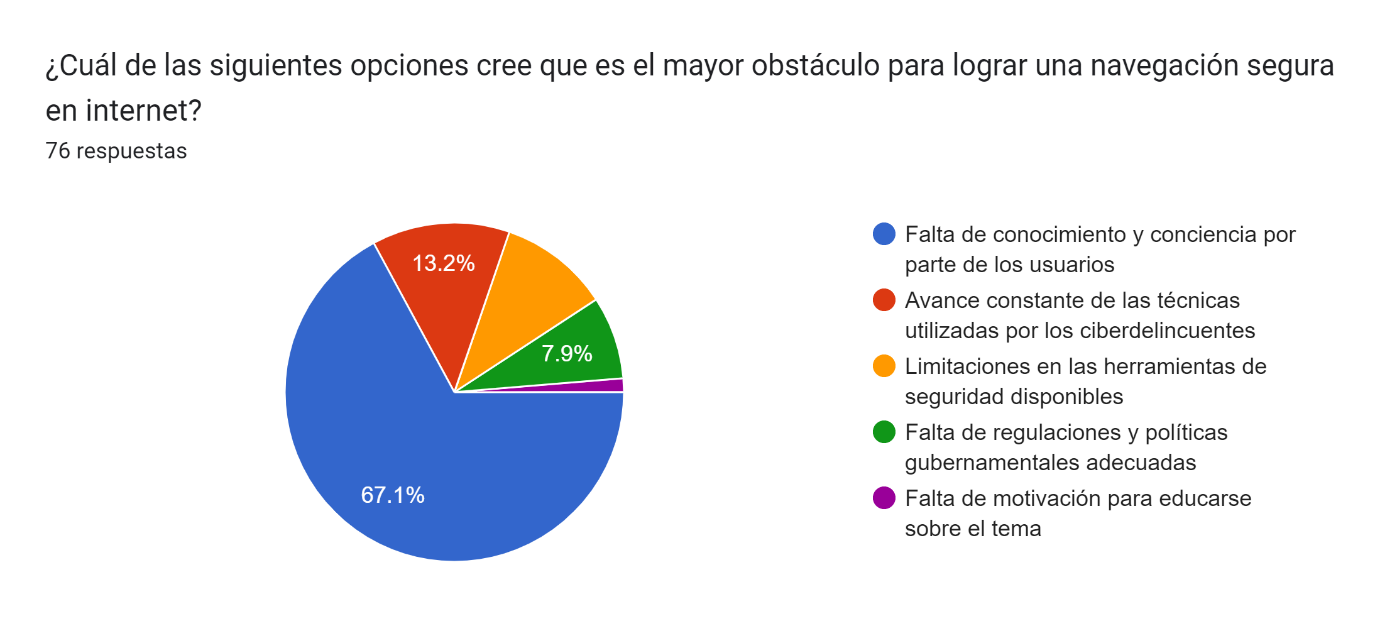


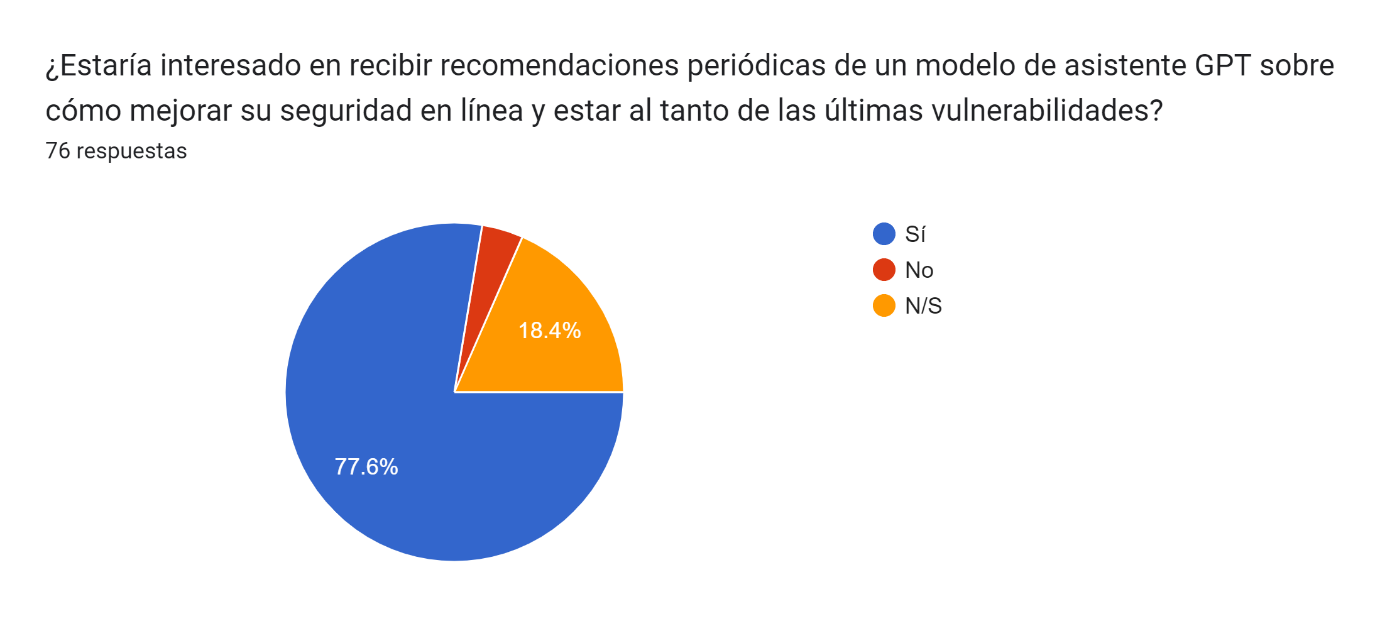


Gráfico, Gráfico circular

Descripción generada automáticamente







# Oportunidades de desarrollo del prototipo

# Conclusión

# Referencias

[1] R. A and S. H, “The Importance of Cybersecurity Education in School,” Mar. 2020.

[2] J. D. Nadeesha and D. M. T. Madusanka, “Awareness of Internet Browsing Security among Undergraduates inRajarata University of Sri Lanka,” Jun. 2021, Accessed: Jun. 19, 2023. [Online]. Available: http://repository.rjt.ac.lk/handle/123456789/3188

[3] M. Eslavova, “De la ciudadanía tradicional a la ciudadanía digital | EPALE,” Apr. 23, 2019. https://epale.ec.europa.eu/bg/blog/ot-tradicionno-grazhdanstvo-km-digitalno-grazhdanstvo (accessed Jun. 11, 2023).

[4] H. H. Konkolewsky, “Digital economy and the future of social security,” *Administration*, vol. 65, no. 4, pp. 21–30, Dec. 2017, doi: 10.1515/ADMIN-2017-0031.

[5] E. G. Popkova and K. Gulzat, “Contradiction of the Digital Economy: Public Well-Being vs. Cyber Threats,” *Lecture Notes in Networks and Systems*, vol. 87, pp. 112–124, 2020, doi: 10.1007/978-3-030-29586-8\_13/COVER.

[6] D. Lyon, “Digital Citizenship and Surveillance| Surveillance Culture:  Engagement, Exposure, and Ethics in Digital Modernity,” *Int J Commun*, vol. 11, no. 0, p. 19, Feb. 2017, Accessed: Jun. 19, 2023. [Online]. Available: https://ijoc.org/index.php/ijoc/article/view/5527

[7] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/J.EGYR.2021.08.126.

[8] R. D. Gordon Graell, “Informática educativa, base para el desarrollo de una ciudadanía digital en Panamá,” *REVISTA ANUAL ACCIÓN Y REFLEXIÓN EDUCATIVA, N.o 47*, pp. 238–261, Jan. 2022.

[9] Z. Ahmad Zukarnain *et al.*, “IMPACT OF TRAINING ON CYBERSECURITY AWARENESS,” *GADING Journal of Science and Technology*, vol. 3, no. 1, 2020, Accessed: Jun. 19, 2023. [Online]. Available: https://www.cybereducationscheme.org/certified-programmes,

[10] R. Banham, “Smaller organizations are targets for hacking and phishing attacks to get information that can harm them or bigger companies they do business with. Cybersecurity threats proliferating for midsize and smaller businesses AccountantsWorld • CPA Charge • OfficeTools Drake Software • Cornell College of Business”.

[11] “Train employees - your best defense - for security awareness,” 2009, Accessed: Jun. 19, 2023. [Online]. Available: http://www

[12] J. P. Francis, “El papel de la ciberseguridad generacional en el ecosistema digital,” Apr. 25, 2022. https://www.laestrella.com.pa/cafe-estrella/tecnologia/220425/papel-ciberseguridad-generacional-ecosistema-digital (accessed Jun. 19, 2023).

[13] R. Urribarri, “Panamá: cobertura informativa de la brecha digital durante la pandemia por covid-19,” *Anu Estud Centroam*, vol. 48, pp. 1–16, Jul. 2022, doi: 10.15517/AECA.V48I0.52862.

[14] “Autoridad Nacional para la Innovación Gubernamental,” Sep. 2022, 2022. https://aig.gob.pa/analizan-el-tren-de-defensa-ante-las-amenazas-de-la-era-digital/#:~:text=En%20el%202021%20se%20registraron,seguridad%20que%20tienen%20las%20empresas. (accessed Jun. 19, 2023).

[15] L. Ávila, “Ciberdelitos no son bien perseguidos en Panamá,” Feb. 13, 2022. https://www.panamaamerica.com.pa/judicial/ciberdelitos-no-son-bien-perseguidos-en-panama-1202128 (accessed Jun. 19, 2023).

[16] M. Agarwal and A. Saxena, “An Overview of Natural Language Processing,” vol. 7, 2019, doi: 10.22214/ijraset.2019.5462.

[17] Y. Lu, “Artificial intelligence: a survey on evolution, models, applications and future trends,” *https://doi.org/10.1080/23270012.2019.1570365*, vol. 6, no. 1, pp. 1–29, Jan. 2019, doi: 10.1080/23270012.2019.1570365.

[18] A. M. Rahmani *et al.*, “Artificial intelligence approaches and mechanisms for big data analytics: a systematic study,” *PeerJ Comput Sci*, vol. 7, pp. 1–28, Apr. 2021, doi: 10.7717/PEERJ-CS.488.

[19] M. M. Mariani, N. Hashemi, and J. Wirtz, “Artificial intelligence empowered conversational agents: A systematic literature review and research agenda,” *J Bus Res*, vol. 161, p. 113838, Jun. 2023, doi: 10.1016/J.JBUSRES.2023.113838.

[20] AWS, “Explicación de los transformadores generativos preentrenados - AWS.” https://aws.amazon.com/es/what-is/gpt/ (accessed Jul. 15, 2023).

[21] T. B. Brown *et al.*, “Language Models are Few-Shot Learners,” *Adv Neural Inf Process Syst*, vol. 2020-December, May 2020, Accessed: Jun. 11, 2023. [Online]. Available: https://arxiv.org/abs/2005.14165v4

[22] E. Varela Tapia, Lady Sangacha-Tapia, I. Acosta, and R. Celi, “Inteligencia Artificial Conversacional para el Diseño de un Asistente Virtual Interactivo,” Jun. 2022, pp. 237–241. doi: 10.54808/CICIC2022.01.237.

[23] INEC, “ESTIMACIÓN Y PROYECCIÓN DE LA POBLACIÓN DEL DISTRITO DE DAVID, POR CORREGIMIENTO, SEGÚN SEXO Y EDAD: AÑOS 2010-20.”

[24] F. Reiss, B. Cutler, and Z. Eichenberger, “Natural Language Processing with Pandas DataFrames,” *PROC. OF THE 20th PYTHON IN SCIENCE CONF*, p. 49, 2021.

[25] U. Gençer Gediz, “How to generate an NLP dataset from any internet source? - Kimola Cognitive,” Mar. 28, 2020. https://kimola.com/cognitive/resources/how-to-generate-an-nlp-dataset-from-any-internet-source (accessed Jun. 19, 2023).

[26] R. Koenig, “NLP for Beginners: Cleaning & Preprocessing Text Data,” 06, 2019. https://towardsdatascience.com/nlp-for-beginners-cleaning-preprocessing-text-data-ae8e306bef0f (accessed Jun. 19, 2023).

@web\_page{Koenig2019,

   author = {Rachel Koenig},

   month = {29},

   title = {NLP for Beginners: Cleaning & Preprocessing Text Data},

   url = {https://towardsdatascience.com/nlp-for-beginners-cleaning-preprocessing-text-data-ae8e306bef0f},

   year = {2019},

}

@article{Reiss2021,

   abstract = {Most areas of Python data science have standardized on using Pandas DataFrames for representing and manipulating structured data in memory. Natural Language Processing (NLP), not so much. We believe that Pandas has the potential to serve as a universal data structure for NLP data. DataFrames could make every phase of NLP easier, from creating new models, to evaluating their effectiveness, to building applications that integrate those models. However, Pandas currently lacks important data types and operations for representing and manipulating crucial types of data in many of these NLP tasks. This paper describes Text Extensions for Pandas, a library of extensions to Pandas that make it possible to build end-to-end NLP applications while representing all of the applications' internal data with DataFrames. We leverage the extension points built into Pandas library to add new data types, and we provide important NLP-specfific operations over these data types and and integrations with popular NLP libraries and data formats.},

   author = {Frederick Reiss and Bryan Cutler and Zachary Eichenberger},

   journal = {PROC. OF THE 20th PYTHON IN SCIENCE CONF},

   keywords = {DataFrames Background and Motivation,Index Terms-natural language processing,Pandas},

   pages = {49},

   title = {Natural Language Processing with Pandas DataFrames},

   year = {2021},

}

@web\_page{,

   author = {Utku Gençer Gediz},

   month = {3},

   title = {How to generate an NLP dataset from any internet source? - Kimola Cognitive},

   url = {https://kimola.com/cognitive/resources/how-to-generate-an-nlp-dataset-from-any-internet-source},

   year = {2020},

}

@article{Agarwal2019,

   abstract = {Natural Language Processing is branch of machine learning that deals with text and speech. Natural Language Processing is a way for computers to analyze, understand, and derive meaning from human language in a smart and useful way. By utilizing Natural Language Processing, developers can organize and structure knowledge to perform tasks such as automatic summarization, translation, named entity recognition, relationship extraction, sentiment analysis, speech recognition, and topic segmentation.},

   author = {Mansi Agarwal and Abhishek Saxena},

   doi = {10.22214/ijraset.2019.5462},

   issn = {2321-9653},

   keywords = {Chatbots,Keyword: Natural Language Processing,ML,Personal Assistant,Speech Recognition,Text-To-Speech (TTS)},

   title = {An Overview of Natural Language Processing},

   volume = {7},

   url = {www.ijraset.com},

   year = {2019},

}

@article{Rahmani2021,

   abstract = {Recent advances in sensor networks and the Internet of Things (IoT) technologies have led to the gathering of an enormous scale of data. The exploration of such huge quantities of data needs more efficient methods with high analysis accuracy. Artificial Intelligence (AI) techniques such as machine learning and evolutionary algorithms able to provide more precise, faster, and scalable outcomes in big data analytics. Despite this interest, as far as we are aware there is not any complete survey of various artificial intelligence techniques for big data analytics. The present survey aims to study the research done on big data analytics using artificial intelligence techniques. The authors select related research papers using the Systematic Literature Review (SLR) method. Four groups are considered to investigate these mechanisms which are machine learning, knowledge-based and reasoning methods, decision-making algorithms, and search methods and optimization theory. A number of articles are investigated within each category. Furthermore, this survey denotes the strengths and weaknesses of the selected AI-driven big data analytics techniques and discusses the related parameters, comparing them in terms of scalability, efficiency, precision, and privacy. Furthermore, a number of important areas are provided to enhance the big data analytics mechanisms in the future.},

   author = {Amir Masoud Rahmani and Elham Azhir and Saqib Ali and Mokhtar Mohammadi and Omed Hassan Ahmed and Marwan Yassin Ghafour and Sarkar Hasan Ahmed and Mehdi Hosseinzadeh},

   doi = {10.7717/PEERJ-CS.488},

   issn = {23765992},

   journal = {PeerJ Computer Science},

   keywords = {Artificial intelligence,Big data,Machine learning,Methods,Systematic literature review},

   month = {4},

   pages = {1-28},

   pmid = {33954253},

   publisher = {PeerJ, Inc},

   title = {Artificial intelligence approaches and mechanisms for big data analytics: a systematic study},

   volume = {7},

   url = {/pmc/articles/PMC8053021/ /pmc/articles/PMC8053021/?report=abstract https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8053021/},

   year = {2021},

}

@article{Lu2019,

   abstract = {Artificial intelligence (AI) is one of the core drivers of industrial development and a critical factor in promoting the integration of emerging technologies, such as graphic processing unit, Inter...},

   author = {Yang Lu},

   doi = {10.1080/23270012.2019.1570365},

   issn = {23270039},

   issue = {1},

   journal = {https://doi.org/10.1080/23270012.2019.1570365},

   keywords = {Industry 4.0,Internet of Things,artificial intelligence,big data,deep learning,graphic processing unit},

   month = {1},

   pages = {1-29},

   publisher = {Taylor & Francis},

   title = {Artificial intelligence: a survey on evolution, models, applications and future trends},

   volume = {6},

   url = {https://www.tandfonline.com/doi/abs/10.1080/23270012.2019.1570365},

   year = {2019},

}

@article{Li2021,

   abstract = {At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace. Recently, many private companies and government organizations around the world are facing the problem of cyber-attacks and the danger of wireless communication technologies. Today's world is highly dependent on electronic technology, and protecting this data from cyber-attacks is a challenging issue. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. To this end, various organizations use various solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data. So far, various methods had been proposed by researchers around the world to prevent cyber-attacks or reduce the damage caused by them. Some of the methods are in the operational phase and others are in the study phase. The aim of this study is to survey and comprehensively review the standard advances presented in the field of cyber security and to investigate the challenges, weaknesses and strengths of the proposed methods. Different types of new descendant attacks are considered in details. Standard security frameworks are discussed with the history and early-generation cyber-security methods. In addition, emerging trends and recent developments of cyber security and security threats and challenges are presented. It is expected that the comprehensive review study presented for IT and cyber security researchers will be useful.},

   author = {Yuchong Li and Qinghui Liu},

   doi = {10.1016/J.EGYR.2021.08.126},

   issn = {2352-4847},

   journal = {Energy Reports},

   keywords = {Cyber security,Cyber-attacks,Emerging trends,Information technology,Key management},

   month = {11},

   pages = {8176-8186},

   publisher = {Elsevier},

   title = {A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments},

   volume = {7},

   year = {2021},

}

@article{Konkolewsky2017,

   author = {Hans Horst Konkolewsky},

   doi = {10.1515/ADMIN-2017-0031},

   issn = {00018325},

   issue = {4},

   journal = {Administration},

   month = {12},

   pages = {21-30},

   publisher = {De Gruyter Open Ltd},

   title = {Digital economy and the future of social security},

   volume = {65},

   year = {2017},

}

@article{Popkova2020,

   abstract = {Purpose: The purpose of the paper is to substantiate the logical interconnection of social consequences of the digital economy and its consequences for cyber security and to develop – based on this interconnection - the scientific and methodological provision of systemic monitoring of the digital economy and the model of managing the digital economy for maximizing public well-being and overcoming the cyber threats. Design/Methodology/Approach: For determining the interdependence (cross-correlation) between human development index (indicator of public well-being) and cyber security index (indicator of cyber threats), the authors use the method of correlation analysis; for determining their dependence on the index of digital competitiveness (indicator of the digital economy) the authors use the method of regression analysis. As a result, the authors determine low information content of the statistical indicators that reflect the integral characteristics of public well-being and cyber security and come to the conclusion on inapplicability of the standard (e.g., econometric) methods in the work. That’s why the method of logical analysis is used for analyzing the qualitative essence of social consequences of cyber threats of the digital economy. Findings: It is proved that social consequences of the digital economy and its consequences for the cyber security are interconnected and could and should be studied and managed as a whole. It is substantiates that when treating the cyber threats it is necessary to focus not on their technical components (causes of threats that are determined by the specifics of digital technologies) but on social components – i.e., objects of threats – various categories of the population. In this case, the influence on public well-being becomes a common basis of the studied consequences. Originality/Value: Based on the determined interconnection, the authors develop the scientific and methodological provision of systemic monitoring of effectiveness of the digital economy, which envisages comparison of its social advantages and allows determining the top-priority objects of the digital economy management. Approbation of the offered methodological provision by the example of the digital economy of Russia in 2018 showed its low effectiveness. In order to increase it, it is recommended to use the developed model of managing the digital economy for maximizing public well-being and overcoming the cyber threats.},

   author = {Elena G. Popkova and Kantoro Gulzat},

   doi = {10.1007/978-3-030-29586-8\_13/COVER},

   issn = {23673389},

   journal = {Lecture Notes in Networks and Systems},

   keywords = {Cyber threats,Digital economy,Effectiveness,Management,Modern Russia,Public well-being},

   pages = {112-124},

   publisher = {Springer},

   title = {Contradiction of the Digital Economy: Public Well-Being vs. Cyber Threats},

   volume = {87},

   url = {https://link.springer.com/chapter/10.1007/978-3-030-29586-8\_13},

   year = {2020},

}

@article{Urribarri2022,

   abstract = {This article reports on documentary research aimed at analyzing the coverage made by the Panamanian media about the digital divide during the first six months of the pandemic. Using Google's advanced search, a corpus of 140 pieces of information was extracted and analyzed using the criteria of newsworthiness and information sources. The results show an episodic and shallow coverage of a complex phenomenon that generated a wide social discontent in a society with high levels of inequality. Recommendations are offered that could contribute to a dissemination aimed at the understanding of this phenomenon as a by-product of social inequality, but also as a deepener of it.},

   author = {Raisa Urribarri},

   doi = {10.15517/AECA.V48I0.52862},

   issn = {2215-4175},

   journal = {Anuario de Estudios Centroamericanos},

   keywords = {19,Panamá,medios de comunicación,pandemia covid},

   month = {7},

   pages = {1-16},

   title = {Panamá: cobertura informativa de la brecha digital durante la pandemia por covid-19},

   volume = {48},

   url = {https://revistas.ucr.ac.cr/index.php/anuario/article/view/52862},

   year = {2022},

}

@web\_page{,

   author = {INEC},

   title = {ESTIMACIÓN Y PROYECCIÓN DE LA POBLACIÓN DEL DISTRITO DE DAVID, POR CORREGIMIENTO, SEGÚN SEXO Y EDAD: AÑOS 2010-20},

}

@article{Mariani2023,

   abstract = {Consumer research on conversational agents (CAs) has been growing. To illustrate and map out research in this field, we conducted a systematic literature review (SLR) of published work indexed in the Clarivate Web of Science and Elsevier Scopus databases. Four dominant topical areas were identified through bibliographic coupling. They are 1) consumers’ trust in CAs; 2) Natural Language Processing (NLP) in developing and designing CAs; 3) communication with CAs; 4) impact of CAs on value creation and the value of CAs for business. We leverage these findings to provide an updated synopsis of extant scientific work. Moreover, we draw a framework whereby we identify the: 1) drivers of and motivators for adoption and engagement with CAs; and 2) the outcomes of CA adoption for both users and organizations. Finally, we leverage the framework to develop an agenda for future research.},

   author = {Marcello M. Mariani and Novin Hashemi and Jochen Wirtz},

   doi = {10.1016/J.JBUSRES.2023.113838},

   issn = {0148-2963},

   journal = {Journal of Business Research},

   keywords = {Artificial intelligence,Bibliometric analysis,Conversational agents,Systematic literature review},

   month = {6},

   pages = {113838},

   publisher = {Elsevier},

   title = {Artificial intelligence empowered conversational agents: A systematic literature review and research agenda},

   volume = {161},

   year = {2023},

}

@web\_page{,

   author = {Luis Ávila},

   month = {2},

   title = {Ciberdelitos no son bien perseguidos en Panamá},

   url = {https://www.panamaamerica.com.pa/judicial/ciberdelitos-no-son-bien-perseguidos-en-panama-1202128},

   year = {2022},

}

@web\_page{,

   author = {Luis Ávila},

   month = {2},

   title = {Ciberdelitos no son bien perseguidos en Panamá},

   url = {https://www.panamaamerica.com.pa/judicial/ciberdelitos-no-son-bien-perseguidos-en-panama-1202128},

   year = {2022},

}

@web\_page{,

   author = {La estrella Panamá},

   month = {5},

   title = {¿Cómo se penalizan los delitos cibernéticos?},

   url = {https://www.laestrella.com.pa/internacional/mundo/140525/delitos-penalizan-ciberneticos},

   year = {2014},

}

@web\_page{,

   month = {9},

   title = {Autoridad Nacional para la Innovación Gubernamental},

   url = {https://aig.gob.pa/analizan-el-tren-de-defensa-ante-las-amenazas-de-la-era-digital/#:~:text=En%20el%202021%20se%20registraron,seguridad%20que%20tienen%20las%20empresas.},

   year = {2022},

}

@article{Lyon2017,

   abstract = {This article argues that to make sense of surveillance today, the concept of surveillance culture should be added to the conceptual tool kit. This goes beyond the important concerns of the  surveillance state  and  surveillance society  to examine how today’s subjects make sense of, respond to, and—in some cases—initiate surveillance activities. Building conceptually on Charles Taylor’s work, the concepts of surveillance imaginaries and surveillance practices are proposed as a means of analysis of how surveillance is engaged today. Previous studies have hinted at surveillance culture both explicitly and implicitly, but more is needed. This article explores further one illustrative dimension—that of online practices of  sharing . These practices are seen, in turn, in relation to  visibility  and  exposure . Finally, the concept of surveillance culture is shown to be relevant to current discussions ethics and of digital citizenship.},

   author = {David Lyon},

   issn = {1932-8036},

   issue = {0},

   journal = {International Journal of Communication},

   keywords = {digital citizenship,online information,surveillance,surveillance culture},

   month = {2},

   pages = {19},

   title = {Digital Citizenship and Surveillance| Surveillance Culture:  Engagement, Exposure, and Ethics in Digital Modernity},

   volume = {11},

   url = {https://ijoc.org/index.php/ijoc/article/view/5527},

   year = {2017},

}

@web\_page{Francis2022,

   author = {Jean Paul Francis},

   month = {4},

   title = {El papel de la ciberseguridad generacional en el ecosistema digital},

   url = {https://www.laestrella.com.pa/cafe-estrella/tecnologia/220425/papel-ciberseguridad-generacional-ecosistema-digital},

   year = {2022},

}

@article{,

   title = {Train employees - your best defense - for security awareness},

   url = {http://www},

   year = {2009},

}

@article{,

   author = {Russ Banham},

   title = {Smaller organizations are targets for hacking and phishing attacks to get information that can harm them or bigger companies they do business with. Cybersecurity threats proliferating for midsize and smaller businesses AccountantsWorld • CPA Charge • OfficeTools Drake Software • Cornell College of Business},

}

@article{,

   abstract = {Studies show that training is a good alternative to deliver cybersecurity knowledge to children. This paper reports on the findings of a study after conducting awareness training programs.},

   author = {Zuriani Ahmad Zukarnain and Mimi Zazira Hashim and Norrini Muhammad and Farah Ahlami Mansor and Wan Nor Hazimah Wan Azib and Universiti Teknologi MARA Kelantan and Bukit Ilmu and Kelantan Malaysia},

   issue = {1},

   journal = {GADING Journal of Science and Technology},

   title = {IMPACT OF TRAINING ON CYBERSECURITY AWARENESS},

   volume = {3},

   url = {https://www.cybereducationscheme.org/certified-programmes,},

   year = {2020},

}

@article{Nadeesha2021,

   abstract = {Internet users face some problems and are particularly vulnerable to unwanted third parties due to depend on the internet for their use. Especially, the students who are studying in higher institutions are surfing the internet for many purposes without considering safe browsing. Evidence of literature and the results of the pilot study motivated the researchers to assess the levels of internet browsing security awareness among undergraduates of Rajarata University of Sri Lanka and to suggest security measures to overcome internet vulnerabilities. Data were collected from 300 undergraduates within six faculties using a structured questionnaire. The questionnaire was aimed on awareness of students in terms of three variables including knowledge of malware, use of strong password, and knowledge of third-party security towards the awareness of internet browsing security. The collected data were analysed using descriptive statistics including frequencies, measure of central tendency and measure of dispersion used to measure the way of responses. The hypotheses were tested using correlation analysis and regression analysis. All the hypotheses were accepted while supporting 52 percent explanatory power of independent variables on awareness of internet browsing security. Then the researchers could identify and verify the level of awareness regarding the secured browsing behaviour of the undergraduates that are not at satisfactory level. Further, based on the findings, the researchers recommended that the university should organize programs to increase the level of knowledge of undergraduates about safe internet browsing. First, it should be started by the faculty level and should track the progress of undergraduate safe browsing behaviour while expanding the study over to other government Universities in Sri Lanka. Keywords: Knowledge of third-party security, knowledge of malware, internet browsing security, use of strong password},

   author = {J.D Nadeesha and D.M.T. Madusanka},

   issn = {2651 – 0006},

   keywords = {Article,Knowledge of third-party security,internet browsing security,knowledge of malware,use of strong password},

   month = {6},

   publisher = {Rajarata university of Sri Lanka-Faculty of Management},

   title = {Awareness of Internet Browsing Security among Undergraduates inRajarata University of Sri Lanka},

   url = {http://repository.rjt.ac.lk/handle/123456789/3188},

   year = {2021},

}

@article{A2020,

   abstract = {Despite  the  fact  that  the  Internet  has  positively impacted  people’s  lives,  there  are  negative  issues  emerged related  to  the  use  of  Internet.  Cases  like  cyber-bully,  online fraud,  racial  abuse,  pornography  and  gambling  had  increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims to these acts. However, past research revealed that the level of awareness among Internet users is still low or moderate. One of the  vital  measures  to  be  taken  is  to  cultivate  knowledge  and awareness  among  Internet  users  from  their  early  age,  i.e., young   children.   Young   children   specifically,   need   to   be educated  to  operate  in  a  safe  manner  in  cyberspace  and  to protect   themselves   in   the   process.   The   objective   of   this systematic  review  paper  is  to  explore  why  it  is  so  critical  that modern  learners  are  educated  about  the  risks  associated  with being active in cyberspace and the strategies that stakeholders can use to promote cyber security education in schools. In this paper,  few  strategies  are  discussed  as  how  cyber  security education can be implemented in schools. },

   author = {Rahman A and Sairi H},

   month = {3},

   title = {The Importance of Cybersecurity Education in School},

   year = {2020},

}

@inproceedings{,

   author = {Eleanor Varela Tapia and Lady Sangacha-Tapia and Iván Acosta and Ricardo Celi},

   doi = {10.54808/CICIC2022.01.237},

   month = {6},

   pages = {237-241},

   title = {Inteligencia Artificial Conversacional para el Diseño de un Asistente Virtual Interactivo},

   year = {2022},

}

@article{Brown2020,

   abstract = {Recent work has demonstrated substantial gains on many NLP tasks and

benchmarks by pre-training on a large corpus of text followed by fine-tuning on

a specific task. While typically task-agnostic in architecture, this method

still requires task-specific fine-tuning datasets of thousands or tens of

thousands of examples. By contrast, humans can generally perform a new language

task from only a few examples or from simple instructions - something which

current NLP systems still largely struggle to do. Here we show that scaling up

language models greatly improves task-agnostic, few-shot performance, sometimes

even reaching competitiveness with prior state-of-the-art fine-tuning

approaches. Specifically, we train GPT-3, an autoregressive language model with

175 billion parameters, 10x more than any previous non-sparse language model,

and test its performance in the few-shot setting. For all tasks, GPT-3 is

applied without any gradient updates or fine-tuning, with tasks and few-shot

demonstrations specified purely via text interaction with the model. GPT-3

achieves strong performance on many NLP datasets, including translation,

question-answering, and cloze tasks, as well as several tasks that require

on-the-fly reasoning or domain adaptation, such as unscrambling words, using a

novel word in a sentence, or performing 3-digit arithmetic. At the same time,

we also identify some datasets where GPT-3's few-shot learning still struggles,

as well as some datasets where GPT-3 faces methodological issues related to

training on large web corpora. Finally, we find that GPT-3 can generate samples

of news articles which human evaluators have difficulty distinguishing from

articles written by humans. We discuss broader societal impacts of this finding

and of GPT-3 in general.},

   author = {Tom B. Brown and Benjamin Mann and Nick Ryder and Melanie Subbiah and Jared Kaplan and Prafulla Dhariwal and Arvind Neelakantan and Pranav Shyam and Girish Sastry and Amanda Askell and Sandhini Agarwal and Ariel Herbert-Voss and Gretchen Krueger and Tom Henighan and Rewon Child and Aditya Ramesh and Daniel M. Ziegler and Jeffrey Wu and Clemens Winter and Christopher Hesse and Mark Chen and Eric Sigler and Mateusz Litwin and Scott Gray and Benjamin Chess and Jack Clark and Christopher Berner and Sam McCandlish and Alec Radford and Ilya Sutskever and Dario Amodei},

   issn = {10495258},

   journal = {Advances in Neural Information Processing Systems},

   month = {5},

   publisher = {Neural information processing systems foundation},

   title = {Language Models are Few-Shot Learners},

   volume = {2020-December},

   url = {https://arxiv.org/abs/2005.14165v4},

   year = {2020},

}

@online{Eslavova2019,

   author = {Maya Eslavova},

   month = {4},

   title = {De la ciudadanía tradicional a la ciudadanía digital | EPALE},

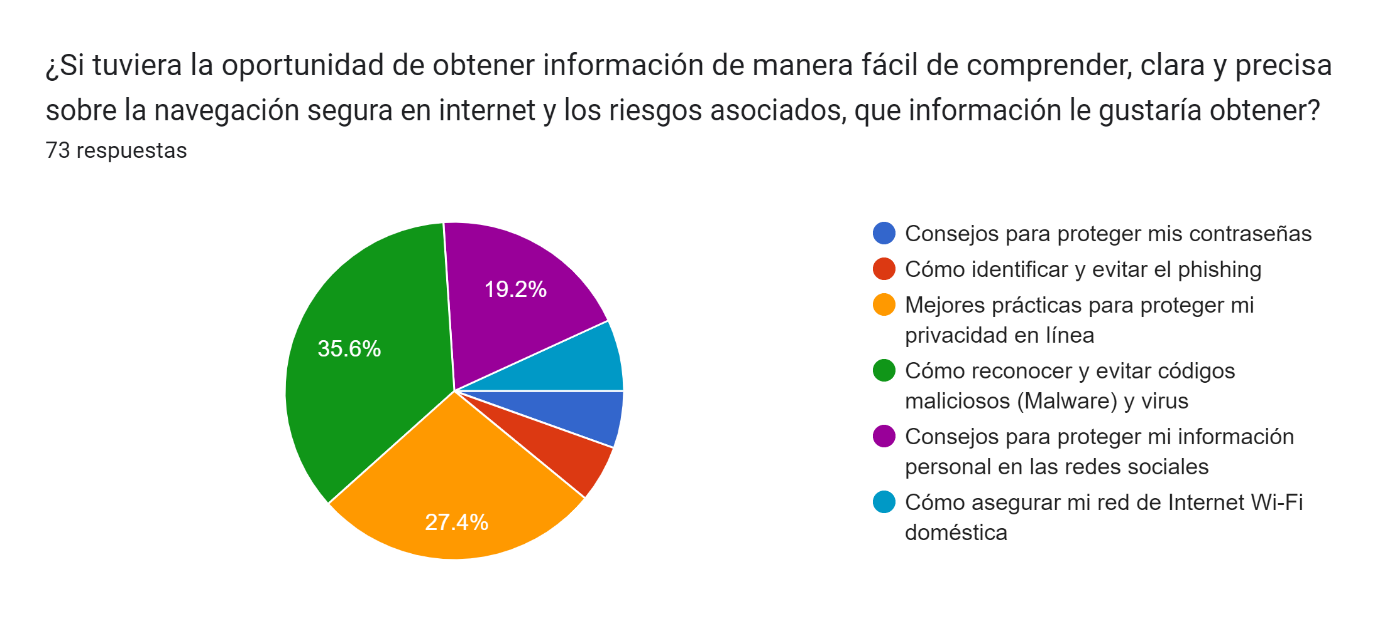
   url = {https://epale.ec.europa.eu/bg/blog/ot-tradicionno-grazhdanstvo-km-digitalno-grazhdanstvo},

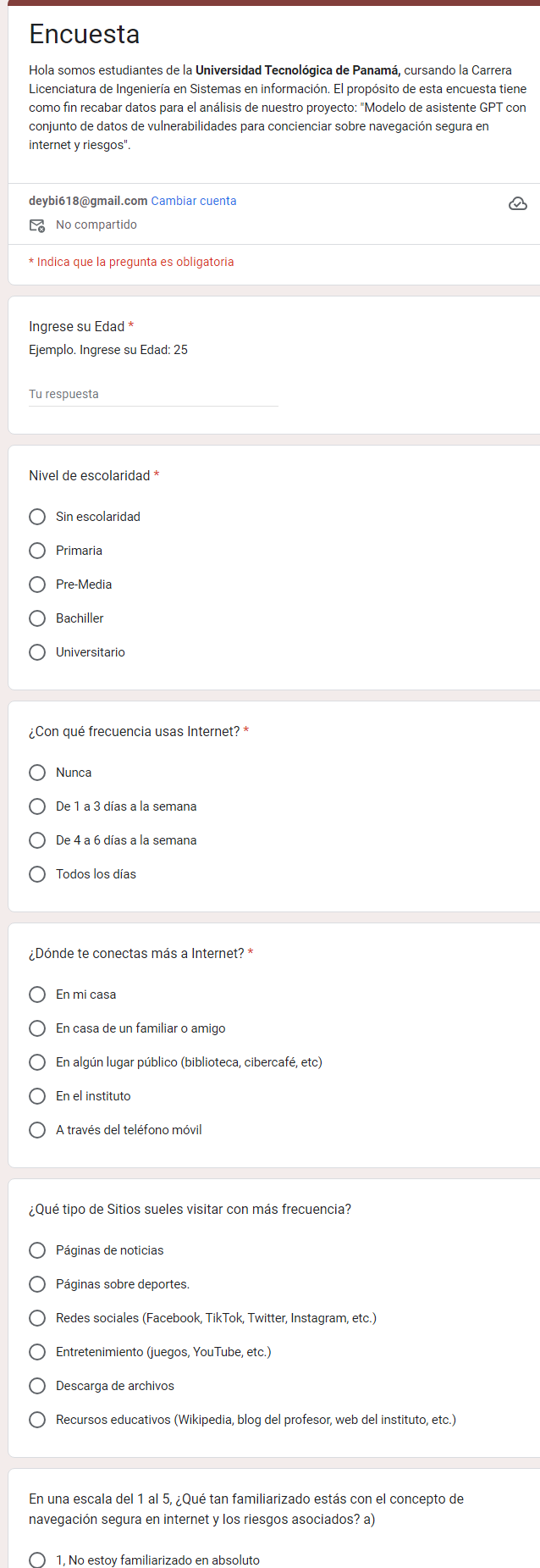
   year = {2019},

}

Anexos:

Gráfico de las respuestas de Formularios. Título de la pregunta: Nivel de escolaridad
. Número de respuestas: 73 respuestas.





Anexos

Encuesta sobre conciencia digital.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

mejor crea dos tablas con los siguientes datos:

configuracion 1: python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=20 --log\_interval=1 --block\_size=64 --batch\_size=12 --n\_layer=8 --n\_head=8 --n\_embd=256 --max\_iters=1000 --lr\_decay\_iters=1000 --dropout=0.2

Configuracion 2: python3 train.py config/train\_assimade.py --device=cpu --compile=False --eval\_iters=50 --log\_interval=5 --block\_size=128 --batch\_size=32 --n\_layer=4 --n\_head=4 --n\_embd=256 --max\_iters=3000 --lr\_decay\_iters=3000 --dropout=0.1

resultado del configuracion 2:

tokens per iteracion: 4096

number of parameters: 3.16M

num decayed parameter tensors: 18, with 3, 193,600 parameters

num non-decayed parameter tensors: 9, with 2,304 parameters

using fused AdamW: False

resultado del configuracion 1:

tokens per iteracion: 768

number of parameters: 6.31M

num decayed parameter tensors: 34, with 6, 322,944 parameters

num non-decayed parameter tensors: 17, with 4,352 parameters