GUÍA DE AUTODEFENSA DIGITAL

Enxeñería Sen Fronteiras

Índice general

1 La importancia de la ciberseguridad en nuestro día a día

¿Por qué hacemos esta guía? Vivimos en un mundo que, con su parte buena y su parte mala, se va moviendo hacia el lado digital a pasos agigantados, y en ocasiones dejando a mucha gente atrás. Este mundo digital, al igual que el presencial, también tiene una serie de riesgos de los que protegerse. Muchas de vosotras quizás tenéis a esa persona de confianza (hija, sobrina, amiga...) a quien consultarle dudas o pedir consejo en cosas relacionadas con las tecnologías de la información (TIC), pero no todo el mundo tiene esa opción. Es por eso que hacemos esta guía, explicando de forma clara y detallada cómo puedes mejorar tu seguridad digital, tengas o no conocimientos previos de ciberseguridad. Antes de comenzar, es importante tener claro que **la seguridad absoluta no existe**, y siempre hay riesgo. Lo que podemos hacer como personas usuarias es poner barreras que nos protejan.

Esta es una guía dinámica. Es decir, la iremos actualizando a medida que nos vayan llegando sugerencias. En este enlace podrás consultar siempre la última versión de la guía en formato PDF. Y en este otro enlace podrás encontrarla en formato editable, por si quieres reutilizarla o contribuir a ella. Permanece atenta a nuestras redes, ya que a lo largo de los próximos meses iremos realizando charlas y talleres para dar a conocer la guía, explicando los distintos apartados de forma sencilla y ayudándote de forma práctica a implementar los consejos que damos en ella. También nos puedes contactar si quieres organizar algún coloquio en tu zona, asociación o grupo.

2 Alternativas libres y encriptadas

Figura 2.1: Peha-Banquet-Degooglisons-CC-By por Peha está licenciada bajo CC BY-SA 4.0.

¿Sabías que es posible vivir sin emplear herramientas que no sean de Google o de Microsoft? Te preguntarás qué tiene de malo usar este tipo de herramientas, tan empleadas hoy en día por el conjunto de la población. En este caso el problema no es tanto de seguridad (que también), sino que más bien se trata de un tema de privacidad. Estas compañías, como muchas otras, ofrecen gran parte de sus servicios completamente gratis. Sin embargo, como se suele decir, si el producto es gratis, en muchas ocasiones el producto eres tú.

Estas compañías recopilan una elevada cantidad de datos de las personas usuarias de su servicio para luego sacarles rentabilidad a través de publicidad, venta a terceras partes, etc. Hay ejemplos claros, como el de Cambridge Analytica donde grandes empresas como Meta (la antigua Facebook) empleó los datos de sus miles de usuarias para luego influir en los resultados del BREXIT o de las primeras elecciones de los Estados Unidos de América

en las que salió elegido Donald Trump. Por otra parte Google y Amazon colaboraron con el estado genocida de Israel en la identificación de objetivos dándole acceso a sus servicios en la nube. Y como estos muchos ejemplos más. Y te preguntarás, ¿qué alternativas tengo? Pues ahí es donde entran los servicios libres.

Antes de comenzar hay que dejar una cosa clara. Ni todas las aplicaciones gratis son libres, ni todas las aplicaciones libres son gratis. El concepto de libertad está directamente relacionado con el respeto a la privacidad de las personas usuarias. Un *software* es libre cuando se puede ejecutar, copiar, distribuir, estudiar, modificar y mejorar. Por lo tanto, el simple hecho de que una aplicación sea gratis, no quiere decir que sea libre.

Además, aunque en muchos casos sucede, que una aplicación sea libre no quiere decir que sea gratuita. Hay aplicaciones libres que ofrecen un servicio completamente de pago, o que ofrecen una versión gratuita con limitaciones. Sin embargo, esta versión gratuita tiende a ser más que suficiente para el uso habitual que se le suele dar. Hay que pensar que estas aplicaciones también llegan a tener una serie de costes asociados, como puede ser los servidores a los que nos conectamos de forma gratuita para emplear algún tipo de servicio.

Luego está la importancia de entender bien el concepto de la nube. La nube no es más que un conjunto de ordenadores conectados entre sí. Cuando tú guardas algo en la nube, realmente lo que estás haciendo es guardarlo en un ordenador central (que llamaremos servidor) que está en otro lugar geográfico. Lo mismo sucede cuando envías un mensaje a otra persona. El mensaje no va directo hasta la otra persona, sino que lo que haces es enviarlo a un ordenador central (conocido como servidor), y luego desde ahí se envía a la persona destinataria. En muchas ocasiones, además, una copia del mensaje permanece guardada en el servidor, para que por ejemplo puedas acceder desde otro dispositivo.

Esto es algo que debemos tener en cuenta para comprender la importancia de conceptos como el de que los datos estén encriptados. ¿Y qué es esto de los datos encriptados? Hablamos de servicios encriptados cuando la empresa o entidad que nos ofrece el servicio no tiene acceso de ningún tipo al dato relativo a nuestro uso. En este caso es importante distinguir entre varios tipos de encriptado:

- **Encriptado en tránsito:** los datos están encriptados durante el envío desde nuestro dispositivo hasta el servidor central. Esto permite que aunque alguien intercepte el mensaje o archivo por el camino, no pueda acceder a su contenido.

- **Encriptado en reposo:** los datos son encriptados mientras están en el servidor central. Es decir, la empresa que ofrece el servicio no puede acceder a mis datos almacenados en su servidor. Por ejemplo, un servicio de almacenamiento de imágenes con encriptado en reposo evita que la empresa pueda acceder al contenido de mis fotos almacenadas.

- **Encriptado en el dispositivo:** los datos están encriptados mientras están en nuestro dispositivo. Esto garantiza que otras aplicaciones no puedan acceder a ellos.

Lo importante es emplear servicios que aplican todos esos encriptados de forma simultánea, lo que se conoce como **encriptado de extremo a extremo**, siendo sus siglas en inglés E2EE (*End to End Encryption*). Esto garantiza que la empresa no tiene ningún tipo de acceso a nuestros datos.

También existe la opción de autoalojar nuestros servicios, es decir, en lugar de depender de servidores externos de correo, calendario, almacenamiento, etc., podemos tener

nuestro propio servidor al que acceder remotamente. Relacionado con esto surge el concepto de redes federadas, que consiste en un punto intermedio entre usar un servidor completamente externo y usar tu propio servidor. Esto consiste en comunidades que se ponen de acuerdo para gestionar sus propios servidores, pudiendo estar conectados hasta cierto punto con los servidores de otras comunidades.

Pero claro, te preguntarás: **¿Y qué alternativas tengo?** Pues bien, a continuación vamos a detallar una serie de alternativas libres a algunos de los servicios de Google y Microsoft más empleados hoy en día basándonos en nuestra experiencia, teniendo en cuenta la seguridad y facilidad de uso.

2.1 Grandes conjuntos de herramientas

Antes de comenzar con las distintas alternativas existentes para cada tipo de servicio (correo, navegador, calendario, etc.) vamos a destacar algunos proyectos y conjuntos de herramientas libres que contienen distintas aplicaciones de gran utilidad.

2.1.1 F-Droid

Consiste en un catálogo de aplicaciones libres para Android, es decir, sería una especie de Google Play Store pero que solo contiene aplicaciones libres. Lo podemos descargar directamente desde su web. Durante la instalación nos aparecerán una serie de mensajes de seguridad de los cuales no nos tenemos que preocupar. Algunas de las aplicaciones que se recomiendan en esta guía solo pueden ser descargadas desde F-Droid, por lo que se recomienda su instalación.

2.1.2 Aurora Store

Es probable que en muchas ocasiones no te quede más remedio que instalar alguna aplicación (libre o no), que solo se puede descargar desde la Google Play Store. Aurora Store, disponible en F-Droid, te permite descargar e instalar cualquier aplicación disponible de Google Play Store sin necesidad de disponer de una cuenta de Google, lo que aumenta nuestra privacidad.

2.1.3 Fossify

En todos los dispositivos móviles hay una serie de herramientas imprescindibles independientemente del uso que le vayamos a dar. Estas herramientas son precisamente las que forman el conjunto de Fossify: galería de imágenes, calendario, contactos, notas, gestor de archivos, reproductor de música, SMS, grabadora de voz, cámara, calculadora, alarma, teclado, marcador... Sin duda uno de los proyectos más destacados de herramientas libres para dispositivos móviles, y que no tiene nada que envidiar a las que nos ofrece Google. Fossify surgió como alternativa al conjunto de herramientas Simple Mobile Tools, después de que este último fuese comprado por la empresa israelí ZipApps, la cual introdujo publicidad y opciones de pago.

2.1.4 FramaSoft

Otro componente clave en nuestro día a día son las plataformas colaborativas, siendo Framasoft uno de los principales proyectos actuales en este campo. Es una asociación francesa sin ánimo de lucro fundada en 2004 y que busca *DesGooglizar* internet, ofreciendo un amplio conjunto de herramientas en línea, como un *pad* colaborativo, una agenda colaborativa, servicio de listas de correo, videollamadas o un gestor de eventos, entre muchas otras. En la sección DesGooglisons puedes encontrar las distintas alternativas que ofrecen. Hay que tener en cuenta que estas herramientas no tienen encriptado de extremo a extremo.

2.1.5 Proton

Nació en Suiza en 2014 cuando un conjunto de personal científico del CERN decidió construir una mejor internet basada en la privacidad. Cuenta con un servicio de correo electrónico, calendario, almacenamiento en la nube, gestor de contraseñas y VPN, todos ellos encriptados para garantizar la privacidad de las personas usuarias.

2.1.6 NextCloud

Nextcloud es un conjunto de programas que permiten la creación de servicios de alojamiento de archivos. Su funcionalidad es similar al *software* Dropbox o Google Drive, con la diferencia de que Nextcloud es libre. Cuenta con muchas herramientas, como edición de documentos de forma colaborativa, notas, tablero de tareas, videollamadas, etc. Para poder emplearla hay que instalarla en un servidor propio, o contratar a alguien que ofrezca tal servicio.

2.1.7 Disroot

Disroot es un proyecto radicado en Ámsterdam que ofrece un amplio conjunto de servicios libres. Al igual que sucede en el caso de Framasoft, los datos no están encriptados de extremo a extremo, lo que se debe tener en cuenta a la hora de emplear los servicios. Sin embargo, en algunos casos, esto no tiene por qué ser un problema. En este enlace tienes el conjunto de herramientas que ofrecen.

2.2 Alternativas por tipo de servicio

Una vez presentados cinco de los proyectos más destacados de herramientas libres (hay muchos más), toca pasar a las alternativas específicas para cada servicio.

2.2.1 Herramientas para ahorrar usando la nube

Cuando empleamos servicios en Internet proporcionados por terceras partes, exponemos nuestra privacidad trasladando información sobre nuestras actividades a las entidades que gestionan el servicio, a las que gestionan los recursos informáticos empleados y a las operadoras de las redes de telecomunicación por las que viaja la información.

Además, en muchos casos puede suponer un gasto innecesario de recursos: si enviamos una foto a una persona que está sentada a nuestro lado empleando el servicio

de mensajería de moda, haremos que la foto viaje a servidores de EE. UU. para regresar nuevamente deshaciendo el camino hasta llegar al teléfono de la persona destinataria.

Existen herramientas libres que nos permiten compartir contenidos con otras personas, o mantener sincronizadas carpetas en diferentes dispositivos minimizando la exposición de nuestra privacidad y el consumo de recursos necesarios en la red Internet.

LocalSend Es una aplicación que puedes emplear en tus ordenadores y teléfonos para enviar puntualmente todo tipo de contenidos de un dispositivo a otro. Solo funciona entre dispositivos que estén conectados en la misma red y tengan instalada la aplicación. Los datos enviados viajarán de uno a otro dispositivo sin pasar por Internet, reduciendo los riesgos de privacidad y los recursos consumidos, y evitando que la saturación en los recursos de Internet afecte a la velocidad del envío.

Es una buena opción para enviar archivos puntualmente entre tus dispositivos o a los dispositivos de las personas con las que sueles compartir espacio (misma red WiFi).

Syncthing Permite mantener sincronizado el contenido de carpetas en diferentes dispositivos, ya sean ordenadores o teléfonos móviles. Los dispositivos pueden estar en la misma red o en diferentes lugares del planeta. Syncthing busca el camino a través de Internet para conectarlos y sincronizar los contenidos. Los requisitos son que los dispositivos a sincronizar estén encendidos simultáneamente el tiempo necesario para sincronizar los datos. Si los datos se sincronizan en más de dos dispositivos, Syncthing irá sincronizando la información puntualmente en los dispositivos que permanezcan encendidos en cada momento.

Syncthing emplea una tecnología similar a la red Torrent, con lo que consigue sincronizar solo las partes de la información que cambian en cada momento sin necesidad de enviar nuevamente el archivo entero. Además, tarda el mismo tiempo en sincronizar dos ordenadores o veinte, lo que lo hace muy interesante para compartir carpetas con contenidos cambiantes entre grupos o equipos de personas.

Puede ser una buena opción para compartir carpetas entre grupos de personas de manera eficiente y privada o para mantener sincronizados contenidos entre tus propios dispositivos.

FreeFileSync Herramienta multiplataforma (GNU/Linux, Android, Windows y Mac) para la gestión de copias de seguridad. Simplemente le tienes que indicar de qué carpeta quieres hacer una copia de seguridad y dónde quieres hacerla, y automáticamente hace la copia de seguridad de los archivos nuevos. En esta sección de su web explican los diferentes modos que tiene la aplicación para realizar las copias de seguridad. Y en su web también tienen una serie de tutoriales explicando el funcionamiento de la herramienta.

2.2.2 Correo electrónico

Proton Mail Es el servicio de correo perteneciente al conjunto de Proton. Está cifrado de extremo a extremo para garantizar la privacidad de los datos, y el plan gratis consta de 1 GB para almacenamiento. Esto es más que suficiente, especialmente si se mantiene limpia la bandeja de entrada. En caso de ser necesario consta de varios planes de pago para aumentar el espacio disponible.

Tuta Mail Tuta es otra de las grandes alternativas de correo electrónico cifrado de extremo a extremo. El plan gratis ofrece 1 GB de almacenamiento. Además, el plan gratis solo permite crear una cuenta de correo por persona.

Thunderbird Cuando hablamos de correo electrónico es necesario diferenciar entre servicio de correo y cliente (la aplicación donde lo consultamos). En el caso de Proton, nos ofrece tanto el servicio de correo como el cliente para este servicio, como en el caso de Gmail. Sin embargo, en ocasiones tenemos otros correos que queremos llevar en nuestro dispositivo móvil, como puede ser el correo de la universidad o el del trabajo. Es aquí donde aparece Thunderbird, un cliente de correo libre para consultar los correos en nuestro móvil o en el ordenador. Cabe destacar que está desarrollado por la Fundación Mozilla, más conocida por su navegador web: Firefox.

Fair Email Solo disponible para Android. Es un cliente de correo electrónico, no ofrece servicio de correo.

2.2.3 Calendario

Proton Calendar Como os podréis imaginar, también pertenece al conjunto de Proton, y también está encriptado. Tiene todas las funciones que se suelen necesitar de un calendario: accesible en línea, creación de eventos colaborativos (incluso con personas que no usen Proton), recordatorios, etc.

Tuta Calendar Al igual que en el caso del correo, Tuta es otra de las alternativas de correo en la nube encriptado.

Calendario de Fossify Al igual que en el caso del correo electrónico, cuando hablamos de calendario hay que diferenciar entre servicio y cliente. Proton Calendar nos ofrece un servicio de calendario y un cliente para este servicio, pero puede darse el caso de que tengamos otros calendarios *online* asociados por ejemplo a la cuenta del trabajo. Y es aquí donde entra el Calendario del conjunto de Fossify permitiéndonos ver y editar esos otros calendarios.

Calendario de Nextcloud Herramienta del entorno Nextcloud que permite crear calendarios colaborativos. Ideal para cuando necesitas compartir un calendario públicamente. Para emplearlo puedes instalar NextCloud en un servidor o emplear una de las múltiples instancias en abierto, como framagenda.org o la de Disroot.org.

Framadate Framadate no es un calendario como tal, sino una herramienta para decidir la fecha para un determinado evento.

2.2.4 Mensajería instantánea

Matrix Otro de los servicios imprescindibles es el de la mensajería instantánea. Matrix es un protocolo de comunicación seguro, descentralizado y encriptado para mensajería. Para ser empleado es necesario instalar alguno de los clientes (una aplicación)

que indican en su página. Element es uno de los clientes más conocidos y empleados. Es multiplataforma, pudiendo ser empleado tanto desde el ordenador como desde un dispositivo móvil. Un detalle a tener en cuenta es el hecho de que no se requiere un número de teléfono móvil para registrarse. Una de las ventajas del servicio de Matrix sobre el siguiente, Signal, es que Matrix permite la descentralización del servicio. ¿Y qué es esto de la descentralización? De eso hablamos en detalle en el capítulo 3.

Signal Es un servicio de mensajería instantánea para móviles que destaca por el protocolo de encriptado propio, disponible en abierto. Permite crear tanto grupos como conversaciones privados. Para registrarse es necesario introducir un número de teléfono móvil.

¿Por qué no incluimos **Telegram**? Consideramos que Telegram no se puede considerar una herramienta de comunicación segura, ya que no es encriptada de extremo a extremo. Sí que es cierto que tiene la opción de conversación segura entre dos personas que sí que es encriptada de extremo a extremo, pero por defecto las conversaciones entre dos personas no son en este modo seguro. Además, las conversaciones de grupos no tienen opción de ser encriptadas de extremo a extremo.

2.2.5 Videollamadas

Jitsi Algo que se volvió muy habitual en nuestro día a día son las videollamadas, y parece que vino para quedarse. Jitsi permite la conexión por vídeo y audio, la grabación de las sesiones, chat interno y muchas otras funciones. Se puede autoalojar en un servidor propio o usar uno de los múltiples servidores que hay en abierto, como el gestionado por el propio equipo de Jitsi. No es necesario instalar nada para emplearlo. La gente de Disroot también ofrece un servidor.

BigBlueButton Probablemente el servicio de videollamadas libre más potente. Está especialmente pensado para el sector educativo, aunque es empleado también en el resto de campos. Permite también la comunicación por vídeo y audio, además de una ventana en la que ir mostrando una presentación en PDF sin necesidad de compartir pantalla, especialmente útil en situaciones con baja velocidad de internet. También cuenta con una opción para grabar las sesiones. Para usarla es necesario instalarla en un servidor o bien buscar algún servidor abierto.

VDO.Ninja Aunque la herramienta está más pensada para compartir nuestra cámara web con otro dispositivo, también permite emplearla para hacer videollamadas. Tiene la ventaja de que el vídeo se transmite punto a punto, sin sobrecargar el servidor (que solo sirve para poner en contacto a las partes). Cuando creamos una sala nos permite editar una serie de parámetros como si le pedimos a la gente que ponga un nombre que se muestre en la pantalla. Para emplearla podemos usar la propia instancia oficial o alguna que haya en abierto.

2.2.6 Ofimática

LibreOffice La *suite* de ofimática libre más conocida y potente. Contiene todo tipo de herramientas: editor de texto, hoja de cálculo, presentaciones, etc. A algunas de vosotras os sonará también OpenOffice, pero este es un proyecto abandonado, y se recomienda cambiar a LibreOffice. Además, si es vuestra primera vez con LibreOffice, o si queréis profundizar un poco más, tienen un conjunto de guías muy útiles.

OnlyOffice Otra *suite* de ofimática libre, menos conocida y potente. Contiene también todo tipo de herramientas: editor de texto, hoja de cálculo, presentaciones, etc. La interfaz gráfica es más similar a la de Microsoft Office. Una de las principales desventajas es que no emplea formatos libres de archivos, sino que emplea los formatos de Microsoft.

PDF Arranger Herramienta de escritorio para unir varios PDF. También permite convertir imágenes a PDF.

2.2.7 Ofimática colaborativa

Etherpad Editor en línea colaborativo, permitiendo a múltiples personas editar a la vez un documento. Para emplearla, o bien se instala en un servidor desde cero, o bien se emplea alguna de las múltiples instancias que hay disponibles, como la de Framapad o el *pad* de Disroot. En este caso los *pads* no están encriptados.

Cryptpad Otra de las herramientas para editar de forma colaborativa, en la que en este caso los *pads* están encriptados de extremo a extremo. También permite crear hojas de cálculo, tableros *kanban*, etc. Para emplearla sin instalarla en un servidor, puedes emplear una de las múltiples instancias en abierto, como la oficial del equipo de Cryptpad o el Cryptpad de Disroot.

Framacalc Herramienta de hojas de cálculo colaborativo ofrecida por la gente de Framasoft. Las hojas de cálculo se eliminan después de 335 días de inactividad (sin acceso y/o sin modificación), para evitar el crecimiento de la base de datos indefinidamente. Además, solo pueden contener un máximo de 100.000 filas y no es posible crear hojas de cálculo de varias hojas ni importar archivos OpenDocument o Microsoft Office. Y por motivos de seguridad, no se pueden eliminar hojas de cálculo a simple solicitud.

2.2.8 Formularios

Liberaforms Herramienta para crear formularios en línea. Permite exportar las respuestas a una hoja de cálculo, activar las notificaciones de correo, etc. Para emplearla, se puede instalar en un servidor o emplear una de las instancias en abierto, como las que ofrece el propio equipo de Liberaforms (gratis, pero limitadas a 250 respuestas por año): usem.liberaforms.org, my.liberaforms.org o erabili.liberaforms.org. También tienen planes de pago que permiten un mayor número de respuestas. Tanto en el plan gratis como de pago, se puede configurar que las respuestas se almacenen de forma

encriptada. La gente de Framasoft también ofrece una instancia (en fase beta) basada en Liberaforms.

Yakforms **Yakforms** Yakforms es otra de las herramientas para crear formularios en línea. Para emplearla puedes instalarla en un servidor o utilizar unas de las múltiples instancias en abierto, como la de Framaforms.org (del equipo de Framasoft). Framaforms tiene un límite de 200 formularios por cada cuenta y de 5000 respuestas por formulario. Además, cada uno de ellos dura 6 meses.

2.2.9 Notas

Standard Notes Una de las alternativas más conocidas. Se puede trabajar de forma local, o crear una cuenta gratis y guardar las notas encriptadas de extremo a extremo en su servidor, de forma que podamos acceder a ellas desde otros dispositivos. Tiene un plan de pagos que incluye una serie de funciones extras.

NotesNook Aunque quizás menos conocida que la anterior, es una alternativa muy potente. Las notas también están encriptadas de extremo a extremo, y el plan gratis incluye alguna función más que en el caso anterior. Como siempre, es cuestión de probar y ver cuál cumple nuestros requisitos.

Joplin Esta es otra de las opciones más destacadas. A diferencia de las anteriores, no permite la sincronización en la nube gratis, para lo que habría que suscribirse o bien autoalojarla en un servidor.

2.2.10 Mapas

Open Street Map Es una iniciativa para crear y proporcionar información geográfica de forma libre, y no solo mapas de las calles. Para ser empleados desde el móvil es más fácil si empleamos una de las múltiples aplicaciones que lo usa como fuente de información geográfica.

OsmAnd Probablemente la aplicación más potente para emplear Open Street Map en nuestro dispositivo móvil. Dispone de un montón de herramientas, como descargar los mapas para consultarlos sin internet, navegador para el coche, seguimiento de rutas, editor del propio Open Street Map y muchas más.

CoMaps Aunque con menos opciones que OsmAnd, es otra alternativa muy recomendable para emplear Open Street Map en nuestro móvil de forma más sencilla. Es un *fork* de OrganicMaps gestionado por la comunidad, y que surgió por problemas de gobernanza.

uMap En ocasiones puede que necesitemos compartir un mapa con puntos señalados o formas dibujadas. Aquí es donde entran herramientas como uMap. Para emplearla, se puede instalar en un servidor o emplear instancias como umap.openstreetmap.fr o framacarte.org.

2.2.11 Navegador web

Firefox Es uno de los navegadores más potentes y conocidos, y es libre, siendo gestionado por la Fundación Mozilla. A diferencia de otras opciones no libres, destaca por un menor consumo de recursos, además del respeto de la privacidad de las personas usuarias.

TOR Si quieres ir un paso más allá, la red Tor proporciona un paso extra de privacidad desviando tu conexión por múltiples puntos, lo que dificulta más el seguimiento de tus búsquedas. En el capítulo 6 explicamos con más detalle el funcionamiento de la red TOR.

2.2.12 Buscador web

Startpage Una de las más conocidas y empleadas. Su sede está en los Países Bajos, estando sometida a la normativa europea de protección de datos. Los resultados obtenidos se basan principalmente en el buscador de Google. Sí, esto puede sonar raro teniendo en cuenta que estamos hablando de herramientas alternativas a Google. Sin embargo, Startpage asegura no almacenar información personal como la dirección IP o historial de búsqueda.

SearX Otra opción es la de Searx, un metabuscador descentralizado. A diferencia de los anteriores, no consiste en un buscador en sí, sino que recoge las búsquedas obtenidas por múltiples buscadores como DuckDuckGo, Google, Bing, Startpage... Esto hace más complejo hacer un seguimiento de la persona usuaria. Como punto negativo está que en ocasiones alguno de los buscadores que emplean lo bloquea temporalmente. Para probarlo puedes probar una de las múltiples instancias disponibles.

2.2.13 Almacenamiento en la nube

Proton Drive Otro de los servicios del conjunto Proton es Proton Drive, que permite almacenar archivos en la nube de forma segura, estando estos encriptados de extremo a extremo. En el plan gratuito contamos con 5 GB, ampliable a través de planes de pago. Su sede y los servidores se encuentran en Suiza. Su seguridad está auditada externamente, lo que quiere decir que una empresa o entidad externa a Proton ha analizado la seguridad de sus servidores.

Filen.io El plan gratuito ofrece 10 GB de almacenamiento encriptado de extremo a extremo. Los servidores y su sede están en Alemania. Es multiplataforma, teniendo versión del cliente para GNU/Linux, Android, iOS, Mac y Windows, además de cliente web. No está auditada externamente.

Internxt Drive Internxt es una plataforma de almacenamiento en la nube centrada en la privacidad, con cifrado de extremo a extremo. El plan gratuito ofrece 1 GB de almacenamiento para siempre, con planes de pago disponibles de hasta 10 TB. La seguridad está auditada externamente. Los archivos cifrados se almacenan en la UE: Francia, Alemania y Polonia. La empresa tiene su sede en España.

Internxt Send A veces solo necesitamos la nube para enviarle a alguien de forma remota un archivo de gran tamaño. Para estos casos, la gente de Internxt tiene este servicio que, en el plan gratuito, nos permite enviar archivos de hasta 5 GB, que están disponibles para descarga durante 15 días, siendo eliminados pasado ese tiempo. Hay que tener en cuenta que en este caso cualquier persona con el enlace podría ver los archivos, por lo que si es información privada se recomienda emplear los otros servicios comentados en esta sección, o protegerlos de forma local con contraseña.

OnionShare OnionShare es una herramienta que te permite compartir archivos de forma segura a través de la red TOR, entre otras funciones. En este caso, tanto la persona que envía el archivo como la que lo recibe deben instalar la aplicación.

Cryptomator Cryptomator es una alternativa intermedia. No ofrece un espacio de almacenamiento como tal, sino que permite emplear servicios de almacenamiento en la nube no privados como Google Drive encriptando los datos de forma sencilla antes de subirlos. Es multiplataforma y gratuito, salvo la versión de Android disponible en las tiendas de aplicaciones, que requiere un pago único para poder usarla.

2.2.14 Gestor de contraseñas

Bitwarden Es uno de los gestores de contraseñas más conocidos y seguros. Es multiplataforma, pudiendo emplearlo tanto en el ordenador como en dispositivos móviles, consta de función de almacenamiento de contraseñas (las cuales se almacenan de forma encriptada), de generación automática de contraseñas seguras, y de envío de texto de forma encriptada. Muchas veces tendemos a emplear contraseñas sencillas, repitiéndolas en múltiples sitios web, lo que disminuye nuestra seguridad en la red. El uso de gestores como Bitwarden mejora nuestra seguridad, como explicamos en detalle en el capítulo 5.

Proton Pass Herramienta perteneciente al conjunto de herramientas de Proton. Tiene funciones similares a las de Bitwarden.

2.2.15 Autenticación en dos pasos (2FA)

FreeOTP La autenticación en dos pasos está muy relacionada con el uso de los gestores de contraseñas. No hay contraseñas 100 % seguras, por lo que es interesante aumentar las capas de protección, y aquí es donde entra la autenticación en dos pasos. Esto no es más que un código de seis dígitos que tenemos que introducir para iniciar sesión tras introducir correctamente nuestra contraseña. Este es un código temporal que va cambiando, y aquí es donde resulta útil el uso de herramientas como FreeOTP, que nos permiten almacenar estos códigos de forma sencilla.

2.2.16 Organización del hogar

KitchenOwl Aplicación multiplataforma con una serie de funcionalidades útiles para personas que comparten hogar, como la lista de la compra o el registrador de gastos compartidos.

2.2.17 Reproducción multimedia

NewPipe NewPipe es un cliente móvil para ver vídeos de YouTube desde tu móvil sin necesitar los servicios de Google y librándote de toda la telemetría. Además, a diferencia de otras alternativas, tiene la ventaja de que no funciona con la API de YouTube, sino que hace web scrapping de la web, lo que te permite obtener un anonimato real. También permite ver los comentarios, seguir canales y descargar vídeos y/o audios.

AntennaPod AntennaPod es un cliente móvil para escuchar podcasts. Tiene opciones para buscar directamente podcasts dentro de la aplicación, descargar episodios y recibir avisos cuando se publique un nuevo podcast, entre otras.

VLC Reproductor de todo tipo de formatos de vídeo y audio.

2.2.18 Edición multimedia

GIMP (GNU Image Manipulation Program) GIMP (acrónimo de GNU Image Manipulation Program) es un programa de escritorio para la edición de imágenes en formato mapa de bits, como por ejemplo fotografías. Contiene todo tipo de herramientas. Hay disponible un amplio conjunto de tutoriales.

InkScape Inkscape es una herramienta de escritorio de dibujo multiplataforma de código abierto para gráficos vectoriales SVG. Las características de SVG soportadas incluyen formas básicas, caminos, texto, canal alfa, transformaciones, gradientes, edición de nodos, exportación de SVG a jpg, agrupación de elementos, etc. Hay disponible un conjunto de tutoriales.

KDEnlive KDEnlive es un software de escritorio de edición de vídeo. Ofrece una amplia variedad de herramientas para cortar, mezclar y aplicar efectos a los vídeos, además de soportar varios formatos de archivos. Hay disponible un conjunto de tutoriales.

2.2.19 Escaneo de documentos

OSS Document Scanner Herramienta útil para escanear documentos con el móvil y exportarlos a PDF. También permite convertir a PDF imágenes que tenemos en el propio móvil, recortarlas, aplicar filtros para destacar el texto y muchas más.

2.2.20 ¿Necesitas una alternativa para otro servicio?

PrivacyTools.io Amplio catálogo de herramientas que respetan la privacidad de las personas usuarias para distintos tipos de servicio. Nosotros en la guía incluimos aquellas con las que teníamos experiencia y que nos parecieron especialmente útiles, pero en su página podréis encontrar muchas más.

AlternativeTo.net Página útil donde se puede introducir el nombre de la aplicación y encontrar distintas alternativas. Hay que tener en cuenta que no todas las alternativas que muestra son libres. Para ver solo las libres, hay que marcar la etiqueta Open Source.

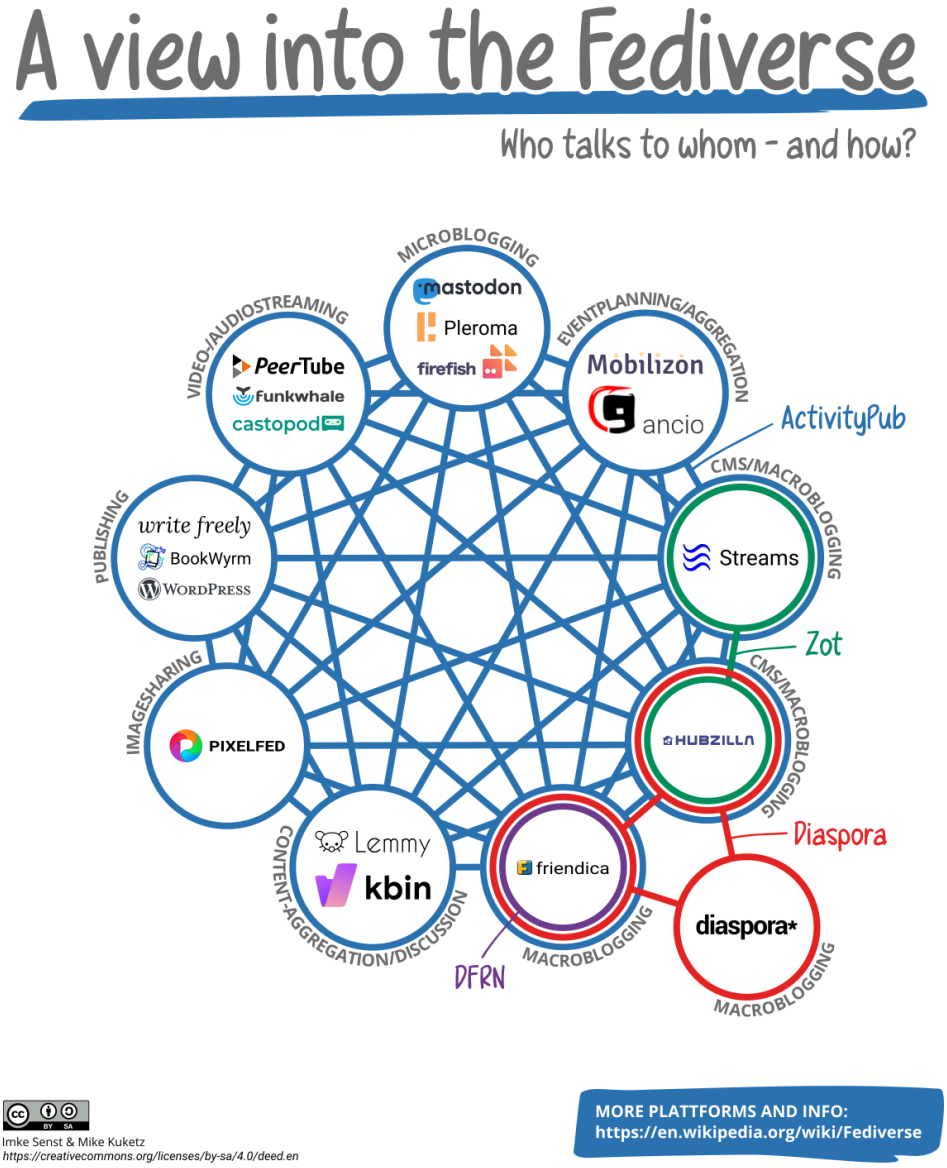
 **Desgooglicemos Internet** Sección de Framasoft que contiene alternativas libres a servicios de Google.

 **CHATONS** CHATONS es el Colectivo de Hosters Alternativo, Transparente, Abierto, Neutral y Solidario (CHATONS son las siglas en inglés). Este colectivo busca dar a conocer estructuras que ofrecen servicios en línea gratuitos, éticos y descentralizados para que sea más fácil encontrar alternativas a servicios ofrecidos por la GAFAM (Google, Apple, Facebook, Amazon, Microsoft) que respeten su privacidad. CHATONS fue iniciado por el colectivo Framasoft en 2016 tras la campaña Desgooglicemos Internet. Tienen esta otra página con alternativas a los principales servicios. Se debe ser consciente del uso que le damos a las herramientas que aparecen, ya que en muchos casos la información no está encriptada de extremo a extremo.

3 El Fediverso: la red social alternativa

Figura 3.1: Degooglisons Internet by David Revoy está licenciada bajo CC BY 4.0.

3.1 ¿Qué es esto del Fediverso?



¿Te imaginas que desde tu cuenta de correo electrónico solo pudieses enviar correos a la gente que usa el mismo proveedor que tú (Gmail, Outlook...)? ¿Y que para enviarle un correo a otra persona que no use el mismo servicio que tú tengas que crearte una cuenta de correo electrónico en su servicio? No, ¿verdad?

Sin embargo, en el mundo de las redes sociales, hasta ahora veíamos normal que para interactuar con la gente de X/Twitter tengas que tener una cuenta en X/Twitter, y que para interactuar con las fotos de alguien que use Instagram, tengas que tener una cuenta en Instagram, adicional a la de X/Twitter, y así sucesivamente con Facebook/Meta, YouTube, TikTok, etc. Aunque en este capítulo nos vamos a centrar en las redes sociales, esto no solo sucede en las redes sociales. Por ejemplo, sucede en las aplicaciones de mensajería. Si solo tienes WhatsApp y le quieres enviar un mensaje a alguien que usa Telegram o Signal, tendrás que crearte una cuenta en esos servicios para poderles escribir. Además, para usar WhatsApp, tu única alternativa es usar la aplicación oficial que te dan, no libre.

El Fediverso precisamente busca romper con esta centralización y que gente con cuentas en diferentes servicios pueda interactuar entre ellas. Para empezar, vamos a aclarar

algunos términos:

- **Cuenta**: Tu cuenta o identidad tiene una dirección única llamada *handle* y está alojada en uno de los muchos servidores, también llamados instancias. Por ejemplo, en el caso de ESF, tenemos una cuenta en el Fediverso con la dirección @esfgalicia@mastodon.gal.
- **Instancia**: Una instancia es básicamente una pequeña red social hospedada en un servidor. Cada instancia puede tener su propio conjunto de reglas sobre qué contenido está permitido. También puedes hospedar tu propia instancia. Cada instancia ejecuta un *software* determinado. Por ejemplo, en nuestro caso la instancia en la que tenemos creada la cuenta es mastodon.gal.
- El *software* usado en una instancia es esencial para la experiencia de la usuaria y sus posibilidades. Entre los *software* más usados se encuentran:
  - **Mastodon**: Uno de los más conocidos. Es un *software* de microblog similar a X/Twitter en cuanto a interfaz y funcionalidades. Microblog significa que tienes un blog con pequeñas (micro) publicaciones que pueden incluir texto, imágenes y vídeo. Normalmente hay un límite de 500 caracteres en las publicaciones de Mastodon.
  - **Peer Tube**: Es un *software* para compartir vídeos similar a YouTube o Vimeo.
  - **PixelFed**: Es un *software* de *photoblogging* similar a Instagram. Tus publicaciones tienen que incluir al menos una imagen y, por supuesto, adicionalmente pueden incluir un texto, *hashtags* o localización.
  - **Lemmy**: Es un *software* para la gestión de foros de internet y un agregador de noticias similar a Reddit. Puedes subir enlaces, imágenes o textos y la gente puede votarlas y comentarlas.
  - **Mobilizon**: Es un planificador de eventos. Puedes crear eventos y añadir localización e información, y la gente puede inscribirse.
- **Protocolo**: Es el conjunto de reglas que hacen que se puedan conectar entre sí diferentes instancias y *software*. El Fediverso emplea el protocolo ActivityPub.
- **Cliente**: Es la aplicación, móvil o de escritorio, que usamos para acceder a nuestra cuenta sin necesidad de usar el navegador (para acceder usando el navegador tendrías que ir a la web de tu instancia, en nuestro caso mastodon.gal, e iniciar sesión allí). A diferencia de las redes sociales tradicionales, donde solo puedes acceder a la red social usando la aplicación oficial que te piden, en el Fediverso existen multitud de aplicaciones (clientes) para acceder a la tuya. La elección de una aplicación u otra depende de los gustos de cada cual: colores, formas de los menús, funcionalidades. Por ejemplo, con el cliente Fedilab puedes acceder a tu cuenta creada en una instancia que emplea el *software* Mastodon, Pleroma, Friendica o Pixelfed.

El Fediverso (*universo federado*) es la suma de todas las cuentas, en todas las instancias usando cualquier *software*, comunicándose entre ellas. El Fediverso incluye más que solo proyectos de redes sociales. Cualquier *software* que se federa mediante uno de los protocolos forma parte del Fediverso. Es decir, desde una cuenta creada en una instancia que emplea el *software* de Mastodon, puedes seguir una cuenta creada en

otra instancia, independientemente de que emplee como *software* Mastodon, PixelFed o Peer Tube, entre otros. Imagina que por ejemplo en tu muro de X/Twitter también te aparecen fotos que sube la gente a Instagram, o los vídeos que suben a YouTube. La de espacio que ahorraríamos en el móvil...

3.2 Ventajas del Fediverso

Una de las grandes ventajas de usar el Fediverso es la descentralización del poder y la eliminación de los monopolios. Si estás leyendo este capítulo es muy probable que te suene un tal Elon Musk. En 2022 compró Twitter por 44 mil millones (*billones* americanos) de dólares. Es bien sabida la deriva que tomó la plataforma en cuanto a censura de contenido, fomento del odio y de la violencia, modificación del algoritmo para fomentar cierto tipo de ideologías, etc. Y todo esto controlado por alguien como Elon Musk. ¿Cuál es la ventaja del Fediverso? Que no hay nadie que lo controle en su conjunto ni se puede comprar. Como mucho, alguien podría llegar a comprar una instancia, pero no el Fediverso en su conjunto, ya que el Fediverso en sí es un protocolo libre. Y de ser el caso, las usuarias solo tendrían que migrarse a otra instancia (sin perder sus publicaciones, ni su contenido, ni sus seguidoras...), y listo. Además, si una instancia comienza a publicar contenido de odio o molesto para el resto de las usuarias del Fediverso, el resto de instancias podrían bloquearla. De esta forma, si la instancia en la que estás bloquea a otra instancia, sus publicaciones ya no te aparecerían y, por encima de todo, esa gente ya no podría interactuar contigo. Y si estás en la instancia a la que bloquean o no estás de acuerdo con el tipo de contenido que se sube, siempre te podrías mudar a otra instancia, ateniéndote a las reglas de cada instancia.

De este modo el Fediverso fomenta la tecnodiversidad entendida, de una manera similar a la biodiversidad, como una variedad de perspectivas técnicas o sociopolíticas imprescindible para la construcción de una sociedad más igualitaria y respetuosa de sus miembros que huya de autoritarismos y se vea orientada hacia el bien común.

Tras la compra de Twitter y la deriva autoritaria que tomó, mucha gente se lanzó a la búsqueda de alternativas. Mucha gente descubrió el Fediverso a través de Mastodon (por su similitud con X/Twitter). Sin embargo, mucha otra se decantó por BlueSky, una red centralizada y propiedad de los mismos individuos que vendieron Twitter a Elon Musk en su momento. Como dijeron nuestros compañeros en un artículo, "ir a Bluesky desde X es, en el ámbito alimentario, como pasar de Nestlé a El Pozo, pero irse al Fediverso es como el consumo en mercados locales".

Otra ventaja del Fediverso es la ausencia de un algoritmo de recomendación de contenido, aunque no todo el mundo defiende que no se incluyan este tipo de algoritmos. Por un lado, es cierto que suena atractivo que alguien ordene por ti de forma automática tu muro para que te aparezcan las publicaciones que es más probable que te interesen, en lugar de verlas todas por simple orden cronológico. Sin embargo, ¿quién va a controlar ese algoritmo? Y sobre todo, ¿qué tipo de sesgos va a tener? Como comentamos al inicio de la guía, es bien sabido el impacto que tuvo el escándalo de Cambridge Analytica en el BREXIT o en la primera elección de Donald Trump, manipulando a las usuarias de Facebook para que votasen a favor del BREXIT y de Donald Trump, respectivamente. Si lo que quieres es no perderte entre tantas publicaciones, existen alternativas como la creación de listas temáticas.

3.3 ¿Y cómo entro en el Fediverso?

Pues es muy sencillo. Simplemente tienes que crearte una cuenta. Para ello, debes elegir una instancia en la que crearla. La gente de imonosxuntas.org tiene un apartado con instancias recomendadas. Una vez escojas una, simplemente tendrás que entrar y crear una cuenta como en cualquier otro servicio de internet que usas en tu día a día y listo. Y luego, si quieres poder acceder a tu cuenta desde una aplicación móvil sin usar el navegador, puedes usar uno de los múltiples clientes disponibles, como por ejemplo Fedilab, Tusky u otras.

Cuando vayas a crear una cuenta en una instancia, lo primero que te van a indicar son las normas específicas de esa instancia: lenguas que puedes usar, tipo de contenido prohibido, etc. Además, hay una serie de costumbres que aplican a todo el Fediverso:

- Si subes una imagen, intenta añadir un texto alternativo en el apartado que te aparece indicado. Ojo, esto no es para hacer de pie de foto, para eso ya está el texto que pones en la publicación. El texto alternativo sirve para describirlas y hacerlas accesibles para personas con dificultades de visión, así que intenta que quede bien explicada.

- Añade una advertencia de contenido cuando publicas información sensible o que pueda resultar desagradable o traumática para otras personas. Esto aplica tanto a imágenes como al texto en sí, y hace que la gente pueda decidir expresamente si quiere cargar ese contenido o no. Para hacerlo, tienes que tocar en el triángulo que aparece debajo de la caja donde se escriben los mensajes.

- Existe una opción para eliminar los mensajes cuando pasa cierto tiempo, y también de definir criterios como por ejemplo que no se eliminen aquellas que marcas con una estrella. Esto lo puedes modificar en los ajustes de la cuenta.

4 La seguridad en la nube. ¿Realmente necesitamos tener todo en la nube?

Seguro que muchas veces has oído hablar del término nube. Ese lugar de Internet donde se pueden guardar infinitos archivos y donde estarán a salvo, ya que nunca se van a perder.

En este capítulo explicaremos con detalle qué es la nube y cómo funciona, para que deje de ser un concepto abstracto y seamos capaces de elegir si queremos usarla o no. A continuación, hablaremos de su impacto, tanto a nivel de privacidad como a nivel ambiental. Por último, haremos una reflexión sobre si realmente es necesaria, y comentaremos algunas alternativas.

4.1 Qué es y cómo funciona

La nube es un conjunto de ordenadores conectados entre sí. De esta forma, cada vez que guardamos algo en la nube, lo estamos guardando en un ordenador central (que llamaremos servidor) que está en otro lugar geográfico. Hay muchos servidores, ya que hay muchas nubes, cada una pertenece a una empresa/entidad. Estos ordenadores, además de guardar todos los archivos que sube la gente (ya sean fotos, vídeos, documentos...), también guardan toda la información que se puede encontrar en Internet. Con esta definición, podría parecer que guardar un archivo en la nube es lo mismo que guardarlo en el ordenador personal (al fin y al cabo, el archivo está en un ordenador). Sin embargo, encontramos grandes diferencias, pues si guardamos un archivo en la nube, podemos recuperarlo desde otro dispositivo. Además, en nuestro ordenador ese archivo puede perderse (nos entra un virus, se nos avería el ordenador, lo perdemos...) y en la nube, aparentemente, no. Veremos esto con detalle.

Para entender el funcionamiento de la nube, explicaremos primeramente cómo funciona una búsqueda en Internet. Supongamos que queremos acceder a la página web https://esf.gal/. Como sabemos, esta página web está almacenada en algún servidor (¡en los servidores se almacena todo lo que está en Internet!). Por lo tanto, después de escribir la dirección en el navegador y pulsar la tecla intro, nuestro ordenador pregunta cuál es el servidor que tiene esa página web, mandando mensajes a través de la red (aire, cables, etc). Una vez que se encuentra el servidor que tiene esa página, este busca en sus discos duros dónde está la página web. Cuando la encuentra, nos la envía de vuelta y ya podemos verla en nuestro navegador. Como sabemos, para que este proceso pueda funcionar es necesario tener conexión a Internet, pues se necesita una red por la que viajen las preguntas para encontrar al servidor y el archivo de vuelta. Si no hay conexión, el navegador nos indicará que no se puede conectar a esa página.

Cuando usamos la nube para un uso particular de almacenamiento de información, el

proceso que ocurre es semejante al de una búsqueda en Internet. Generalmente, para poder guardar algo en la nube, tenemos una cuenta que nos permite hacer este procedimiento. Esta cuenta es necesaria para poder distinguir cuáles son nuestros archivos y que no se mezclen con los de otras personas. Cada cuenta tiene un cierto espacio de almacenamiento en la nube, es decir, no podemos meter todos los archivos que queramos. Esto tiene sentido, pues el servidor necesita reservar espacio en su disco duro para cada persona. Si cada persona pudiese meter lo que quisiera en la nube, el servidor necesitaría tener infinitos discos duros, lo que es inviable. Una vez que tenemos algo en la nube, permanece en ese ordenador central. De esta forma, cada vez que queremos ver ese archivo, solo hay que pedirle al ordenador central que nos lo devuelva. Estos ordenadores están conectados a Internet, por lo que cuando entramos en nuestra cuenta y pulsamos en el nombre del archivo, el servidor nos lo manda por la red para que lo podamos visualizar desde nuestro ordenador. Como lo único que necesitamos es conexión a Internet y nuestro nombre de usuaria y contraseña, podemos acceder al archivo desde cualquier dispositivo y lugar del mundo, algo que no ocurre si está guardado en nuestro ordenador.

Este mismo proceso tiene lugar cuando queremos usar cualquier aplicación o servicio que necesite conexión a Internet (datos o WiFi, por ejemplo) para su funcionamiento. Por ejemplo, en el caso de la mayoría de aplicaciones de mensajería instantánea, los mensajes que se mandan no van de nuestros móviles al móvil de la persona con la que nos estamos comunicando. Esto se debe a que esos mensajes ocupan espacio, por lo que se tienen que guardar en algún sitio. En nuestros móviles no se pueden guardar, ya que no tienen tanta capacidad de almacenamiento. Como ya puedes suponer, los mensajes se guardan en la nube que utiliza la aplicación de mensajería instantánea en cuestión. Cuando mandamos un mensaje a una persona, estamos haciendo lo mismo que cuando subimos un archivo a la nube: desde nuestra cuenta, le mandamos algo al servidor, en este caso, un mensaje. El servidor lo recibe, mira a quién se lo queremos enviar y lo guarda en un espacio que tiene en el disco (asociado a la conversación entre nosotros y esa persona). Una vez que lo tiene guardado, se lo envía a la persona con la que estamos hablando, que recibe el mensaje que le enviamos. De esta forma, el servidor tiene almacenadas todas nuestras conversaciones.

Como dijimos antes, parece que si queremos que un archivo no se pierda, tenemos que guardarlo en la nube, pues está más seguro. Sin embargo, si la nube son ordenadores, ¿no debería estar igual de seguro que en nuestro ordenador? ¿O es que los ordenadores que se utilizan son más potentes o resistentes que los nuestros? En algunos casos puede ser que esto ocurra, pero en general, no es así. El sistema que se utiliza para no perder la información es la duplicación de los datos. Es decir, todos los datos están duplicados en otro servidor. Así, si se avería algún disco duro u ordenador, siempre se podrá usar el otro para coger la información, por lo que no se pierde. Hay que destacar que estos servidores duplicados están en lugares diferentes del mundo, ya que si estuviesen en el mismo lugar y hubiese un incendio, los dos quedarían destruidos, siendo imposible recuperar la información. Es por este motivo por el que se dice que en la nube no se pierden los archivos, pues las grandes empresas tienen mucho poder y dinero para tener réplicas de ordenadores.

4.2 Privacidad

Como vimos, la probabilidad de pérdida de un archivo en la nube es pequeña, y tiene la ventaja de poder acceder a los ficheros desde lugares remotos. Sin embargo, estas ventajas se ofrecen a costa de tener nuestros datos almacenados en un ordenador ajeno. Esto hay que tenerlo muy presente: cada vez que subimos algo a la nube (archivos privados, fotos en redes sociales, mensajes privados...), deja de ser nuestro. Al subirlo, estamos confiando en la nube correspondiente, y dejamos que gestione nuestros archivos como quieran. Recordamos que el lugar donde se almacenan los archivos no deja de ser un conjunto de ordenadores, y como tales, se puede acceder a la información que hay dentro. De esta forma, nuestros datos pueden ser privados en lo que concierne al resto de usuarias, pero ya no para la empresa que los almacena. Aunque hay políticas de privacidad, muchas veces cuando aceptamos un servicio no leemos todo lo que permitimos hacer con nuestros datos. Un ejemplo puede ser aplicaciones que etiquetan las fotos. Para esto, es necesario usar modelos de inteligencia artificial, que necesitan ser entrenados con muchas fotos, y pueden estar usándose nuestras fotos para tal fin.

Tenemos que pensar siempre que cuando guardamos información en la nube, estamos utilizando los servicios de una empresa, muchas veces sin pagar nada, por lo que ellos pueden utilizar esa información como les convenga. Hay que tener cuidado con lo que se guarda en la nube. No es lo mismo guardar trabajos de clase que guardar información personal, como datos bancarios, contraseñas, DNI... De nuevo, tenemos que ser conscientes de que los archivos, una vez subidos, dejan de ser nuestros exclusivamente; hay que saber lo que queremos conservar.

4.3 Impacto ambiental

El lugar donde se encuentran todos estos ordenadores que conforman la nube se llama Centro de Procesamiento de Datos (CPD). Este lugar no solo contiene servidores, sino también sistemas de refrigeración y ventilación (ya que los dispositivos se calientan al usarse), de alimentación eléctrica, de seguridad, de respaldo (tener varias copias del mismo archivo), etc. Como podemos observar, solo en electricidad y refrigeración (agua, aire...) se consume mucha energía, ya que en los CPDs, en función de su tamaño, puede haber desde decenas hasta miles de ordenadores y discos duros. Si a esto le sumamos los componentes necesarios para fabricarlos (plástico, minerales...), el gasto de recursos es inmenso.

Si creamos una cuenta de almacenamiento en la nube, como ya sabemos, el servidor nos tiene que reservar un espacio para nosotros en los discos duros. Si este espacio no llega, la empresa tendrá que comprar más discos duros. Pero cuantos más dispositivos, más calor se concentra, por lo que para que no se averíen, tienen que usar más agua para refrigerar, por ejemplo. Además, tienen que usar más energía para que puedan funcionar todos correctamente.

Debido a esto, hay que ser conscientes del impacto medioambiental que supone el simple hecho de guardar un archivo en la nube en vez de en un ordenador personal.

4.4 ¿Es necesaria?

Tal y como acabamos de ver, la nube tiene puntos positivos y puntos negativos. Podemos pensar que los positivos compensan a los negativos, pero hay muchas otras maneras de obtener las ventajas que nos da la nube.

Si queremos acceder a los ficheros desde otro dispositivo, en vez de guardarlos en la nube, podemos guardarlos en un pendrive, que podemos llevar con nosotros a donde queramos. De esta forma, nuestros archivos siguen siendo privados, y además no necesitamos conexión a Internet para recuperarlos.

En el caso de no querer perder los archivos, podemos tener varias copias en nuestro dispositivo, o comprar un disco duro externo donde vayamos copiando la información de vez en cuando. De esta forma, el impacto medioambiental es mucho menor, ya que nosotros no necesitamos sistema de refrigeración, y siempre tendremos copias a nuestra disposición.

Sobre las aplicaciones, por ejemplo, hay un uso desmedido de la nube. Se está apostando por guardar toda la información, pero la mayoría no se necesita guardar. Por ejemplo, en la aplicación de la linterna, no sería necesario saber el día y hora que la encendemos, pero la mayoría de aplicaciones sí que guardan esta información, y para ello necesitan la nube, porque la capacidad del teléfono no es suficiente.

Para la mensajería instantánea o videojuegos, hay un paradigma que se conoce como *peer-to-peer* (P2P, entre iguales), donde los datos no pasan por un servidor, sino que van directamente desde un dispositivo a otro. Esto lo utilizan algunos para aumentar la velocidad, ya que en los juegos, por ejemplo, emplear un servidor puede disminuir la calidad, ya que cualquier retraso puede afectar a la precisión y experiencia de la jugadora. En el caso de la mensajería instantánea, los mensajes solo permanecerían en el móvil mientras no se cierre la aplicación (almacenados en RAM), o aparecerían solo los últimos mensajes, en caso de que se utilice el almacenamiento del propio teléfono.

En conclusión, debemos analizar el uso que hacemos de la nube, y decidir si realmente la necesitamos, explorando otras alternativas.

5 Contraseñas seguras y autenticación en dos pasos

Las contraseñas seguras y la autenticación en dos pasos son herramientas fundamentales para proteger nuestra privacidad y evitar accesos no autorizados a nuestras cuentas en línea. En un mundo donde las amenazas digitales son cada vez más frecuentes, adoptar buenas prácticas en el manejo de contraseñas e implantar métodos adicionales de verificación se convierte en una barrera esencial contra posibles ataques. En este capítulo, exploraremos las claves para crear contraseñas robustas, gestionar múltiples credenciales de forma segura y emplear la autenticación en dos pasos como una capa extra de seguridad que puede marcar la diferencia.

5.1 Contraseñas seguras

Crear contraseñas seguras es el primer paso para proteger nuestra información personal y evitar accesos no autorizados a nuestras cuentas. Una contraseña débil puede ser descifrada con facilidad a través de técnicas como el ataque por fuerza bruta o la adivinación, dejando expuestos datos sensibles. Y te preguntarás, ¿y qué contraseña es segura? No existen contraseñas 100 % seguras, al igual que no existen cerraduras 100 % seguras. Eso sí, hay unos principios básicos a la hora de elegir una contraseña:

- **No uses la misma contraseña para distintos servicios**: Si empleas la misma contraseña para varios servicios, en caso de que haya una filtración en alguno de ellos, el resto de cuentas que tengan esa misma contraseña quedarán comprometidas. Uno de los métodos básicos para acceder a la cuenta de alguien es probar contraseñas que fueron filtradas en algún momento. Por lo tanto, es importante emplear una contraseña distinta para cada servicio.
- **No uses contraseñas cortas ni que incluyan información personal**: Las contraseñas deben ser lo más largas y complejas posibles. Normalmente tendemos a emplear contraseñas sencillas que nos sea fácil de recordar. Error. Debemos emplear gestores de contraseñas como Bitwarden o Proton Pass (como explicamos en el capítulo 2) que nos permitan emplear contraseñas complejas y distintas, sin preocuparnos por tener que recordarlas. ¿Y cómo de segura? Pues muchos servicios de internet te dicen el número mínimo y máximo de caracteres que puede tener una contraseña. Intenta poner una contraseña lo más larga y aleatoria posible.

Herramientas útiles para detectar filtraciones de nuestras contraseñas:

- Have I Been Pwned?: Herramienta útil para ser avisado si tu correo aparece en alguna filtración de nombres de usuaria y contraseñas de algún servicio en línea.

- Monitor de Mozilla: Misma utilidad que la herramienta anterior.

5.2 Autenticación en dos pasos

La autenticación en dos pasos (2FA, por sus siglas en inglés) es una medida adicional de seguridad que requiere dos factores distintos para verificar la identidad de una usuaria al iniciar sesión en un servicio o acceder a una cuenta. Esto va más allá del tradicional uso de una sola contraseña, aumentando la protección contra accesos no autorizados. Es decir, que además de introducir la contraseña, también se te solicita una segunda autenticación. Los métodos de autenticación más habituales son:

- Autenticación por SMS: Una vez introduces correctamente tu contraseña, te llega un código por SMS que debes introducir para iniciar sesión.
- Autenticación por correo electrónico: en este caso, el código te llegará por correo.
- Empleando un generador de códigos: Esta es la opción más recomendada y segura. En este caso el código se obtiene desde una aplicación móvil específica, como puede ser FreeOTP. Este código cambia cada pocos segundos (normalmente cada 30 segundos) y es válido solo durante ese período de tiempo, lo que dificulta que alguien sin autorización acceda a la cuenta.

    - **Configuración inicial:**
        - La usuaria activa la autenticación en dos pasos en el servicio o aplicación deseada. Esto se suele encontrar en la sección de seguridad o similar.
        - El servicio proporciona un código QR o una clave secreta que debe ser introducida o escaneada con el generador.
        - El generador usa esta información para empezar a generar códigos únicos vinculados a la cuenta.
    - **Proceso de inicio de sesión:**
        - La usuaria introduce su contraseña como de costumbre.
        - El servicio solicita el código generado por la aplicación generadora.
        - La usuaria abre el generador, copia el código actual y lo introduce en el servicio.
        - El servidor verifica el código comparándolo con el que debería estar vigente en ese momento. Si coinciden, el acceso es concedido.
    - **Dispositivos de respaldo y recuperación:** Muchos servicios ofrecen códigos de recuperación o permiten configurar varios métodos de 2FA para evitar quedarse sin acceso en caso de pérdida del dispositivo.

6 VPN, proxies y red Tor. Qué diferencias hay y cuándo utilizarlas.

En el contexto de la seguridad y privacidad en línea, el uso de herramientas como VPNs, proxies y la red Tor juega un papel fundamental para proteger nuestros datos y nuestra identidad. Estas tecnologías permiten ocultar nuestra dirección IP, cifrar el tráfico de navegación y acceder a contenidos restringidos, ofreciendo diferentes niveles de anonimato y seguridad. En este capítulo, analizaremos el funcionamiento de cada una de estas herramientas, sus ventajas y limitaciones, así como los escenarios en los que es recomendable emplear cada una para reforzar nuestra protección en la red.

6.1 Conceptos previos

Antes de explicar qué es una VPN, un proxy, la red TOR y cuáles son sus diferencias, vamos a explicar una serie de conceptos:

- **Dirección IP**: La dirección IP (Internet Protocol) es un identificador único que recibe un dispositivo cuando se conecta a Internet, similar a una dirección postal pero en el mundo digital. Sirve para que los datos puedan llegar al destino correcto, permitiendo que los dispositivos se comuniquen entre sí. Existen dos tipos principales: las IP públicas, que identifican la conexión a Internet de una red, y las IP privadas, que identifican dispositivos dentro de una red local, como la de casa. Así, la dirección IP permite rastrear tu actividad en línea y tu localización aproximada, por lo que protegerla es importante para tu privacidad.

- **Cifrado de datos**: El cifrado de datos es un proceso que convierte la información original en un formato ininteligible para que solo pueda ser leída por aquellas personas o sistemas que tengan la clave para descifrarlo. Funciona como un candado digital: la información es protegida mediante algoritmos matemáticos que la transforman en una cadena de caracteres aparentemente aleatoria.

  Por ejemplo, si envías un mensaje cifrado, aunque alguien lo intercepte, no podrá entenderlo sin la clave correcta para descifrarlo. Este proceso es fundamental para proteger la información cuando se transmite por Internet (como correos electrónicos o compras en línea) o cuando se almacena en un dispositivo, garantizando que sea segura y privada.

- **Servidor**: Un servidor es un ordenador o sistema informático diseñado para gestionar, almacenar y proporcionar datos, servicios o recursos a otros ordenadores o dispositivos llamados clientes. Se puede entender como un centro de control que

proporciona lo que los clientes solicitan, ya sean páginas web, archivos, correos electrónicos u otro tipo de información. Por ejemplo: Cuando visitas un sitio web, tu navegador (cliente) hace una solicitud al servidor donde está almacenada la página, y este responde enviándote el contenido para que puedas visualizarlo. Si usas una aplicación de correo, esta se conecta al servidor de correo para enviar o recibir mensajes.

- **Rastreo en línea**: El rastreo en línea es el proceso mediante el cual las empresas, sitios web o plataformas recopilan y almacenan información sobre las actividades que realizas mientras navegas por Internet. Este seguimiento se realiza utilizando diferentes herramientas y tecnologías, como cookies, píxeles de seguimiento o scripts de rastreo, que registran datos sobre tus preferencias, hábitos de navegación e incluso tu localización.

  Por ejemplo, cuando visitas una tienda en línea, es posible que guarden información sobre los productos que consultaste o añadiste al carro. Más tarde, puedes ver anuncios de esos mismos productos en otros sitios web. Esto es un ejemplo de cómo funciona el rastreo en línea.

  Los datos que se pueden recopilar incluyen:

  - Las páginas web que visitas.
  - El tiempo que pasas en cada sitio.
  - Las búsquedas que haces.
  - Tu dirección IP, que puede indicar tu localización.
  - La información sobre el dispositivo y navegador que usas.

  El rastreo en línea puede tener diferentes fines:

  - Publicidad personalizada: Mostrar anuncios relevantes según tus intereses.
  - Análisis de datos: Mejorar servicios y comprender mejor el comportamiento de las usuarias.
  - Segmentación de usuarias: Crear perfiles detallados para ofrecer contenido u ofertas específicas.

- **Proveedor de Servicio de Internet (ISP)**: Un ISP (Proveedor de Servicio de Internet, por sus siglas en inglés Internet Service Provider) es una empresa o entidad que proporciona a las usuarias acceso a Internet. Básicamente, el ISP es la puerta que conecta tu red doméstica o dispositivo a la red global de Internet. Funciones principales de un ISP:

  - Acceso a Internet: El ISP ofrece conexiones a Internet a través de diferentes tecnologías, como DSL (líneas de suscripción digitales), cable, fibra óptica, conexiones satelitales o conexiones móviles.
  - Dirección IP: El ISP asigna una dirección IP (un identificador único en la red) al dispositivo de la usuaria. Esta dirección IP puede ser estática (siempre la misma) o dinámica (puede cambiar con cada conexión).
  - Servicios adicionales: Además del acceso a Internet, los ISP también pueden ofrecer servicios complementarios como correo electrónico, alojamiento web, VPN, o incluso acceso a televisión por cable o servicios de telefonía.

¿Cómo funciona un ISP?

Cuando una persona o empresa quiere acceder a Internet, contrata un ISP que le ofrece una conexión adecuada para sus necesidades. El ISP proporciona la infraestructura y los servidores necesarios para enrutar las solicitudes de conexión a través de diferentes redes hasta llegar al destino en la web. Su función también incluye mantener la infraestructura que permite la conexión, como routers, servidores DNS (para traducir los nombres de dominio en direcciones IP), y otros equipos que aseguran el buen funcionamiento de la conexión.

Rastreo a través del ISP:

Es importante notar que, cuando navegas por Internet, tu ISP puede ver el tráfico que envías y recibes, incluyendo los sitios web que visitas. Por lo tanto, el ISP puede rastrear y registrar tu actividad en línea.

- **Redes públicas y privadas** Es muy importante diferenciar entre redes públicas y privadas, ya que aunque el control de la privacidad es importante en ambos casos, en el caso de las redes públicas es clave:

  - **Red pública**: Una red pública es una conexión de red que está disponible para cualquier persona y, generalmente, no requiere permisos específicos para acceder a ella. Ejemplos típicos son redes Wi-Fi gratuitas en cafeterías, aeropuertos, bibliotecas u hoteles.
  - **Red privada**: Una red privada es una red restringida a la que solo pueden acceder usuarias autorizados. Estas redes suelen ser usadas en hogares, empresas o instituciones para ofrecer conexión segura y controlada a los dispositivos conectados.

- **Navegación pública vs navegación privada**

  La **navegación privada** es una funcionalidad que ofrecen la mayoría de los navegadores web para que las usuarias puedan navegar sin que se guarden ciertas informaciones en el dispositivo, como el historial de navegación, las cookies o los datos de los formularios. Características principales:

  - No se guardan datos locales: El navegador no almacena el historial de navegación, las cookies o los datos de sesión. Al cerrar la ventana de navegación privada, se borra todo.
  - Útil para sesiones temporales: Es útil si no quieres dejar rastro de tu actividad en el dispositivo, por ejemplo, cuando usas un computador público o compartido.
  - No protege contra rastreadores en línea: A pesar de que no se guardan los datos en el dispositivo, la navegación privada no oculta tu identidad o actividad en línea de los sitios web o de los proveedores de servicio de Internet (ISP)

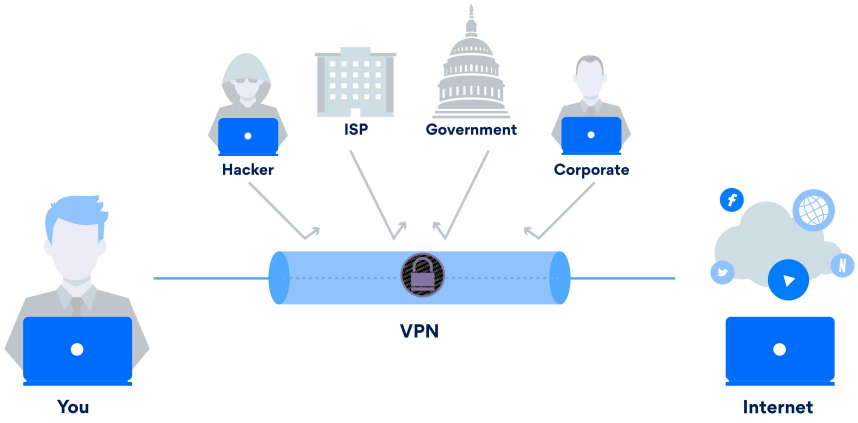
  Esta navegación privada tiene una serie de limitaciones:

  - No evita que los sitios web rastreen tu actividad mediante la dirección IP o mediante otros mecanismos de rastreo como las huellas digitales del navegador.
  - No te proporciona anonimato o protección contra espiar tus datos.

La **navegación anónima**, por otro lado, se refiere a técnicas o herramientas que ocultan tu identidad o información personal mientras navegas en la web. El objetivo principal es mejorar la privacidad, haciendo que sea más difícil rastrear tus actividades en línea. Para esto se emplean las VPNs o las redes TOR, que buscan añadir una capa de protección extra, y que explicaremos en detalle más abajo. Hay que tener en cuenta que este tipo de navegación puede reducir la velocidad de navegación, ya que el tráfico tiene que pasar por varios servidores antes de llegar a su destino. Además, por supuesto, no es infalible, y las autoridades u otras entidades podrían ser capaces de rastrear tu actividad con herramientas avanzadas.

- **Punto de acceso**: Un punto de acceso es un dispositivo que permite a los dispositivos, como teléfonos, ordenadores o tabletas, conectarse a Internet. Es decir, es nuestra puerta de entrada al resto de la red. Funciona como un puente entre los dispositivos y la red principal, transmitiendo y recibiendo señales.

6.2 ¿Qué es una VPN?



Una **VPN** (Virtual Private Network, o Red Privada Virtual en español) es una tecnología que permite crear una conexión segura y cifrada entre un dispositivo (como un ordenador o un teléfono móvil) y un servidor remoto a través de Internet. Este servidor actúa como un punto de acceso a la red, permitiendo que los datos que se envían y reciben entre el dispositivo y la red pública (Internet) viajen de forma protegida y anónima.

La función principal de una VPN es **garantizar la privacidad y seguridad en la navegación en línea**, cifrando la comunicación entre la usuaria y el servidor de Internet, y haciendo que sea mucho más difícil para terceros, como cibercriminales o proveedores de servicios de Internet (ISPs), interceptar o espiar esa información.

6.2.1 ¿Cómo funciona una VPN?

- **Cifrado de datos:** La VPN utiliza protocolos de cifrado para encriptar los datos que viajan entre el dispositivo de la usuaria y el servidor de la VPN. Esto significa que incluso si alguien intentase interceptar los datos en tránsito, no podría leerlos, ya que estarían codificados de manera que solo el servidor de destino o el dispositivo de origen puedan descifrarlos. Hay que tener en cuenta que no todos los servicios

de VPN envían los datos de forma encriptada. Uno de los más conocidos, gratuito, y que sí encripta la información es Proton VPN.

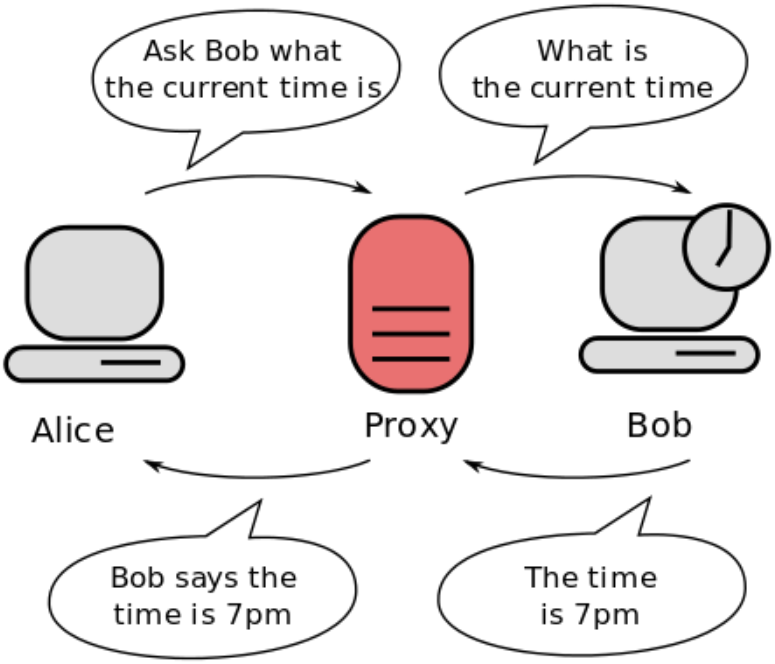
- **Túnel seguro:** La conexión establecida entre el dispositivo y el servidor de la VPN se llama un túnel. Este túnel es privado y protege los datos, haciendo que no sean accesibles a nadie que intente espiar o interrumpir la conexión. Esto impide que otras personas en la misma red (como en una red Wi-Fi pública) puedan acceder a tus datos o a lo que estás haciendo en línea.
- **Cambiar la dirección IP:** Una de las principales ventajas de una VPN es que puede ocultar tu verdadera **dirección IP**, que es un identificador único asociado a tu dispositivo cuando te conectas a Internet. Al conectarte a un servidor VPN, tu dirección IP real queda oculta y es sustituida por la dirección IP del servidor VPN. Esto puede mejorar tu privacidad en línea, haciendo más difícil para terceros rastrearte o determinar tu localización real.
- **Acceso a contenidos bloqueados:** Como tu dirección IP se sustituye por la del servidor VPN, también puede permitirte acceder a contenidos o servicios bloqueados en tu región geográfica. Por ejemplo, si un sitio web o servicio está disponible solo en Estados Unidos, pero tú estás en Europa, una VPN puede hacerte parecer que estás en EE.UU. para acceder a ese contenido.
- **Seguridad en la navegación en redes públicas:** Las VPNs son especialmente útiles cuando se usan redes Wi-Fi públicas, como las que se encuentran en cafés, aeropuertos o bibliotecas. En este tipo de redes, la seguridad es mucho más débil y los cibercriminales pueden intentar interceptar la comunicación. La VPN protege tus datos al cifrarlos y asegurar que no sean fácilmente accesibles.

6.2.2 Limitaciones y desventajas de una VPN

- **Velocidad:** Al usar una VPN, puede haber una disminución de la velocidad de navegación debido al cifrado y al paso de los datos por el servidor remoto. Esto puede ser un problema cuando se realizan tareas que requieren mucho ancho de banda, como la transmisión de vídeo en alta definición.
- **Confianza en el servidor VPN:** Al utilizar una VPN, estás confiando en el servidor de la VPN para proteger tu privacidad. Si el servidor VPN no está bien protegido o si el proveedor de VPN mantiene registros de actividad, la privacidad de la usuaria puede verse comprometida.
- **Accesibilidad a servicios:** Algunos servicios, como plataformas de transmisión de vídeo o sitios web, pueden bloquear las conexiones VPN para evitar que las usuarias accedan a contenidos restringidos por región.

En resumen, una **VPN** es una herramienta útil para mejorar la seguridad y la privacidad en línea, cifrando la comunicación y ocultando tu dirección IP, pero también presenta algunas limitaciones que deben tenerse en cuenta al utilizarla.

6.3 ¿Qué es un Proxy?



Un **proxy** es un servidor que actúa como intermediario entre un cliente, como un ordenador o un dispositivo móvil, y un servidor al que se quiere acceder a través de Internet. En otras palabras, cuando una usuaria hace una solicitud para acceder a un sitio web o servicio en línea, el proxy reenvía esta solicitud en nombre de la usuaria, recoge la respuesta del servidor y luego envía la información de vuelta a la usuaria.

Este proceso tiene varias funciones y beneficios, tales como:

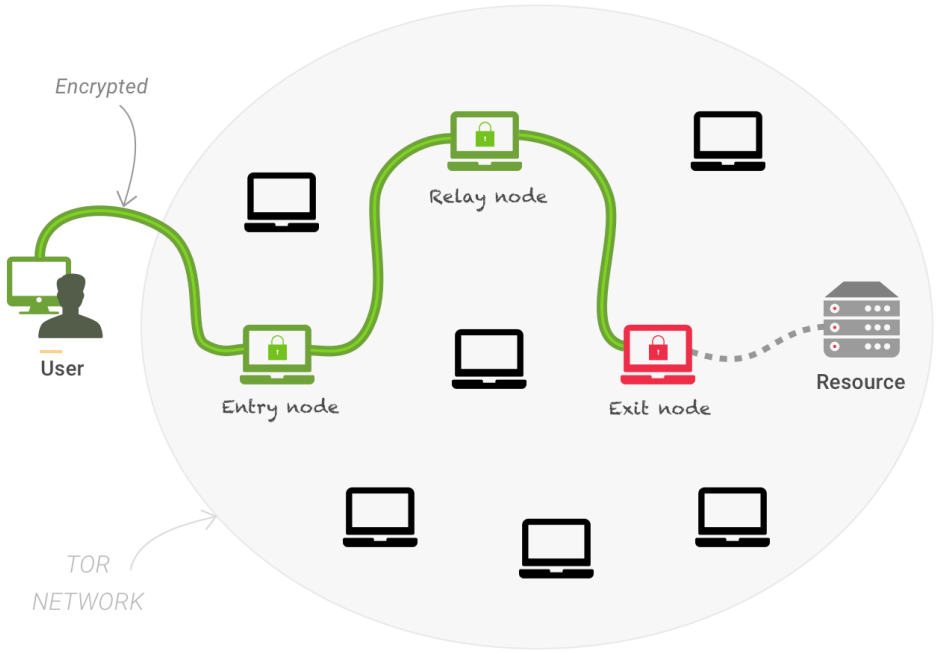
- **Privacidad y anonimato:** El proxy oculta la dirección IP de la usuaria, haciendo que las solicitudes a Internet parezcan venir del propio proxy y no del dispositivo de la usuaria. Esto puede ser útil para mejorar la privacidad en la navegación y para evitar que se rastreen las actividades de la usuaria en línea.
- **Control de acceso:** El proxy puede bloquear el acceso a sitios web específicos o filtrar el contenido basado en políticas de acceso, como las que se implementan en redes corporativas o en escuelas.
- **Mejora del rendimiento:** Un proxy puede almacenar en caché (o guardar localmente) las páginas o recursos web más solicitados. Esto significa que cuando otra usuaria hace la misma solicitud, el proxy puede entregar el contenido directamente desde su caché, mejorando la velocidad de acceso y reduciendo el uso de ancho de banda.
- **Seguridad adicional:** Al actuar como intermediario, un proxy puede ofrecer ciertas medidas de seguridad, como la detección de sitios maliciosos, el análisis de tráfico para encontrar posibles amenazas y la protección contra ciertos tipos de ataques.

Sin embargo, aunque los proxies ofrecen ciertos beneficios, **también tienen limitaciones importantes en comparación con otras tecnologías como las redes privadas virtuales (VPNs)**. La principal diferencia es que un proxy no cifra la conexión entre la usuaria

y el servidor. Esto significa que, a diferencia de una VPN, la comunicación a través de un proxy no está protegida contra la escucha por terceros, por lo que no ofrece la misma seguridad en conexiones sin cifrar.

En resumen, un proxy es útil para mejorar la privacidad, controlar el acceso a sitios web y mejorar el rendimiento, pero no proporciona el nivel de seguridad y privacidad que se puede obtener con una VPN.

6.4 ¿Qué es la Red TOR?



La **red TOR** (The Onion Router) es una red descentralizada de servidores que permite la navegación anónima en Internet. Su principal objetivo es proporcionar a las usuarias la capacidad de navegar sin que su identidad o actividad sean rastreadas. El funcionamiento de TOR se basa en el uso de múltiples capas de cifrado, que actúan como lóbulos de una cebolla, de ahí el nombre *onion routing*, enrutamiento de cebolla.

6.4.1 Proceso de cifrado

Cuando una usuaria envía datos a través de TOR, estos son cifrados en múltiples capas, de forma similar a las capas de una cebolla. Cada nodo de la red TOR solo puede descifrar una de las capas, garantizando que ningún nodo intermedio tenga acceso al contenido completo de la comunicación ni a su origen y destino final al mismo tiempo. El **proceso de cifrado** funciona así:

- La usuaria TOR elige un camino aleatorio de nodos de la red (por defecto son tres nodos, aunque se puede incrementar el número).
- El tráfico es cifrado usando un **cifrado en capas**, aplicando una capa de cifrado para cada nodo por el que pasará el tráfico.

- El primer nodo de la ruta (nodo de entrada) descifra la primera capa, pero solo sabe quién es el usuario y el siguiente nodo de la ruta.
- El segundo nodo elimina su capa de cifrado, pero solo sabe de dónde vino el mensaje (el primer nodo) y a quién debe enviarlo (el tercer nodo).
- El tercer nodo (nodo de salida) elimina la última capa de cifrado y envía el tráfico a su destino final en internet.

Este proceso de enrutamiento múltiple y cifrado en cada paso hace que, al final, el origen de la solicitud se vuelva irreconocible para el servidor de destino, ya que el tráfico es cifrado en múltiples capas y enviado a través de varios puntos en la red antes de llegar a su destino. Además, hay algunos servicios que se encuentran directamente dentro de la red TOR, los dominios terminados en .onion, de forma que en ningún momento es preciso salir de la red TOR.

6.4.2 Ventajas de la red TOR

Las principales **ventajas de la red TOR** son las siguientes:

- **Anonimato:** Al pasar a través de varios nodos, la dirección IP de la usuaria queda oculta, haciendo imposible rastrear su localización o su identidad a través de su conexión a la red. Esto hace que TOR sea popular entre las usuarias que desean mantener su anonimato en línea.
- **Evasión de censura:** TOR permite a las usuarias acceder a sitios web y servicios bloqueados o censurados en algunos países o redes, ya que oculta su identidad y origen. Esto es especialmente útil para periodistas, activistas y usuarias que operan en países con altas restricciones de acceso a la información.
- **Seguridad mejorada:** La comunicación a través de la red TOR está cifrada en varias capas, lo que proporciona una protección adicional contra escuchas y ataques. Esto es útil especialmente cuando se accede a sitios web sensibles o se intercambian datos confidenciales.

6.4.3 Desventajas de la red TOR

Sin embargo, la red TOR también presenta ciertas desventajas (hay que recordar que la seguridad al 100 % no existe):

- **Velocidad de conexión**: La principal de ellas es que, debido al enrutamiento en múltiples capas y nodos, la velocidad de navegación puede ser considerablemente más lenta en comparación con otras formas de navegación en Internet.
- **Vulnerabilidad al salir de la red TOR**: TOR no garantiza la seguridad total, ya que los nodos de salida de la red pueden ser vulnerables a ataques, y el tráfico encriptado solo se mantiene seguro entre los nodos de la red, pero no en el nodo de salida, donde se descifra y puede ser escuchado por partes mal intencionadas. Sin embargo, en este caso, aunque podrían saber a qué recurso se está accediendo, no podrían saber quién está accediendo, ya que ha pasado a través de varios nodos TOR. En el caso de acceder a **dominios .onion**, no se llega a salir de la red TOR, por lo que ya no existe tal vulnerabilidad.

- **Nodos maliciosos**: Otra vulnerabilidad es que un atacante con control de múltiples nodos podría intentar relacionar el tráfico de entrada y salida, aunque tendría que coincidir que justo la ruta pase a través de los nodos de un mismo atacante.

En resumen, la red TOR es una herramienta poderosa para mantener el anonimato y la privacidad en línea, pero también tiene limitaciones en términos de velocidad y seguridad en el nodo de salida. Su utilización es recomendada para aquellas usuarias que desean acceder a Internet de forma anónima o eludir la censura en línea. Para poder emplearla, debes descargar el navegador desde su página oficial.

6.5 Comparativa entre VPN, Proxy y red TOR

Característica	VPN	Proxy	Rede TOR
Anonimato	Alto: Oculta la IP y cifrado completo	Medio: Oculta la IP, pero no cifra todo el tráfico	Alto: Oculta la IP y cifra todo el tráfico
Seguridad	Alto: Cifrado de todo el tráfico	Bajo: Solo oculta la IP, sin cifrado	Alto: Cifrado de múltiples capas y anonimato
Rendimiento	Medio: Ligeramente más lento debido al cifrado	Rápido: Sin cifrado, pero puede ser más lento dependiendo del servidor	Lento: Debido al enrutamiento de múltiples nodos
Accesibilidad	Accede a cualquier sitio	Accede a sitios específicos a través del servidor proxy	Accede a sitios censurados o bloqueados
Censura	Elude la censura, pero depende del proveedor	Elude la censura, pero solo si está configurado correctamente	Elude la censura de forma eficaz, ocultando el origen del tráfico
Facilidad de uso	Relativamente sencillo de configurar	Sencillo de configurar, pero con limitaciones	Requiere software especializado (Tor Browser)
Privacidad	Alta, pero depende del proveedor de VPN	Baja: el servidor puede registrar la actividad	Alta, ya que no hay un único punto de fallos que registre la actividad
Compatibilidad	Funciona con cualquier aplicación que use Internet	Funciona principalmente para HTTP/HTTPS, es decir, navegadores.	Funciona principalmente con el navegador Tor
Herramienta libre	Proton VPN	-	Navegador Tor

Cuadro 6.1: Comparativa entre VPN, Proxy y Red TOR

7 DNS seguro. Qué es y alternativas seguras

7.1 ¿Qué es un DNS?

El DNS (**Sistema de Nombres de Dominio**) es un servicio fundamental de Internet que funciona como una especie de agenda telefónica de sitios web. Permite traducir los nombres de dominio (como **www.example.com**) en direcciones IP numéricas (como **192.168.1.1**) que los ordenadores utilizan para comunicarse entre sí. Sin el DNS, tendríamos que recordar la dirección IP exacta de cada sitio web que queremos visitar, lo que sería muy complicado. En resumen, el DNS facilita la navegación en Internet al hacer que los nombres de dominio sean más fáciles de usar, a la vez que permite la comunicación entre los dispositivos de red.

7.2 Impacto del DNS en nuestra privacidad

El servicio DNS, aunque fundamental para la navegación en Internet, también puede afectar a nuestra privacidad. Cada vez que accedemos a una página web, nuestro dispositivo envía una solicitud al servidor DNS para obtener la dirección IP asociada al nombre de dominio. Durante este proceso, el servidor DNS puede registrar información sobre los sitios web que visitamos, junto con nuestra dirección IP, lo que permite el seguimiento y la creación de perfiles de navegación.

Si usamos servidores DNS públicos o los proporcionados por los proveedores de servicios de Internet (ISP), estos servidores pueden recopilar y almacenar nuestros datos de navegación, incluso compartirlos con terceros, como anunciantes o autoridades gubernamentales. Esto puede resultar en un riesgo para nuestra privacidad, especialmente si no se implementan medidas adecuadas para proteger la información que circula en nuestras conexiones.

Por otro lado, al utilizar servicios de DNS seguros y privados, como DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT), podemos minimizar la posibilidad de que nuestros datos sean espiados o manipulados, garantizando así una mayor confidencialidad en nuestra navegación en Internet. Al encriptar las solicitudes DNS, se impide que terceros intercepten o registren las páginas que visitamos, mejorando nuestra privacidad en línea.

7.3 Sistemas de DNS

Existen varios tipos de sistemas de DNS que difieren en la forma en que gestionan y protegen las solicitudes de nombre de dominio. A continuación, explicamos los principales:

7.3.1 DNS tradicional

El sistema DNS tradicional se basa en la resolución de nombres de dominio a través de servidores DNS públicos o proporcionados por los proveedores de servicios de Internet (ISP). Cuando una usuaria quiere acceder a un sitio web, su solicitud de DNS es enviada a un servidor DNS, que resuelve el nombre de dominio y devuelve la dirección IP correspondiente. Este sistema, aunque útil, puede dejar nuestra información de navegación expuesta a posibles rastreos y vulnerabilidades, especialmente si no se utiliza cifrado.

7.3.2 DNS sobre HTTPS (DoH)

El **DNS sobre HTTPS** (DoH) es un protocolo que cifra las solicitudes DNS al transmitirlas a través de HTTPS, lo que impide que terceros intercepten o registren nuestras solicitudes de DNS. Al usar DoH, las solicitudes de DNS son tratadas de manera similar a las solicitudes de páginas web y, por lo tanto, son difíciles de espiar. Este sistema mejora la privacidad y la seguridad en la navegación al proteger los datos de DNS de ataques de intermediarios, como los ataques man-in-the-middle.

7.3.3 DNS sobre TLS (DoT)

El **DNS sobre TLS** (DoT) es otro protocolo que cifra las solicitudes DNS, pero a diferencia de DoH, DoT utiliza el protocolo de seguridad TLS (Transport Layer Security) para cifrar las solicitudes de DNS. El principal objetivo de DoT es garantizar que las solicitudes DNS no puedan ser espiadas ni manipuladas al pasar por la red. Similar a DoH, DoT también mejora la privacidad y la seguridad, protegiendo nuestras solicitudes de DNS de ser interceptadas por terceros.

7.3.4 DNS privados o personalizados

Algunas personas u organizaciones optan por usar **DNS privados o personalizados**, que son servidores DNS configurados de forma específica para mejorar la privacidad y la seguridad. Estos servidores no registran o comparten los datos de navegación de la usuaria con terceros, garantizando un mayor nivel de confidencialidad. Ejemplos de servicios de DNS privados son Cloudflare o NextDNS.

7.4 Ventajas de DoH y DoT

Tanto el **DNS sobre HTTPS** (DoH) como el **DNS sobre TLS** (DoT) mejoran la seguridad y la privacidad de las solicitudes DNS mediante el cifrado. Sin embargo, existen diferencias en las ventajas que ofrecen cada uno de estos protocolos:

7.4.1 Ventajas de DNS sobre HTTPS (DoH)

- **Mejora de la privacidad**: Al usar DoH, las solicitudes de DNS son tratadas como tráfico HTTPS, lo que dificulta su identificación y espionaje por los ISP u otras entidades que monitorizan la red.

- **Integración con navegadores**: DoH es fácilmente integrable en navegadores web populares, como Firefox, mejorando la privacidad sin necesidad de configuración adicional a nivel de sistema operativo.
- **Evadir censura**: Dado que las solicitudes DNS a través de DoH son transportadas como tráfico HTTPS estándar, que es el mismo protocolo usado para acceder a páginas web seguras. Esto hace que el tráfico DNS se oculte dentro del tráfico normal de navegación por internet, siendo más difícil para los gobiernos o los ISP bloquear o filtrar las solicitudes DNS, lo que permite la navegación en redes con censura estricta.
- **Protocolo estándar web**: Como DoH usa HTTPS, se beneficia de la infraestructura segura existente de Internet, lo que facilita su implementación y mejora la interoperabilidad.

7.4.2 Ventajas de DNS sobre TLS (DoT)

- **Menos impacto en la latencia**: DoT usa un puerto específico (853) para la transmisión de las solicitudes DNS cifradas, lo que permite que las solicitudes de DNS se realicen de forma más eficiente sin afectar otras aplicaciones o tráfico web.
- **Separación de tráficos**: A diferencia de DoH, que envía solicitudes DNS como tráfico HTTPS, DoT mantiene un puerto separado, lo que facilita la identificación y gestión del tráfico DNS cifrado en redes corporativas o servicios que desean monitorizar o filtrar solicitudes DNS de forma específica.
- **Seguridad y fiabilidad**: DoT ofrece una mayor fiabilidad y control en las conexiones, dado que puede ser configurado para asegurar la conectividad en redes que implementan proxys o firewalls más restrictivos. Aunque también cifra las solicitudes DNS, su implementación puede ser más simple en algunos ámbitos corporativos o de servicio.

7.4.3 Resumen de las diferencias principales

En resumen, la principal diferencia entre DoH y DoT reside en la forma en que las solicitudes DNS son transportadas y en el uso de puertos. **DoH es ideal** para mejorar la privacidad al ocultar las solicitudes de DNS dentro del tráfico HTTPS, mientras que **DoT** puede ser preferible para aquellos que necesitan una solución más específica para servidores o redes con mayor control sobre el tráfico DNS, y que solo permiten el protocolo DoT.

7.5 ¿Cómo configurar el DNS seguro?

La forma de configurar el DNS seguro varía en función del dispositivo, sistema operativo, etc. Lo más fácil es que le eches un vistazo a la guía que tiene la gente de NextDNS. En ella explican cómo configurar el DNS en distintos tipos de dispositivos. Como indican arriba de todo, para que el DNS no caduque a los siete días es necesario registrarse en su web. El plan gratuito es suficiente, mientras que los planes de pago están pensados para empresas o entidades que tienen un uso más elevado del servicio. La ventaja de

este servicio de NextDNS es que, además de comunicar tus consultas de forma anónima, también incluye una serie de opciones para filtrar publicidad, bloquear ciertas páginas web, programar las horas de uso y muchas otras más.

7.6 Ojo, el DNS seguro no nos hace completamente anónimas

A pesar de que los métodos de cifrado DNS como DoH (DNS sobre HTTPS) y DoT (DNS sobre TLS) protegen la privacidad al ocultar el dominio que consultas, al cifrar las solicitudes DNS, los proveedores de servicios de Internet (ISP) todavía tienen acceso a la dirección IP a la que te conectas. Esto significa que, aunque el ISP no pueda ver directamente el nombre del dominio (ejemplo.com) que estás consultando, puede ver la IP a la que el dominio resuelve (193.4.52.2). Dado que cada dominio tiene asociada una dirección IP, el ISP puede, a través del análisis de las IPs a las que te conectas, saber los dominios que visitas. Además, los ISP también podrían optar por bloquear directamente ciertas direcciones IP, en lugar de bloquear los dominios. Esto permitiría bloquear el acceso a sitios o servicios sin tener que censurar los nombres de los dominios, lo que puede ser más difícil de detectar para las usuarias. Por lo tanto, incluso con métodos de cifrado DNS, los ISP u otras entidades con acceso a la red pueden tener cierto grado de visibilidad sobre el tráfico que circula por su infraestructura.

Es probable que ahora mismo te preguntes: Entonces, ¿qué ventaja tiene usar DNS seguros si, al fin y al cabo, el ISP puede saber igualmente las webs que visito?

Para empezar, hay que tener en cuenta que el empleo de DNS seguros no solo te protege de tu ISP. Si no usas un DNS cifrado, existe el riesgo de que las solicitudes DNS sean manipuladas durante la transmisión. Los ataques de hombre en el medio (MITM, Man In The Middle) permiten a un atacante interponerse en las comunicaciones y cambiar las respuestas DNS, redirigiendo el tráfico a sitios falsos. Usar un DNS cifrado impide que esto suceda, haciendo que la conexión sea mucho más segura.

Además, muchos sitios web comparten la misma dirección IP a través de técnicas como el hospedaje compartido o CDNs (Content Delivery Networks), como CloudFare. Esto hace que, si el ISP bloquea una dirección IP, no está bloqueando un único sitio web, sino que se puede bloquear toda una serie (cientos de miles incluso) de sitios o servicios que comparten esa IP. Esto hace más difícil para un ISP o entidad censora bloquear un dominio específico solo por IP, siendo mucho más fácil bloquear el nombre del dominio directamente (bloqueo contra el que sí te protege el empleo de DNS seguros).

Por lo tanto, usar DNS seguros (DoH o DoT) puede mejorar la privacidad de las consultas DNS, pero, si bien no impide que el ISP sepa la IP del destino, la existencia de CDNs o sitios que comparten IP hace que el bloqueo por IP sea menos efectivo y más indiscriminado, además de que dificulta que el ISP sepa exactamente qué dominio estás visitando.

Para evitar que el ISP sepa la IP que visitas, además de emplear un servicio de DNS seguro, deberías emplear un servicio de VPN o la red TOR, ya mencionados en el capítulo anterior.

8 Mejorar la seguridad de nuestro navegador

8.1 La importancia de la seguridad de nuestro navegador

En la actualidad, el navegador web es una de las herramientas más utilizadas para acceder a información en línea, realizar compras, trabajar e interactuar con las redes sociales. Sin embargo, también es la puerta de entrada para nuestra privacidad y seguridad en internet. A través del navegador, compartimos datos personales, accedemos a sitios web e interactuamos con diversas plataformas, por lo que es crucial garantizar que nuestra navegación sea lo más segura y privada posible.

Muchas veces, los navegadores web recopilan y almacenan información sobre nuestra actividad en línea, como *cookies*, historial de navegación o datos personales. Además, existen una serie de riesgos asociados al uso del navegador, como el seguimiento de nuestra actividad, la exposición a sitios web maliciosos o el robo de información sensible. Por ello, es fundamental adoptar medidas que protejan nuestra privacidad y seguridad mientras navegamos.

En este capítulo, exploraremos diferentes estrategias y herramientas que podemos emplear para mejorar la seguridad y la privacidad en nuestro navegador, desde el uso de navegadores libres hasta la configuración de extensiones que bloquean rastreadores y protegen nuestros datos personales.

8.2 Diferencia entre navegador y motor de búsqueda. Alternativas seguras

Un **navegador web** y un **motor de búsqueda** son dos elementos esenciales para navegar por internet, pero tienen funciones distintas.

Un **navegador web** es un software que permite a las usuarias acceder a sitios web y visualizar su contenido. Ejemplos populares de navegadores son Google Chrome, Mozilla Firefox, Safari y Microsoft Edge. El navegador es el programa que empleamos para interactuar con las páginas web, y también se encarga de gestionar las conexiones seguras, almacenar *cookies* e historial de navegación, y ofrecer funcionalidades adicionales mediante extensiones.

Por otra parte, un **motor de búsqueda** es un servicio en línea que ayuda a las usuarias a encontrar sitios web mediante la introducción de palabras clave o frases. Los motores de búsqueda, como Google, Bing o DuckDuckGo, indexan millones de sitios web y permiten a las usuarias realizar búsquedas para encontrar el contenido que desean. El motor de

búsqueda sirve como una guía para localizar información en internet, pero no tiene un control directo sobre cómo se accede o se muestra ese contenido en el navegador.

Mientras el navegador gestiona la interacción con las páginas web, el motor de búsqueda solo facilita la localización de esa información. La diferencia entre ambos es fundamental, ya que los motores de búsqueda también recopilan información sobre nuestras consultas, y por tanto también son un posible riesgo para nuestra privacidad.

8.2.1 Alternativas libres

Existen alternativas libres y de código abierto tanto para navegadores como para motores de búsqueda que respetan mejor nuestra privacidad y seguridad en línea. A continuación, se destacan algunos ejemplos de cada uno:

- **Navegadores libres (ya explicados en la sección 2.2.11):**
  - **Mozilla Firefox**
  - **Tor Browser**
- **Motores de búsqueda libres (ya explicados en la sección 2.2.12):**
  - **StartPage**
  - **SearX**

El uso de navegadores y motores de búsqueda libres no solo mejora nuestra privacidad, sino que también contribuye al apoyo de proyectos que promueven un internet más abierto y libre, sin depender de grandes corporaciones que recopilan y comercializan nuestros datos personales.

8.3 Extensiones libres que aumentan nuestra privacidad

Las extensiones para los navegadores son herramientas poderosas que nos permiten mejorar nuestra privacidad y seguridad en línea. Muchas de estas extensiones están diseñadas para bloquear rastreadores, mejorar el control sobre nuestras *cookies*, proteger contra sitios maliciosos y mejorar la seguridad de nuestra navegación. A continuación, se exponen algunos ejemplos de extensiones de software libre que podemos utilizar para mejorar nuestra privacidad en internet (todas ellas disponibles, al menos, en Firefox):

- **uBlock Origin**: Un bloqueador de anuncios y rastreadores de código abierto que permite bloquear de forma eficaz anuncios intrusivos, rastreadores y *scripts* no deseados, mejorando la privacidad y la velocidad de carga de las páginas.
- **Privacy Badger**: Desarrollado por la Electronic Frontier Foundation (EFF), Privacy Badger detecta y bloquea automáticamente los rastreadores que están siguiendo a la usuaria sin su consentimiento, mejorando la privacidad sin la necesidad de configurar reglas manualmente.
- **HTTPS Everywhere**: Desarrollada por la EFF, esta extensión fuerza a las páginas web a utilizar HTTPS en lugar de HTTP, garantizando así que nuestras conexiones sean cifradas y seguras. Sin embargo, la mayoría de navegadores ya incluyen esta opción en sus configuraciones, por lo que se puede modificar directamente.

Estas extensiones de software libre proporcionan una forma sencilla y eficaz de mejorar nuestra privacidad y seguridad al navegar por internet. A pesar de que las extensiones de navegador son herramientas útiles para mejorar nuestra privacidad y seguridad, es fundamental tener cuidado con los permisos que les concedemos. Muchas veces, las extensiones solicitan permisos para acceder a información sensible o modificar el funcionamiento del navegador, por lo que es importante revisar cuidadosamente los permisos que nos piden antes de instalar cualquier extensión. Además, es recomendable instalar solo extensiones que provengan de fuentes seguras, como las que se encuentran en la tienda oficial del navegador, ya que estas pasan un control de seguridad para evitar que sean maliciosas o invasivas. Por ejemplo, Firefox tiene una categoría de extensiones verificadas que garantizan un mayor nivel de confianza. También debemos tener en cuenta que, en algunos casos, puede ser necesario desactivar temporalmente ciertas extensiones para poder visualizar algunos sitios web correctamente, ya que algunos sitios pueden bloquear o no ser compatibles con las funciones de bloqueo de anuncios o rastreadores, por ejemplo. Por eso, es importante mantener un equilibrio entre la protección de nuestra privacidad y la funcionalidad del navegador.

8.4 Otras configuraciones útiles

Además de las extensiones, existen otras configuraciones en el navegador que pueden mejorar notablemente nuestra privacidad y seguridad. A continuación, se explican algunos ajustes importantes que podemos aplicar:

- **Bloqueo de rastreadores:** Muchos navegadores modernos permiten activar el bloqueo de rastreadores de forma nativa o a través de configuraciones de extensiones. Esto impide que sitios web rastreen nuestra actividad y recopilen datos sin nuestro consentimiento. Es importante activar estas opciones para reducir la cantidad de información personal que se recopila sin darnos cuenta.

- **Borrar los datos al cerrar el navegador:** Configurar el navegador para eliminar automáticamente el historial de navegación, *cookies*, caché y otros datos al cerrar el navegador es una buena práctica para proteger nuestra privacidad. Esto evita que otras personas que usen el mismo dispositivo puedan acceder a nuestra actividad previa.

- **Contraseña maestra:** Activar una contraseña maestra en el navegador puede ser útil para proteger contraseñas almacenadas en el gestor de contraseñas del navegador. Esto garantiza que, incluso si alguien tiene acceso al dispositivo, no pueda acceder fácilmente a nuestras cuentas en línea sin conocer esta contraseña adicional.

- **Desactivar el seguimiento de posición:** Muchos navegadores permiten desactivar la función de seguimiento de posición o acceso a nuestra ubicación. Al desactivar esta opción, evitamos que sitios web y servicios puedan acceder a nuestra ubicación física sin nuestro consentimiento.

- **Usar un DNS seguro:** Cambiar la configuración del DNS para usar servicios de DNS seguros, como el DoH o DoT, puede mejorar nuestra privacidad y evitar que nuestro ISP u otros terceros puedan rastrear nuestras consultas DNS.

- **Desactivar complementos no necesarios:** Muchos navegadores permiten activar o desactivar complementos y *scripts*. Es importante desactivar los complementos que no necesitamos, ya que pueden ser un punto de entrada para ataques de *malware* o ser utilizados para recopilar información sobre nuestra actividad.

- **Usar navegación privada en ordenadores compartidos:** Cuando usamos un ordenador compartido o público, es altamente recomendable emplear el modo de navegación privada o incógnito. Este modo impide que el navegador guarde el historial de navegación, las *cookies* y los datos de sesión, ya que se borran una vez lo cerramos. Al usar este modo, evitamos que otras personas que usen el mismo dispositivo puedan ver nuestras actividades en línea o acceder a información sensible, como cuentas en línea o contraseñas guardadas. Además, en caso de que varias personas suelan compartir un ordenador, se recomienda que cada una tenga su propio perfil de usuaria en el ordenador, y que eviten compartir uno solo.

9 Mejorar la seguridad de nuestra WiFi

9.1 Contraseña del WiFi

Una contraseña fuerte es esencial para proteger tu red WiFi de accesos no autorizados. Utilizar una contraseña larga, compleja y única, que combine letras mayúsculas, minúsculas, números y símbolos, ayuda a evitar que ciberdelincuentes o programas automáticos quieran acceder a tu red. Al crear una contraseña, debes evitar usar información personal fácil de adivinar, como tu nombre o fechas de nacimiento. La mejor opción es usar un generador de contraseñas o una frase larga y única. Una contraseña de 12 o más caracteres es más segura. Si es posible, utiliza un generador de contraseñas para crear claves robustas que no sean fáciles de adivinar, como BitWarden o Proton Pass.

9.2 Configuración del router

- Nombre de usuaria y contraseña del router: Muchos routers vienen con un nombre de usuaria y contraseña por defecto que puede ser fácilmente adivinado. Es fundamental cambiar estas credenciales para impedir que cualquiera acceda a la configuración del router sin autorización. De no hacerlo, cualquiera que se conecte a tu WiFi podría acceder a tu router y cambiar configuraciones que atenten directamente contra tu privacidad.
- Cambio del nombre de red (SSID): El nombre de red (SSID) debe ser cambiado para que no sea fácilmente identificable. No uses datos personales en el SSID, ya que puede facilitar la identificación de tu red.
- Configuración del protocolo de seguridad (WPA3): Asegúrate de configurar tu red WiFi con un protocolo de seguridad fuerte, como WPA3, que ofrece una mayor protección que los protocolos anteriores como WPA2.
- Desactivación de la administración remota: En algunos casos, los routers tienen un modo de administración remota que permite que accedas a la configuración del router desde cualquier lugar a través de Internet. Para aumentar la seguridad, desactívalo y así evitar accesos no autorizados a la configuración del router.
- WiFi de invitadas: Es recomendable crear una red WiFi separada para los invitados, de modo que no puedan acceder a tus dispositivos y archivos personales. La mayoría de los WiFis permiten hacerlo de forma sencilla accediendo al panel de administración.

- Uso de DNS seguros: En algunos casos, puedes modificar el DNS que trae configurado tu router, que suele ser el DNS del ISP, y usar un DNS seguro que se aplique a todos los dispositivos que se conecten a él (salvo que esos dispositivos tengan configurado un DNS seguro propio). Sin embargo, en algunos casos cambiar el DNS en el router no es posible ya que el ISP limita las configuraciones que puedes modificar. En este último caso, o bien cambias el router o bien activas el DNS directamente en tus dispositivos.

10 Ciberataques Típicos

Los ataques cibernéticos son una de las mayores amenazas para la seguridad y privacidad en Internet. Estos ataques, que varían en complejidad y alcance, tienen como objetivo obtener acceso no autorizado a información sensible, interrumpir la comunicación o causar daños a sistemas informáticos. A continuación, describimos algunos de los ataques más comunes, sus objetivos y las mejores prácticas para protegerse de ellos.

10.1 Phishing

El phishing es una técnica de ataque que se utiliza para engañar a las víctimas para que revelen información personal sensible, como contraseñas, números de tarjetas de crédito o datos bancarios. Los atacantes envían correos electrónicos o mensajes que simulan ser de una entidad de confianza (como un banco o un servicio en línea popular) para engañar a la víctima y que esta haga clic en un enlace que la redirigirá a una página falsa.

En este tipo de ataques se imitan los enlaces web o direcciones de correo reales cambiando algún carácter o simulando ser direcciones reales. Los correos electrónicos o mensajes de phishing son cada vez más sofisticados, y muchas veces incluyen logotipos y diseños de páginas web reales, haciendo que sea difícil distinguir entre un correo electrónico auténtico y uno de phishing. La principal diferencia es que los enlaces o formularios que incluyen nos dirigen a sitios web falsos, donde los atacantes recogen tus datos personales.

Ejemplos: Existen diversos tipos de correos o mensajes de phishing, algunos de los cuales incluyen:

- **Páginas web falsas que imitan páginas reales**: Un ejemplo común de phishing es la creación de páginas web falsas que imitan perfectamente la página oficial de una empresa, banco o servicio en línea. Estas páginas utilizan el mismo diseño, logotipos e incluso la misma URL (con pequeñas variaciones, como un número o letra adicional). La principal diferencia es que, al introducir tus datos personales o contraseñas, estos son recogidos por el atacante. Un ejemplo típico puede ser una página falsa de inicio de sesión, donde la URL puede parecer similar, como https://www.paypall.com en vez de https://www.paypal.com. Si te fijas, la diferencia está en la 'l' añadida al final.

- **Enlaces falsos con texto engañoso**: Otro ejemplo común de phishing es cuando se muestra un enlace con un texto que parece fiable, pero en realidad el enlace dirige al atacante a un sitio web malicioso. Por ejemplo, un correo electrónico puede contener un enlace que dice "Para más información, accede a https://gl.wikipedia.org", pero cuando pases el cursor sobre el enlace, verás que la URL realmente lleva

a un sitio completamente diferente. En este caso, puedes ver que al pinchar en https://gl.wikipedia.org realmente estás siendo redirigido a https://galicia.isf.es/.

- **Uso de caracteres de alfabeto diferente**: Otro truco que se emplea en el phishing es el uso de caracteres que se parecen a los del alfabeto latino, pero que realmente pertenecen a otro alfabeto. Por ejemplo, un atacante puede utilizar caracteres cirílicos o griegos que son visualmente semejantes a las letras del alfabeto latino. Una URL falsa como http://www.google.com (donde la 'o' es un carácter cirílico que parece una 'o' normal) puede engañar a la víctima haciendo que piense que está visitando el sitio web oficial de Google, cuando en realidad está siendo dirigida a un sitio malicioso.

- **Subdominios**:Un ejemplo común de ataque de phishing relacionado con los subdominios es cuando un atacante crea un subdominio que parece oficial, pero que en realidad no lo es, intercambiando el subdominio y el dominio principal. Por ejemplo, un correo en el que nos envían un correo diciendo que tenemos una notificación pendiente y que tenemos que iniciar sesión en https://xunta.sede.gal/identificate, para robarnos la contraseña, cuando la dirección real de la sede electrónica de la xunta es https://sede.xunta.gal/identificate. Recordatorio importante: los subdominios deben ser leídos de derecha a izquierda. Otro ejemplo similar ocurre cuando intentan hacernos creer que tenemos que entrar en https://sede.xunta.gal-identificate.gal, en lugar de https://sede.xunta.gal/identificate. Es importante leer las direcciones enteras.

- **Códigos QR falsos**: Hoy en día estamos habituadas a tener que escanear códigos QR para muchas cosas: ver el menú en un restaurante, ver información sobre cuándo llega el próximos autobús, etc. Escaneamos el QR, le damos a abrir, y listo. Sin embargo, debemos tener más cuidado. Cuando escaneamos un código QR debemos fijarnos antes de darle a abrir a qué página nos está dirigiendo (la mayoría de las aplicaciones muestran primero el enlace y luego piden confirmación para abrirlo), y tener en cuenta los consejos mencionados anteriormente. Por ejemplo, alguien podría haber pegado un QR falso encima del auténtico, y redirigirnos a una página muy semejante a la auténtica, pero con el objetivo de robarnos información de algún tipo.

10.2 Spoofing

El spoofing es un ataque en el que un atacante finge ser otra persona o sistema para engañar al destinatario o a la red. Este ataque puede ocurrir en diversas formas, como spoofing de direcciones de correo electrónico, de IP o de DNS. El objetivo principal es engañar a las usuarias o sistemas para que confíen en el atacante y, así, obtengan acceso a datos o sistemas.

Ejemplos:

- **Spoofing de correo electrónico**: El spoofing de correo electrónico es un ataque en el que el atacante falsifica la dirección del remitente de un correo electrónico para que parezca que proviene de una fuente fiable, cuando en realidad fue enviado desde otra fuente. Por ejemplo, aunque en el encabezado del correo aparezca que fue enviado desde a@email.com, el atacante puede modificar los datos para que

parezca que el correo proviene de esa dirección, cuando en realidad fue enviado desde otro servidor. Esto puede engañar a la víctima, haciéndola creer que el correo es de confianza, lo que puede llevar a que realice acciones como hacer clic en enlaces o descargar archivos maliciosos.

Esto ocurre porque el protocolo de correo electrónico, como SMTP (Simple Mail Transfer Protocol), no verifica de forma exhaustiva la autenticidad de la dirección del remitente. La dirección del remitente que aparece en el encabezado de un correo electrónico puede ser manipulada fácilmente por el atacante. El servidor de correo que envía el mensaje solo transmite la información del remitente que se le indica, sin realizar validaciones profundas sobre si esa dirección realmente pertenece a quien dice que pertenece.

Para evitar este tipo de ataques, es recomendable verificar la autenticidad de los correos, no hacer clic en enlaces sospechosos y emplear protocolos de seguridad.

- **SMS Spoofing**: El spoofing por SMS es un tipo de ataque en el que los ciberdelincuentes envían mensajes de texto que parecen venir de una fuente fiable, como un banco o una empresa conocida. Para ello, los atacantes pueden manipular el número de teléfono o el nombre que aparece en el encabezado del mensaje, haciendo que se asemeje a que el mensaje viene de, por ejemplo, tu banco y aparezca en la misma conversación en la que el banco te envió previamente otros SMS. Esto se consigue a través de una técnica llamada alphanumeric sender ID o sender name, que permite que, en lugar de ver un número de teléfono, se muestre un nombre o etiqueta, como el nombre del banco. Así, al recibir el SMS, la usuaria puede ver algo como "BANCO" en vez de un número, lo que genera confianza en el mensaje.

  Aunque este mecanismo puede ser útil para identificar mensajes oficiales, también puede ser explotado por los atacantes para falsificar el origen del SMS y hacer que parezca venir de una fuente fiable. Por ejemplo, el atacante puede configurar su sistema para que aparezca el nombre de un banco o de una empresa conocida, cuando en realidad está enviando el mensaje desde un número diferente. Esto facilita que las víctimas caigan en un intento de phishing o fraudes, ya que confían en la apariencia del mensaje sin verificar su autenticidad.

  Por eso, es importante ser cauteloso con los mensajes recibidos, incluso cuando parece que vienen de una fuente oficial, y no confiar únicamente en el nombre o número que aparece en el encabezado del SMS. Verificar siempre los enlaces, números y remitentes puede evitar caer en ataques de spoofing.

10.3 Ataque Man-in-the-Middle (MITM)

Un **ataque Man-in-the-Middle (MITM)** es un tipo de ataque en el que la persona atacante intercepta y, en algunas ocasiones, manipula la comunicación entre dos partes que están intentando comunicarse entre sí. En este ataque, la víctima y el destino de la comunicación (por ejemplo, un servidor u otra usuaria) creen que se están comunicando de forma directa, pero en realidad, todo el tráfico pasa por el atacante, que puede leer, alterar o redirigir esa información.

10.3.1 ¿Cómo funciona un ataque MITM?

- **Intercepción de comunicación**: El atacante se coloca entre las dos partes que se están comunicando. Esto puede ocurrir, por ejemplo, en redes Wi-Fi públicas o no seguras, donde el atacante se hace pasar por un punto de acceso (access point) legítimo, conocido como un ataque de Evil Twin. Las víctimas se conectan a su red, y todo su tráfico de datos pasa por ella.

- **Descifrado de la comunicación**: Si las comunicaciones entre las dos partes están cifradas (como sucede con el protocolo HTTPs), el atacante puede ser capaz de realizar un downgrade o forzar la conexión a un protocolo menos seguro (por ejemplo, HTTP sin cifrar), o en ciertos casos, aprovechar vulnerabilidades en protocolos de encriptado para descifrar el tráfico.

- **Manipulación de datos**: El atacante también puede modificar los datos que se están transmitiendo entre las víctimas. Por ejemplo, puede alterar una transacción financiera, cambiando el número de la cuenta al que se debe realizar un pago, o añadir datos maliciosos en un mensaje que la víctima espera recibir.

- **Falsificación de identidad**: El atacante también puede hacerse pasar por una de las partes en la comunicación. Esto puede implicar enviar mensajes o solicitar información como si fuese una de las víctimas, añadiendo más complejidad al ataque.

10.3.2 Ejemplo típico de un ataque MITM

Un ejemplo común ocurre cuando una usuaria se conecta a una red Wi-Fi pública no segura, como las que se encuentran en cafeterías o aeropuertos. El atacante establece un punto de acceso que simula ser una red pública abierta. Las víctimas que se conectan a esa red envían tráfico sin cifrar que pasa directamente por el atacante. En este punto, el atacante puede espiar todo el tráfico entre la usuaria y los servidores a los que está intentando conectarse, y puede incluso alterar las solicitudes o respuestas.

Otro escenario en el que se puede producir un MITM es cuando se establece una comunicación HTTPS, pero el atacante consigue engañar a la víctima para que la conexión no se cifre correctamente o pueda acceder a claves de cifrado. Esto puede ser hecho, por ejemplo, mediante un ataque de SSL Stripping, donde el atacante redirige el tráfico HTTPS a HTTP no cifrado. Hay que tener en cuenta que hay páginas que tienen versión HTTP y versión HTTPs.

10.3.3 Cómo evitar un ataque MITM

- **Usar HTTPS**: Siempre que sea posible, asegurate de que las webs utilicen HTTPS en vez de HTTP. El HTTPS cifra la comunicación entre el navegador y el servidor, haciendo mucho más difícil que un atacante pueda interceptar o modificar los datos.

- **Verificar los certificados SSL/TLS**: Al acceder a sitios web, revisa que el certificado SSL/TLS sea válido y que el navegador indique que la conexión es segura (normalmente aparece un candado verde en la barra de dirección).

- **Evitar redes Wi-Fi públicas no seguras**: Siempre que sea posible, evita conectarte a redes Wi-Fi públicas o no cifradas e intente compartir wifi desde tu móvil. Si tienes

que usar una Wi-Fi pública usa una VPN para cifrar todo el tráfico y evitar que un atacante pueda interceptarlo.

- **Habilitar la autenticación de dos factores (2FA)**: La autenticación en dos pasos puede evitar que un atacante obtenga acceso a cuentas importantes, incluso si consigue interceptar la contraseña.

10.3.4 Resumen

Un ataque MITM permite al atacante interceptar, manipular o falsificar la comunicación entre dos partes, lo que puede llevar al robo de información sensible o a la alteración de transacciones. La mejor manera de defenderse contra este tipo de ataque es garantizar que las comunicaciones sean seguras (usando HTTPS), evitar redes no seguras y usar mecanismos de protección adicionales como las VPNs o la autenticación de dos factores.

10.4 Ransomware

El **ransomware** es un tipo de malware que tiene como objetivo secuestrar los datos de una víctima y pedir un rescate para liberarlos. Este tipo de ataque está orientado a la extorsión, pues el atacante intenta forzar a la víctima a pagar una suma de dinero, normalmente en criptomonedas, para que la víctima pueda recuperar el acceso a sus archivos o sistemas. Existen diferentes tipos de ransomware, pero todos comparten la misma estrategia básica de encriptar los archivos o bloquear el acceso al sistema.

10.4.1 Cómo funciona el Ransomware

- **Infección inicial**: El primer paso de un ataque de ransomware es la infiltración en el sistema víctima. Esto puede ocurrir de diversas maneras, como a través de correos electrónicos de phishing, sitios web comprometidos o vulnerabilidades de software. Los ciberdelincuentes también pueden emplear bots u otros métodos automatizados para propagar el malware.

- **Encriptado de archivos**: Una vez que el malware se ejecuta en el sistema de la víctima, este comienza a encriptar los archivos. La mayoría de los ransomware usa algoritmos de cifrado fuertes para garantizar que los archivos no puedan ser abiertos o utilizados sin la clave de descifrado (que solo tiene el atacante). Los archivos afectados pueden ser documentos, fotos, vídeos, bases de datos o cualquier otro tipo de archivo valioso.

- **Exhibición del rescate**: Después de encriptar los archivos, el ransomware muestra un mensaje a la víctima, informando sobre el secuestro y exigiendo un rescate. Normalmente, este mensaje especifica el importe que debe pagar la víctima, así como las instrucciones para realizar el pago (normalmente en criptomonedas, debido a su naturaleza anónima).

- **Bloqueo del sistema**: Algunos tipos de ransomware también pueden bloquear completamente el acceso al sistema o a la red de la víctima, impidiendo que se puedan

realizar cualquier actividad hasta que se pague el rescate. Este tipo de ataque también puede incluir el cifrado de dispositivos de almacenaje conectados a la máquina principal o a redes internas.

- **Filtración de datos**: Algunas variantes de ransomware, como el Ransomware as a Service (RaaS), también roban datos sensibles antes de encriptarlos, para usarlos como parte de la extorsión. En estas variantes, los atacantes amenazan con divulgar o vender los datos robados si la víctima no paga el rescate.

10.4.2 Ejemplos de Ransomware Famosos

Existen varios tipos de ransomware que se hicieron famosos por afectar a organizaciones e individuos en todo el mundo:

- **WannaCry**: Este ataque, que se produjo en mayo de 2017, afectó a miles de dispositivos en todo el mundo, incluyendo hospitales, empresas y agencias gubernamentales. Utilizó una vulnerabilidad en el sistema operativo Windows, conocida como EternalBlue, para propagar el malware y encriptar los archivos de las usuarias.
- **NotPetya**: Otro ataque importante, dirigido también a dispositivos con el sistema operativo Windows, afectó a empresas y entidades en Europa, especialmente en el sector financiero y en el ámbito de las infraestructuras críticas. Aunque inicialmente parecía ser un ataque de ransomware, su objetivo real era la destrucción de datos, ya que la clave de descifrado nunca fue proporcionada.
- **Ryuk**: Este es un ransomware que fue dirigido principalmente a organizaciones grandes y gobiernos, y dirigido a dispositivos con el sistema operativo Windows. A diferencia de otros tipos de ransomware, Ryuk está muy enfocado en el robo de datos de alto valor y en la exigencia de grandes sumas de dinero por el rescate. Ryuk también se usa en combinación con otros tipos de malware, como TrickBot, para obtener acceso a las redes internas de las víctimas.

10.4.3 Cómo protegerse del Ransomware

- **Realiza copias de seguridad regulares**: Tener copias de seguridad actualizadas es la mejor defensa contra el ransomware. Si un sistema es secuestrado, puede restaurarse rápidamente a partir de una copia de seguridad sin tener que pagar el rescate. Es importante que las copias de seguridad estén almacenadas en lugares externos o en nubes seguras que no sean accesibles desde la red local. Hay que tener en cuenta que no es una solución segura al 100 %, ya que el ransomware puede ser preparado para que se ejecute tiempo después de infectar a los dispositivos, por lo que las copias de seguridad podrían llegar a estar infectadas también,
- **Mantén el software actualizado**: La mayoría de las infecciones de ransomware aprovechan vulnerabilidades de software para infiltrarse en los sistemas. Mantener los sistemas operativos, las aplicaciones y los programas antivirus actualizados puede reducir el riesgo de infecciones.
- **No hagas clic en enlaces o archivos sospechosos**: Muchas veces, los ataques de ransomware comienzan a través de correos electrónicos de phishing o sitios web

comprometidos. No hagas clic en enlaces o descargues archivos de fuentes no fiables. También debes ser cautelosa cuando se reciben mensajes de remitentes desconocidos, especialmente si incluyen archivos adjuntos o enlaces.

- **Usar software de seguridad robusto**: Asegúrate de tener instalado un programa antivirus actualizado y configurar un firewall para impedir la entrada de malware en tu red. Algunos programas antivirus también tienen detección de ransomware, lo que puede ayudar a bloquear el malware antes de que se ejecute. También hay que tener en cuenta que casi la totalidad de ataques están dirigidos a dispositivos con el sistema operativo Windows, por lo que emplear alternativas libres como GNU/Linux disminuye las posibilidades de ser infectada.

10.4.4 Conclusión

El ransomware sigue siendo una amenaza significativa para empresas e individuos, causando daños financieros y pérdida de datos. Adoptar buenas prácticas de seguridad, como realizar copias de seguridad regulares, mantener el software actualizado y ser cautelosa con las fuentes y enlaces de correos electrónicos, puede ayudar a minimizar los riesgos y proteger la información personal y corporativa. Si bien pagar el rescate puede parecer una solución, es importante recordar que no hay garantías de que el atacante libere los datos o no vuelva a atacar en el futuro. Y si eres infectada, el primer paso debe ser avisar a las autoridades.

10.5 Keylogging

El **keylogging** es un tipo de ataque informático en el que el atacante instala un programa malicioso (conocido como keylogger) en el sistema de la víctima. El objetivo del keylogger es registrar las teclas que la víctima pulsa en el teclado, pudiendo capturar información sensible como contraseñas, números de tarjetas de crédito, mensajes privados y otra información confidencial.

10.5.1 Cómo funciona el Keylogging

Un keylogger puede operar de diferentes formas. Lo más común es que el software malicioso se instale sin el conocimiento de la víctima, por ejemplo, a través de correos electrónicos de phishing o software de descargas comprometidas. Una vez instalado en el sistema, el keylogger comienza a monitorizar las acciones del teclado y a almacenar los datos sobre las teclas pulsadas.

Los keyloggers pueden ser de diferentes tipos:

- **Keyloggers de software**: Este tipo de keylogger es una aplicación maliciosa que se ejecuta en el sistema de la víctima. Puede ocultarse en el fondo y ser difícil de detectar. Los keyloggers de software son los más comunes y pueden registrar todas las teclas, incluyendo contraseñas y datos bancarios, sin que la víctima se dé cuenta.

- **Keyloggers de hardware**: Este tipo de keylogger es un dispositivo físico que se conecta entre el teclado y el ordenador. Puede ser colocado en el conector USB o PS/2, o en el propio teclado, para registrar las teclas pulsadas. Su ventaja es que no

depende del sistema operativo, por lo que puede registrar las teclas incluso cuando el sistema operativo está infectado o no funciona correctamente.

Keyloggers de pantalla táctil: En los dispositivos móviles, los keyloggers también pueden capturar las acciones realizadas en pantallas táctiles. Aunque no registran las teclas de forma directa, pueden capturar los movimientos de giros o toques realizados en la pantalla e incluso las teclas virtuales que se pulsan en dispositivos móviles.

10.5.2 Ejemplos de Keylogging

Un ejemplo de keylogger muy común es el software malicioso que se infiltra a través de correos electrónicos de phishing. Vamos a imaginar que un atacante envía un correo de phishing simulando ser una entidad fiable, como un banco o un servicio en línea. El correo puede incluir un enlace que lleva a un sitio web falso o un archivo adjunto. Si la víctima hace clic en el enlace o abre el archivo, el keylogger puede ser instalado en su sistema sin que se percate, comenzando a registrar las teclas pulsadas.

Un ejemplo más específico de keylogger de hardware sería un dispositivo que se conecta entre el teclado y el ordenador, siendo invisible a la víctima. Estos dispositivos pueden ser usados, por ejemplo, en cibercafés o en ordenadores públicos para robar información sensible sin que la víctima sea consciente de su presencia.

10.5.3 Cómo protegerse del Keylogging

- **Mantén el sistema operativo y las aplicaciones actualizadas**: Los keyloggers, como otros tipos de malware, a menudo explotan vulnerabilidades en los sistemas operativos o en las aplicaciones para infiltrarse. Mantener el sistema y las aplicaciones actualizadas ayuda a cerrar esas brechas de seguridad.

- **Evitar clics en enlaces sospechosos**: No hagas clic en enlaces o descargues archivos de fuentes no confiables. Los keyloggers de software suelen instalarse cuando se hace clic en un enlace malicioso o se descarga un archivo de phishing.

- **Usar contraseñas de dos factores**: Incluso si un keylogger captura tus contraseñas, el uso de contraseñas de dos factores (2FA) puede añadir una capa adicional de seguridad. Aunque el atacante tenga tu contraseña, necesitaría acceso al dispositivo adicional (como un teléfono móvil) para completar la autenticación.

- **Evitar dispositivos públicos o compartidos**: No emplees teclados públicos u ordenadores compartidos para introducir información sensible, como contraseñas o datos bancarios. Si tienes que usar un equipo compartido, considera usar un teclado virtual o una aplicación de autenticación adicional.

- **Usar teclados virtuales o programas de protección contra keyloggers**: Algunas herramientas permiten introducir texto sin usar el teclado físico, como teclados virtuales en la pantalla o programas que protegen contra keyloggers detectados. Estas herramientas pueden ofrecer una capa adicional de seguridad cuando se introducen datos sensibles.

10.5.4 Conclusión

El keylogging es una amenaza importante para la seguridad y la privacidad de las usuarias. Las víctimas pueden sufrir robo de datos sensibles sin saber que están siendo vigiladas. Para protegerse de este tipo de ataque, es fundamental tomar medidas preventivas como el uso de software de seguridad actualizado, la práctica de buenos hábitos de navegación y la adopción de medidas de autenticación fuertes, como la autenticación en dos pasos.

10.6 Conclusión de los ataques informáticos

Los ataques informáticos son una amenaza constante en nuestra vida digital, y los ejemplos que presentamos son solo algunos de los muchos que existen. Desde el phishing hasta los ataques de man-in-the-middle o el uso de malware como los keyloggers, los atacantes emplean técnicas sofisticadas para obtener acceso a información sensible y vulnerar nuestra privacidad. Sin embargo, con cuidado y conocimiento, podemos reducir considerablemente el riesgo de ser víctimas de estos ataques. La implantación de prácticas de seguridad, como el uso de contraseñas fuertes, la autenticación en dos pasos, y la precaución al interactuar con nuestras cuentas en línea, puede ayudar a proteger nuestra información. Lo más importante es mantenerse informado, estar alerta ante posibles amenazas y actuar para garantizar nuestra seguridad en el mundo digital.

11 Los Sistemas Operativos. Alternativas libres y seguras.

En este capítulo os hablaremos del sistema operativo, explicando qué es y la importancia de usar alternativas libres.

11.1 ¿Qué es un sistema operativo?

Un **sistema operativo** es el software fundamental que gestiona y controla el hardware de un ordenador, móvil u otro dispositivo electrónico. Actúa como un puente entre la usuaria y el hardware, permitiendo que se ejecuten aplicaciones y garantizando que los recursos del sistema (procesador, memoria, almacenamiento, dispositivos de entrada/salida, etc.) se utilicen de forma eficiente.

11.1.1 Funciones principales de un sistema operativo

- **Gestión de procesos**: controla la ejecución de los programas, asignando tiempo de procesador y garantizando que funcionen correctamente sin interferencias.
- **Gestión de la memoria**: distribuye la memoria disponible entre los diferentes programas en ejecución.
- **Gestión de almacenamiento**: organiza y controla el acceso a los archivos y directorios en el disco duro u otros medios de almacenamiento.
- **Gestión de dispositivos**: permite que el hardware, como impresoras, teclados o cámaras, funcione correctamente y sea reconocido por el sistema.
- **Seguridad y permisos**: protege los datos de la usuaria, evita accesos no autorizados y gestiona cuentas de usuaria.
- **Interfaz de usuaria**: ofrece una forma de interactuar con el ordenador, ya sea mediante una línea de comandos (CLI) o una interfaz gráfica (GUI).

11.1.2 Ejemplos de sistemas operativos

- **Para ordenadores**: GNU/Linux (Ubuntu, Debian, Fedora…), Windows, macOS.
- **Para móviles**: Android, iOS.
- **Para servidores y dispositivos embebidos**: FreeBSD, OpenWRT...

Sin un sistema operativo, los dispositivos electrónicos serían muy difíciles de usar, ya que cada programa tendría que gestionar directamente el hardware.

11.2 ¿Por qué es importante emplear sistemas operativos libres?

Un **sistema operativo libre** es aquel que respeta las libertades de las usuarias para ejecutar, estudiar, modificar y distribuir el software. Ejemplos destacados son **GNU/Linux** y **FreeBSD**. Optar por un sistema operativo libre ofrece múltiples ventajas, tanto en términos de seguridad como de privacidad y control sobre el propio dispositivo.

11.2.1 Ventajas de emplear software libre

- **Transparencia y seguridad**: El código fuente está disponible para que cualquiera pueda revisarlo, detectar vulnerabilidades y mejorarlo. Esto reduce la posibilidad de puertas traseras o software malicioso oculto.
- **Privacidad**: Sistemas privativos como Windows recopilan datos de las usuarias sin su consentimiento explícito. Los sistemas libres, en cambio, permiten un mayor control sobre la información personal.
- **Control total**: Las usuarias pueden modificar y adaptar el sistema a sus necesidades, sin restricciones impuestas por empresas que buscan maximizar sus beneficios.
- **Personalización**: Existen múltiples distribuciones (versiones) de GNU/Linux, permitiendo escoger la que mejor se adapte a cada uso (trabajo, juegos, servidores, etc.).
- **Actualizaciones constantes**: La comunidad desarrolladora mantiene y mejora los sistemas operativos libres de manera continua, asegurando que los errores y vulnerabilidades sean corregidos rápidamente.
- **Sostenibilidad y revalorización del hardware**: Muchos sistemas operativos libres están optimizados para funcionar en equipos antiguos, dándoles una nueva vida y reduciendo la necesidad de comprar nuevos dispositivos.
- **Independencia tecnológica**: El software libre no está controlado por una única corporación, evitando situaciones donde una empresa puede decidir dejar de dar soporte a un sistema, forzando a las usuarias a cambiar de hardware o software.

11.2.2 Problemas del software privativo

- **Código cerrado**: No se puede ver ni modificar, por lo que las usuarias dependen totalmente de la empresa desarrolladora.
- **Monopolios y restricciones**: Empresas como Microsoft y Apple imponen condiciones sobre cómo usar sus sistemas, limitando la libertad de las usuarias.
- **Recolección de datos**: Muchos sistemas privativos integran sistemas de rastreo y telemetría que espían los hábitos de las usuarias.

- **Obsolescencia programada**: Algunos sistemas operativos privativos dejan de dar soporte a hardware antiguo para incentivar la compra de nuevos dispositivos, aumentando la basura electrónica.

11.3 Alternativa libre para el ordenador. Qué es GNU/Linux y cómo instalarlo

GNU/Linux es un sistema operativo basado en el núcleo **Linux** y en el conjunto de herramientas del proyecto **GNU**. La combinación de estos elementos permite crear un sistema libre, seguro y altamente personalizable, empleado tanto en servidores como en dispositivos personales.

11.3.1 Diferencia entre el núcleo (kernel) y una distribución

Para comprender GNU/Linux, es importante diferenciar entre el **núcleo** y las **distribuciones**:

- **Kernel**: Es la parte fundamental del sistema operativo, encargada de gestionar el hardware y permitir la comunicación entre el software y los componentes físicos del ordenador (procesador, memoria, disco duro, etc.). Linux es el núcleo usado en todas las distribuciones GNU/Linux.
- **Distribución**: Es una versión de GNU/Linux que incluye el núcleo Linux, herramientas de software, gestores de paquetes y una interfaz gráfica. Existen muchas distribuciones, adaptadas a diferentes usos y necesidades.

11.3.2 Ejemplos de distribucións populares

- **Linux Mint**: Basada en Ubuntu o Debian (la versión LMDE), con una interfaz similar a Windows para facilitar la transición de nuevas usuarias.
- **Ubuntu**: También ideal para usuarias principiantes, con buena compatibilidad de hardware y una gran comunidad de soporte.
- **Debian**: Estable y segura, preferida en servidores y sistemas que requieren fiabilidad a largo plazo.
- **Arch Linux**: Para usuarias avanzados que quieren personalizar completamente su sistema desde cero.

11.3.3 Sabores de una distribución: los entornos de escritorio

En GNU/Linux, el núcleo del sistema y sus aplicaciones pueden funcionar con diferentes **entornos de escritorio**, que determinan la apariencia y funcionalidad de la interfaz gráfica. Muchas distribuciones ofrecen distintos "sabores" basados en el mismo sistema, pero con distintos entornos de escritorio para adaptarse a las preferencias de la usuaria.

¿Qué es un entorno de escritorio?

Un entorno de escritorio es un conjunto de software que proporciona una interfaz gráfica de usuaria (GUI). Incluye gestores de ventanas, paneles, iconos, menús y herramientas de configuración. A diferencia de otros sistemas operativos que tienen una única interfaz predeterminada (como Windows), en GNU/Linux se puede escoger entre varias opciones según el rendimiento, la estética o las funcionalidades que se prefieran.

Principales entornos de escritorio

- **Cinnamon**:
  - Diseño clásico e intuitivo, muy similar a Windows.
  - Interfaz elegante y con efectos visuales agradables sin perder rendimiento.
  - Distribuciones que lo usan: Linux Mint (entorno por defecto), Debian Cinnamon, etc.
- **GNOME**:
  - Usa un diseño basado en gestos y una barra lateral (llamada dock) en lugar del menú clásico.
  - Consume más recursos.
  - Distribuciones que lo usan: Ubuntu (edición principal), Fedora, Debian, etc.
- **KDE Plasma**:
  - Altamente personalizable y con efectos visuales avanzados.
  - Ofrece muchas opciones de configuración y herramientas nativas potentes.
  - Distribuciones que lo usan: Kubuntu, KDE Neon, openSUSE, etc.
- **XFCE**:
  - Enfoque en ser ligero y rápido, ideal para equipos con pocos recursos.
  - Interfaz clásica y sencilla, sin consumir demasiada memoria RAM.
  - Distribuciones que lo usan: Xubuntu, Manjaro XFCE, Debian XFCE, etc.
- **LXQt**:
  - Aún más ligero que XFCE, pensado para equipos antiguos o con poca potencia.
  - Interfaz sencilla y funcional, con bajo consumo de recursos.
  - Distribuciones que lo usan: Lubuntu, LXQt en Arch Linux, etc.
- **MATE**:
  - Basado en el antiguo GNOME 2, manteniendo un diseño tradicional y eficiente.
  - Distribuciones que lo usan: Ubuntu MATE, Debian MATE, Manjaro MATE, etc.

¿Cómo escoger un entorno de escritorio?

La elección de un entorno de escritorio depende de las necesidades y preferencias de la usuaria. Si se busca un sistema ligero para un ordenador antiguo, opciones como XFCE o LXQt son recomendables. Si se quiere una experiencia moderna y fluida, GNOME o KDE Plasma son buenas opciones. Por otro lado, Cinnamon y MATE son ideales para quienes prefieren una interfaz clásica y fácil de usar, equilibrando consumo de recursos y estética.

Muchas distribuciones permiten instalar múltiples entornos de escritorio y cambiarlos en la pantalla de inicio de sesión, por lo que siempre es posible probar diferentes opciones hasta encontrar la más adecuada.

11.3.4 Cómo instalar GNU/Linux en un ordenador

La instalación y uso de GNU/Linux puede parecer compleja al principio, pero sigue un proceso sencillo. En ESF tenemos una serie de Bancos de Reciclaje Electrónico con Software Libre donde estaremos encantadas de ayudarte. También tenemos un vídeo en el que un voluntario explica los distintos pasos. Los pasos básicos son los siguientes:

1. **Escoger una distribución**: Dependiendo de las necesidades de la usuaria, se puede descargar una ISO desde el sitio web oficial de la distribución elegida.
2. **Crear un USB de instalación**: Se puede emplear el comando `dd` o herramientas como **Balena Etcher**.
3. **Arrancar desde el USB**: Reiniciar el ordenador y acceder a la BIOS/UEFI (normalmente pulsando F2, F12 o Supr al iniciar) para seleccionar el USB como dispositivo de arranque.
4. **Probar o instalar**: Muchas distribuciones permiten probar el sistema en modo Live antes de instalarlo. Si se decide instalar:
   - Seleccionar el idioma y la configuración del teclado.
   - Configurar las particiones del disco (la opción automática es suficiente para la mayoría de las usuarias).
   - Escoger un nombre de usuaria y contraseña.
   - Iniciar el proceso de instalación.
5. **Reiniciar el ordenador**: Una vez finalizada la instalación, retirar el USB cuando lo indique en la pantalla e iniciar el sistema GNU/Linux instalado. Y listo.

11.4 Alternativas libres para móviles y cómo instalarlas

La mayoría de los teléfonos inteligentes funcionan con sistemas operativos privativos como Android (la versión que incluye los Google Play Services, y que es la instalada en la mayoría de los dispositivos) o iOS, que restringen la libertad de la usuaria y recopilan una gran cantidad de datos personales. Afortunadamente, existen alternativas libres y más respetuosas con la privacidad que permiten recuperar el control sobre el dispositivo.

11.4.1 Sistemas operativos libres para móviles

Existen varias opciones de sistemas operativos libres basados en Android, pero que no incluyen servicios y telemetría de Google. Aquí vamos a destacar tres:

- GrapheneOS:
  - Basada en Android, pero con importantes mejoras de seguridad y privacidad.
  - No incluye servicios de Google, garantizando más independencia y menor rastreo.
  - Solo es compatible con dispositivos Pixel.
- LineageOS:
  - Una de las opciones más populares, basada en Android pero sin software privativo de Google.
  - Permite instalar microG opcionalmente, para compatibilidad con aplicaciones que requieren los servicios de Google.
  - Compatible con una amplia variedad de dispositivos. Aquí podéis ver la lista de dispositivos compatibles.. Y dentro de cada uno encontrarás una guía detallada de la instalación.
- /e/OS:
  - Sistema operativo libre con servicios sustitutivos de Google. Se basa en Android, por lo que es compatible con la mayoría de aplicaciones.
  - Ofrece una tienda de aplicaciones con aplicaciones libres y privativas analizadas en términos de rastreo.
  - Aquí puedes ver la lista de dispositivos compatibles.. También encontrarás las instrucciones de cómo instalarlo.

11.4.2 No siempre se puede

Por desgracia, a diferencia del caso de los ordenadores, no todos los móviles permiten cambiar el sistema operativo, ya que algunos vienen bloqueados de fábrica. Un ejemplo más de cómo los fabricantes buscan que vayas cambiando de móvil cada pocos años y generando más basura. A la hora de comprar un móvil nuevo, es recomendable visitar las páginas web de proyectos como LineageOS o GrapheneOS para ver la lista de dispositivos soportados.

Instalar un sistema operativo libre en el móvil permite recuperar la privacidad y el control sobre el dispositivo, pero requiere cierta planificación y conocimiento técnico. Si se elige la opción adecuada, puede ser una excelente alternativa a Android con Google o a iOS.

11.5 Tails OS, un sistema operativo para ir un paso más allá.

Tails OS (The Amnesic Incognito Live System) es una distribución de Linux basada en Debian, diseñada específicamente para preservar la privacidad y el anonimato de sus usuarias. Funciona como un sistema en vivo, ejecutándose desde un USB sin dejar rastros en el ordenador utilizado. Esto lo convierte en una herramienta ideal para aquellas personas que necesitan proteger su identidad y comunicaciones en casos más extremos.

11.5.1 Características principales

- **Anonimato en línea:** Todas las conexiones de Tails están obligatoriamente canalizadas a través de la red Tor, garantizando que la actividad de la usuaria permanezca oculta.
- **No deja rastros:** Al ejecutarse en modo live, Tails no guarda ninguna información en el ordenador a menos que la usuaria lo especifique. Una vez apaguemos el ordenador, todo nuestro rastro se borra inmediatamente, como si no hubiéramos hecho nada.
- **Herramientas de seguridad integradas:** Incluye aplicaciones como el navegador Tor, mensajería cifrada y herramientas de cifrado de archivos para una comunicación segura.

11.5.2 ¿Para quién está pensado?

Tails es especialmente útil para periodistas, activistas, denunciantes y cualquier persona que precise trabajar en condiciones de alta seguridad. Un ejemplo conocido es Edward Snowden, quien utilizó Tails para comunicarse con periodistas al revelar documentos clasificados.

11.5.3 Instalación y uso

Para emplear Tails, se necesita una memoria USB de al menos 8 GB y un ordenador que pueda arrancar desde USB. El proceso de instalación implica descargar la imagen del sistema desde el sitio oficial de Tails y seguir las instrucciones para crear el medio de arranque. En su web tenéis una guía completa sobre cómo instalarlo.

En resumen, Tails es una herramienta poderosa para aquellos que buscan mantener su privacidad en el mundo digital, proporcionando un entorno seguro y efímero para realizar actividades sensibles sin dejar huellas.

11.6 Conclusión

El uso de sistemas operativos libres es fundamental para garantizar la libertad digital, la privacidad y la seguridad de las usuarias. Además, contribuye a un modelo tecnológico más ético y sostenible. Optar por sistemas como **GNU/Linux** no solo permite mayor control sobre nuestros dispositivos, sino que también fomenta una sociedad más justa e independiente de las grandes corporaciones tecnológicas.

12 Smartphones: los mayores recaudadores de información. Consejos para aumentar nuestra seguridad.

Los teléfonos móviles se han convertido en un elemento esencial en nuestra vida diaria, pero también representan un riesgo para nuestra privacidad. Además de todos los consejos mencionados en los capítulos anteriores, en este se dan una serie de consejos específicos para proteger tu privacidad en los dispositivos móviles.

12.1 Consejos generales

- **Actualizaciones del sistema y de las aplicaciones**: Mantener el sistema operativo y las aplicaciones siempre actualizados es una de las mejores defensas contra vulnerabilidades. Las actualizaciones suelen incluir parches de seguridad que corrigen fallos descubiertos recientemente, por lo que es esencial instalar las actualizaciones cuanto antes.

- **Uso de un pin o patrón para proteger tu dispositivo**: es recomendable que para usar tu dispositivo tengas que introducir algún pin, contraseña o patrón de desbloqueo. Esto evita que alguien que tenga acceso a tu dispositivo no pueda acceder a tus aplicaciones y datos. **Ojo con la biometría**. Es cierto que usar nuestra huella o nuestro rostro para desbloquear nuestro dispositivo es muy práctico, sin tener que andar metiendo el pin, patrón o contraseña. Sin embargo, alguien podría acceder a tu dispositivo (e incluso a tu cuenta del banco) si por ejemplo te quedas inconsciente. En el caso del desbloqueo facial, incluso hay casos en los que se logró desbloquear el dispositivo usando una fotografía.

- **Bloqueo específico de aplicaciones**: Si quieres usar igualmente el desbloqueo por biometría, es recomendable que para aplicaciones críticas como puede ser la del banco o tu gestor de contraseñas actives de forma específica el bloqueo por patrón o pin.

- **Permisos de las aplicaciones**: Revisa y controla los permisos que concedemos a las aplicaciones. Muchas aplicaciones piden acceso innecesario a datos o funciones del dispositivo, como la cámara, el micrófono o la localización. Solo concede los permisos estrictamente necesarios para el funcionamiento de la aplicación.

- **Descarga de aplicaciones de fuentes oficiales**: Evita instalar aplicaciones de fuentes no verificadas, e instálalas solo a través de tiendas oficiales como F-Droid, Google Play o la App Store. Las aplicaciones descargadas de fuentes externas pueden contener malware u otros programas maliciosos.
- **Configurar un DNS privado**: Como comentamos en el capítulo 7 sobre DNS seguros, recomendamos configurar un DNS seguro en tu móvil.
- **Emplear aplicaciones libres en la medida de lo posible**: Échale un ojo al capítulo 2 en el que te hablamos sobre alternativas libres a las que usar en tu día a día.
- **Emplear sistemas operativos libres**: En el capítulo 11 te hablamos de qué es un sistema operativo, y en la sección 11.4 te damos una serie de sistemas operativos libres alternativos al Android de Google y a iOS.

12.2 Riesgos de la previsualización de las notificaciones

Muchos dispositivos móviles permiten que las notificaciones de las aplicaciones se muestren en la pantalla de bloqueo o como pancartas emergentes, incluso sin desbloquear el dispositivo. Aunque esta funcionalidad puede ser útil para ver rápidamente mensajes o alertas importantes, también presenta riesgos de seguridad y privacidad.

12.2.1 Exposición de información personal

Si las notificaciones muestran contenido sensible, otras personas podrían acceder a esa información sin necesidad de desbloquear el dispositivo. Esto puede incluir:

- **Códigos de verificación enviados por SMS o aplicaciones de autenticación**, facilitando ataques de suplantación de identidad.
- **Mensajes privados en aplicaciones de mensajería**
- **Correos electrónicos con información confidencial**, como datos bancarios o detalles laborales.
- **Notificaciones de aplicaciones financieras** que podrían revelar saldos o movimientos bancarios.

12.2.2 Facilidad para ataques de Shoulder Surfing

El llamado **Shoulder Surfing** consiste en que alguien observe la pantalla del dispositivo sin permiso, aprovechando situaciones cotidianas, como el uso del móvil en transporte público o en lugares concurridos. Si la previsualización de las notificaciones está activada, una persona puede:

- Leer mensajes privados sin que la usuaria se percate.
- Ver códigos de autenticación de un solo uso (OTP) en tiempo real.
- Obtener información sobre contactos, eventos u otras actividades de la usuaria.

12.2.3 Filtración de información en ambientes laborales

En un entorno profesional, la previsualización de notificaciones puede comprometer información sensible:

- Mensajes con datos de clientes o proyectos que no deberían ser vistos por terceras personas.
- Correos electrónicos internos con información estratégica de la empresa.
- Notificaciones de reuniones o eventos confidenciales que pueden ser aprovechados por terceros.

12.2.4 Medidas de protección

Para minimizar los riesgos asociados a la previsualización de las notificaciones, se recomienda:

- **Desactivar la previsualización en la pantalla de bloqueo**: En los ajustes del sistema, se puede configurar para que solo se vea el remitente o que no se muestre ninguna información hasta que el dispositivo esté desbloqueado.
- **Usar la autenticación biométrica o PIN para ver notificaciones**: En muchos sistemas, es posible configurar que las notificaciones solo se muestren tras la autenticación de la usuaria.
- **Restringir notificaciones sensibles**: Muchas aplicaciones permiten configurar cómo se muestran sus notificaciones, evitando que contenido crítico aparezca en lugares accesibles.
- **Tener cuidado en lugares públicos**: Evitar exponer la pantalla del móvil en lugares donde otras personas puedan ver la información que aparece.

12.3 Riesgos de los smartwatches y el acceso a las notificaciones

Los relojes inteligentes (smartwatches) se han convertido en dispositivos populares que permiten recibir notificaciones, monitorizar actividad física e interactuar con el teléfono sin necesidad de sacarlo del bolsillo. Sin embargo, su comodidad viene acompañada de ciertos riesgos para la privacidad y la seguridad, especialmente cuando tienen acceso total a las notificaciones y a su contenido.

12.3.1 Acceso total a mensajes y datos sensibles

Muchos smartwatches requieren permiso para acceder a todas las notificaciones del teléfono para poder mostrarlas en su pantalla. Esto significa que pueden recibir y almacenar:

- Mensajes privados de aplicaciones

- Correos electrónicos completos
- Códigos de verificación de doble factor (2FA), facilitando ataques de suplantación de identidad.
- Notificaciones de bancos u otras entidades financieras con información sensible.

La mayoría de los smartwatch contienen software privativo, por lo que no podemos saber qué tratamiento le da el fabricante a esos datos. Por ejemplo, podría compartirlos con terceros para distintos tipos de usos. Además, si el smartwatch no tiene mecanismos de seguridad adecuados, cualquier persona puede acceder a esos datos simplemente observando su pantalla o manipulándolo sin restricciones.

12.3.2 Interceptación de datos mediante Bluetooth

Los smartwatches suelen conectarse al teléfono a través de Bluetooth, una tecnología que puede ser vulnerable a ataques como:

- **Ataques de sniffing**: Un atacante puede interceptar la comunicación entre el smartwatch y el teléfono si la conexión no está cifrada correctamente.
- **Ataques Man-in-the-Middle (MitM)**: Si la conexión Bluetooth es comprometida, un atacante puede modificar o escuchar las notificaciones sin que la usuaria lo sepa.
- **Emparejamientos no autorizados**: Algunas vulnerabilidades permiten que dispositivos desconocidos se conecten a un smartwatch sin autorización de la usuaria.

12.3.3 Medidas de protección

Para minimizar los riesgos asociados al uso de smartwatches con acceso a notificaciones, se recomienda:

- **Configurar la privacidad de las notificaciones**: Desactivar la previsualización de mensajes completos en el smartwatch y permitir solo las más necesarias.
- **Activar mecanismos de bloqueo**: Si el smartwatch permite establecer un PIN o algún tipo de bloqueo, activarlo para evitar accesos no autorizados.
- **Revisar los permisos de las aplicaciones**: Asegurarse de que solo las aplicaciones esenciales tienen acceso a las notificaciones.
- **Proteger la conexión Bluetooth**: Mantener Bluetooth desactivado cuando no se use y evitar emparejamientos en lugares públicos.

12.3.4 Conclusión

La integración de los smartwatches con las notificaciones del teléfono es muy útil, pero también introduce riesgos de seguridad y privacidad. La configuración adecuada de los permisos y el uso de medidas de protección puede ayudar a reducir estos riesgos y garantizar un uso más seguro de estos dispositivos.

13 Compras por Internet

Compra local y de proximidad.

Sí, parece obvio, pero a veces olvidamos que la mejor forma de protegernos a la hora de hacer nuestra compra por internet es no comprar en internet. Además, apoyar al comercio local y de proximidad tiene una serie de incontables beneficios añadidos.

Sin embargo, puede que en ocasiones no te quede otra que comprar algo por internet, bien porque no lo encuentras en las tiendas de tu barrio, por ser un producto de segunda mano que se vende por internet, comprar entradas para un evento, pago de servicios que solo permiten hacerlo por internet, etc. A continuación, dejamos una serie de consejos para mejorar tu seguridad y evitar sustos.

13.1 Verificar la legitimidad de la tienda

Antes de realizar una compra, es fundamental asegurarse de que la página web es fiable:

- **Comprobar la URL**: Asegurarse de que comienza por **https://**, indicando una conexión cifrada.
- **Evitar enlaces sospechosos**: No hacer clic en enlaces recibidos por correos electrónicos o mensajes no solicitados.
- **Buscar información sobre la tienda**: Consultar opiniones de otras personas en foros, redes sociales y plataformas de consumidores.
- **Comprobar datos de contacto**: Páginas fiables suelen incluir direcciones físicas, números de teléfono y políticas de privacidad claras.

13.2 Proteger los datos de pago

Los datos bancarios son uno de los objetivos principales de los ciberdelincuentes. Para protegerlos:

- **Usar métodos de pago seguros**: Optar por tarjetas virtuales de prepago con una cantidad limitada de dinero. De esta forma, si alguien consigue todos los datos de tu tarjeta, no podría acceder a tu cuenta principal. Es un servicio ofrecido por casi todos los bancos de forma gratuita.

- **Evitar guardar los datos de la tarjeta**: Muchas tiendas permiten guardar la información de pago para futuras compras sin necesidad de tener que introducir nuevamente el código de seguridad que te manda el banco por SMS, pero es más seguro ingresarla manualmente en cada transacción, ya que si alguien accede a tu cuenta de esa tienda podría comprar cosas sin ningún límite.
- **Emplear PayPal**: PayPal es una de las principales alternativas para comprar por internet de forma segura. Por un lado, hace de puente entre nuestro banco y la tienda electrónica, sin necesidad de exponer nuestros datos bancarios. Por otro lado, en caso de haber algún problema con el producto comprado, si nosotros no llegamos a un acuerdo con la tienda, PayPal se encarga de protegerte y que te devuelvan el dinero. Sin embargo, es importante tener en cuenta ciertas cosas de PayPal para que sea aún más segura:
  - **Activa la autenticación en dos pasos**: Es recomendable activar la autenticación en dos pasos de tu cuenta de PayPal para que al iniciar sesión para pagar, tengas que introducir un código que te llegue por SMS o por la aplicación móvil de PayPal.
  - **Revisa los comercios seguros**: Por defecto, tras hacer una compra PayPal añade de las tiendas en las que compras en una lista de comercios seguros, sin necesidad de tener que introducir nuestra contraseña de PayPal cuando vamos a pagar. Es importante revisar qué comercios tenemos ahí, e intentar no tener ninguno para que siempre tengamos que autenticarnos.
  - **Empléalo como monedero, no asociado a tu banco**: Aunque PayPal permite vincular una tarjeta y/o cuenta bancaria de la que extraerá el dinero en tus compras, es recomendable no hacerlo. Una alternativa es ir metiéndole dinero a medida que lo necesitemos, y de esta forma si alguien accede a nuestra cuenta tendrá un límite de dinero que podrá gastar.
- **Activar la autenticación en dos pasos**: Siempre que sea posible, usar verificación adicional para confirmar pagos.
- **Revisar los extractos bancarios**: Comprobar regularmente los movimientos de la cuenta para detectar cargos sospechosos. Además, en muchos bancos puedes activar que te llegue un aviso cuando se hace algún movimiento.
- **No actives el acceso por biometría**: Como comentamos en la sección 12.1, en caso de que tengas activada la biometría para desbloquear tu dispositivo móvil, es importante que a la aplicación del banco no se pueda acceder sin introducir un segundo pin, contraseña o patrón. Piensa que si alguien consigue que desbloquees el móvil con tu biometría sin ser consciente, podría acceder a tu cuenta bancaria.

13.3 Seguridad en la conexión y en el dispositivo

Asegurar la conexión y el dispositivo desde el que se realizan las compras puede evitar ataques:

- **No comprar desde redes Wi-Fi públicas**: Estas redes pueden ser interceptadas por atacantes. Lo ideal es compartir datos desde tu móvil. Si no hay otra opción, usar una VPN para cifrar la conexión.

- **Mantener el dispositivo actualizado**: Tener el sistema operativo y el navegador actualizados para protegerse de vulnerabilidades.
- **Evitar descargar aplicaciones de fuentes desconocidas**: Si se usa una app para comprar, descargarla solo desde tiendas oficiales como F-Droid o la Play Store.

13.4 Cuidado con las estafas y ofertas falsas

Muchas estafas aprovechan ofertas demasiado buenas para ser ciertas o promesas engañosas:

- **Desconfiar de precios excesivamente bajos**: Si un producto cuesta mucho menos que en otras tiendas, puede ser un fraude.
- **Observar los detalles de las políticas de devolución**: Páginas fraudulentas pueden no ofrecer devoluciones o incluir cláusulas abusivas.
- **Evitar presiones para comprar rápido**: Muchas estafas usan tácticas como "oferta limitada" o "quedan pocas unidades" para forzar decisiones apresuradas.
- **Cuidar los sorteos y premios falsos**: Muchos correos electrónicos y anuncios afirman que la usuaria ha ganado un premio, pero realmente buscan robar información. Si no lo has hecho, échale un vistazo a la sección 10 donde hablamos de este tipo de ciberataques.

13.5 Correo electrónico y notificaciones sospechosas

Los ataques de phishing, como mencionamos en la sección 10.1, suelen estar relacionados con compras en línea. Para evitar caer en estos engaños es recomendable:

- **No abrir enlaces en correos no solicitados**: Si una tienda o banco envía un correo inesperado, acceder a su web manualmente en vez de hacer clic en el enlace.
- **Comprobar la dirección del remitente**: Un correo legítimo viene de una dirección oficial, no de una que contenga errores o dominios extraños.
- **No compartir datos personales por correo**: Ninguna empresa fiable pedirá claves o datos bancarios por mensaje.

13.6 Revisiones después de la compra

Una vez realizada una compra, es recomendable tomar precauciones adicionales:

- **Revisar los cargos en la cuenta bancaria**: Si aparece un cargo inesperado o duplicado, contactar con el banco de inmediato.
- **Verificar el estado del envío**: Usar solo números de seguimiento oficiales, evitando mensajes falsos con enlaces sospechosos.
- **Guardar comprobantes de compra**: Tener registros de la transacción facilita reclamaciones en caso de problemas.

13.7 Conclusión

Las compras en línea pueden ser cómodas y seguras si se toman las precauciones adecuadas. Verificar la autenticidad de las tiendas, proteger los datos de pago, mantener los dispositivos seguros y estar atentos a las estafas ayuda a evitar fraudes y a garantizar una experiencia más fiable. Y ya sabes, siempre que puedas, compra local y de proximidad.

14 Uso en organizaciones

El uso de tecnologías digitales en organizaciones de todo tipo está tan normalizado como su uso de forma individual. Podría parecer que si tienes una buena cultura de autodefensa digital de forma individual, también la tienes de forma colectiva. Pero no es así: de forma colectiva es mucho más importante. ¿Por qué? Porque no te expones solo tú, sino que expones (y te exponen) a las demás personas que integráis la organización. Más aún, expones la propia causa de la organización.

Si a nivel individual ya vimos que estamos expuestos, y que hay individuos y otras organizaciones interesadas en obtener información de nosotros que no queremos compartir, a nivel colectivo ocurre lo mismo.

Por un lado, todas las personas que la integran van a ser objetivos potenciales por los mismos motivos que lo somos cada uno de nosotros de forma individual. Por otro lado, dependiendo de la razón de ser de la organización y de la fuerza que tenga, habrá distintas organizaciones contrarias a vosotras, reaccionarias a vuestros propósitos. Dependiendo de cuánto incomodéis a esas organizaciones y de los medios que tengan, intentarán obtener información sobre vosotras, y una forma de hacer esto es a través de las tecnologías digitales. Pongamos varios ejemplos: No corre el mismo riesgo una organización ecologista concienciada con el mantenimiento de la playa de su ayuntamiento que una que va en contra de los intereses de una multinacional con mucho poder político como ALTRI, que un sindicato que esté en lucha contra una gran empresa de la ciudad, que una organización de inquilinas y afectadas por la hipoteca que cuestione la mercantilización de la vivienda, o que una organización por la liberación de Palestina en la costa oriental del Mediterráneo. La primera puede que nunca sufra un ataque. La segunda probablemente sea espiada para obtener información de las movilizaciones y del discurso para anticiparse y sacar sus posturas en los medios de comunicación, o incluso usar esa información para intentar crear divisiones. La tercera podría sufrir ataques de la empresa contra la que están en lucha, y no sería la primera vez que sindicalistas acaban con problemas legales por culpa de información de la organización que acabó en manos de quien no debía. La cuarta, en vista a los recientes casos, una organización muy poderosa intentará no únicamente hacer ataques digitales, sino infiltrar personas: el Estado. En la última, un fallo puede costar la vida de muchas personas.

Con todo, no podemos olvidar que la organización puede integrar personas con diversos conocimientos, tiempo y habilidades para el cambio. Cada organización debe sopesar qué tan fácil es usar tecnologías digitales más seguras (o usar menos tecnologías digitales en general), valorando los beneficios, los riesgos y el esfuerzo.

En los apartados anteriores vimos diferentes alternativas para las comunicaciones, el almacenamiento de datos o el trabajo en documentos de forma colaborativa, entre otras. Este apartado lo enfocaremos a servir de guía para que cada organización reflexione sobre para qué y cómo quiere usar la tecnología digital, y que sea consciente de sus riesgos.

14.1 Las comunicaciones

A la hora de decidir los canales de comunicación de la organización, tanto con el exterior (redes sociales o página web) como internamente, debe pensarse en qué tipo de información queremos transmitir, a quién y, sobre todo, qué información vamos a estar comunicando sin nosotros quererlo. Hay que recordar que, sobre todo a través de los canales privados, lo que transmitimos por la red siempre va a dejar un rastro imposible de eliminar. Por eso, además de ser cuidadosas con lo que transmitimos, debemos usar, dentro de las posibilidades de la organización, canales seguros como vimos en los otros apartados.

Debemos valorar qué cosas pueden ser comprometedoras si las comunicamos digitalmente. Quizás podamos comunicarlas presencialmente. Además, debemos proteger la identidad de las personas que no quieren ser expuestas o no tienen por qué ser expuestas, y no dejar constancia de información sacada de contexto. Por ejemplo, podemos usar grupos de mensajería en los que no se compartan los números de teléfono, evitar sacar capturas de pantalla de fragmentos de conversaciones y enviarlos a otros grupos, mandar números de teléfono por grupos cuando únicamente lo necesita una persona, mandar fotos de DNIs u otra información personal, entre otros. Algunas de estas prácticas ya no es solo que disminuyan la soberanía digital de la organización, sino que además van en contra de la Ley General de Protección de Datos.

Por último, aunque parezca evidente, debemos tener claro con qué personas estamos compartiendo la información. Si publicamos algo en una web, debemos ser conscientes de que lo que publicamos tiene que ser algo que queremos que conozca cualquier persona que la visite. De igual forma, si tenemos un grupo privado porque por ahí mandamos información que no queremos que salga del interno, debemos ser cuidadosas con las personas que aceptamos en los grupos de comunicación. Recordad que hay organizaciones a las que les gusta infiltrarse en otras.

14.2 La nube

Al igual que en el caso de las comunicaciones, primero de todo debemos valorar qué información necesitamos tener almacenada en la nube. Quizás ni necesitamos una nube. Si la utilizamos, debemos intentar, de nuevo dentro de las posibilidades de la organización, usar tecnologías seguras. Recordemos que sigue existiendo la posibilidad de compartir documentos físicos, y que dependiendo de lo que hagamos puede que los beneficios y comodidades de hacerlo en la nube no compensen los riesgos.

Además, al igual que con las comunicaciones, debemos evitar subir a la nube toda información innecesaria, y que a veces subimos sin darnos cuenta, o sin pararnos a pensar que no tienen por qué tenerla todos los integrantes de la organización, siendo mejor enviarla por privado.

14.3 El teléfono

El teléfono es un dispositivo que normalmente usamos tanto para comunicarnos como para conectarnos a la nube, o para almacenar información, que en parte adquirimos a través de la cámara o del micrófono. Por eso, es un dispositivo muy crítico. Si alguien

accede a nuestro teléfono podría acceder a los grupos de comunicación, a la nube, a los números de teléfono de las compañeras, a fotos, a audios, etc. De nuevo, dependiendo de la actividad de la organización, podemos molestarnos en ser más o menos cuidadosos, y sobre todo valorar qué tipo de información queremos guardar en el teléfono. ¿Necesitamos tener todas las fotos en el móvil o guardar a los contactos con la descripción "Nombre Apellido Organización"? De igual forma, recordemos que podemos movernos sin móvil. ¡Quizás sea contraproducente llevarlo a determinados sitios! Por ejemplo, a una manifestación o acción que sospechamos que va a acontecer sin problemas, podemos llevarlo e incluso sacar fotos para después subirlas a redes sociales. Sin embargo, si sospechamos que puede haber cargas y detenciones, quizás sea mejor no llevarlo, ya que si nos detienen, acceder a un teléfono móvil es muy sencillo, y recordemos que estaríamos exponiendo a toda la organización. ¡Por no hablar de que nos podrían infiltrar el móvil!

14.4 Conclusión

Debemos tener especial cuidado en no transmitir información sin darnos cuenta, sobre todo información personal o comprometedora. Además, no debemos compartir en colectivo aquella información que únicamente necesita una persona.

Tenemos que tener presente a través de qué canal estamos comunicando la información, si se trata de un canal abierto, un canal de personas afines o uno privado. Para mantener la seguridad de cada canal, debemos ser conscientes de las personas a las que aceptamos en cada uno de ellos.

Por último, debemos intentar usar tecnologías seguras. Esto puede ser un esfuerzo grande para la organización, ya que puede haber muchas personas con limitación o reticencias a cambiar a este tipo de alternativas. Forzarlas puede crear reticencias e incluso abandonos. Por eso, las personas más concienciadas y con más conocimientos en esta área, deben fomentar, educar y acompañar en el uso de tecnologías seguras, valorando hasta qué punto vale la pena ir más rápido en el cambio para tener más seguridad, o más lento para no dejar a nadie atrás. No hay que olvidar que una cadena es igual de fuerte que su eslabón más débil, y de poco vale que como organización tengamos una alta conciencia sobre la soberanía digital, si luego dejamos atrás a las compañeras que no adquieren esa conciencia.

Existen varias páginas y foros con información sobre la autodefensa digital para organizaciones. Para las que quieran complementar información, una de ellas es esta: https://406.neocities.org/

15 Móviles y adolescentes

El impacto del acceso descontrolado y cada vez más temprano a móviles inteligentes con internet sin restricciones, está creando muchos conflictos y preocupaciones en la comunidad educativa y también en las familias.

Desde Enxeñería Sen Fronteiras, pensamos que la formación y la actitud de las progenitoras/tutores, junto con los centros escolares, es la clave para solucionar este problema social, un ejemplo de libro de cómo las "tecnologías extractivas" (hechas para hacernos pasar mucho tiempo delante de las pantallas y monetizar nuestra vida digital) nos cogen sin defensas.

No se trata simplemente de manejar conceptos como DNS o control parental. Si nos limitamos a todo este arsenal técnico, sin trabajar las actitudes y valores más profundos de las niñas y adolescentes, será como poner puertas al mar. Conseguiremos, eso sí, una generación impresionante de hackers, expertas en saltarse todas esas barreras.

Desde las familias, hay dos bases importantes sobre las que trabajar, y nos parecen elementos que influyen de manera determinante en cómo podemos educar mejor digitalmente (y también en otros ámbitos) a niñas y adolescentes.

La primera de ellas es **dar ejemplo**. Si no hay acción ejemplar en casa, será complicada la formación de las adolescentes, que suelen señalar también a las personas adultas de su entorno como malas usuarias de los teléfonos inteligentes. Y los datos no les quitan la razón… Es común que las jóvenes tiendan a tener comportamientos en la línea de lo que ven en su hogar. Si hay un uso excesivo e inadecuado del móvil (a horas intempestivas, dejando de lado la comunicación o las actividades con quienes tenemos alrededor), se sentirán legitimadas a usarlo también ellas, pensando además que pueden controlarlo.

La segunda es **dedicar tiempo** a nuestras niñas y adolescentes. Esto da para reflexiones más profundas sobre cómo está montado nuestro sistema socioeconómico, lo que nos demanda la máquina del extractivismo y lo que nos deja de fuerzas para los cuidados. Tal vez deberíamos darle la vuelta a las prioridades, pero eso muchas veces no está en nuestras manos, y tenemos que jugar con las cartas que nos tocan. Lo que sí podemos es no caer en esa exposición a pantallas desde muy jóvenes (incluso bebés), para que sea más fácil darles de comer, o que estén tranquilas en casa o en la cafetería, o en los viajes en coche... El camino largo es dedicarles tiempo, todo el que podamos, no sustituirnos por pantallas ni delegar la educación y el ocio en *reels* de redes sociales. También hablar desde pequeñas de estos temas de educación digital, sexual, etc.

El mundo digital está ahí, es una realidad más (antes solo teníamos la "realidad real"), y no podemos obviar la acción ejemplar que tenemos que tener también en casa, ni tampoco crear burbujas artificiales a la gente joven. Por mucho que se consiga un pacto para el no acceso a smartphones hasta los 16 años, o restringir el uso de las redes sociales hasta esta edad, la educación digital tiene que venir desde mucho antes para que luego cuando tengan acceso a él no estén indefensas. Para eso también tenemos que revisarnos como adultas. Lo ideal, ciertamente, es retrasar lo posible el acceso libre a internet con

estos dispositivos, pero hablando de las razones con las afectadas, aprendiendo formas de poner límites, cultivando la corresponsabilidad y conociendo más de temas técnicos para protegerse. También, por qué no, participando en movimientos de profesorado y progenitoras que trabajan por llevar al debate social y a las políticas públicas ese acceso paulatino y con sentido a los smartphones.