Surface web

También llamada **Clearnet** o **Internet visible**, está formada por las **páginas de internet que están indexadas en los motores de búsqueda**. En esta red somos fácilmente rastreables a través de nuestra dirección IP.

Además, está compuesta por todas las páginas y servicios como Google, Facebook, Twitter, entre otros. Según estimaciones estaría compuesta por más de 4.700 millones de páginas indexadas.

Deep Web

También llamado **Internet o Web profundas**, hace referencia al **contenido que no se encuentra indexado en los motores de búsqueda convencionales** (Google, Bing, Yahooo…). Está formada por páginas o dominios de Internet que no están disponibles para que los usuarios puedan visitarlos libremente, se encuentran protegidos y requieren credenciales de acceso.

En este sentido, en la Internet profunda se encuentran **servidores, bases de datos personales, plataformas privadas y repositorios a los que no podemos acceder de forma convencional**, ya que **en la mayoría de los casos se requiere iniciar sesión o introducir una contraseña** para ver su contenido.

Algunas de las partes más grandes de la web profunda incluyen:

- **Bases de datos:** colecciones de archivos tanto públicas como privadas protegidas que no están conectadas a otras áreas de la web, solo para que se busquen dentro de la propia base de datos.

- **Intranets:** redes internas de empresas, gobiernos e instalaciones educativas utilizadas para comunicar y controlar aspectos privados dentro de sus organizaciones.

Ejemplos de páginas en la **Deep Web:**

- Archivos guardados en la nube (DropBox, Google Drive, Mega)
- Páginas de cuentas bancarias (al iniciar sesión en la página del banco)
- Revistas académicas (trabajos publicados en portales científicos)
- Bandeja de entrada del correo electrónico
- Servicios de streaming (Netflix, HBOMAX, Hulu, Amazon)
- Perfiles de redes sociales (Twitter, Instagram, Facebook, Tik Tok).

Dark web

Es una porción de Internet que **está oculta intencionalmente y que no es indexada por los motores de búsqueda**. A diferencia de la Deep Web, **el contenido de la Dark Web no es accesible a través de navegadores web convencionales.**

La **Dark Web** está compuesta por varias **Dark Nets**, que son redes independientes. Para acceder**, es necesario utilizar software especializado**, configuraciones específicas y contar con ciertos conocimientos técnicos.

Por ejemplo, **la red Onion**, a la cual se accede a través del **navegador TOR**, es una **Dark Net** entre otras que existen. Las URL de la red Onion podemos identificarlas fácilmente porque terminan con la extensión .onion.

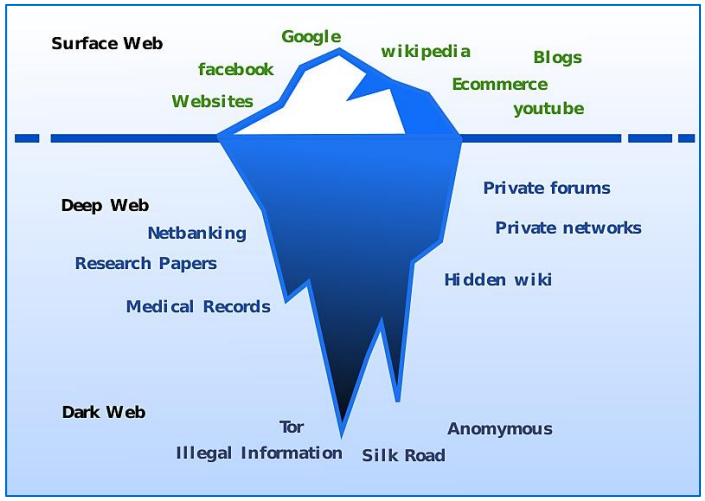
Tor (red Onion), I2P o Freenet son diferentes **Dark Nets** que existen dentro de la **Dark Web.**

Esta zona de Internet es popularmente conocida por actividades ilegales, como tráfico de drogas, venta de armas, pornografía infantil, tráfico de personas, cibercrimen organizado, terrorismo, venta de datos robados, fraudes y otros tipos de actividades delictivas.

Las personas que acceden a la **Dark Web** suelen utilizar herramientas que además de anonimato permitan ocultar su identidad y no dejar rastros de su actividad en línea. Por ejemplo, **redes VPN o el uso de Proxys**.

Pese a que es famosa por la actividad ilegal, vale la pena mencionar que en la **Dark Web también hay contenido legítimo**, como sitios web que ofrecen servicios de privacidad y seguridad en línea,

recursos para periodistas y activistas que trabajan en zonas de conflicto, así como sitios web de organizaciones que luchan contra la censura y la vigilancia en línea.



Dark Net

El concepto de **Dark Net** refiere a una zona de la Internet a la cual se puede acceder mediante software especializado y protocolos de encriptación que garantizan el anonimato y la privacidad de los usuarios. La **Dark Web** está compuesta por diferentes **Dark Nets**.

La **Dark Net** es un conjunto de redes privadas independientes que no están indexadas por los motores de búsqueda y a las que no se puede acceder a través de navegadores web comunes. Ejemplos de estas **Dark Nets** son las redes **Onion, I2P o Freenet**.

Dark Nets como la **red Onion** enmascaran la dirección IP del usuario y enrutan la conexión a través de múltiples servidores para ocultar la identidad y la ubicación de las personas.

En los siguientes artículos y vídeos se habla sobre Surface Web, Deep Web, Dark Web y Dark Net:

Artículos:

- Surface Web, Deep Web, Dark Web y Dark Net: Aprende sus diferencias
- Dark web y Deep web: Qué son, diferencias y las ciberamenazas que esconden
- Qué es la DarkWeb, la DeepWeb y la DarkNet y cuáles son sus diferencias
- ¿En qué se diferencian la Deep Web, Dark Web, Dark Net y Surface Web? Aquí la respuesta

Vídeos:

- ¿Qué es la DARK WEB, la DEEP WEB y la SURFACE WEB? Definición y diferencias
- Diferencias entre Surface Web, Deep Web y Dark Web

Tor (The Onion Router)

Cuando hablamos de la **red Tor** nos referimos a un proyecto creado para desarrollar una red de comunicaciones basada en el intercambio de mensajes de forma anónima. Esto es posible gracias a una serie de organizaciones y también usuarios particulares que donan su ancho de banda. Así las conexiones se enrutan de forma anónima.

El **navegador Tor** se basa en esta red. De esta forma permite que al utilizarlo naveguemos de forma anónima por Internet y ocultar así la dirección IP real, por ejemplo.

El nombre viene de **The Onion Router**. Está basado en una estructura de capas, de ahí el nombre de cebolla. Estas capas son lo que aportan un anonimato al usuario. Así podemos, por ejemplo, ocultar la dirección IP cuando entramos en un sitio en concreto.

Esta red descentralizada nos permite navegar por la **Deep Web.** Hay que indicar que para que esto sea posible se necesitan nodos para poder mantener así la privacidad. Hay miles de nodos disponibles.

El navegador Tor

Está disponible tanto para sistemas operativos de escritorio, como son **Windows, Linux o macOS**, como también para **Android**, en el caso de dispositivos móviles. Es un programa totalmente gratuito y de código abierto. Utilizarlo es sencillo y vamos a mostrar los pasos que hay que realizar para instalarlo y su puesta en funcionamiento.

Descarga

Lo primero que hay que hacer es descargar el programa. Para ello tienes que ir a la página web del proyecto TOR. Allí encontrarás la sección de descargas y las diferentes opciones que tienes disponibles. Solo tendrás que elegir la que necesites, por ejemplo, la aplicación para Windows o para Android.

Una vez le des a Descargar, automáticamente comenzará a bajar el archivo. También verás los botones para descargar la versión Alfa, que es de pruebas, así como el código fuente del programa, en caso de que quieras analizarlo. Además, podrás descargar el navegador en otro idioma si lo necesitas.

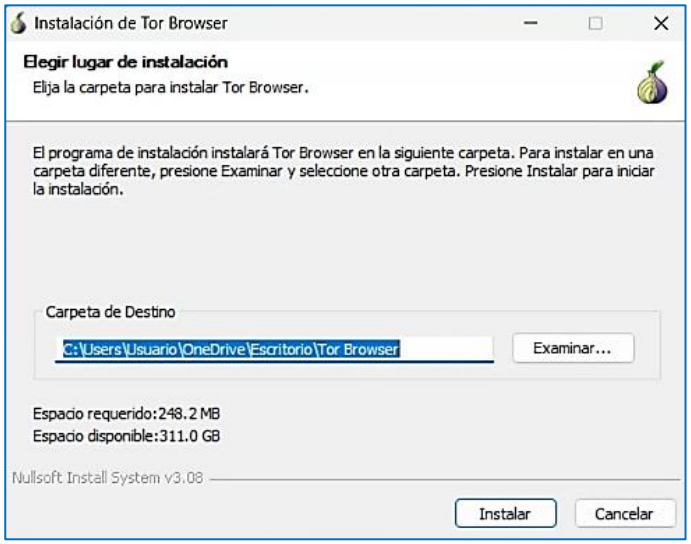
Es importante que siempre que instales un programa, más aún si se trata del navegador o alguna herramienta que se conecte a la red, sea desde fuentes oficiales. Por ello te aconsejamos que únicamente descargues Tor Browser desde su sitio web oficial y evites cualquier plataforma de terceros, ya que podrías toparte con un archivo que ha sido modificado de forma maliciosa.

Instalación

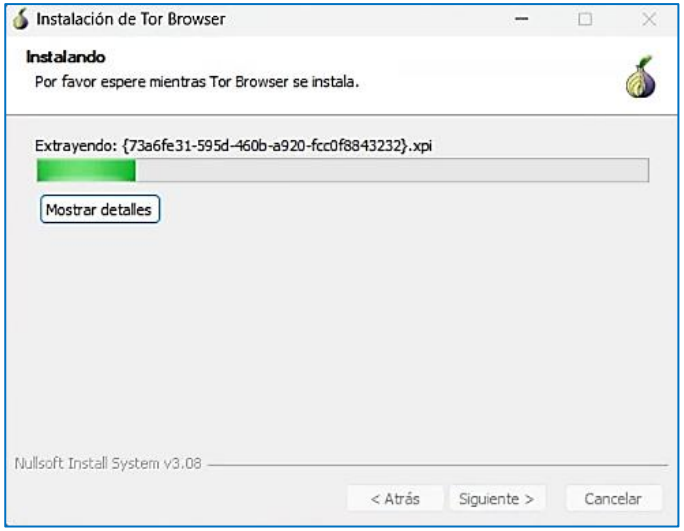
Ejecutar el programa de instalación:

Seleccionar el idioma:

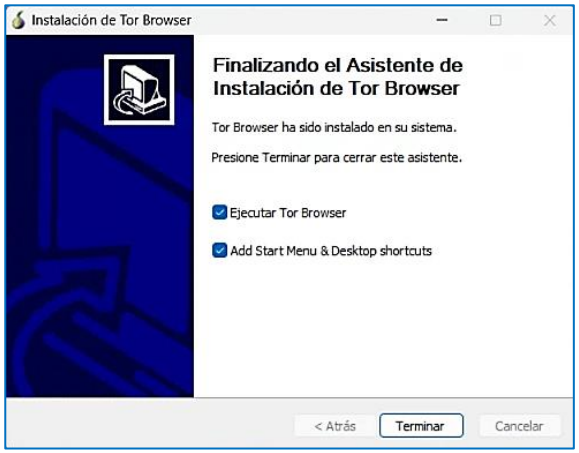
Elegir el lugar de la instalación (Por defecto, en el escritorio):



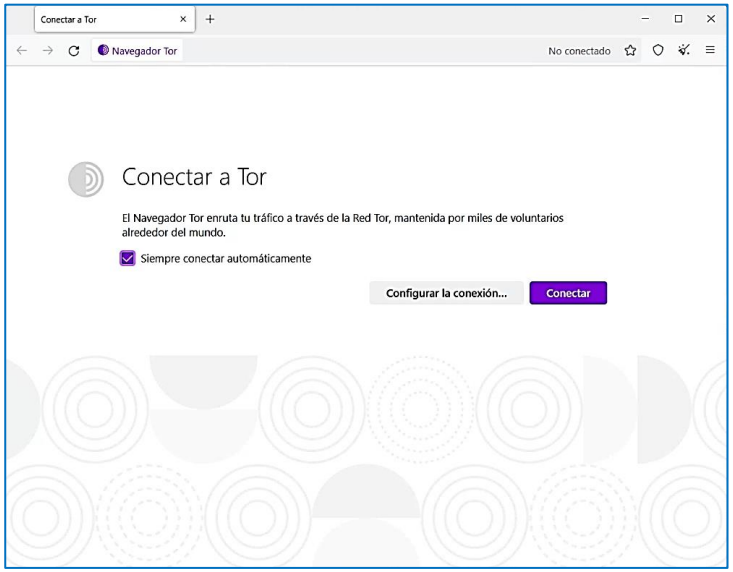
Pulsar **Instalar:**



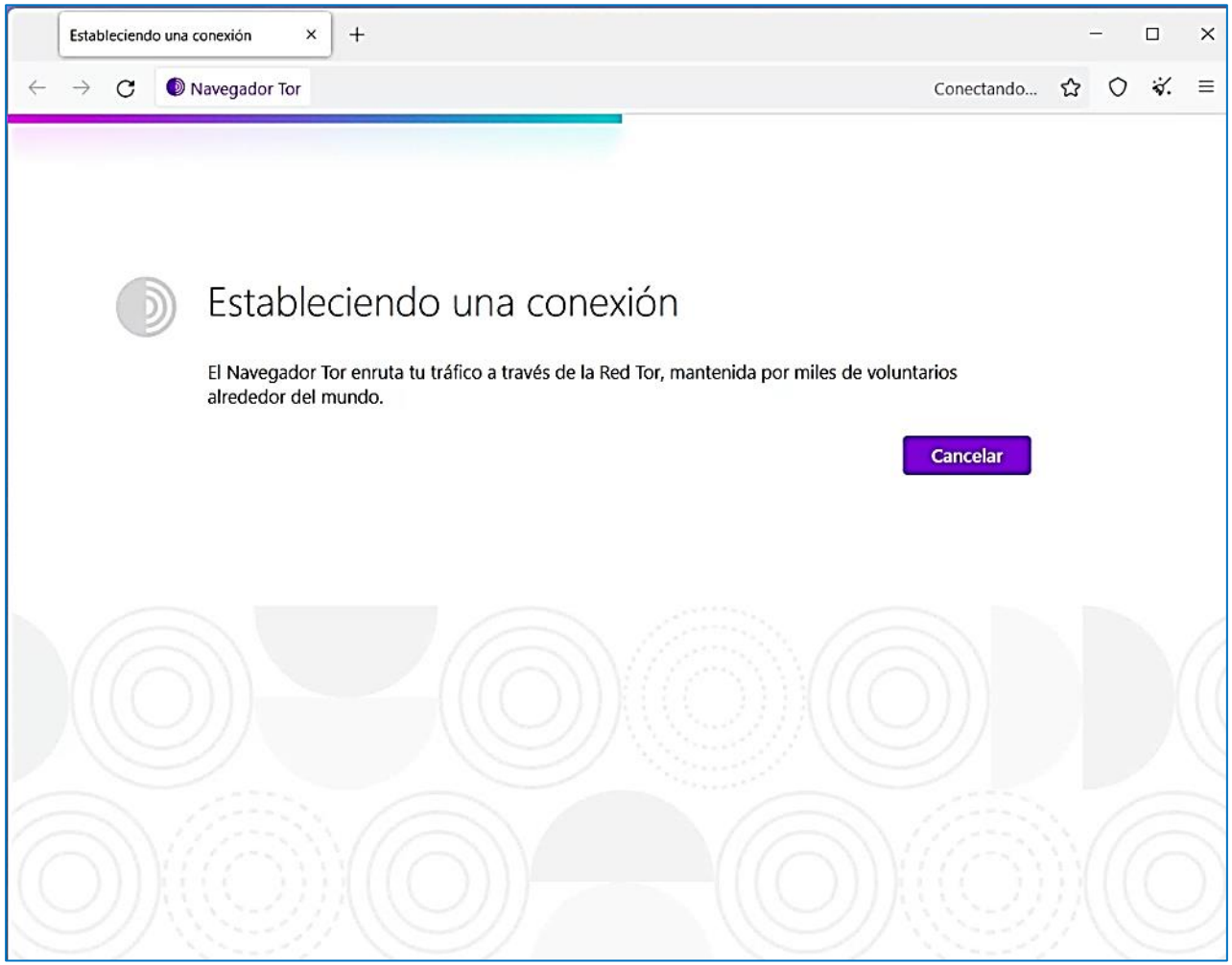
Pulsar **Terminar:**



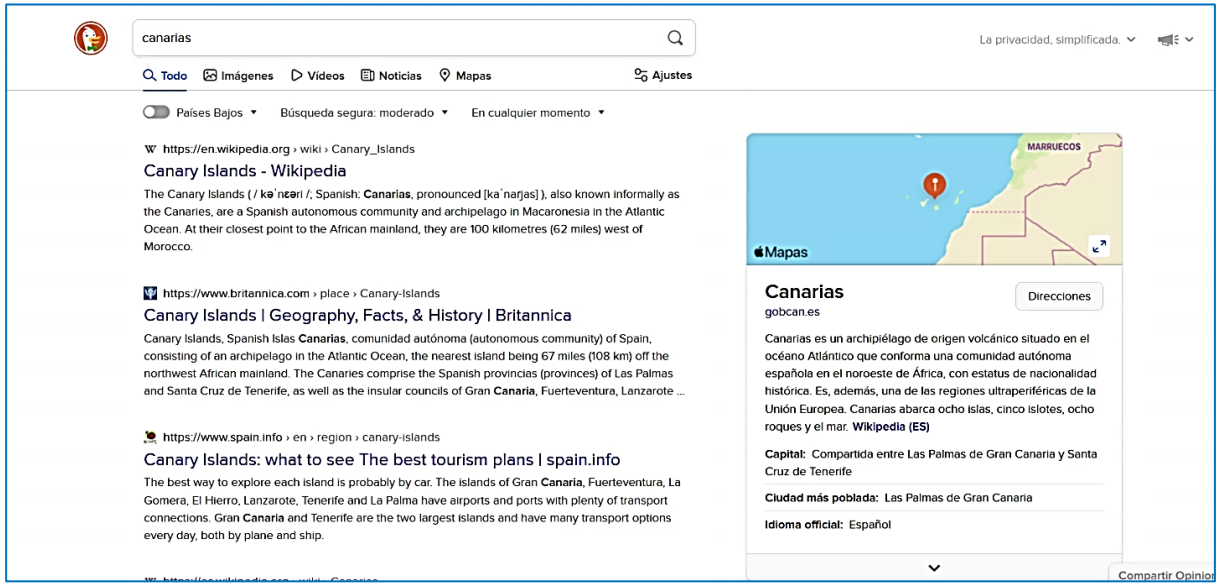
Se abre el navegador, tiene la siguiente **Interface.** Podemos indicarle que se conecte automáticamente a la **red Tor** cada vez que lo ejecutemos:



Establece conexión con la **red Tor**:



El navegador tiene la siguiente **apariencia.** Utiliza por defecto el buscador DuckDuckGo:



Si observamos la Ip que muestra está localizada en un lugar diferente al habitual:

Mientras que en nuestro navegador habitual:

La Red TOR

En los siguientes artículos y vídeos se habla sobre Surface Web, Deep Web, Dark Web y Dark Net:

Artículos:

- Red TOR: qué es, cómo funciona y cómo se usa
- Cómo usar Tor Browser para ser anónimo en Internet
- ¿Qué es el navegador Tor?
- Guía de anonimato con Tor
- Tor vs. VPN: ¿cuál es la diferencia?
- Tor contra VPN: ¿cuál es más seguro?
- ¿Es seguro de usar el navegador Tor?

Vídeos:

- Uso del Navegador Tor Browser
- Cómo Configurar y Usar la red TOR para Navegar de Forma SEGURA en la DEEP WEB e Internet
- Cómo Usar Tor Desde Cero

Enlaces:

- HTTPS y TOR
- TORMAP

Se pide:

1. Elaborar un documento explicando los conceptos: Surface, Deep y Dark web
2. Explica que es la red Tor, su funcionamiento y características.
3. Instala el Navegador de la red Tor. Muestra con capturas de pantalla y comentarios los pasos realizados.