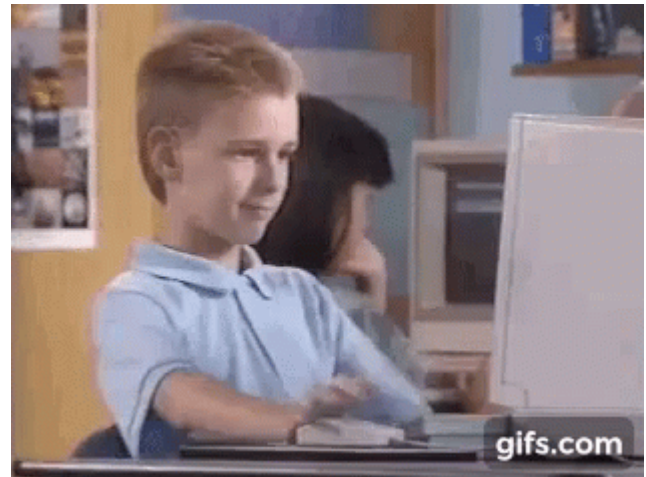


1.5 Cualquiera puede escribir una página web

La **creación de páginas web** se ha vuelto **más accesible** con el avance de las tecnologías y las herramientas disponibles. Actualmente, existen **múltiples opciones para crear y diseñar páginas web**, desde **editores de texto básicos hasta potentes sistemas de gestión de contenido** (CMS) como WordPress, Joomla o Drupal.



Web Webdeveloper por arthur44e [vía Tenor.com](#)

La facilidad con la que cualquier persona puede publicar contenido en Internet presenta tanto **oportunidades como desafíos**. Por un lado, **permite la libre expresión y el intercambio de información diversa**. Sin embargo, también puede dar lugar a la **difusión de información falsa, bulos y fake news** que pueden ser perjudiciales y engañosos.

La capacidad de hacer pasar el contenido por verídico, aunque sea falso o tenga una **intencionalidad manipuladora**, es una preocupación importante en la era de la información en la que vivimos. Esto se debe a que **la información falsa puede propagarse rápidamente a través de las redes sociales y otras plataformas en línea, llegando a un gran número de personas antes de que se pueda verificar su veracidad**.

Para combatir esta problemática, es fundamental fomentar la alfabetización mediática y digital en la sociedad. Las personas deben ser conscientes de la importancia de **verificar la información antes de compartirla o creer en ella**. Esto implica aprender a **evaluar las fuentes**, contrastar la información con múltiples fuentes confiables, **analizar el contexto en el que se presenta** y ser **consciente de posibles sesgos o**

intenciones ocultas.

Además, **es responsabilidad de los usuarios de Internet y de las plataformas en línea reportar y denunciar contenido falso o manipulador cuando lo encuentren**. Las empresas y plataformas digitales también tienen un papel importante en la lucha contra la desinformación, implementando políticas y algoritmos que prioricen la calidad y la veracidad de la información.

En última instancia, es un desafío continuo para la sociedad en su conjunto **encontrar un equilibrio entre la libertad de expresión y la responsabilidad de difundir información veraz y confiable**.

Información, pero al revés

La educación, la **conciencia crítica** y la **colaboración entre usuarios, plataformas y entidades reguladoras** son clave para abordar este problema y **promover un entorno en línea más confiable y seguro**.

Descubre algunos ejemplos de desinformación propagada en internet

- **Bulos y fake news sobre eventos actuales:** Durante **eventos importantes** como elecciones, crisis políticas o desastres naturales, es común ver la **propagación de información falsa**. Por ejemplo, la difusión de resultados electorales falsos, imágenes manipuladas de catástrofes o rumores infundados sobre personalidades públicas.
- **Manipulación de imágenes y videos:** Se han dado casos en los que se manipulan imágenes o videos para hacer que parezcan reales, pero en realidad están editados para engañar al público. Esto puede incluir la alteración de imágenes de noticias, la creación de **deepfakes** o la utilización de técnicas de edición para **modificar el contexto de una situación**.
- **Cuentas y perfiles falsos en redes sociales:** Algunas personas **crean perfiles falsos en redes sociales** con la intención de difundir información engañosa o influir en la opinión pública. Estas cuentas suelen utilizar estrategias de manipulación, como la creación de **identidades ficticias o la difusión masiva de mensajes con contenido falso**. También lo hacen para timos personales y phishing.

- **Sitios web y blogs engañosos:** Existen páginas web y blogs que **se hacen pasar por fuentes confiables o expertos** en determinados temas, pero en realidad difunden información falsa. Estos sitios pueden utilizar un diseño profesional y un lenguaje convincente para **engañar a los lectores** y hacer que la información parezca legítima.
- **Cadena de mensajes en aplicaciones de mensajería:** En aplicaciones de mensajería como WhatsApp, es común recibir **cadenas de mensajes que contienen información falsa o teorías de conspiración**. Estos mensajes suelen **apelar a las emociones o difundir alarmismo** sin fundamentos verificables.

Para realizar todas esas tácticas de desinformación se emplean diversas técnicas. Algunas de las más comunes abarcan:

- **Diseño y apariencia profesional:** Estas webs suelen tener un diseño atractivo y bien estructurado, **similar al de sitios web legítimos**. Utilizan logotipos, colores y tipografías que **transmiten credibilidad y confianza**.
- **Contenido persuasivo:** El contenido de estas webs se redacta de manera **convincente y persuasiva**, utilizando un lenguaje formal y profesional. Pueden **incluir citas o referencias falsas** para respaldar sus afirmaciones y hacer que parezcan más legítimas.
- **Uso de nombres y dominios similares:** Algunas webs falsas intentan confundir a los usuarios utilizando nombres o dominios similares a los de sitios web auténticos. Esto puede incluir la **adición o eliminación de una letra**, el uso de **extensiones de dominio poco conocidas** o el **uso de subdominios** que se asemejen a nombres conocidos.
- **Testimonios y reseñas falsas:** Para generar confianza, estas webs pueden **incluir testimonios y reseñas falsas** de supuestos clientes satisfechos. Estos testimonios suelen estar fabricados y no tienen una base real.
- **Imitación de elementos de confianza:** Pueden utilizar logotipos de empresas conocidas, sellos de seguridad, certificados o premios ficticios para dar la **apariencia de estar respaldados por organizaciones reconocidas**.

Los *hackers* se van de pesca



Al igual que las webs falsas, **los correos electrónicos pueden ser utilizados para difundir información engañosa** o intentar engañar a los usuarios. Algunas estrategias comunes que se emplean en los **correos electrónicos fraudulentos** (también SMS o mensajes en redes sociales) o de *phishing* comprenden:

- **Suplantación de identidad:** Los remitentes de correos electrónicos fraudulentos pueden hacerse pasar por una persona o entidad de confianza, como un banco, una empresa conocida o una institución gubernamental.
- **Urgencia o amenazas:** Estos correos electrónicos suelen utilizar un **tono urgente o amenazador** para instar al destinatario a tomar una **acción inmediata**. Pueden afirmar que la cuenta del destinatario ha sido comprometida o que **se enfrentan a consecuencias** legales si no siguen las instrucciones proporcionadas.
- **Enlaces o adjuntos maliciosos:** Los correos electrónicos fraudulentos pueden contener **enlaces que dirigen a sitios web falsos diseñados para robar información personal o credenciales de inicio de sesión**. También pueden incluir **archivos adjuntos maliciosos** que contienen *malware* o *virus*.
- **Gramática y ortografía deficientes:** A menudo, los correos electrónicos fraudulentos contienen **errores gramaticales o de ortografía** evidentes. Esto puede ser una señal de alerta de que el correo electrónico **no es legítimo**.

Es importante que seamos cautelosas al abrir correos electrónicos, especialmente aquellos de remitentes desconocidos o que parecen sospechosos. No hacer clic en enlaces ni descargar archivos adjuntos de correos electrónicos que generen dudas sobre su autenticidad.

Siempre es recomendable **verificar la legitimidad del remitente** antes de proporcionar información personal o confidencial.

Los envidiosos dirán que es *Photoshop*

<https://giphy.com/embed/t1HJXy5Q5NKA8>

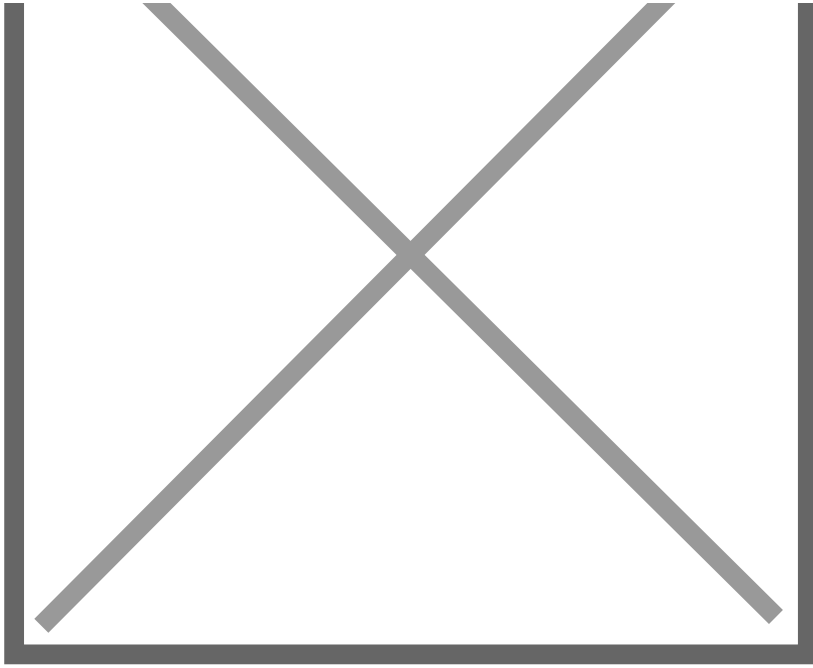
The Simpsons Photoshop via GIPHY



Las imágenes también pueden ser manipuladas para respaldar información falsa o engañosa. La manipulación de imágenes se realiza a través de **programas de edición de imágenes**, donde se pueden realizar **modificaciones en el contenido, el contexto o la apariencia** de una imagen para darle un **significado diferente al original**. Algunas técnicas comunes de manipulación de imágenes incluyen:

- **Edición de contenido:** Se pueden agregar, eliminar o modificar elementos en una imagen para cambiar su significado. Por ejemplo, se pueden **agregar personas, objetos o textos falsos** a una imagen para **crear una narrativa engañosa**.
- **Alteración de contextos:** Se puede cambiar el **contexto o la ubicación** de una imagen para hacer que parezca que ocurrió en un momento o lugar diferente. Esto se utiliza a menudo para difundir información errónea o para **respaldar afirmaciones falsas**.
- **Modificación de atributos visuales:** Se pueden ajustar los **colores, contrastes, brillos** y otros atributos visuales de una imagen para alterar su percepción. Esto se utiliza para manipular el **estado de ánimo, la interpretación o la atención del espectador**.

Ejemplos de imágenes manipuladas con ángulos, zoom, tonos y colores en las noticias.



"Marcha contra el terrorismo en

París con presencia de líderes mundiales. La foto de arriba se ve masiva, no así la de abajo." extraída del artículo de Pablo Rodríguez en *Fotos manipuladas que cambiaron la realidad sin pudor a la audiencia hasta que quedaron al descubierto.*

Es importante tener en cuenta que **las imágenes por sí solas no siempre son pruebas concluyentes de la veracidad de una afirmación**. Es recomendable realizar una **verificación adicional y buscar fuentes confiables** y diversas para respaldar cualquier información basada en imágenes, especialmente cuando se trata de contenido controvertido o impactante.

Además de esto las imágenes **se pueden manipular manualmente con diferentes programas de edición** como los que ya conocemos (Adobe Photoshop, GIMP, Adobe After Effects, Final Cut Pro, Blender, y otras más "livianas" usadas como entretenimiento como Face App, Snapchat ...)

La inteligencia artificial (IA) tiene la capacidad de manipular imágenes para hacer que parezcan reales a través de **técnicas de generación de imágenes y procesamiento de imágenes**. Una de las técnicas más populares es el **uso de las Redes Generativas Antagónicas** (GAN, por sus siglas en inglés).

Descubre qué son y cómo funcionan las GAN

Las **GAN** son un tipo de **arquitectura de redes neuronales** que consta de dos componentes principales: **el generador y el discriminador**.

El generador crea nuevas imágenes a partir de un conjunto de datos de entrenamiento, mientras que **el discriminador evalúa si esas imágenes son reales o falsas**. Ambas redes se entrenan de forma adversarial, lo que significa que **se mejoran mutuamente en un proceso de aprendizaje continuo**.

La IA puede aprender a generar imágenes realistas al analizar un gran número de imágenes de referencia y **aprender los patrones y características que hacen que una imagen parezca real**. Con el tiempo, el generador puede generar imágenes que son visualmente similares a las imágenes de entrenamiento, y el discriminador se vuelve más difícil de engañar, lo que resulta en **imágenes generadas que son cada vez más convincentes**.

Este tipo de manipulación de imágenes puede tener **diversas aplicaciones, tanto positivas como negativas**. Por un lado, se puede utilizar **en campos como el diseño gráfico, el cine, los videojuegos** y la realidad virtual para **crear contenido visualmente impactante y realista**. Por otro lado, también plantea desafíos y preocupaciones en términos de la creación y propagación de imágenes falsas, conocidas como **deepfakes**, que pueden ser utilizadas para **desinformar, difamar o manipular la opinión pública**.

Puedes consultar el artículo **¿Qué es el deepfake?** de la web de **seon.io** para conocer ejemplos concretos del mismo.

Un ejemplo claro pueden ser las polémicas imágenes que se crearon del Papa Francisco de fiesta creadas con el programa **Midjourney**. En el **artículo La inteligencia artificial recreó al Papa Francisco de fiesta y estas son las 5 mejores fotos de la web MDTech** se pueden visualizar.



Publicada por la

Redacción MDTech en su artículo.

De momento podemos consolarnos en que a Midjourney, así como a otras IA, se le da bastante mal "dibujar" manos, al igual que a la mayoría del alumnado...



Binabakat Ang Kamay por
KissessShihtzu vía Tenor.com

<https://giphy.com/embed/3o7bucM2EI3wXWwc4o>

Drawing GIF By Alice Suret-Canale
via GIPHY

Es importante tener en cuenta que **la manipulación de imágenes con IA también plantea importantes cuestiones éticas y de responsabilidad**. Es fundamental desarrollar **sistemas de detección y verificación confiables** para identificar imágenes manipuladas y promover la alfabetización digital para que las personas puedan discernir entre imágenes reales y falsas.

Algunas aplicaciones y herramientas IA para generar imágenes pueden ser:

- **DeepArt.io**: Utiliza redes neuronales para aplicar estilos artísticos a imágenes y generar composiciones artísticas únicas.

- **DeepDream:** Desarrollado por Google, aplica algoritmos de aprendizaje profundo para crear imágenes psicodélicas y surrealistas.
- **DALL·E:** Un modelo de IA creado por OpenAI que puede generar imágenes a partir de descripciones textuales.
- **StyleGAN:** Una arquitectura de GAN desarrollada por Nvidia que se utiliza para generar imágenes realistas de personas, paisajes y objetos.
- **FakeApp:** Una aplicación basada en GAN que permite intercambiar rostros en videos y crear deepfakes.

Se recomienda un uso responsable y consciente de estas herramientas, respetando los derechos de privacidad y evitando su mal uso.

Hecha la trampa, hecha la ley

<https://giphy.com/embed/KeuFUkFtP05s0f3Egj>

Magnify Joaquin Reyes GIF por Movistar Plus+ via GIPHY

Dadas las creaciones de la IA, también **se han creado herramientas y apps capaces de descubrir el algoritmo**. Aquí tienes algunas herramientas en línea, aplicaciones y software que pueden ayudar a **analizar imágenes o vídeos en busca de manipulaciones**:

- **FotoForensics:** Es una herramienta en línea que analiza imágenes en busca de manipulaciones. Puede ayudar a detectar ciertos indicios de manipulación en imágenes, como **artefactos digitales o inconsistencias en el contenido visual**. Utiliza **algoritmos de análisis forense** para detectar posibles manipulaciones en imágenes.
- **Forensically:** Aplicación online que permite detectar y analizar manipulaciones en imágenes. Ofrece diversas funciones, como la **detección de ruido digital, análisis de metadatos y detección de clonación**.

- **InVID Verification Plugin:** Es una **extensión para navegadores web** que ayuda a los usuarios a verificar la autenticidad de imágenes y vídeos en línea. Proporciona herramientas para el **análisis de metadatos, la verificación de origen y la búsqueda de duplicados**.
- **Amped Authenticate:** Es un software forense de imágenes y vídeos utilizado en la aplicación de la ley y por profesionales de la seguridad. Permite detectar manipulaciones, analizar metadatos y realizar un análisis detallado de la autenticidad de los medios.
- **Izitrú*:** Es una plataforma que utiliza técnicas de análisis forense para verificar la autenticidad de imágenes. Utiliza algoritmos y aprendizaje automático para detectar posibles manipulaciones y proporciona un **informe detallado sobre la autenticidad de la imagen**. (* Puede que les hayan comprado el dominio y ahora no lo recuperen).
- **Serimag Forensic Services:** Es una empresa española especializada en servicios forenses digitales. Ofrece soluciones y análisis forenses para la autenticación y verificación de imágenes y vídeos, incluyendo la detección de manipulaciones y el análisis de metadatos.

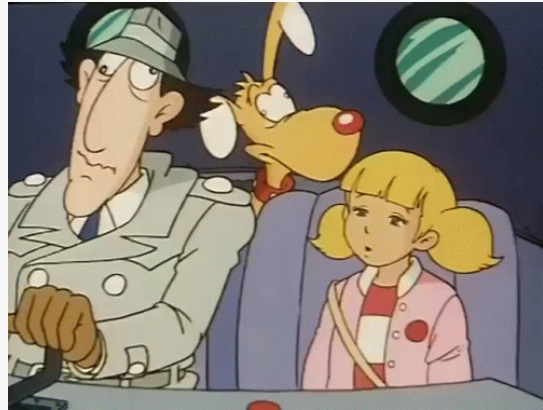
Recuerda que la **lucha contra el fraude** y la promoción del **uso ético de las IA y los GAN** requiere una combinación de **conocimientos técnicos, conciencia crítica y acciones responsables**.

"@polisía" o servicio forense en la web

Un **servicio forense digital** se refiere a un conjunto de **técnicas y procedimientos utilizados para investigar y analizar evidencia digital con el fin de resolver casos legales o delitos relacionados con el ámbito digital**. Los servicios forenses digitales pueden abarcar una amplia gama de áreas, como la **recuperación de datos, el análisis de dispositivos electrónicos, la identificación y autenticación de archivos digitales, la investigación de delitos cibernéticos**, entre otros.

Los expertos forenses digitales utilizan **herramientas y técnicas especializadas para preservar, recopilar, examinar y analizar la evidencia digital de manera forense, garantizando su integridad y cumpliendo con los estándares legales y las mejores prácticas**. Esto implica seguir un enfoque sistemático y riguroso, documentando cada paso del proceso y asegurando que la evidencia pueda ser presentada en un tribunal de justicia si es necesario.

El Inspector Gadget no era nada sin Sophie



Inspector Gadget por dizzyeyes vía Tenor.com

Estos servicios **se pueden aplicar en una amplia variedad de casos** en los que se requiere investigar y analizar evidencia digital. Algunos ejemplos pueden ser:

- **Investigaciones de delitos cibernéticos:** Cuando se sospecha de un delito cometido a través de medios electrónicos, como el **robo de información, el fraude en línea, el acoso cibernético o la difusión de contenido ilegal**.
- **Incidentes de seguridad informática:** Cuando se produce una violación de la seguridad en sistemas informáticos o redes, y es necesario **determinar el alcance del incidente, identificar al intruso y recopilar pruebas** para tomar acciones legales o mejorar la seguridad.
- **Disputas legales y litigios:** En casos legales que involucren evidencia digital, como la **violación de derechos de autor, la difamación en línea o el robo de propiedad intelectual**.
- **Investigaciones internas en empresas:** Cuando se sospecha de **actividades ilegales o violaciones de políticas** dentro de una organización, y es necesario recopilar y analizar evidencia digital para sustentar una investigación interna.

Existen varias empresas y organizaciones que ofrecen servicios forenses digitales. Algunos ejemplos de estas empresas son:

- **BDeV Digital Forensic Experts:** Es una empresa española especializada en servicios forenses digitales, incluyendo análisis forense de dispositivos electrónicos, recuperación



de datos y análisis de evidencia digital.

- **Forensic de PwC:** Ofrece servicios forenses digitales para investigaciones de delitos cibernéticos, incidentes de seguridad informática y litigios relacionados con la tecnología.
- **Cibernos Forensic Services:** Proporciona servicios de análisis y peritaje forense digital para casos legales y disputas comerciales, así como consultoría en seguridad informática.

Revision #14

Created 13 May 2023 18:44:22 by Elena I. Moncayo

Updated 11 September 2023 18:22:39 by Elena I. Moncayo