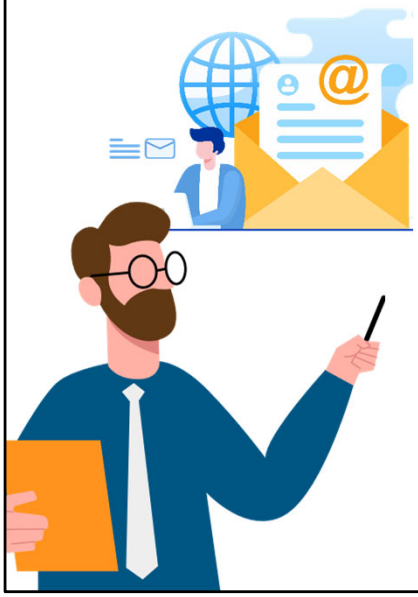
Taller “Seguridad en dispositivos, datos y más…”

ÍNDICE

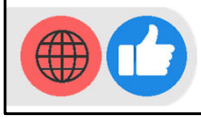


Introducción

1. Seguridad y privacidad en servicios de correo electrónico y redes sociales.
2. Los riesgos de usar una única contraseña para todos los servicios.
3. Descarga de *software* / servicios de sitios oficiales.
4. Descarga de *apps* de sitios oficiales.
5. Copias de seguridad, almacenamiento en la nube y cifrado.

INTRODUCCIÓN

En este taller nos centraremos en las **buenas prácticas relacionadas con el uso seguro y las buenas prácticas en seguridad**.



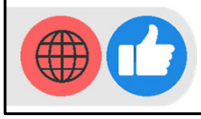
En la actualidad, los servicios web más populares son aquellos basados en el **uso de la información personal de los usuarios**, como es el caso de las redes sociales o el correo electrónico.

Por este motivo, la concienciación en materia de seguridad y privacidad al navegar por Internet se ha convertido en un elemento fundamental para **minimizar el impacto de los riesgos y amenazas vinculadas a la vulnerabilidad de nuestros datos**.

En este taller nos centraremos en las **buenas prácticas relacionadas con el uso seguro de los servicios web más populares**.

1. SEGURIDAD Y PRIVACIDAD DE CORREO ELECTRÓNICO Y REDES SOCIALES

La **configuración de seguridad y privacidad** de nuestros servicios es fundamental para **protegernos frente las amenazas.**



El **correo electrónico** y las **redes sociales** son servicios de Internet que permiten a sus usuarios **conectarse e intercambiar información con otras personas**.

Ambos servicios forman parte de la vida de muchas personas, sin embargo, a pesar de su uso masivo, la concienciación en el uso responsable del correo y las redes sociales es aún una de las asignaturas pendientes más importantes.

La **configuración de seguridad y privacidad de nuestras redes sociales y correo electrónico juegan un papel vital para comenzar a protegernos frente al conjunto de amenazas** al que pueden verse expuestos sus usuarios: infecciones de *malware*, estafas, robos de información, *grooming, cyberbulling*, o *sexting*, entre otras.

1.1 CONFIGURACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO

Pautas para **minimizar los riesgos**:

El uso del **correo electrónico** está muy extendido y cualquier actividad en Internet puede traer una amenaza contra nuestra seguridad. Sin embargo, existen pautas a seguir para configurarlo de forma segura, y minimizar los riesgos:

- **Utilizar contraseñas seguras**. Una contraseña robusta es aquella que contiene letras, números, mayúsculas y minúsculas, caracteres especiales y entre 8 y 10 caracteres. Además, si utilizamos combinaciones de palabras y una para cada servicio, supondrán un gran obstáculo para los atacantes.
- **Iniciar sesión en dispositivos de confianza**. Así, nos aseguraremos de que no dejamos nuestra cuenta abierta o que terceros puedan recuperar nuestras credenciales mediante algún *malware* con el que robar contraseñas.
- **Activar verificación en dos pasos**. Una capa extra de seguridad para nuestra cuenta es utilizando la autenticación de dos factores para introducir un código de seguridad cada vez que nos conectemos: Microsoft Outlook y Gmail.
- **Añadir un número de teléfono o correo alternativo**. De esta forma, estaremos facilitando la recuperación de nuesta cuenta en caso de que alguien consiguiese acceder a ella.
- **Ignorar los correos maliciosos**. Es probable que nos lleguen mensajes maliciosos, como:
    - *Spam*: mensajes no deseados, generalmente de publicidad, que persiguen ganar dinero con el porcentaje pequeño de destinatarios que realmente caigan en el fraude que se envía en el mensaje.

    - *Phishing*: mensajes maliciosos basados en ingeniería social que buscan engañar a sus víctimas para obtener contraseñas, números de tarjetas de crédito, datos de cuentas bancarias, etc.
- En estos casos, lo mejor es ignorar el mensaje, no descargar ningún adjunto y, en caso de incluir una url, revisarla antes con el cursor para ver a donde redirige realmente.
- **Aplicar un filtro de *spam***. La mayoría de gestores de correo electrónico permiten aplicar un filtro a nuestra bandeja de entrada para despreciar aquellos mensajes que contengan publicidad o intenciones maliciosas: Microsoft Outlook y Gmail.
- **Cifrar la información sensible**. En caso de enviar un correo con información personal de carácter sensible, es recomendable cifrar previamente el contenido o, en su defecto, el propio correo. Existen distintos protocolos de cifrado, siendo el más habitual en los gestores de correo el **s/MIME**: Microsoft Outlook y Gmail.

Además, los distintos navegadores cuentan con opciones y modificaciones desde su aplicación que nos permiten ajustar y mejorar estas funcionalidades:

- Opciones de seguridad: Microsoft Outlook y Gmail.
- Opciones de privacidad: Microsoft Outlook y Gmail.

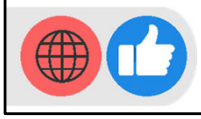
1.2 IDENTIFICACIÓN DE RIESGOS EN REDES SOCIALES

Robos de datos y *malware*

Suplantación de identidad

Fake News o bulos

Acoso



Las redes sociales son un entorno donde la mayor parte de los usuarios se sienten confiados y no se preocupan de las amenazas que abundan en Internet. Sin embargo, nada más lejos de la realidad pues en las redes sociales abundan los perfiles falsos, el *malware* y los ciberdelincuentes:

- **Robo de datos y *malware*:** los ataques de tipo *phishing* son comunes a través de los sistemas de mensajería interna de las redes sociales, así como las publicaciones con promociones y chollos que tratan de llevarnos a una web fraudulenta, de hacer que nos descarguemos un *malware* o engañarnos para que les demos nuestras credenciales o datos bancarios.
- Estos fraudes basados en ataques por ingeniería social son muy comunes y se dan no solo en las redes sociales, sino a través de cualquier canal de comunicación, ya sea en Internet o fuera de este.
- **Suplantación de identidad**: es el principal problema al que nos enfrentamos al utilizar redes sociales. Consiste en recopilar información del usuario a través de las redes sociales y crear un perfil falso con el que llevar a cabo otras actividades ilícitas.
- ***Fake news* o bulos**: Internet está lleno de bulos, pero las redes sociales son uno de los medios donde más extendida está la desinformación. La rapidez con la que puede viralizarse una noticia falsa es mucho mayor que la de una noticia real que, sumado a la falta de buenas prácticas para contrastar información, convierten la desinformación en un riesgo a tener en cuenta al utilizar las redes sociales.
- **Acoso**: algunas personas utilizan las redes sociales para intimidar a otros usuarios

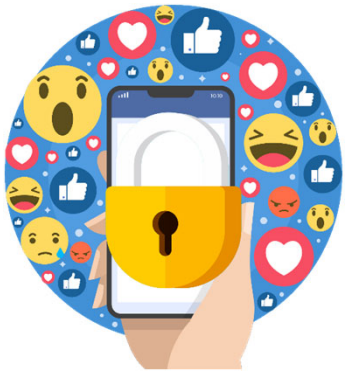
mediante insultos, amenazas, compartiendo fotos o vídeos comprometidos, o mediante la difusión de rumores falsos. Existen varios tipos:

- *Ciberbullying* : generalmente entre menores de edad y de forma reiterada e intencionada mediante la humillación y el abuso contra la víctima.
- *Grooming*: es el acoso que se produce por parte de un adulto hacia menores de edad con intenciones sexuales.
- Sextorsión: se trata de una forma de acoso donde el atacante finge estar en posesión o realmente tiene material íntimo o de carácter sexual de la víctima para extorsionarla y obtener dinero o más material.
- *Sexting*: corresponde al envío de material de índole sexual entre dos personas. Aunque no tiene por qué terminar en un fraude, como la sextorsión, entraña graves riesgos para nuestra seguridad el enviar este tipo de contenido.

Al ciberacoso están expuestos tanto los menores como los adultos, pudiendo generar situaciones verdaderamente dramáticas y complicadas. Si en una red social sufrimos algún tipo de acoso, tenemos que ignorar y bloquear al acosador y guardar las pruebas del acoso: sacar pantallazos y no borrar los mensajes, por ejemplo. Además, debemos informar de la situación al centro de seguridad de la red social y denunciar el acoso a las Fuerzas y Cuerpos de Seguridad del Estado.

1.3 CONFIGURACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LAS CUENTAS DE REDES SOCIALES

Podemos **mejorar la seguridad y privacidad** de nuestras cuentas.



A diario, incluso de forma inconsciente, revelamos información acerca de lo que hacemos, de donde estamos y a donde vamos, de lo que comemos, de cuando nos vamos a dormir, o de cómo nos sentimos.

Además, cualquier interacción que hagamos dentro de la red social con otros contactos o publicaciones también aporta información adicional que puede afectar a nuestra privacidad.

Por defecto, **no siempre las configuraciones en las redes sociales son las óptimas para nuestra seguridad**. Sin embargo, si dedicamos unos minutos, podemos mejorar de forma significativa la seguridad y privacidad de nuestras cuentas.

1.3.1 FACEBOOK

Configuración y privacidad > Configuración > Privacidad:

Para acceder a las opciones de seguridad y privacidad de esta famosa red social, deberemos hacer clic en el desplegable de la esquina superior derecha (Cuenta) y seleccionar **Configuración y privacidad > Configuración > Privacidad**.
En **Tu actividad**, podremos modificar:

- **¿Quién puede ver las publicaciones que hagas a partir de ahora?** para decidir la audiencia que tendrán nuestras publicaciones a partir de ese momento. Pueden ser nuestros **Amigos**, **Amigos, excepto** algún contacto en particular, **Público** para cualquier usuario dentro y fuera de Facebook, o **Más** para seleccionar **Amigos concretos** o **solo nosotros (Solo yo)**. También podemos personalizar una lista para excluir a determinados contactos en determinadas publicaciones. Mediante la opción **Limita la audiencia de tus publicaciones antiguas en tu biografía**, podremos aplicar el filtro anterior a todas las publicaciones antiguas.
- **Revisa todas tus publicaciones y los contenidos en los que se te ha etiquetado**. Así podremos seleccionar, editar o eliminar cualquier publicación donde nos hayan etiquetado en el pasado.

Desde **Cómo pueden encontrarte y ponerse en contacto contigo las personas**, podremos modificar:

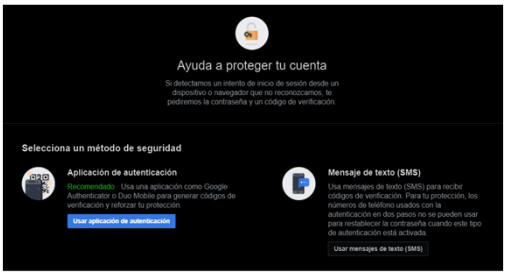
- **¿Quién puede enviarte solicitudes de amistad?** Para permitir que todos los usuarios de la red social puedan hacerlo, solo aquellos amigos de nuestros amigos.
- **¿Quién puede ver tu lista de amigos?** Esta opción permite aplicar un filtro para

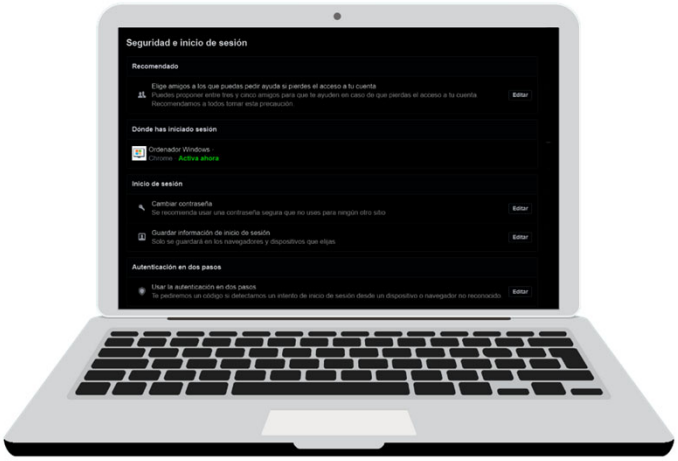
determinar qué usuarios pueden ver nuestros contactos: **Público, Amigos, Amigos (excepto), Amigos (concretos) o Solo yo**.

- **¿Quién puede buscarte con la dirección de correo electrónico que has proporcionado?** Del mismo modo, podemos especificar si queremos que nos encuentren en la red social a partir de nuestro correo electrónico.
- **¿Quién puede buscarte con el número de teléfono que has proporcionado?** Al igual que la opción anterior, podemos filtrar qué usuarios pueden encontrarnos a partir del número de teléfono.
- **¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?** Desactivar esta opción nos desenlazará de los motores de búsqueda, por lo que no podrán encontrar nuestro perfil a través de Google, por ejemplo. Sin embargo, puede llevar algún tiempo.

1.3.1 FACEBOOK (II)

Desde **Configuración > Seguridad e inicio de sesión**:





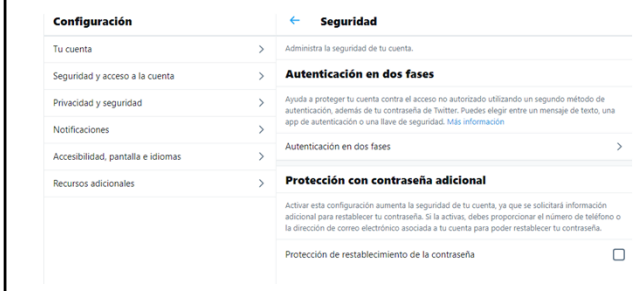
Para acceder a las opciones de seguridad de Facebook, deberemos seguir los mismos pasos, pero esta vez elegiremos **Configuración > Seguridad e inicio de sesión**.

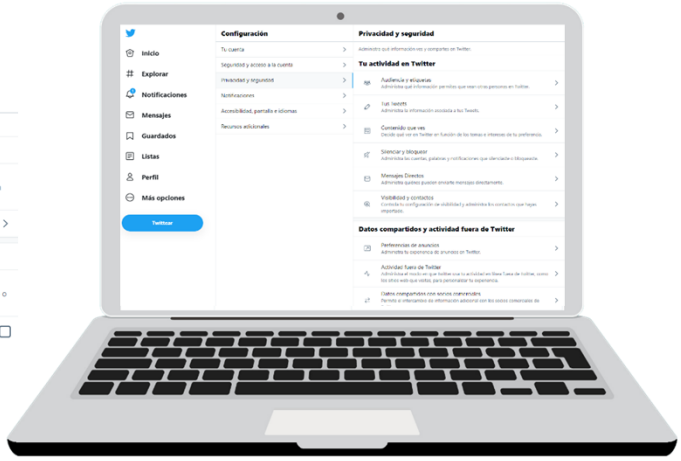
- **Dónde has iniciado sesión**: nos permitirá conocer en qué dispositivos está iniciada nuestra sesión, así como el navegador y la ubicación.
- **Inicio de sesión**: desde aquí podremos cambiar nuestra contraseña o guardar información de inicio de sesión para no tener que volver a introducir nuestras credenciales de acceso la próxima vez que utilicemos el mismo navegador. Así mismo, podremos eliminar esta opción desde la misma configuración.
- **Autenticación en dos pasos**: para configurar esta mejora en la seguridad de nuestra cuenta a partir de una *app* de autenticación o un SMS a un número de móvil. También podremos ver los inicios de sesión autorizados o utilizar contraseñas especiales en las aplicaciones de Facebook para no utilizar nuestra cuenta como forma de acceso.
- **Configurar seguridad adicional**: desde estas opciones podremos seleccionar el canal por el que queremos recibir las alertas sobre inicios de sesión sospechosos, así como elegir un grupo de entre 3 y 5 amigos para ponernos en contacto en caso de perder nuestra cuenta. Ellos podrán enviarnos un código y url a la web para recuperar la cuenta.
- **Opciones avanzadas**: estas opciones permiten cifrar las notificaciones por correo electrónico de la propia red social, así como recuperar cuentas externas que utilicen a cuenta de Facebook como inicio de sesión. Finalmente, también podemos ver un

registro de todos los correos recibidos de la propia red social, muy útil para comprobar si nos ha llegado un *phishing* haciéndose pasar por este servicio.

1.3.2 TWITTER

Más opciones (…) y luego en **Configuración y privacidad > Privacidad y seguridad**:





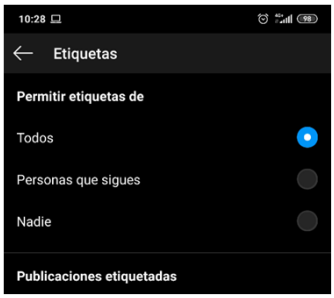
Para revisar la configuración de seguridad de nuestro perfil de Twitter, deberemos hacer clic en **Más opciones** (…) y luego en **Configuración y privacidad > Privacidad y seguridad:**

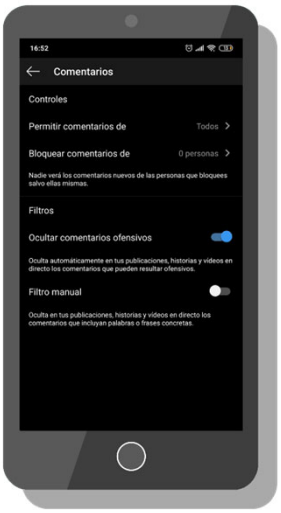
- **Tweets**: aquí podremos seleccionar las opciones:
  - Protege tus Tweets, para mostrar nuestras publicaciones solo a aquellos usuarios que nos siguen.
  - Etiquetado de fotos, para configurar quién tiene permitido etiquetarnos.
- **Mensajes directos**: desde aquí podremos configurar si queremos recibir mensajes directos de cualquier usuario de Twitter, si queremos aplicar un filtro de calidad y evitar que lleguen a nuestra bandeja de entrada, y mostrar confirmaciones de lectura para informar de cuándo un mensaje ha sido leído.
- **Visibilidad y contactos**: permite que las personas puedan encontrarnos en la red social desde nuestro correo electrónico o nuestro número de teléfono. También podemos administrar todos nuestros contactos.
- **Seguridad**: nos aparecerán diversas opciones que nos permitirán:
  - Mostrar u ocultar contenido que pueda ser sensible o delicado.
  - Marcar el contenido que pueda contener material delicado.
  - Silenciar cuentas o palabras concretas.
  - Bloquear cuentas.
  - Aplicar filtros para eliminar de nuestro muro aquellos contenidos o publicaciones que no queramos ver, o a determinados usuarios.

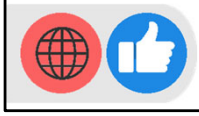
- **Personalización y datos**: si marcamos esta opción, la red social recabará información sobre nosotros para personalizar nuestra experiencia, ajustar el tipo de noticias, publicaciones y anuncios que se nos muestren. Además, podremos ajustar esta personalización en función de otros factores, como nuestra ubicación, permitiendo a Twitter acceder e intercambiar estos datos con terceros.
    - Desde Consulta tus datos de Twitter, podremos gestionar y eliminar toda la información recabada por la red social, como nuestros intereses, actividad de la cuenta, historial y conexiones.

1.3.3 INSTAGRAM

Seleccionaremos las **opciones** y luego **Configuración > Privacidad**:







Para acceder a las opciones de privacidad de nuestra cuenta, deberemos hacer clic sobre nuestro perfil desde la *app*. Una vez dentro, seleccionaremos las **opciones**, y haremos clic en **Configuración > Privacidad**;

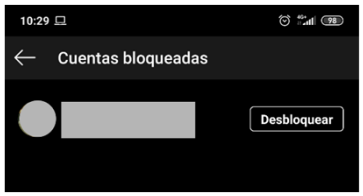
- **Comentarios**: nos permitirá añadir filtros para los usuarios que tienen permitido enviarnos comentarios o bloquear los de determinados contactos. También podemos añadir filtros manuales para el tipo de contenido, así como ocultar comentarios ofensivos.
- **Etiquetas**: de un modo similar, podremos permitir que nos etiqueten Todos, Personas que seguimos o Nadie. También podremos aprobar las etiquetas de forma manual cada vez que intenten etiquetarnos.
- **Menciones**: funciona igual que la opción anterior, pudiendo elegir quién tiene permitido mencionarnos.
- **Historia**: disponemos de varias opciones:
    - **Ocultar historia a**, si queremos ocultar nuestra historia a algún contacto.
    - **Mejores amigos**, para añadir contactos a esta lista en particular.
    - **Permitir respuestas con mensajes**, a todos, a nadie o a personas que seguimos.
    - **Guardado**, para seleccionar el tipo de almacenamiento de los vídeos y fotos de nuestras publicaciones en el archivo o directamente en la memoria de nuestro dispositivo.
    - **Contenido compartido**, para permitir a otros contactos compartir nuestras

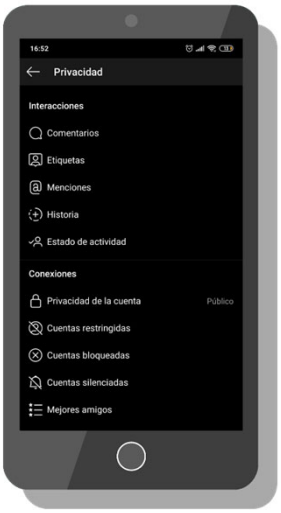
historias en sus muros, a modo de mensajes o compartir automáticamente nuestras publicaciones en Facebook.

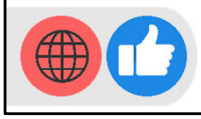
- **Estado de actividad**: permite que los usuarios que seguimos o con quienes hemos intercambiado mensajes puedan ver la última vez que hemos utilizado la *app*.

1.3.3 INSTAGRAM (II)

- Privacidad de la cuenta.
- Cuentas restringidas.
- Cuentas bloqueadas.
- Cuentas silenciadas.
- Mejores amigos.
- Cuentas que sigues.



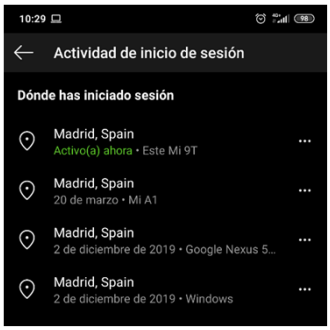


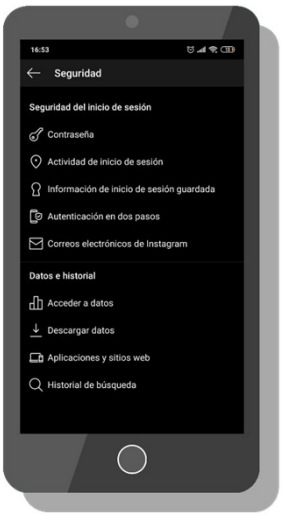


- **Privacidad de la cuenta**: en esta opción podremos configurar nuestra cuenta como privada. De este modo, solo las personas que queramos podrán ver nuestras publicaciones.
- **Cuentas restringidas**: así podremos bloquear a un usuario sin necesidad de notificarlo, ningún otro usuario de nuestra red podrá ver sus comentarios y no sabrá cuando nos hemos conectado.
- **Cuentas bloqueadas**: desde aquí podremos desbloquear a los usuarios que hayamos bloqueado previamente.
- **Cuentas silenciadas**: desde aquí podremos desbloquear a los usuarios que hayamos silenciado previamente. El silencio aplica a sus publicaciones y/o historias.
- **Mejores amigos**: para gestionar aquellos usuarios que queremos incluir en esta lista en concreto. Así, podrás compartir publicaciones solo con ellos.
- **Cuentas que sigues**: esta opción nos permitirá gestionar todas las cuentas que seguimos y nos siguen, para dejar de hacerlo, silenciar o administrar sus notificaciones.

1.3.3 INSTAGRAM (III)

Desde **opciones > Configuración > Seguridad**:



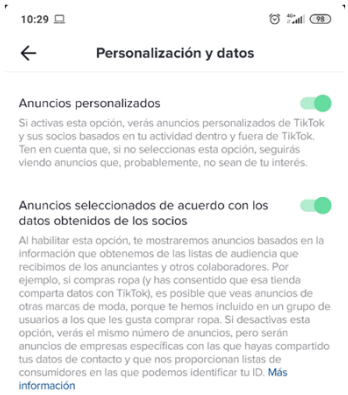


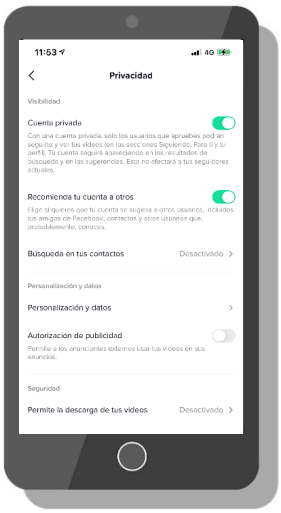
Desde **opciones > Configuración** también podemos acceder al menú de **Seguridad** y modificar sus opciones:

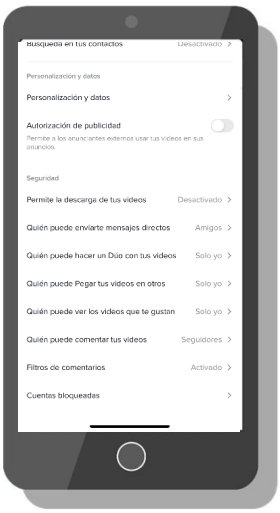
- **Contraseña**: para cambiar nuestra contraseña.
- **Actividad de inicio de sesión**: para revisar donde hemos iniciado sesión, a qué hora y mediante qué dispositivo.
- **Información de inicio de sesión guardada**: para guardar o no el registro de los inicios de sesión.
- **Autenticación en dos pasos**: para añadir esta capa extra de seguridad. Desde aquí podremos ingresar un número de teléfono al que nos enviarán el código de seguridad, descargar una aplicación de autenticación para agilizar la verificación en dos pasos desde una *app* y acceder a nuestros códigos de recuperación en caso de que no podamos acceder a nuestro dispositivo móvil para recuperar nuestra cuenta.
- **Correos electrónicos de Instagram**: para comprobar los correos que la red social nos ha enviado en relación con la seguridad u otro tipo.
- **Datos e historial**: estas opciones permiten comprobar y descargar el registro de datos de nuestra cuenta. Desde los inicios de sesión, los cambios en la configuración de nuestra cuenta, información de perfil y contactos y el historial de búsqueda.

1.3.4 TIKTOK

Deberemos seleccionar las opciones y hacer clic en **Privacidad**.







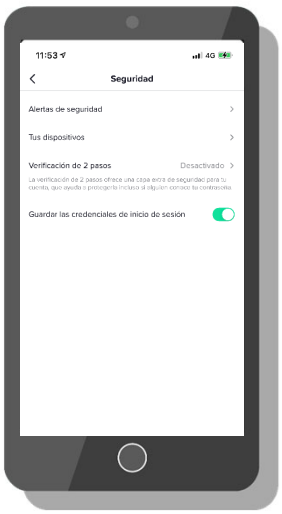
Para acceder a las opciones de la aplicación, es necesario hacer clic en nuestro perfil "**Yo**" abajo derecha de la *app*, luego deberemos seleccionar las opciones arriba a la derecha y hacer clic en **Privacidad**.

- **Cuenta privada**: si lo activamos, nuestra cuenta solo será visible para los usuarios que aprobemos.
- **Recomienda tu cuenta a otros**: si queremos que nuestra cuenta les aparezca a otros usuarios en cuentas similares a la nuestra.
- **Búsqueda en tus contactos**: para encontrar a las personas que conoces
- **Personalización y datos**: desde esta opción podremos ver el tipo de uso que se hará de los datos recogidos por la aplicación vinculados a la personalización de nuestra cuenta:
    - Anuncios personalizados: se mostrarán anuncios personalizados basados en nuestra actividad dentro y fuera de la *app*.
    - Anuncios seleccionados de acuerdo con los datos obtenidos de los socios: mostrará anuncios de terceros que intercambien información con la *app* y con los que hayamos interactuado.
    - Colaboradores externos en materia de medición del rendimiento de anuncios: nos mostrará la lista completa de empresas que recaban y analizan los datos que la aplicación les comparte sobre sus usuarios para crear los anuncios personalizados.
    - Tus intereses de publicidad: muestra el tipo de contenido que la *app* considera

que puede interesarnos en forma de publicidad.
    - Descargar tus datos: podremos descargar una copia de los datos recogidos por la *app*, aunque puede tardar hasta 30 días. Incluye información sobre nuestro perfil y datos personales, nuestra actividad e interacciones, así como los ajustes en la configuración de la *app*.
- **Seguridad**: diferentes opciones como quien puede ver o descargar tus vídeos

1.3.4 TIKTOK (II)

Deberemos seleccionar las opciones y hacer clic en **Seguridad**.

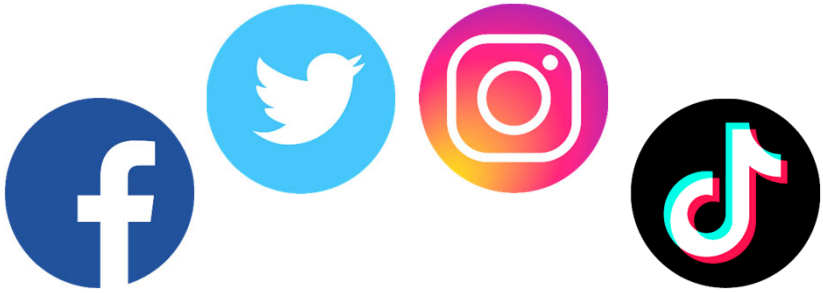


Para acceder a las opciones de la aplicación, es necesario hacer clic en nuestro perfil "**Yo**" abajo derecha de la *app*, luego deberemos seleccionar las opciones arriba a la derecha y hacer clic en **Seguridad**.

- **Alertas de seguridad:** para comprobar si se ha encontrado alguna actividad inusual
- **Tus dispositivos**: dispositivos donde se ha iniciado sesión con la cuenta
- **Verificación en dos pasos**
- **Guardas las credenciales de inicio de sesión**

1.4 DENUNCIAR UNA SUPLANTACIÓN O ROBO DE CUENTA

Las redes sociales ponen a nuestra disposición un servicio para **denunciar cuentas**:



Si nos encontramos con que **nos han robado nuestra cuenta, no podemos acceder y/o un perfil que está suplantando nuestra identidad**, recuerda que las redes sociales ponen al servicio de los usuarios un servicio para denunciar estas cuentas:

- Denunciar suplantación de identidad en Facebook.
- Denunciar una cuenta robada en Facebook.
- Denunciar una suplantación de identidad en Twitter.
- Denunciar una cuenta robada en Twitter.
- Denunciar una suplantación de identidad en Instagram.
- Denunciar una cuenta robada en Instagram.
- Denunciar una cuenta en TikTok.

Por tanto, hay que practicar periódicamente el *egosurfing* para saber qué se publica en Internet sobre nosotros para que, en caso de que se haga un mal uso de nuestros datos, podamos tomar las medidas que correspondan. Pero, además, deberemos ponerlo en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado, y para ello deberemos aportar todo tipo de datos, información y pruebas.

Actividad 1

¿Crees que tienes configurada correctamente tu red social favorita? Ante la duda, la mejor opción es dedicar unos minutos a revisar los ajustes de seguridad y privacidad para evitar que terceros con malas intenciones vean nuestras publicaciones.

¿Crees que tienes configurada correctamente tu red social favorita? Ante la duda, la mejor opción es dedicar unos minutos a revisar los ajustes de seguridad y privacidad para evitar que terceros con malas intenciones vean nuestras publicaciones.

2. LOS RIESGOS DE UNA ÚNICA CONTRASEÑA PARA TODOS LOS SERVICIOS

¿La misma contraseña para todo? ¡No lo pongamos tan fácil!

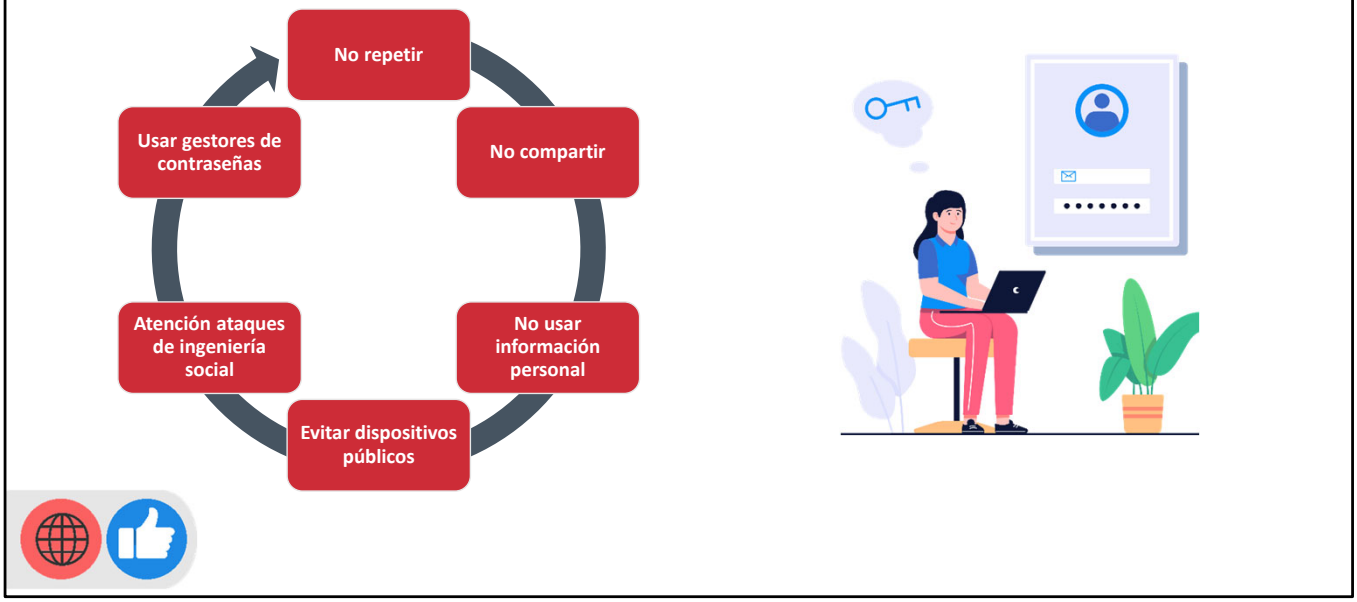
¿La misma contraseña para todo? ¡No lo pongamos tan fácil! Las contraseñas son la llave de nuestra identidad digital, por esto es sumamente importante que las cuidemos. Una contraseña débil podría exponer información muy sensible sobre nosotros, y el atacante podría llegar a realizar las siguientes acciones:

- Leer, modificar o eliminar todo nuestro historial de correos enviados y recibidos desde nuestra cuenta de correo electrónico. Es más, podría enviar correos en nuestro nombre o utilizar nuestra cuenta de correo para enviar *spam*.
- Escribir y publicar un post en nuestro nombre.
- Hacer compras online o cancelar pedidos, haciéndose pasar por nosotros.
- Publicar cualquier tipo de información (fotos, comentarios, vídeos,...) en nuestros perfiles de redes sociales. También podría eliminar o modificar el resto de la información que existe en estos perfiles (experiencia laboral, lugar en el que vivimos, teléfono móvil, correo electrónico de contacto…).
- Acceder a nuestra cuenta bancaria desde el portal de nuestro banco y hacer una transferencia de nuestro dinero a su cuenta.
- Modificar nuestros datos personales y credenciales de cualquier servicio al que haya conseguido acceso, impidiéndonos entrar y utilizar ese servicio.

Existe una forma de comprobar si nuestra cuenta ha podido ser comprometida. Solo tenemos que acceder a la web **Have i been Pownd** e introducir nuestro correo electrónico. Así, sabremos si debido a algún ciberincidente, nuestras credenciales han

podido ser comprometidas.

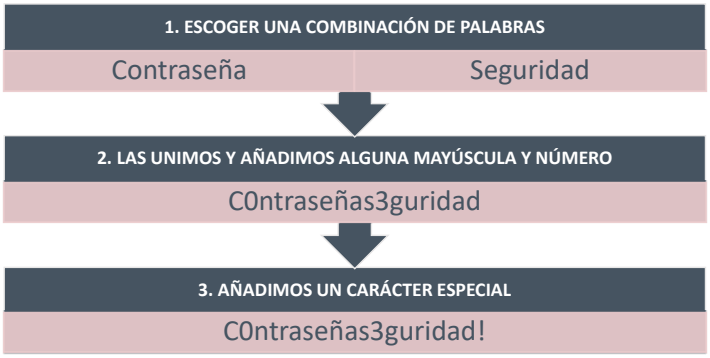
2.1 BUENAS PRÁCTICAS

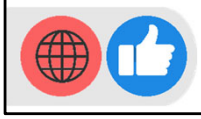


Para prevenir las fugas de información y protegernos de los ciberataques, es recomendable seguir las siguientes **buenas prácticas**:

- No usemos la misma contraseña en distintos servicios y cuentas de Internet.
- Nunca compartamos nuestras contraseñas con nadie.
- Evitemos incluir nuestro nombre o palabras comunes. La contraseña debe ser difícil de adivinar.
- Evitemos utilizar ordenadores públicos para ingresar en redes sociales. Recordemos cerrar sesión, sobre todo cuando utilicemos un equipo compartido con otras personas.
- Debemos pensar dos veces antes de hacer clic o descargar cualquier contenido, puede ser el señuelo de un ataque por ingeniería social.
- Los **gestores de contraseñas** nos ayudarán a no tener que memorizar todas nuestras claves. Con saber una contraseña maestra, podremos gestionar todas nuestras credenciales. Además, estos *software* nos recordarán cuándo es hora de actualizar la contraseña, así como cuándo estamos utilizando una clave poco segura.

2.1 BUENAS PRÁCTICAS (II)





Si a pesar de todo, seguimos sin tener claro si estamos utilizando una contraseña robusta, solo deberemos seguir los siguientes pasos:

- Escogeremos una combinación de palabras (2 o 3), que tengan alguna relación entre sí, pero no con nosotros, es decir, ni nuestro cumpleaños, nombre, mascota, etc. Por ejemplo: Contraseña y Seguridad.
- Las uniremos y añadiremos, al menos, una mayúscula: Contaseñaseguridad
- Luego, añadiremos algunos números: C0ntraseñas3guridad
- Y, finalmente, un carácter especial: C0ntraseñas3guridad!

Listo, con estos sencillos pasos podremos convertir nuestras contraseñas débiles, en una versión más robusta con la que prevenir lo ataques a nuestras contraseñas.

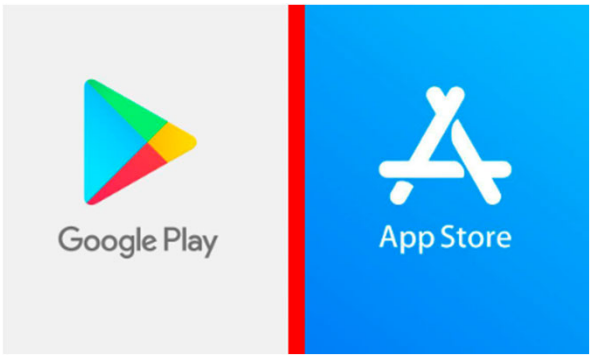
ACTIVIDAD 2

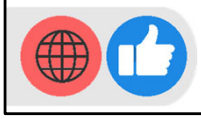
Los gestores de contraseñas son una herramienta muy útil para mantener nuestras cuentas seguras. Ahora practicaremos con un gestor de contraseñas.

Los gestores de contraseñas son una herramienta muy útil para mantener nuestras cuentas seguras. Aprovecha, entra en la sección de herramientas de la OSI y descarga alguno de sus gestores de contraseñas. Prueba a configurarlo con tus contraseñas principales y verás lo útil que puede llegar a ser.

3. DESCARGA DE *SOFTWARE* / SERVICIOS DE SITIOS OFICIALES

A la hora de **descargar un software de Internet**, es fundamental que lo hagamos desde el **sitio web del fabricante o la web oficial**.





A la hora de descargar un *software* de Internet, es fundamental que lo hagamos desde el sitio web del fabricante o la web oficial. Si lo hacemos desde **sitios webs no oficiales, o utilizamos *software* pirata**, corremos el **riesgo** de:

- Descargar *malware* u otros programas que, sin ser maliciosos, pueden dar problemas de rendimiento o entrar en conflicto con otros *software* legítimos o nuestro antivirus.
- Incurrir en un delito contra la propiedad intelectual del *software* original.
- Acabar en una lista de correos *Spam*.
- Ser víctima de un fraude y perder nuestro dinero.
- No tener acceso al servicio técnico oficial o a las actualizaciones de seguridad.

Si necesitamos descargar un programa en concreto, **debemos acudir siempre a la web del fabricante**. En la OSI encontrarás una **gran variedad de alternativas de *software* libre y legítimo**.

Finalmente, debemos recordar mantener nuestro antivirus activo y actualizado para prevenir varios de los riesgos mencionados. Además de mantener siempre nuestro sistema operativo actualizado, es decir, siempre que nos salte el aviso de actualización, no posponerlo, actualizarlo siempre lo antes posible.

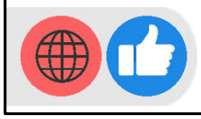
3.1 CÓMO DETECTAR FRAUDES

Dirección web o URL

Anuncios y *banners*

Alertas de virus y actualizaciones

Precio



Las webs de descarga ilegal o no oficiales suelen tener unas características comunes. Si prestamos atención, podremos evitar caer en este tipo de fraudes:

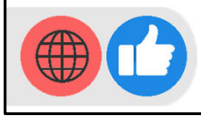
- Dirección web o URL: la dirección nos puede ayudar a detectar casos sospechosos. Debe estar relacionada con el nombre del producto o con el de su fabricante y no deberemos utilizar webs cuyo nombre sea similar a: "todo_descargas", "*free_downloads*", "*pirate_free*", etc. En muchos casos, la dirección puede parecer la oficial, pero si nos fijamos bien podremos ver algunas diferencias.
- Anuncios y *banners* publicitarios: son más fiables aquellas web que no contienen publicidad o cuando esta está relacionada con el producto que buscamos.
- Si los anuncios entorpecen nuestra navegación o aparecen en forma de ventanas emergentes o "*pop-ups*" molestos, no estaremos en la web oficial del producto.
- Alertas de virus y actualizaciones: al acceder a algunas webs aparecen nuevas ventanas o *pop-ups*, solicitando que actualicemos programas que tenemos instalados, o nos informan de que nuestro antivirus necesita actualizarse. Incluso, nos avisan de que nuestro equipo está infectado por un virus.
- No debemos hacer caso de este tipo de alertas ya que se tratan de intentos de ataque por ingeniería social.
- Precio: normalmente tenemos una idea sobre el precio del *software* que buscamos o, como mínimo, si es un *software* gratuito (*open-source*) o de pago. Otras veces no sabemos el precio de un producto y buscamos la solución gratuita que mejor se

adapta a nuestras necesidades.

- Si tenemos una idea aproximada acerca del precio de la aplicación, debemos ser precavidos y evitar los chollos u ofertas sospechosas.

4. DESCARGA DE *APPS* DE SITIOS OFICIALES

Es fundamental utilizar las **tiendas oficiales**. Sin embargo, a veces **los filtros pueden fallar**.



A la hora de descargar una *app* para nuestro dispositivo móvil, al igual que ocurre con el *software* de nuestro ordenador, es necesario que tomemos una serie de medidas preventivas para evitar acabar descargando *malware* en nuestro sistema. Lo primero y más importante será utilizar las tiendas oficiales, como Google Play o la *App* Store.

Sin embargo, hay veces que estas *app*s fraudulentas se saltan los filtros de las tiendas oficiales, por lo que, para evitar caer en la trampa, debemos seguir estas recomendaciones:

- **Comprobar quién es el desarrollador de la aplicación**. Así podremos comprobar si el desarrollador es fiable, o si se trata de una *app* copia de una más famosa.
- **Revisar el número de descargas de la *app***. Si descargamos una aplicación popular, el número de descargas debería ser oficial.
- **Echar un vistazo a los comentarios**. Nos ayudará a saber si la *app* funciona correctamente o si es maliciosa.
- **Revisar los permisos solicitados**. Una vez instalada la app, es conveniente comprobar los permisos que nos solicita para funcionar. Si son más de los que debería pedir la app para funcionar correctamente, deberíamos desconfiar.

ACTIVIDAD 3

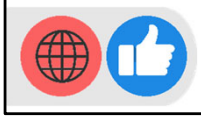
Seguro que has descargado alguna *app* en tu *smartphone* o *tablet* alguna vez. Como forma de poner en práctica los buenos hábitos recién explicados, entra en la tienda oficial de tu sistema operativo, busca una *app* y revisa los comentarios, el desarrollador y los permisos que pide al instalarla.

También, puedes acceder a las aplicaciones instaladas en tu dispositivo para analizar los permisos otorgados.

Seguro que has descargado alguna *app* en tu *smartphone* o *tablet* alguna vez. Como forma de poner en práctica los buenos hábitos recién explicados, entra en la tienda oficial de tu sistema operativo, busca una *app* y revisa los comentarios, el desarrollador y los permisos que pide al instalarla.
También, puedes acceder a las aplicaciones instaladas en tu dispositivo para analizar los permisos otorgados.

5. COPIAS DE SEGURIDAD Y ALMACENAMIENTO EN LA NUBE

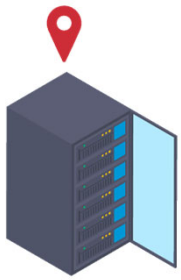
Es un hecho que las copias de seguridad son una salvaguarda necesaria. El poder disponer de ellas en la nube nos ofrece muchos **beneficios** pero, **¿están realmente a salvo estos datos?**



Hoy en día, todos tenemos información guardada en nuestros dispositivos y otra gran parte alojada en la nube, como copia de respaldo o para liberar espacio de almacenamiento.

Es un hecho que la nube nos ofrece muchos beneficios pero, **¿están realmente a salvo estos datos? ¿Hay alguna forma de mejorar la seguridad de la información subida a la nube?**

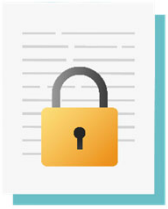
5.1 USAR UN SERVICIO SEGURO



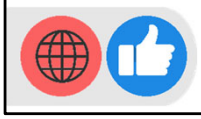
Ubicación de la información

Presencia de terceros

Confidencialidad de la información



Mecanismos de cifrado

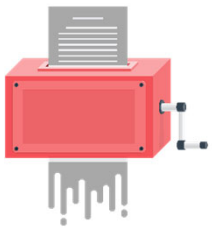


Antes de elegir un **proveedor de servicio en la nube**, debemos analizar detenidamente los **aspectos de seguridad** que nos ofrece y realizar algunas comprobaciones:

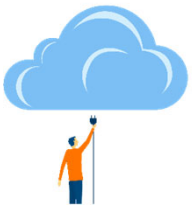
- La ubicación de nuestra información. Conviene informarse sobre la legislación y garantías de protección de nuestros datos del país donde se encuentren.
- Presencia de terceros. Si terceras organizaciones pueden llegar a tener acceso a nuestros datos, debemos firmar un consentimiento.
- Confidencialidad de nuestra información. Para asegurar nuestra privacidad, debemos asegurarnos de que la web cuenta con certificado digital y se accede mediante https.
- Mecanismos de cifrado. Es recomendable conocer e informarse sobre los mecanismos de cifrado del servicio. Algunos utilizan mecanismos adicionales para maximizar nuestra seguridad.

5.1 USAR UN SERVICIO SEGURO (II)

Políticas de seguridad y privacidad

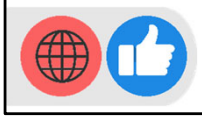


Eliminación segura



Condiciones de uso

Ejerce tus derechos



- Políticas de seguridad y privacidad. Podemos comprobar las políticas en el apartado de “Aviso legal” de la web del servicio. Allí podremos asegurarnos de que se cumplen con las medidas de seguridad exigibles para garantizar la seguridad, integridad y posterior recuperación de nuestros datos.
- Eliminación segura. Se garantiza el borrado seguro de nuestros datos una vez se finaliza el contrato con el servicio.
- Finalidad de uso. Debemos asegurarnos de que nuestros datos personales no se van a utilizar con fines comerciales o que no consideremos adecuados dentro de las condiciones de uso.
- Derechos ARCO: Todo usuario debe tener control sobre sus datos personales. Esto es garantizado a través de los derechos ARCO:
    - Acceso: posibilidad de solicitar información sobre el trato que se está haciendo de nuestros datos.
    - Rectificación: permite solicitar la modificación de los datos.
    - Cancelación: permite solicitar la supresión de los datos que resulten inadecuados o excesivos.
    - Oposición: permite oponerse al tratamiento de nuestros datos personales.

ACTIVIDAD 4

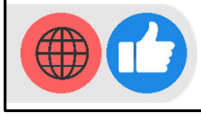
Ahora usaremos una aplicación para realizar copias de seguridad de nuestros datos en un disco duro o una unidad de red.

Seguro que has descargado alguna *app* en tu *smartphone* o *tablet* alguna vez. Como forma de poner en práctica los buenos hábitos recién explicados, entra en la tienda oficial de tu sistema operativo, busca una *app* y revisa los comentarios, el desarrollador y los permisos que pide al instalarla.
También, puedes acceder a las aplicaciones instaladas en tu dispositivo para analizar los permisos otorgados.

5.2 CIFRADO DE DATOS PERSONALES

¿Debemos subir los datos a la nube sin cifrarlos?¿O es recomendable llevar información de carácter personal en nuestros USBs y discos duros sin cifrar?

CONFIDENCIALIDAD INFORMACIÓN



<u>¿Qué garantías de seguridad debemos comprobar antes de decantarnos por uno u otra servicio en la nube?</u> <u>Lo más importante que debe garantizarnos es la **confidencialidad de la información.**</u>

Para asegurarnos de que nuestra información va a estar protegida, es recomendable llevar a cabo un cifrado de la misma antes de subirla a la nube. De este modo, solo aquellos usuarios que conozcan la clave podrán acceder a los datos.

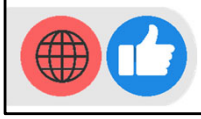
Para esto último, disponemos de varias herramientas gratuitas que nos permitirán añadir esta capa extra de seguridad fácilmente, como Cryptomator o Veracrypt, aunque en la OSI te ofreceremos muchas otras opciones.

5.3 BUENAS PRÁCTICAS

Para **maximizar la seguridad y disponibilidad de nuestra información**, deberemos:

Contraseña robusta

Copia de seguridad en soportes alternativos

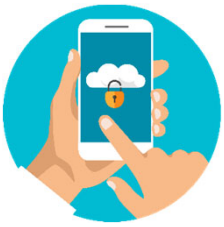


Finalmente, si nuestro objetivo es maximizar la seguridad y disponibilidad de nuestra información, es conveniente llevar a cabo las siguientes buenas prácticas vinculadas al almacenamiento seguro:

- Contraseña robusta: una de las cosas que puede ayudar a proteger la privacidad de nuestros datos es una contraseña robusta (entre 8 y 10 caracteres, minúsculas y mayúsculas, números y caracteres especiales). Si el servicio lo permite, utilicemos un sistema de autenticación en dos pasos.
- Copias de seguridad en soportes alternativos: la nube es una buena alternativa para almacenar nuestras copias, pero es mejor diversificar las copias de respaldo en diferentes repositorios. Es recomendable establecer copias de seguridad automáticas, aparte de las que hagamos nosotros por necesidad:
    - Windows: podemos utilizar la funcionalidad integrada dentro del sistema, en las opciones de configuración “Copias de seguridad y restauración”.
    - Mac: disponen de una herramienta para ello llamada “Time Machine”.
    - Android: desde Ajustes > Copia seguridad y restablecimiento podremos configurarla.
    - iOS: disponemos de esta funcionalidad desde i*Cloud*.

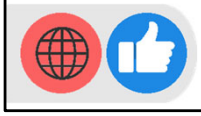
5.3 BUENAS PRÁCTICAS (II)

Compartir ficheros con quien quieres



Permisos

Clasificación de la información



- Compartir ficheros con quien quieres: independientemente del servicio que utilicemos para almacenar y compartir información en la nube, es importante revisar con quién estamos compartiendo estos datos, y revisar frecuentemente que lo estamos haciendo con la persona o personas correctas.
- Permisos: a la hora de compartir archivos en la nube, la mayoría de los servicios permite asignar permisos a los usuarios. Si no lo gestionamos debidamente, un tercero podría editarla o incluso borrarla.
- Clasificación de la información: es importante clasificar la información que manejamos y separar aquella más sensible. De este modo, en caso de ataque o fuga de información minimizaríamos los riesgos.

ACTIVIDAD 5

Ahora que conoces la importancia de llevar a cabo el cifrado de archivos y carpetas, ¿por qué no lo intentas? Usaremos una aplicación para llevar a cabo el cifrado de alguna carpeta con varios archivos en su interior.

Ahora que conoces los pasos a seguir para llevar a cabo el cifrado de archivos y carpetas, ¿por qué no lo intentas? Lleva a cabo el cifrado de alguna carpeta con varios archivos en su interior. Puede resultarte muy útil la próxima vez que crees tu copia de seguridad.

¿PREGUNTAS?

INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

OSI Oficina de Seguridad del Internauta