CIBERSEGURIDAD

Competencia Básica Digital

Bienvenide, bienvenida o bienvenido al curso de Competencia Básica Digital.

A lo largo de este curso y, probablemente, también en el futuro, **vas a necesitar utilizar herramientas informáticas siguiendo unas normas básicas de seguridad.**

En esta situación de aprendizaje vamos a hacer un resumen de lo más importante sobre esas herramientas y las normas básicas de seguridad que conviene seguir.

Sumario

COMPONENTES FÍSICOS DEL ORDENADOR

Un ordenador ha sido diseñado y construido con el fin de **recibir, almacenar, procesar y emitir información.** Cada uno de sus componentes ha sido diseñado y construido para realizar alguna de esas funciones:

- **Entrada y salida de información:** se realiza a través de puertos de distinto tipo (USB, HDMI, VGA, etc).
- **Procesamiento:** se realiza en la CPU (Unidad Central de Procesamiento), construida con uno o varios microprocesadores.
- **Almacenamiento:** tradicionalmente se han venido utilizando discos duros, pero actualmente se utiliza todo tipo de dispositivos de almacenamiento, incluyendo pendrives USB, tarjetas de memoria o, incluso, almacenamiento en nube[1].

1 Es decir, en un dispositivo externo que puede ser incluso otro ordenador situado a kilómetros del usuario.

Ada Lovelace (Imagen: Dominio público CC0 1.0 Universal)

Ada Lovelace pensó que era posible dar una serie de instrucciones a la máquina de calcular de Babbage (una calculadora mecánica que nunca llegó a construirse) para que funcionase de forma automática.
Sería un ordenador con una unidad central de procesamiento totalmente mecánica y un sistema de almacenamiento basado en papel perforado.
En 1843 Ada publicó lo que se considera el primer programa informático de la historia. Pero enseguida se hizo pública su condición femenina y, en consecuencia, su idea fue olvidada.

Sobre Ada Lovelace y otras científicas e ingenieras podéis encontrar información en el cómic Científicas, de Raquel Gu.

Un complemento necesario de cualquier ordenador son los **periféricos**, generalmente diseñados de forma que se permita el intercambio de información entre humanos y máquinas: teclados, ratones, monitores, cámaras, etc.
Finalmente debe tenerse en cuenta que todos estos dispositivos necesitan algún sistema de alimentación de energía. Algunos se alimentan directamente de la red eléctrica, mientras otros se alimentan del propio ordenador a través de alguno de sus puertos.

ALMACENAMIENTO DE LA INFORMACIÓN

Todos los ordenadores necesitan algún dispositivo para almacenar la información. Inicialmente se utilizaron tarjetas de papel perforadas, pero actualmente los sistemas de almacenamiento más habituales son:

- **Disco duro (HDD[2]):** basados en sistemas magnéticos, de gran capacidad pero pesados y frágiles debido a su mecanismo. Suelen ser internos, formando parte de muchos ordenadores, pero también los hay externos.
- **Unidad de estado sólido (SSD[3]):** basadas en memorias *flash*. No tienen partes móviles (lo que es una ventaja respecto a los HDD) y son muy rápidas. Sin embargo el riesgo de que dejen de funcionar inesperadamente y se pierda toda la información es mucho más alto que en los HDD.
- **Pendrives:** basados en memoria *flash*, como las SSD. Ligeros, con cierta resistencia a golpes y al polvo, baratos y sencillos de utilizar, pero con el riego de perder la información almacenada ante una variación del voltaje suministrado por un puerto USB.
- **Tarjetas de memoria:** basadas en memoria *flash*, rápidas, baratas, ligeras y de pequeño tamaño. Muy usadas en dispositivos pequeños como smartphones, tablets, cámaras digitales y ordenadores de placa única. Similares a los pendrives en cuanto a prestaciones, rapidez y fiabilidad.
- **Discos ópticos:** CD y DVD, principalmente, cada día menos utilizados. Su principal riesgo es que una rozadura los vuelva ilegibles.
- **Nube:** almacenamiento en red. Tiene la ventaja de estar accesible allí donde haya acceso a la red, sin necesidad de transportar ningún dispositivo. Esta práctica, además, permite compartir archivos de forma pública o con determinados usuarios.

2 Hard Disk Drive.
3 Solid State Drive.

Dado que no existe ningún dispositivo de almacenamiento totalmente seguro y que, además, siempre existe el riesgo de que se produzca un accidente o un robo, **se recomienda almacenar los archivos importantes en distintos dispositivos o sistemas al mismo tiempo, y no guardarlos ni transportarlos físicamente en el mismo lugar.**

CONEXIÓN EN RED

Actualmente existen distintos sistemas que permiten la comunicación inalámbrica[4] entre distintos dispositivos. Los sistemas más habituales hoy en día son:

- **Bluetooth:** muy utilizado para dispositivos de bajo consumo energético y a corta distancia, como teléfonos móviles y altavoces.
- **Wifi:** muy utilizado en la creación de redes locales, como la de un conjunto de ordenadores e impresoras en una zona de un edificio.
- **3G/4G/5G:** utilizados por operadores de Internet para cubrir grandes extensiones. Muy utilizada por smartphones,

4 Sin cables.

Hedy Lamarr, estrella de Hollywood e inventora de un sistema utilizado actualmente en comunicaciones inalámbricas como Wifi y otras (Imagen: dominio público).

Hedy Lamarr y el compositor George Antheil patentaron un sistema de comunicaciones por radio en el que emisor y receptor iban cambiando de frecuencias constantemente pero de forma sincronizada, haciendo imposible la intercepción de comunicaciones.
El objetivo era equipar a los torpedos con un sistema de guía que no pudiese ser inutilizado por las fuerzas alemanas. El invento fue rechazado por la marina y olvidado en el fondo de un cajón durante años.
Actualmente la idea de Hedy Lamarr es la base de desarrollos tecnológicos como el Bluetooth o el WiFi.

La vida de Hedy Lamarr estuvo marcada por su pasión por la ciencia y la ingeniería, por su huída del régimen nazi y por su trabajo como actriz de Hollywood. El cómic Objetivo Hedy Lamarr es una ficción con algunas partes de realidad,pero sí os interesa otro cómic más fiel a la historia real podéis buscar en Científicas.

SOFTWARE PROPIETARIO Y SOFTWARE LIBRE

Tipos de software

Software[5] propietario

Software propietario es aquel cuyos derechos de copia, modificación y difusión están restringidos por derechos de propiedad intelectual. A veces está permitida su libre descarga y utilización, en cuyo caso estaremos hablando de **shareware**.

Software de código abierto (Open source software)

Logo de la iniciativa Open Source

El software de código abierto es aquel del que se ha publicado su código fuente[6], facilitando así la comprensión de su funcionamiento[7].

5 El software es el conjunto de programas informáticos de un ordenador. Los componentes físicos constituyen el hardware.

6 Instrucciones que sigue el ordenador al ejecutar el programa, escritas en un lenguaje inteligible para humanos (en el ordenador cualquier software es una sucesión ininteligible de unos y ceros, ilegible para seres humanos).

7 La mayor parte del software propietario no ha hecho público su código fuente, siendo este accesible solamente a los empleados de la empresa desarrolladora y a los de otras que trabajan bajo licencia.

Software libre (Free software)

Logo de la Free Software Foundation

Software libre es aquel que cumple las cuatro libertades siguientes:

- **Libertad 0**: la libertad de usar el programa, con cualquier propósito (uso)[8].
- **Libertad 1**: la libertad de **estudiar** cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades (estudio)[9].
- **Libertad 2**: la libertad de **distribuir** copias del programa, con lo cual se puede ayudar a otros usuarios (distribución)[10].
- **Libertad 3**: la libertad de **mejorar** el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie (mejora)[11].

La licencia de software libre más usada es la GPL (GNU Public License).

8 El software propietario, salvo que sea shareware o alguna versión de prueba, no suele otorgar esta libertad si no se paga previamente.

9 Para esto es necesario que el código fuente haya sido publicado, lo que implica que el software libre debe ser de código abierto (aunque el software de código abierto podría no ser libre si no cumple alguna de las cuatro libertades).

10 Es decir: que cualquiera que disponga de una copia del software lo puede distribuir libremente, cosa ilegal con la mayor parte del software propietario.

11 Es decir: no solo es posible estudiar su funcionamiento y modificarlo, sino que además es posible la difusión de la versión modificada. Todo esto sin necesidad de pedir ningún permiso, aunque cumpliendo con los requisitos de la licencia libre bajo la que el software haya sido publicado.

Elementos básicos del sistema operativo. Instalación y desinstalación de aplicaciones.

Todos los sistemas operativos tienen un **núcleo con las instrucciones principales del sistema. Sobre este núcleo corren las aplicaciones que normalmente utilizamos.**

Antiguamente era habitual la comunicación entre humanos y máquinas en modo texto, pero eso requería un proceso de aprendizaje lento y poco accesible para la mayor parte de la población. En aquella época no se podía utilizar un ordenador si no se tenían unos conocimientos básicos de MS-DOS[12], Linux[13] o similares.

La situación cambió con la aparición de entornos gráficos como Windows[14], Gnome[15] y otros, que volvieron sencillo e intuitivo el uso de sistemas operativos. El uso del modo texto se ha quedado reducido a tareas de nivel medio o avanzado.

La instalación y desinstalación de aplicaciones también es **ahora mucho más sencilla gracias a los entornos gráficos**, aunque hay diferencias notables entre sistemas operativos. **En Windows, por ejemplo, es habitual el uso de archivos autoejecutables que se ocupan de la instalación de aplicaciones**, mientras que **en GNU/Linux lo habitual es el uso de sistemas de gestión de software que acceden a repositorios *on line* e instalan los paquetes de archivos necesarios para el funcionamiento de un determinado software.**

12 Microsoft Disk Operative System, utilizado por Microsoft antes de la existencia de Windows.

13 Aunque popularmente se llama "Linux" a todo el conjunto GNU/Linux lo cierto es que Linux es solamente el núcleo del sistema.

14 En sus primeras versiones Windows no era un sistema operativo sino un entorno gráfico que corría sobre MS-DOS.

15 Uno de los entornos gráficos más populares en sistemas GNU/Linux.

Organización y almacenamiento de la información

Todos los sistemas operativos almacenan la información en forma de paquetes llamados **archivos**. Estos archivos se ordenan en conjuntos lógicos llamados **directorios o carpetas**. Una carpeta o directorio puede incluir otras subcarpetas o subdirectorios.

Todos estos archivos y carpetas o directorios se almacenan en partes de dispositivos de almacenamiento llamadas **particiones**. Un dispositivo de almacenamiento puede tener una o varias particiones.

En cada partición se gestionan los archivos y las carpetas o directorios conforme a unas normas que dependen del sistema de archivos utilizado. Es posible formatear un dispositivo de almacenamiento y cambiar su sistema de archivos[16].

16 Los pendrives y tarjetas de memoria, por ejemplo, suelen venir formateados de fábrica con el sistema FAT 32, típico de antiguas versiones de Windows, pero es posible formatearlos para cambiar su sistema de archivos a EXT3, típico de sistemas GNU/Linux, por ejemplo.

¡CUIDADO! El formateo de una partición o de un dispositivo suele provocar la pérdida de la información que contiene. A veces es posible recuperar parte de la información si se dispone de los medios y conocimientos adecuados, pero no siempre.

De hecho se recomienda el formateado de dispositivos de almacenamiento con la mejor forma de borrado de la información.

Los archivos pueden ser creados, copiados, transferidos de una carpeta o directorio a otra, modificados o borrados.

¡CUIDADO! Enviar un archivo a la papelera no es lo mismo que borrarlo. De la papelera se puede recuperar fácilmente, mientras que si ha sido borrado, en teoría, no se puede recuperar.

A veces es posible recuperar un archivo que el usuario considera borrado. El ordenador no lo borra realmente, sino que etiqueta la zona del dispositivo ocupada por el archivo como reescribible, pero sin borrarla necesariamente.

Algunos usuarios, además, desconocen la existencia de carpetas y archivos ocultos, incluyendo algunas papeleras de reciclaje.

Es por todo esto que se considera que la forma más segura de borrado es el formateo.

SEGURIDAD Y AMENAZAS.

Actualización del software

Constantemente se están descubriendo vulnerabilidades tanto en los sistemas operativos[17] (GNU/Linux, Windows, MacOS, iOS, Android, etc) como en los programas que corren sobre ellos.

Estas vulnerabilidades pueden ocasionar problemas que van desde la pérdida de archivos hasta el secuestro de sistemas informáticos por terceras personas, pasando por el robo de información confidencial y la suplantación de identidades.

Conscientes de estos riesgos los desarrolladores de software suelen publicar actualizaciones para evitar este tipo de problemas. **Es conveniente mantener actualizado el software en la medida que sea posible.**

Los sistemas operativos actuales tienen sistemas que revisan y actualizan el software, siempre y cuando las licencias estén actualizadas y el usuario dé su autorización.

17 Software sobre el que funcionan las distintas aplicaciones que utilizamos en un ordenador.

Antivirus y firewalls

El término ***malware*** se refiere a cualquier tipo de **software creado para acceder a sistemas informáticos ajenos y realizar acciones no deseadas por el usuario del sistema afectado**. El *malware* puede propagarse de dos formas:

- Oculto en un archivo informático. Se instala cuando el usuario abre el archivo infectado. A este tipo de *malware* se le conoce como **virus**.
- Replicándose a sí mismo y difundiéndose a través de redes informáticas. En ocasiones pueden llegar a consumir tal ancho de banda que ralentizan el funcionamiento de las redes. A este tipo de software se le conoce como **gusano**.

Las acciones que puede realizar el malware son muy diversas. Algunas no pasan de ser una simple broma, pero otras constituyen graves delitos:

- Sustituir o modificar del navegador para introducir publicidad no deseada.
- Provocar el mal funcionamiento o el bloqueo de parte del software.
- Apertura de puertas traseras que permitan el control remoto del sistema informático por terceras personas. Al software que realiza esta acción se le conoce popularmente como **troyano**[18].
- Buscar información en el disco duro y enviarla a terceras personas.
- Secuestrar el sistema informático mediante el encriptado[19] de los discos duros.

No existe sistema informático que sea totalmente inmune a este tipo de ataques, si bien algunos sistemas (por su diversidad, sistemas de permisos y otros detalles) son más difíciles de atacar que otros.

Se han desarrollado defensas para proteger a los sistemas informáticos:

- **Cortafuegos (firewall)**: sistemas de software, hardware[20] o una combinación de ambos que filtran las comunicaciones de un sistema informático con el exterior bloqueando aquellas que no cumplan unas especificaciones de seguridad. En algunas redes se instalan varios firewalls entre distintos sectores según su uso, creando lo que se llama **zonas desmilitarizadas**, separadas por un firewall de la intranet[21] y por otro de una red externa, generalmente Internet.
- **Antivirus**: software que revisa el sistema informático buscando malware.

18 En referencia a la leyenda del caballo de Troya, un caballo gigante de madera que los habitantes de la ciudad de Troya creyeron un regalo e introdujeron dentro de su ciudad sin saber que dentro llevaba un grupo de soldados griegos que, de noche, abrieron las puertas de la ciudad para iniciar su invasión.

19 Modificación de la información que la hace ilegible excepto para quien tiene las claves necesarias para desencriptarla. Se han dado casos de ataques en los que se encriptaba el sistema informático de la víctima y se pedía un rescate.

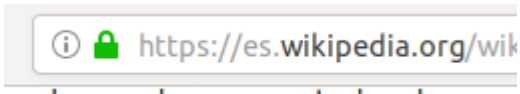
20 Hardware: componentes físicos de un ordenador, tales como la unidad central del proceso, el teclado, el monitor, etc.

21 Una intranet es un grupo de ordenadores conectados entre sí, generalmente dentro de un mismo edificio o de un mismo organismo o empresa. A menudo se instalan firewalls que protegen la intranet de ataques externos.

Hábitos de protección

Es conveniente seguir algunos hábitos de protección informática:

- **Mantener actualizado el software**, especialmente el antivirus.
- **No abrir correos de procedencia dudosa**[22], especialmente si llevan un adjunto[23].
- **No rellenar formularios con nuestros datos personales en páginas web que no sean seguras.** Las páginas seguras tienen una URL que comienza como **https://**, mientras que las páginas web normales comienzan por **http://** Algunos navegadores indican si la página es segura mostrando la imagen de un candado.



Candado mostrado por el navegador Firefox en la Wikipedia.

- **Desconfía de los correos electrónicos en los que se le envíe un enlace a un formulario donde se le pidan sus datos bancarios.** Asegúrate, en todo caso, de que la página a la que se le ha dirigido es segura y que es realmente de la entidad bancaria en cuestión. En la mayoría de los casos no se trata de un mensaje de una entidad bancaria real, sino de una práctica de búsqueda de datos personales conocida como **fishing**[24].
- **Destruye la información en papel que contenga datos personales antes de tirarla a la basura.** Esta información podría ser utilizada por terceras personas para introducirse en un sistema infromático ajeno mediante **trashing**[25] e **ingeniería social**[26].

22 Por ejemplo: un premio en un concurso en el que no hemos solicitado participar, imágenes o vídeos pornográficos, ofertas de empleo de origen desconocido, o cualquier otro contenido que pueda ser un cebo.

23 A menudo el adjunto (un archivo de texto, un vídeo, una fotografía, etc) está infectado con malware. Algunos tipos de malware tienen la capacidad de buscar los contactos de correo electrónico y enviar correos infectados a todas las direcciones que encuentre.

24 En inglés "ir de pesca". Los sistemas de webmail suelen incorporar filtros que desvían estos mensajes a la bandeja de spam (correo no deseado) pero no siempre funcionan: a veces permiten el paso de estos correos infectados hasta las bandejas de recepción de correos y otras envían a la bandeja de spam mensajes importantes (por eso conviene revisar la bandeja de spam de vez en cuando).

25 "Buscar en la basura": albaranes, facturas, expedientes y otros documentos aparentemente sin importancia pueden contener información personal utilizable por terceras personas.

26 A partir de unos pocos datos personales (obtenidos, por ejemplo, de documentos abandonados en la basura) es posible convencer a una persona de que está recibiendo una llamada telefónica de una empresa, institución o similar y utilizar su confianza para obtener así más información. El objetivo final suele ser el acceso remoto a un sistema informático o una suplantación de identidad.

- **No uses claves fáciles de averiguar** como su número de teléfono o fecha de cumpleaños. No las escribas en papel ni las comparta con otras personas.
- **Habilita, siempre que puedas, sistemas de autenticación en dos pasos (2FA).**
- **No te deshagas de soportes de memoria (discos duros, pendrives, etc) sin asegurarte de haberlos borrado primero**, ya que podrían contener información personal. Lo más seguro es su formateo, ya que el simple borrado no elimina realmente la información[27].
- **Desconfía de soportes de memoria (pendrives, CD, DVD) de procedencia desconocida.** Podrían estar infectados[28].

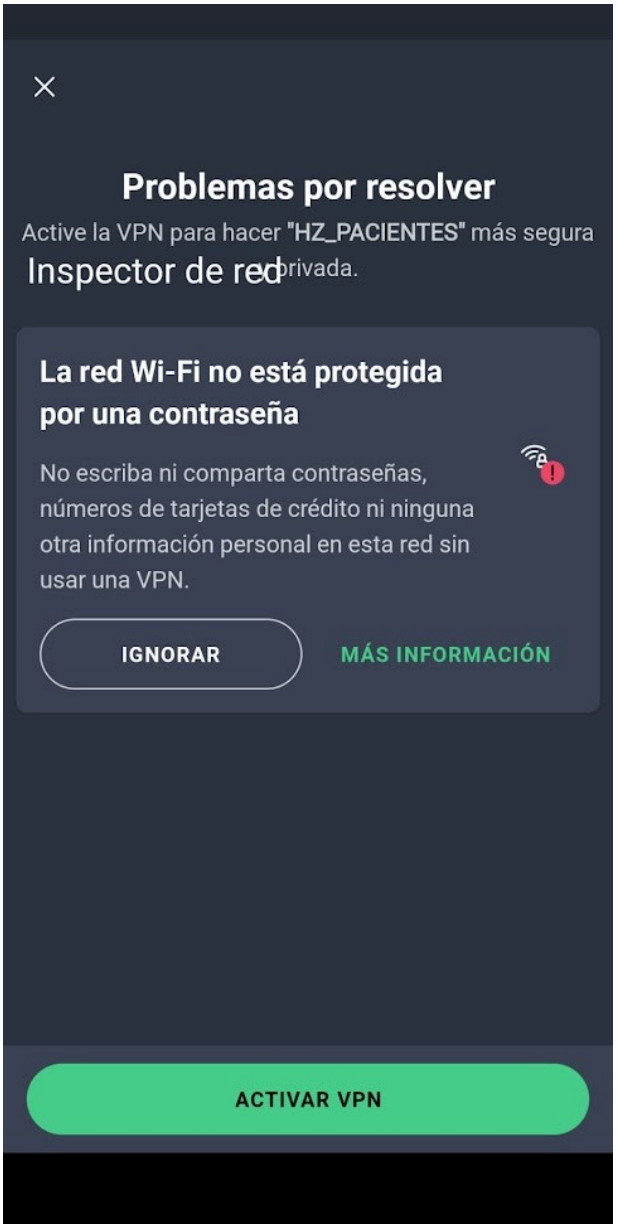
- **Guarda sus tarjetas en carteras con protección contra RFID**, o estarás expuesto a que te roben dinero simplemente acercando un dispositivo de lectura a su bolsillo.

Las tarjetas con tecnología RFID permiten realizar pequeños pagos simplemente con acercarlas a un lector, pero esto constituye un riesgo ya que un lector (oculto en un bolso, por ejemplo) podría aproximarse lo suficiente a la tarjeta como para realizar un cobro sin que el titular de la tarjeta fuese consciente de ello. Existen carteras que protegen a las tarjetas contra este tipo de actos.

- **No te conectes a redes WiFi abiertas (son habituales en grandes superficies, bares, restaurantes, etc) sin tomar precauciones.** En caso de hacerlo es conveniente, al menos, utilizar un **Red Privada Virtual (VPN).**

27 Cuando "borramos" un archivo informático de un disco duro la información de dicho archivo, en realidad, no es borrada. Lo que hace el ordenador es eliminar las señales que localizan el archivo y dejar esa zona del disco duro como disponible para ser reescrita. Una búsqueda detallada de la información almacenada en el disco duro podría, en teoría, recuperar ese archivo que el sistema considera borrado. El formateo, sin embargo, elimina totalmente la información (recientemente fue objeto de juicio en los tribunales el caso de unos discos duros que fueron formateados 35 veces para eliminar la información que contenían).

28 Un viejo truco consiste en abandonar un pendrive infectado en una mesa de una cafetería frecuentada por los empleados de alguna gran empresa u organismo administrativo. Si uno de los empleados encuentrta el pendrive y, movido por la curiosidad, lo intenta abrir desde su puesto de trabajo podría dar acceso remoto a la persona que abandonó el pendrive en la cafetería.



Recomendación que aparece en mi smartphone al detectar la WiFi del Hospital de Zafra

Las **VPN (Virtual Private Network, Red Privada Virtual)** son sistemas que conectan nuestros equipos a una red virtual que funciona como si fuese una red local y, a través de ella, a Internet. De esta forma se consiguen varios objetivos:

- **Añadir una capa de seguridad adicional a nuestra navegación.** A efectos prácticos es como si estuviésemos navegando dentro de una Intranet.
- **Nuestro proveedor de acceso a Internet no va a poder controlar el tipo de información a la que tenemos acceso o que enviamos a través de la red (pero el gestor de la VPN sí: cuidado).**
- **Los servidores de Internet nos percibirán como si estuviésemos conectando desde el lugar donde esté situado el servidor VPN**, lo que nos permitirá saltarnos algunos bloqueos geográficos. De esa forma es posible, por ejemplo, acceder desde un país a servicios de Internet que no están accesibles para quienes se conecten desde ese país, pero sí para quienes se conecten desde el país donde está el servidor de la VPN.

NAVEGACIÓN SEGURA

Configuración básica de un navegador web

Un navegador o *browser* es un software que lee HTML y muestra su contenido como lo que conocemos como website. Durante la navegación, además, puede almacenar datos de distintos tipos, de los que algunos de los más importantes son los siguientes:

- **Historial**: un registro de las páginas web visitadas.
- **Cookies**: datos de todo tipo recogidos al visitar cada página web. Suelen ser una recopilación de las preferencias del usuario, búsquedas realizadas, compras, etc.
- **Usuarios y contraseñas**: son datos introducidos por el usuario para identificarse en un servicio web. Por comodidad suelen guardarse en la memoria del ordenador para no tener que volver a ser introducidas en cada visita.

Estos datos, almacenados en el ordenador del usuario, tienen como función principal facilitar la navegación. Pero el acceso a dichos datos por otras personas pueden aportar información más o menos importantes sobre:

- Nuestros usuarios y contraseñas.
- Las páginas web que visitamos.
- Las compras que realizamos, etc.

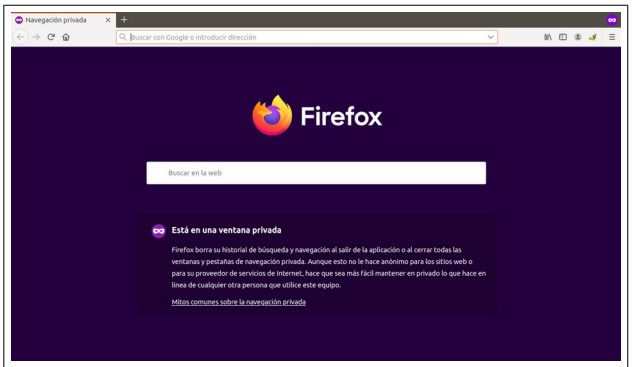
Es por eso que los navegadores pueden ser configurados para:

- Admitir o rechazar cookies.
- Guardar o rechazar el historial y las contraseñas.

También es posible el borrado de toda esta información en cualquier momento.

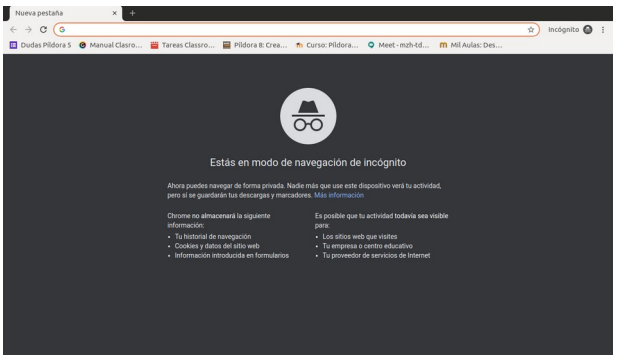
También es posible abrir una sesión de navegación "oculta" en la que, por defecto, el navegador no almacena ningún dato en la memoria del ordenador del usuario.

Sin embargo este tipo de sesiones no puede evitar almacenar datos de la visita en servidores externos (la IP[29], por ejemplo), por lo que la privacidad no es total.



Ventana de *navegación privada* en Firefox

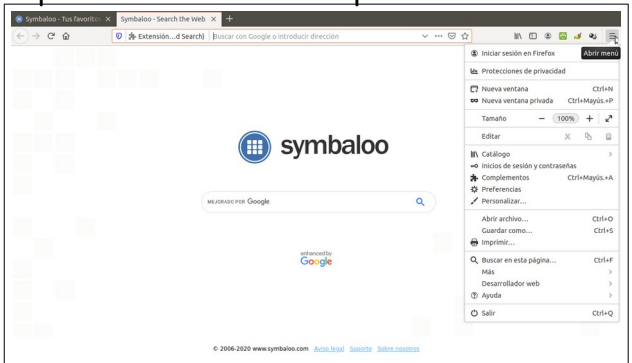
29 Un número que localiza nuestro ordenador en la red de manera similar a como lo hace un número de teléfono.



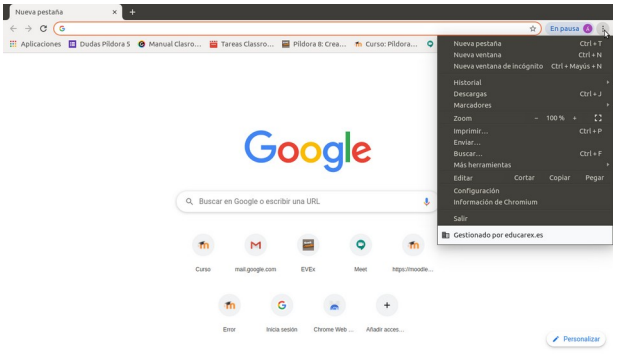
Ventana de *navegación de incógnito* en Chromium

Chrome, el navegador al que Chromium imita en su código, también ofrece una navegación de incógnito. Pero recientemente se hizo público el hecho de que Google estába recopilando datos cuando se suponía que no lo hacía.

El acceso a la configuración de un navegador y a la navegación oculta suele estar, en un ordenador, en la esquina superior derecha de la pantalla.



Acceso a la configuración de Firefox



Acceso a la configuración de Chromium

ARTÍCULOS RECOMENDADOS:

En El kiosko de la navegación por Internet puedes encontrar más consejos para navegar por Internet.

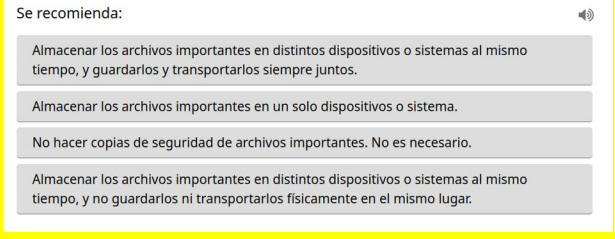
Configuración básica de un usuario de redes sociales

La configuración de un usuario de redes sociales es muy extensa, pero hay algunas recomendaciones:

- **La contraseña no debería ser algo fácil de imaginar**, como la fecha del cumpleaños, el número de teléfono o el DNI.
- **Aceptar que las notificaciones se envíen a una cuenta de correo podría saturar esa cuenta.**
- **Para desvincular las opiniones personales de los posicionamientos de alguna institución o colectivo** con el que se esté relacionado se suele indicar en la "bio" la expresión "Mis opiniones son solo mías" o similar.

- **El colectivo trans está normalizando la costumbre de indicar, en la "bio", los pronombres utilizados por esa persona para indicar su identidad de género**[30]. De esta forma las mujeres incluirían el pronombre "ella", los hombres "él", y algunas personas no binarias[31] prefieren "elle". Hay quien los indica, también, en inglés.
- **Algunas plataformas tienen un tipo de cuenta especiales** para personas de cierta relevancia social (políticos, cantantes, deportistas, etc) que funcionan de forma diferente a los usuarios normales. Otras plataformas permiten certificar la autenticidad de la cuenta para que el resto de los usuarios puedan diferenciar la cuenta real de otra falsa.

JUEGO:



Ciberseguridad (Licencia MIT 2025 Ángel Vázquez Hernández)

ARTÍCULOS RECOMENDADOS:

En El kiosko de las redes sociales puedes encontrar noticias y otros artículos de interes sobre redes sociales.

Gracias por tu atención. Puedes dejar un comentario en mi libro de visitas.

30 Aunque comenzaron haciéndolo las personas trans algunes activistas han pedido a las personas cis que hagan lo mismo para, al normalizar su uso, deje de ser una costumbre que señale a las personas trans.

31 No todas y no siempre. Hay personas no binarias que usan pronombres masculinos o femeninos.