

# Recurso Pedagógico Taller Formativo

## Riesgos y fraudes en redes sociales y protección de nuestra identidad digital

## ÍNDICE

<b>1. Objeto del documento.....</b>	<b>4</b>
<b>2. Organización y estructura .....</b>	<b>5</b>
<b>3. Objetivo .....</b>	<b>6</b>
<b>4. Metodología y recursos .....</b>	<b>7</b>
<b>5. Contenidos.....</b>	<b>8</b>
5.1. Diapositiva 1. Presentación del taller .....	8
5.2. Diapositiva 2. Índice .....	8
5.3. Diapositiva 3. Introducción .....	8
5.4. Diapositiva 4. Redes sociales y nuestra identidad digital .....	8
5.5. Diapositiva 5. Buenas prácticas al utilizar las redes sociales.....	9
5.6. Diapositiva 6-7. Buenas prácticas al utilizar las redes sociales. Evitar compartir cierta información .....	9
5.7. Diapositiva 8-17. Buenas prácticas al utilizar las redes sociales. Configurar las opciones de privacidad y seguridad .....	11
5.8. Diapositiva 18. Actividad 1 .....	13
5.9. Diapositiva 19-20. Buenas prácticas al utilizar las redes sociales. Controlar nuestro círculo de contactos .....	13
5.10. Diapositiva 21-26. Buenas prácticas al utilizar las redes sociales. Descargar nuestra vida de las redes sociales.....	14
5.11. Diapositiva 27-28. Buenas prácticas al utilizar las redes sociales. Practicar <i>Egosurfing</i> .....	15
5.12. Diapositiva 29. Actividad 2 .....	16
5.13. Diapositiva 30. Fraudes comunes en redes sociales .....	16
5.14. Diapositiva 31-32. Fraudes comunes en redes sociales. Robo de cuentas 17	17
5.15. Diapositiva 33-34. Fraudes comunes en redes sociales. Suplantación de identidad (perfiles falsos) .....	17
5.16. Diapositiva 35-36. Fraudes comunes en redes sociales. Contactos fraudulentos .....	19
5.17. Diapositiva 37-38. Fraudes comunes en redes sociales. Anuncios y publicaciones maliciosas.....	19
5.18. Diapositiva 39-40. Fraudes comunes en redes sociales. Bulos y <i>fake news</i> 20	20
5.19. Diapositiva 41-42. Fraudes comunes en redes sociales. Concursos fraudulentos .....	21
5.20. Diapositiva 43-44. Fraudes comunes en redes sociales. <i>Sextorsión</i> y amores en línea .....	21
5.21. Diapositiva 45. Cuestionario de evaluación 1 .....	22
5.22. Diapositiva 46. Cuestionario de evaluación 2 .....	22
5.23. Diapositiva 47. Cuestionario de evaluación 3 .....	23
5.24. Diapositiva 48 . Cuestionario de evaluación 4 .....	23
5.25. Diapositiva 49 . Cuestionario de evaluación 5 .....	23
5.26. Diapositiva 50 . Cuestionario de evaluación 6 .....	23
5.27. Diapositiva 51. Cuestionario de evaluación 7 .....	23
5.28. Diapositiva 52. Cuestionario de evaluación 8 .....	23
5.29. Diapositiva 53. Cuestionario de evaluación 9 .....	24
5.30. Diapositiva 54. Cuestionario de evaluación 10.....	24

5.31. Diapositiva 55. Final del taller .....	24
<b>6. Recursos de evaluación .....</b>	<b>25</b>
6.1. Cuestionario de evaluación .....	26
<b>ANEXO .....</b>	<b>28</b>
Recursos para ampliar .....	28

## ÍNDICE DE FIGURAS

---

No se encuentran elementos de tabla de ilustraciones.

## ÍNDICE DE TABLAS

---

No se encuentran elementos de tabla de ilustraciones.

## 1. OBJETO DEL DOCUMENTO

---

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **Taller Formativo ‘Riesgos y fraudes en redes sociales y protección de nuestra identidad digital’**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

## 2. ORGANIZACIÓN Y ESTRUCTURA

---

La estructura del taller estará compuesta por X temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. Redes sociales y nuestra identidad digital.
2. Buenas prácticas al utilizar las redes sociales
  - a. Evitar compartir cierta información
  - b. Configurar las opciones de privacidad y seguridad
  - c. Controlar nuestro círculo de contactos
  - d. Practicar *Egosurfing*
3. Fraudes comunes en redes sociales
  - a. Robo de cuentas
  - b. Suplantación de identidad (perfiles falsos)
  - c. Contactos fraudulentos
  - d. Anuncios y publicaciones maliciosas
  - e. Bulos y *Fake News*
  - f. Concursos fraudulentos
  - g. *Sextorsión* y amores en línea

### 3. OBJETIVO

---

Este taller tiene como objetivo principal **proporcionar a los alumnos las habilidades y conocimientos necesarios para configurar correctamente sus perfiles en redes sociales y detectar los fraudes y publicaciones maliciosas más comunes, así como buenas prácticas a la hora de usar estas plataformas y cuidar su identidad digital.** Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

## 4. METODOLOGÍA Y RECURSOS

---

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual:** Las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa:** El alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
  - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en PowerPoint.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades.** Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.
- **Cuestionario de evaluación.** Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

## 5. CONTENIDOS

---

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

### 5.1. Diapositiva 1. Presentación del taller

Presentación del taller “**Riesgos y fraudes en redes sociales y protección de nuestra identidad digital**”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017 + canales WhatsApp y Telegram.

### 5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Redes sociales y nuestra identidad digital.
2. Buenas prácticas al utilizar las redes sociales
  - a. Evitar compartir cierta información
  - b. Configurar las opciones de privacidad y seguridad
  - c. Controlar nuestro círculo de contactos
  - d. Practicar *Egosurfing*
3. Fraudes comunes en redes sociales
  - a. Robo de cuentas
  - b. Suplantación de identidad (perfiles falsos)
  - c. Contactos fraudulentos
  - d. Anuncios y publicaciones maliciosas
  - e. Bulos y *Fake News*
  - f. Concursos fraudulentos
  - g. Sextorsión y amores en línea

### 5.3. Diapositiva 3. Introducción

Las plataformas de redes sociales han evolucionado mucho durante los últimos años, convirtiéndose en espacios donde compartir nuestra vida con nuestros amigos y familiares. Estas herramientas de ocio almacenan una inmensa cantidad de información personal que, si no tenemos cuidado, puede terminar en malas manos y exponer nuestra privacidad a ciberdelincuentes y empresas que no dudarán en utilizarla para sacar un beneficio a nuestra costa.

Por eso, es fundamental que aprendamos las buenas prácticas vinculadas al uso de redes sociales, así como a identificar y evitar los fraudes más comunes de este tipo de servicios. A lo largo del presente taller analizaremos estas cuestiones en profundidad con ejemplos e instrucciones paso a paso.

### 5.4. Diapositiva 4. Redes sociales y nuestra identidad digital

A medida que avanza la tecnología y los usuarios pasamos más tiempo conectados a la Red, las aplicaciones y plataformas como las redes sociales también evolucionan, pasando de sitios online donde subir y reaccionar a las fotografías, vídeos y publicaciones de nuestros contactos a una herramienta con la que definir nuestra [identidad digital](#).



Toda nuestra actividad online, así como nuestras publicaciones, lo que dicen de nosotros y cómo reaccionamos a las publicaciones de otros deja un rastro tras de sí que nos define y conforma nuestra identidad digital. Podríamos definirla como la imagen virtual que vamos creando sobre nosotros, y que está formada por nuestros gustos, datos personales, opiniones y publicaciones en Internet, pero también está formada por lo que otros dicen de nosotros.

Precisamente, por ello es tan importante que la cuidemos y protejamos, ya que puede ser utilizada en nuestra contra si, por ejemplo, permitimos que se haga un uso fraudulento con nuestra identidad, utilice nuestros datos personales sin nuestro consentimiento, compartimos contenido que no debemos o que pueda ofender a otros, etc.

A continuación, vamos a conocer algunas prácticas y consejos que podemos aplicar a en nuestro día a día cuando utilizamos nuestras redes sociales para proteger nuestra privacidad y mantener intacta nuestra identidad digital.

## 5.5. Diapositiva 5. Buenas prácticas al utilizar las redes sociales

Cuando publicamos una foto, contestamos un comentario o subimos cualquier publicación a nuestras redes estamos exponiendo parte de nosotros a la Red. Es nuestra responsabilidad controlar que estas interacciones no pongan en peligro nuestra privacidad, aunque a veces no somos del todo conscientes de ello y cometemos algunos errores.

Pautas como tener cuidado con lo que publicamos o limitando lo que otros usuarios pueden ver de nosotros son algunos ejemplos de estas buenas prácticas a llevar a cabo en redes sociales. Veámoslas más detenidamente.

## 5.6. Diapositiva 6-7. Buenas prácticas al utilizar las redes sociales. Evitar compartir cierta información

Es común que utilicemos las redes para anunciar buenas noticias, como un nuevo trabajo, que nuestro equipo ha ganado un partido o recomendar alguna canción de nuestro artista favorito. Sin embargo, ¿qué ocurriría si en vez de eso publicásemos nuestra tarjeta bancaria, nuestra dirección o nuestro número de teléfono y esta información acabase en manos equivocadas?

Para evitarlo, es recomendable que [evitemos publicar o exponer la siguiente información](#) en nuestras publicaciones, o en Internet:

1. **Correo electrónico:** es común emplear el correo electrónico para registrarnos en redes sociales y muchos otros servicios de Internet. Sin embargo, eso no quiere decir que tengamos que exponerlo de forma pública. Si lo hacemos, corremos el riesgo de convertirnos en víctimas de publicidad no deseada (*spam*) y correos fraudulentos (*phishing*).
2. **Número de teléfono:** al igual que ocurre con el correo, publicar abiertamente nuestro número de teléfono nos convertirá automáticamente en el objetivo de los ciberdelincuentes, así como de otros usuarios con malas intenciones, ya que podrán utilizarlo para gastarnos bromas pesadas o, en el peor de los casos, utilizarlo para llevar a cabo todo tipo de fraudes y engaños basados en ingeniería social para obtener más datos personales.

También es común el uso de nuestro teléfono para registrarnos en servicios de tarificación especial sin nuestro consentimiento.

3. **Dirección y ubicación:** compartir esta información es muy peligroso, ya que no conocemos las intenciones de los usuarios que están al otro lado, pudiendo utilizar estos datos para identificar donde vivimos, cuáles son los lugares que frecuentamos, nuestras rutinas y cuando no estamos en casa.  
Existen casos de usuarios cuyos bienes fueron robados estando de vacaciones por compartir su dirección y anunciar en redes sociales que se encontraban de vacaciones lejos de casa.
4. **Fotografías/Vídeos de otras personas:** tenemos todo el derecho a subir fotografías con nuestros amigos y familiares. Sin embargo, en el momento en que aparecen otras personas, especialmente menores, es recomendable que solicitemos permiso antes de hacerlo, especialmente si la foto puede ser comprometida o puede acarrearle consecuencias negativas en un futuro a dicha persona.  
Subir fotografías o vídeos de otras personas de carácter comprometedor, íntimo o sexual a la Red puede suponer una gran amenaza para su seguridad y tener consecuencias muy graves, como la sextorsión y el ciberacoso, por lo que debemos evitarlas siempre que podamos.
5. **Fotografías íntimas o de carácter sexual:** subir o compartir este tipo de contenidos de carácter comprometedor, íntimo o sexual a la Red, ya sea a redes sociales o a otro tipo de servicios puede tener consecuencias muy graves, como sextorsión o ciberacoso, ni tampoco sabemos cómo podría afectarnos en el futuro a nuestra reputación. Es fundamental que tengamos en cuenta la pérdida de privacidad a la que nos exponemos con este tipo de prácticas, especialmente cuando no estamos seguros del uso que se hará de este contenido.
6. **Documentos personales:** nuestro DNI, carnet de conducir, contrato de trabajo o información sobre nuestra tarjeta de crédito o cuenta bancaria son datos muy sensibles. Exponerlos supondría un riesgo muy alto de sufrir suplantación de identidad o el uso de estos datos de forma fraudulenta, como es el que lleven a cabo compras o transferencias sin nuestro consentimiento, por ejemplo.
7. **Opiniones, quejas o comentarios comprometedores:** podemos pensar que nuestra red social es un lugar donde decir lo que queramos, pero ¿qué ocurriría si uno de nuestros contactos utilizase esta información en nuestra contra? Una crítica o queja desafortunada o un comentario negativo sobre nuestro trabajo podría no tomarse demasiado bien por parte de otras personas y tener consecuencias para nosotros.
8. **Conversaciones privadas:** del mismo modo, información personal y comentarios dichos en la intimidad por terceros no deberían ser compartidos sin su aprobación. Las conversaciones privadas no son algo que debamos compartir con otras personas, ni mucho menos en Internet, especialmente si contienen datos personales, revelan secretos o información que la otra persona preferiría no difundir.

## 5.7. Diapositiva 8-17. Buenas prácticas al utilizar las redes sociales. Configurar las opciones de privacidad y seguridad

La gran mayoría de redes sociales pone a disposición de sus usuarios diferentes opciones de configuración con las que modificar la seguridad de nuestra cuenta y limitar la cantidad de información que publicamos de forma abierta al resto de usuarios.

A continuación, veamos las principales opciones de configuración para las redes sociales más famosas:

**A) Facebook:** tanto si estamos en el ordenador como en un dispositivo móvil, para acceder a esta configuración deberemos hacer clic sobre el **icono de la flecha** de la parte superior derecha y hacer clic en **'Configuración y privacidad'**. Luego, pulsaremos en **'Configuración'** para acceder al menú completo:

- En **'Seguridad e inicio de sesión'**, accederemos a las opciones de seguridad. Las opciones más importantes son:
  - **Dónde has iniciado sesión:** para comprobar los dispositivos en los que hemos iniciado sesión, identificar dispositivos sospechosos y desactivar nuestra cuenta.
  - **Inicio de sesión:** para cambiar nuestra contraseña a una más robusta o si creemos que nuestra seguridad ha podido ser vulnerada.
  - **Autenticación en dos pasos:** esta función nos permitirá añadir un paso adicional siempre que iniciemos sesión, donde se nos enviará un código temporal a otro dispositivo que deberemos ingresar para acceder a nuestra cuenta, evitando que un tercero pudiese entrar incluso si conociese nuestra contraseña.
  - **Configurar seguridad adicional:** aquí podremos activar las alertas siempre que Facebook perciba un inicio de sesión desde un dispositivo o un navegador que no sean los habituales. También podremos añadir un método adicional de recuperación de cuenta al añadir amigos con los que contactar en caso de perder nuestro acceso a la cuenta, en caso de robo por ejemplo.
- En **'Privacidad'** podremos modificar algunas opciones sobre lo que otros pueden ver de nosotros, como:
  - **Tu actividad:** para decidir quién puede ver nuestras publicaciones o el tipo de contenido que solemos ver.
  - **Cómo pueden encontrarte y ponerse en contacto contigo las personas:** para decidir la interacción que los usuarios desconocidos pueden tener con nosotros, por ejemplo, para evitar que nos envíen peticiones de amistad usuarios con los que no tengamos amigos en común.
- En **'Perfil y etiquetado'** también podremos limitar el tipo de información que está accesible para otros usuarios:
  - **Ver y compartir:** nos permitirá decidir si queremos que otros usuarios publiquen en nuestro muro o, incluso, evitar que otros usuarios vean lo que nuestros contactos publican sobre nosotros en nuestro perfil.
  - **Etiquetar:** impedirá que usuarios desconocidos nos etiqueten en sus publicaciones, limitándolo solo a nuestros amigos, por ejemplo.

- **Revisar:** servirá de filtro para que, antes de que se suba a nuestro muro una publicación en la que nos han etiquetado, podamos revisarla y evitar contenido no deseado o que pueda dañar nuestra imagen.

Dentro de la configuración podremos modificar y mejorar nuestra seguridad y privacidad todo lo que queramos. En el siguiente [enlace](#) encontraremos mucha información sobre cómo hacerlo.

**B) Instagram:** para acceder a la configuración, deberemos hacer **clic sobre nuestra foto de perfil** y luego pulsar en el **icono con las tres líneas > 'Configuración'**. En el desplegable, encontraremos las diferentes opciones:

- **'Privacidad':** dentro de esta opción podremos llevar a cabo diferentes ajustes:
  - **'Cuenta privada':** para evitar que usuarios que no formen parte de nuestros contactos puedan ver nuestro perfil.
  - **'Interacciones':** para configurar si queremos que cualquier usuario, solo nuestros contactos, o solo algunos contactos puedan enviarnos mensajes, etiquetarnos en fotos o historias, etc.
  - **'Conexiones':** para configurar las cuentas que tengamos bloqueadas de alguna forma, por ejemplo cuentas falsas o con comportamientos no deseados.
- **'Seguridad':** las opciones de seguridad nos ayudarán a proteger mejor nuestra cuenta:
  - **'Seguridad del inicio de sesión':** estas opciones sirven para modificar nuestra contraseña, comprobar dónde y con qué dispositivos nos hemos conectado a nuestra cuenta, y así identificar inicios sospechosos, y activar la verificación en dos pasos. Esta última añadirá una capa extra de protección al obligarnos a utilizar un código temporal enviado a otro dispositivo cada vez que queramos iniciar sesión.
  - **'Acceder a datos':** estas opciones sirven para comprobar todo lo que hemos subido a la red social y descargarlo, de modo que si queremos eliminar la cuenta no perdamos nada.

En el siguiente [enlace](#) encontraremos mucha más información sobre cómo configurar detenidamente nuestra cuenta y proteger nuestra privacidad.

**C) Twitter:** para acceder a la configuración pulsaremos sobre la foto de nuestro perfil y luego en **'Configuración y privacidad'**. Dentro de **'Privacidad y seguridad'**, veremos varias opciones:

1. **Audiencia y etiquetas:** proteger tweets y etiquetado de fotos.
2. **Tus tweets:** indicar si tu contenido multimedia es delicado.
3. **Contenido que ves:** según temas e intereses.
4. **Silenciar y bloquear:** configurar cuentas, palabras y notificaciones.
5. **Mensajes directos:** para evitar que desconocidos puedan enviarnos mensajes.
6. **Espacios:** configurar si los seguidores pueden ver que espacios escuchas.

Podemos encontrar más información sobre la seguridad y privacidad de nuestra cuenta en el siguiente [enlace](#).

## 5.8. Diapositiva 18. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

### Actividad 1:

Por muy concienciados que estemos, siempre podemos cometer un error o despistarnos. Para evitarlo, es conveniente que configuremos nuestras redes sociales de modo que estén lo más protegidas posibles contra fugas de información, protección de nuestras cuentas y para limitar la visibilidad de nuestro perfil. Dedica unos minutos para configurar correctamente tu red social favorita.

## 5.9. Diapositiva 19-20. Buenas prácticas al utilizar las redes sociales. Controlar nuestro círculo de contactos

Es habitual que las empresas, así como personalidades famosas o *'influencers'* hagan uso de las redes sociales para llegar a más usuarios y promocionar su producto o marca. Sin embargo, los usuarios no tenemos esta necesidad, y abarcar un círculo de contactos lo más amplio posible puede tener consecuencias muy negativas.

Cada uno es libre de agregar y comunicarse con quien quiera, pero debemos saber que agregar contactos desconocidos puede ser peligroso para nuestra privacidad, ya que estamos exponiendo nuestro perfil y la información que contiene a usuarios cuyas intenciones desconocemos.

- Podría tratarse de un ciberdelincuente buscando usuarios que publiquen información de carácter personal o sensible para robarla o suplantar su identidad.
- También podría tratarse de cuentas falsas o *'bots'* cuyo único objetivo es compartir enlaces maliciosos y propagar algún tipo de virus o *malware*.
- Podría tratarse de usuarios cuyo único objetivo sea crear conflicto en redes sociales, criticando nuestro contenido, realizando publicaciones agresivas o inapropiadas o dañando nuestra identidad digital.
- Igualmente, podría dedicarse a sacar capturas de nuestras publicaciones y reenviarlas a terceros. Independientemente de si borremos o no estos contenidos, nuestro contacto tendría capturas de todos nuestros mensajes, contenidos compartidos, reacciones a otras publicaciones, etc., que podrían ser utilizados en nuestra contra en el futuro.

Nuestra recomendación es que tengamos control sobre nuestros contactos, intentando limitarlo únicamente a aquellos usuarios que conozcamos o, en su defecto, que hayamos

podido investigar lo suficiente como para descartar los ejemplos anteriores. Del mismo modo, debemos ser conscientes de que, aunque eliminemos nuestras publicaciones, otros han podido guardar una copia, por lo que es fundamental que nos rodeemos de usuarios de confianza.

Si vamos a compartir nuestra vida digital con ellos, lo mejor es asegurarnos de que son usuarios de fiar.

## 5.10. Diapositiva 21-26. Buenas prácticas al utilizar las redes sociales. Descargar nuestra vida de las redes sociales

Con el uso, las redes sociales almacenan una gran cantidad de información sobre nosotros y nuestras interacciones, llegando a conformar toda una vida en este tipo de plataformas. Para tener visibilidad de toda ella, los contactos que hemos agregado y con los que hemos interactuado, las publicaciones que hemos hecho o por si queremos eliminar nuestra cuenta pero no queremos deshacernos de toda esta información, las redes sociales cuentan con una función para [descargar todos los datos almacenados sobre nosotros](#).

**A) Facebook:** podemos descargar una copia de nuestros datos desde su aplicación móvil o a través de la web. Para ello, seguiremos los siguientes pasos:

1. Accederemos a '**Configuración y privacidad**' > '**Configuración**' > '**Privacidad**' > '**Tu información de Facebook**' > '**Descargar tu información**'.
2. A continuación, podremos '**añadir o eliminar categorías de datos a tu solicitud**', personalizando el contenido a descargar. Adicionalmente, podremos seleccionar el formato de la descarga (HTML o JSON), la calidad de los archivos multimedia, así como establecer un intervalo de fechas de la información deseada.
3. Una vez personalizado y configurado las opciones de la solicitud, seleccionaremos '**Crear archivo**' para confirmarlo.
4. Finalmente, en la sección '**Configuración y privacidad**' > '**Configuración**' > '**Privacidad**' > '**Tu información de Facebook**' > '**Copias disponibles**' aparecerá el estado de nuestra solicitud como '**Pendiente**'. Cuando recibamos una notificación de que el proceso ha finalizado (puede tardar varios días), aparecerá la opción para '**Descargar**' toda nuestra vida en Facebook.

**B) Instagram:** se trata de un proceso sencillo donde la red social nos enviará un archivo en formato .Zip con todos los datos de nuestra cuenta (fotos, comentarios, información del perfil, etc.), a través de correo electrónico. Para ello, seguiremos los siguientes pasos:

1. Entrar en la siguiente [página web](#), donde tendremos que registrarnos y darle al botón '**Siguiente**'. También podemos acceder a la misma información en las opciones de perfil del usuario en '**Configuración**' > '**Seguridad**' > '**Descarga de datos**'.



2. Posteriormente nos pedirán de nuevo que confirmemos nuestra contraseña y, en un **plazo de 48 horas**, nos enviarán la copia de seguridad solicitada al correo electrónico asociado al perfil.
3. Finalmente, recibiremos un correo electrónico con el enlace para **descargar todos los datos asociados a nuestra cuenta**.

Una vez accedido al enlace, tendrás que volver a introducir tus credenciales de acceso a la cuenta y clicar en **Descargar datos**.

**C) Twitter:** esta red social permite descargar nuestro **archivo de Twitter**, donde se puede obtener una visión global de toda nuestra información, desde el primer *tweet* al último. Para ello, deberemos:

1. Acceder a '**Configuración y privacidad**' > '**Tu cuenta**' > '**Descargar un archivo con tus datos**'. Tras introducir la contraseña, podremos '**Solicitar archivo**'.
2. Cuando la descarga esté lista, Twitter enviará un aviso mediante una notificación si la solicitud es a través de la aplicación móvil, o a través de un correo electrónico (a la cuenta asociada al perfil) en el caso de solicitud vía web.
3. Finalmente, en la sección '**Descarga tus datos de Twitter**', tras pulsar en '**Descargar archivo**', tendremos que introducir las credenciales de acceso y se procederá a la descarga de un .zip con el archivo de la cuenta de Twitter.

## 5.11. Diapositiva 27-28. Buenas prácticas al utilizar las redes sociales. Practicar *Egosurfing*

Internet es el mayor banco de información del mundo, pudiendo encontrar datos de cualquier cosa, incluido sobre nosotros mismos. Para saber qué información hay sobre nosotros en Internet existe una práctica conocida como [\*Egosurfing\*](#). Consiste en utilizar las redes sociales y los buscadores de Internet, como Google, utilizando términos de búsqueda relativos a nosotros, como nuestro nombre, apellidos, DNI, etc., para localizar información sobre nosotros en páginas webs y otras plataformas.

Se trata de una buena práctica que todos deberíamos realizar periódicamente, para saber qué se dice de nosotros, cómo se dice, quién lo dice y con qué objetivo. Así podremos identificar posible información que no debería estar publicada y que queramos que sea eliminada, y proteger nuestra identidad digital.

Practicar el *Egosurfing* dentro de las redes sociales u otras plataformas como foros o webs de contactos puede ayudarnos a descubrir si existen [perfiles falsos suplantando nuestra identidad](#), usando nuestra descripción, datos personales o fotografías.

Para hacerlo, tan solo deberemos acceder a la red social que prefiramos e introducir la siguiente información:

- Nombre y apellidos
- Nombre de usuario

- Correo electrónico

También podemos utilizar cualquier dato identificativo, como un apodo o número de teléfono. Luego, tan solo tendremos que aplicar los filtros de búsqueda para encontrar perfiles falsos, comentarios o publicaciones sobre nosotros, fotografías o vídeos donde aparezcamos, etc. Con suerte, no encontremos nada o, como mucho, alguna publicación que no recordábamos o donde se hable de nosotros pero no fuésemos conscientes de ello. Y, en el caso de encontrar algo grave, podremos denunciarlo a la red social:

- En [Facebook](#).
- En [Instagram](#).
- En [Twitter](#).

## 5.12. Diapositiva 29. Actividad 2

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

### Actividad 2:

Ahora que ya sabemos en qué consiste el *Egosurfing*, deberíamos ser capaces de llevarla a la práctica. Haz una búsqueda en Internet y en tus redes sociales sobre ti y apunta todo aquello que consideres importante, que contenga información personal o que no sabías que existía.

## 5.13. Diapositiva 30. Fraudes comunes en redes sociales

El auge de las redes sociales y la inmensa cantidad de usuarios que las utilizamos las ha convertido en uno de los objetivos principales de los ciberdelincuentes. A través de técnicas de ingeniería social y la suplantación de identidad, los atacantes han encontrado un medio por el que lanzar todo tipo de fraudes y estafas para tratar de engañar a los usuarios y obtener sus datos personales o un beneficio económico directamente.

Por suerte, la mayoría de este tipo de estafas siguen el mismo modus operandi y podemos identificarlas fácilmente si prestamos atención a los detalles y hemos seguido los consejos y buenas prácticas vistas anteriormente.

Los [fraudes más comunes](#) son:

- Robo de cuentas mediante ataques de ingeniería social y cuentas desprotegidas.
- Suplantación de identidad, robo de información y creación de perfiles falsos.
- Contactos fraudulentos cuyo único objetivo es crear conflictos, compartir enlaces fraudulentos o a webs poco fiables.
- Anuncios y publicaciones a sitios web maliciosos, poco fiables o contenido ilícito.
- Noticias falsas, bulos y cadenas de mensajes que fomentan la desinformación (*fake news*).
- Concursos y promociones fraudulentos.
- *Sextorsión* y otros fraudes relacionados con amores en línea.



## 5.14. Diapositiva 31-32. Fraudes comunes en redes sociales. Robo de cuentas

Una cuenta protegida con una contraseña débil o con pocas medidas de seguridad extra puede convertirse en el objetivo de muchos ciberdelincuentes.

El robo de cuentas es una práctica común que **consiste en el uso de técnicas de ingeniería social para obtener nuestras credenciales por medio de engaños, o en el ataque directo a nuestras contraseñas**, con [técnicas como ataques por diccionario o fuerza bruta](#) para obtener acceso.

Un ejemplo común es cuando recibimos un correo donde los atacantes simulan ser la red social, y nos informan de que necesitan que hagamos clic en un enlace para verificar nuestro perfil. Al entrar, veremos una web muy parecida, casi idéntica, a la original que no nos hará sospechar en un principio. Después, ingresaremos nuestros datos y, automáticamente, nos enviarán a la URL oficial, como si nada hubiese ocurrido.

Sin saberlo, habremos compartido nuestras credenciales con los ciberdelincuentes. Luego, cambiarán los datos de acceso para que no podamos volver a entrar, permitiéndoles tener control total sobre nuestra cuenta y pudiendo suplantar nuestra identidad.

### ¿Cómo nos protegemos?

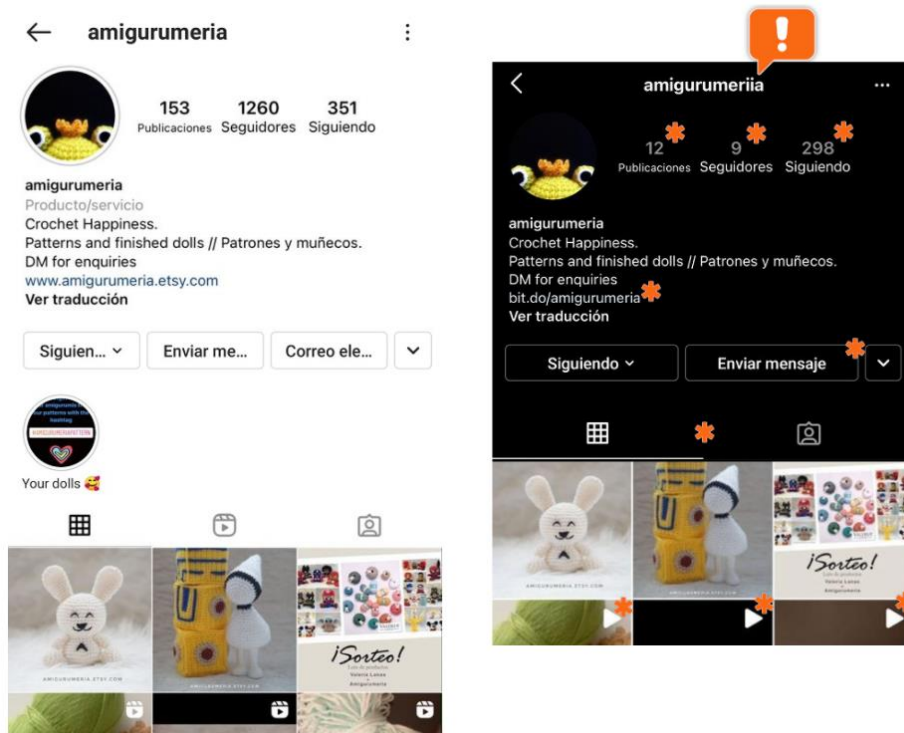
- Utilización de una contraseña robusta, con más de 10 caracteres, mayúsculas y minúsculas y caracteres especiales. Por ejemplo: **M1redsicual11!**
- No compartir la contraseña con nadie ni con otras cuentas. Debe ser única e irrepetible.
- Utilizar mecanismos de protección adicionales, como la [verificación en dos pasos](#).
- Evitar conectarnos a nuestras cuentas en dispositivos públicos, desconocidos o, incluso, de amigos o familiares. Y, en caso de hacerlo, asegurarnos de haber cerrado sesión, [eliminado los datos de navegación](#) y modificar nuestra contraseña.
- Estar atentos y utilizar el sentido común para no dejarnos engañar y detectar correos electrónicos que puedan ser fraudulentos, elaborados a partir de ingeniería social (*phishing*).

## 5.15. Diapositiva 33-34. Fraudes comunes en redes sociales. Suplantación de identidad (perfiles falsos)

La suplantación en redes sociales es otro tipo de fraude muy común que consiste en la creación de perfiles falsos sirviéndose de información que otros usuarios publican en este tipo de plataformas.

Los atacantes suelen **suplantar la identidad de cuentas de marcas conocidas o personas famosas o 'influencers'** para ganarse la confianza de sus seguidores, engañarlos y hacerles llegar enlaces fraudulentos, concursos y sorteos falsos, con el objetivo de obtener más datos personales o un beneficio económico.

En este ejemplo vemos cómo los atacantes crearon una cuenta doble de la original con un nombre muy similar, en el que tan solo variaba alguna letra o símbolo. La descripción, imagen de perfil y fotografías también eran el mismo que la original, confundiendo a los usuarios que comenzarían a seguir a esta última pensando que sería una cuenta real.



Del mismo modo, muchos son los ciberdelincuentes que crean cuentas falsas de usuarios normales y corrientes. El objetivo suele ser engañar a los contactos del usuario legítimo para que accedan a enlaces o descarguen *software* malicioso creyendo que están hablando con el auténtico. Su *modus operandi* es siempre el mismo, primero obtienen toda la información, fotografías y vídeos que la cuenta hace público en su perfil para crear una cuenta casi idéntica (a menudo se diferencian por algún carácter en su nombre, alias o *nickname*). De este modo, los contactos creerán que se trata de la cuenta legítima, y el atacante aprovechará para estafarlos o, incluso, para dañar su reputación online compartiendo noticias falsas, publicaciones controvertidas o atacando a sus contactos.

### ¿Cómo nos protegemos?

- Revisar la fecha de creación de la cuenta sospechosa, el número de seguidores y el tipo de publicación que suele subir a sus redes.
- Comprobar la verificación de la cuenta, ya que muchas redes sociales permiten añadir un identificador a las cuentas más populares para indicar que se trata de la original, y evitar la suplantación de identidad.
- Desconfiar de peticiones de amistad por parte de desconocidos.
- Comprobar el perfil en otras redes sociales o en Internet para identificar posibles casos de fraudes o duplicidad en las cuentas. Del mismo modo, practicar *egosurfing* nos ayudará a localizar cuentas falsas que estén utilizando nuestro nombre de usuario o correo electrónico, por ejemplo.
- Configurar nuestras cuentas en modo privado, de modo que toda nuestra información, publicaciones, fotografías, etc. sea solo visible para nuestros contactos.

## 5.16. Diapositiva 35-36. Fraudes comunes en redes sociales. Contactos fraudulentos

Las redes sociales son plataformas para compartir nuestra vida con nuestros contactos, sin embargo, existe una creencia falsa de que cuanto más contactos tengamos mejor. Es cierto que las marcas que tienen presencia en redes sociales, así como algunas personalidades famosas, utilizan estas plataformas para ampliar su negocio y darse visibilidad.

El tener en nuestra red de contactos un gran número de usuarios puede ser una ventaja en esos casos, pero a nosotros, los usuarios, esta práctica puede ocasionarnos más problemas que beneficios. Los contactos desconocidos pueden tener intenciones maliciosas, como compartir enlaces maliciosos, archivos infectados, noticias falsas, bulos y cadenas de mensajes o actuar como ‘trolls’ cuyo único objetivo es incendiar las redes con comentarios y publicaciones ofensivas para incomodar y atacar a otros.

Por otro lado, también puede ocasionarnos graves problemas de privacidad al compartir todo lo que subimos a la red social (fotografías, comentarios, vídeos, opiniones, ubicaciones...) con desconocidos que podrían utilizar esta información con intenciones maliciosas (crear cuentas falsas, ataques de ingeniería social, daño a nuestra reputación, etc.).

### ¿Cómo nos protegemos?

- Limpiar nuestra red de contactos y tratar de mantener solo aquellos contactos que conocemos o con los que tenemos alguna relación y evitar, en la medida de lo posible, usuarios desconocidos.
- Configurar nuestro perfil para evitar que usuarios desconocidos puedan enviarnos mensajes privados que puedan contener elementos maliciosos, etiquetarnos en publicaciones que no queremos o, incluso, enviarnos peticiones de amistad.
- Hacer uso de las funciones de bloqueo y eliminación de usuarios que todas las redes sociales disponen para sus usuarios. Así, podremos deshacernos de aquellos contactos más problemáticos.
- Comprobar los perfiles de estos usuarios podrá aportarnos mucha información. Si tienen descripciones pobres, fotografías o vídeos escasos o copiados de otra cuenta, sus publicaciones son siempre iguales y sospechosas (concursos, enlaces u otro tipo de fraudes).

## 5.17. Diapositiva 37-38. Fraudes comunes en redes sociales. Anuncios y publicaciones maliciosas

Si somos usuarios de redes sociales, es muy probable que no nos haya costado nada crearnos una cuenta en estas plataformas. Esto es debido a que muchas redes sociales se financian por medio de anuncios publicitarios que podemos ver entre las publicaciones de nuestros contactos.

Es muy común que tras ir bajando por nuestro muro, nos encontremos con algún anuncio. O, en su defecto, que aún usuario reenvíe o publique el anuncio que alguna marca o servicio online ha hecho dentro de la plataforma. Si bien estas publicaciones no tienen por qué ser malas, no podemos descuidarnos.

Debido a la cantidad de visitas y usuarios registrados, los ciberdelincuentes aprovechan para ‘colar’ [anuncios y publicaciones maliciosas](#) que nos redirigen a webs poco fiables o que suplantan la identidad de otras webs legítimas. El fraude reside en que estas webs maliciosas tienen como objetivo hacerse con nuestros datos, conseguir que instalemos algún tipo de *software* malicioso o que realicemos compras de productos que jamás llegarán a nuestras manos.

### ¿Cómo nos protegemos?

- Denunciar las publicaciones ayudará a limpiar las redes sociales de este tipo de prácticas. Es una función disponible en la mayoría de ellas que, además, podemos usar para ocultar anuncios que no nos interesen.
- Añadir mecanismos de bloqueo de anuncios, ya sea desde la configuración de nuestro perfil en redes sociales o instalando complementos, extensiones o *plugins* en nuestro navegador.
- Analizar el contenido del anuncio para detectar si es o no una publicación fraudulenta. Algunas tiendas online se anuncian con rebajas muy atractivas, con productos de marcas muy conocidas.

Si entramos en la web, podremos identificar si se trata de una web fiable o falsa comprobando la información de la empresa, revisando los comentarios y valoraciones de otros usuarios, buscando la web en nuestro buscador favorito para ver si está vinculada a algún fraude o analizando directamente la URL para ver si utiliza ‘https’ y el certificado digital (seguro).

## 5.18. Diapositiva 39-40. Fraudes comunes en redes sociales. Bulos y fake news

Las [noticias falsas](#) han encontrado en las redes sociales un medio por el que viralizarse y extenderse mucho más rápidos que las noticias reales. Por ello, los bulos, cadenas de mensajes y demás publicaciones que fomentan la desinformación se han popularizado tanto en los últimos años.

El mayor riesgo de este tipo de fraudes es que causan desinformación y desconfianza entre la población, llegando a impactar en cuestiones sanitarias, como ocurrió durante la pandemia por COVID19, donde circularon por redes sociales muchas noticias falsas sobre los efectos secundarios de vacunas y otros tratamientos.

También son una amenaza para nuestra identidad digital, ya que muchas noticias tienen como objetivo atacar y desprestigiar a otras personas o marcas. Y los usuarios que comparten este tipo de publicaciones, una vez se desmienten, suelen perder credibilidad, al igual que los medios que publican estas noticias falsas o ‘fake news’.

### ¿Cómo nos protegemos?

- Buscar la fuente de la noticia o artículo y contrastarla en Internet nos ayudará a verificar si es una noticia real o se trata de una falsa.
- Revisar la URL en el caso de que nos compartan un enlace para analizar si dispone de certificado de seguridad y empieza por https. Esta medida por sí sola no es suficiente para identificar webs fiables, ya que los ciberdelincuentes más detallistas podrían adquirir este certificado pagando.
- Mirar más allá del titular, ya que suelen recurrir a titulares muy llamativos y sensacionalistas para apelar a nuestras emociones y generar interés. Además, es

común que las noticias falsas utilicen titulares que luego no tienen nada que ver con su contenido o lo tergiversan.

- Comprobar el formato en busca de errores ortográficos, traducciones mal hechas, imágenes de poca calidad o, incluso, robadas de otros sitios. Podemos hacer una [búsqueda inversa en Google imágenes](#) para comprobar esto último.

## 5.19. Diapositiva 41-42. Fraudes comunes en redes sociales. Concursos fraudulentos

Hoy en día, los concursos, promociones y sorteos en redes sociales se han convertido en una actividad muy popular entre ciertas marcas y usuarios influyentes en la Red.

Aprovechando la difusión y capacidad de viralización de las publicaciones y mensajes de las redes sociales, algunos ciberdelincuentes han encontrado la oportunidad perfecta para atraer la atención de los usuarios por medio de este tipo de concursos que, con estrategias engañosas, buscan robar nuestros datos, como nombre, correo, dirección y tarjetas bancarias, y luego venderlos a terceros, para finalmente utilizarlos en campañas de *spam* o, en el peor de los casos, para distribución de fraudes y *malware*.

Diferenciar este tipo de concursos fraudulentos de los legítimos no es complicado, ya que solo necesitaremos investigar un poco y leer detenidamente las condiciones del concurso para identificarlos.

### ¿Cómo nos protegemos?

- Comprobar la fuente para contrastar la información. Si una marca concreta lanza un concurso, lo habitual es que hayan creado una campaña de marketing para publicarlo en su web o canales de redes sociales.
- Revisar las bases legales para saber si se trata de un fraude o no, y es que muchas veces nos dejamos llevar por la emoción del momento o las prisas y pasamos por alto lo más importante, ningún sorteo real se lleva a cabo sin bases legales.
- Chequear las URLs, así podremos comprobar a qué dirección nos están llevando, si estamos en un sitio legítimo o no. Una web fiable siempre comenzará por “https” durante el proceso de recogida de datos.
- Analizar los comentarios, ya que muchos usuarios escriben sus experiencias en Internet y, si han sido víctimas, lo publicarán para evitar que otros caigan en el mismo engaño.
- Buscar fallos ortográficos y gramaticales. La mayoría de fraudes o promociones de dudosa reputación usan traductores para la creación del contenido.
- Contrastar las imágenes y comprobar que éstas no estén sacadas de Internet, sean de mala calidad o copias de otros fraudes y/o concursos. Google por ejemplo te permite comprobar si la imagen es una copia y su procedencia desde su buscador de imágenes: <https://images.google.com>

## 5.20. Diapositiva 43-44. Fraudes comunes en redes sociales. Sextorsión y amores en línea

Uno de los objetivos principales de las redes sociales es que nos relacionemos, conozcamos gente y hagamos nuevas amistades. También, es habitual que estas plataformas nos ayuden a conocer a alguien con el que lleguemos a tener una relación especial que pueda trascender la pantalla. En ocasiones, estas prácticas pueden derivar

en *sexting*, es decir, intercambiar contenidos de carácter sexual e íntimo, como fotografías y vídeos entre dos usuarios por la Red de forma consensuada.

Por otro lado, los ciberdelincuentes son conscientes de esto y es habitual que se haga pasar por usuarios en busca del amor para engañar a sus víctimas, ganarse su confianza y finalmente extorsionarlas para solicitar dinero, información personal, control sobre sus dispositivos u obtener más fotografías y vídeos íntimos para luego chantajearlos.

Este último caso se conoce como *sextorsión* y no siempre requiere que hayamos tenido contacto previo con un ciberdelincuente, ni siquiera que hayamos enviado este tipo de contenidos a nadie. A veces nos pueden llegar correos electrónicos o mensajes solicitándonos dinero a cambio de no divulgar estas fotografías o vídeos íntimos sobre nosotros. El ciberdelincuente asegurará disponer de este material, argumentando que tiene acceso a nuestra cámara web, por ejemplo.

Ante la duda de no saber si realmente tienen fotos, vídeos o información íntima de nosotros, muchos usuarios terminan siendo extorsionados.

### ¿Cómo nos protegemos?

- No enviar dinero, ya que realizar el pago no garantiza que no sigan extorsionándonos. Es más, estaremos favoreciendo este tipo de prácticas y, además, en la mayoría de casos ni siquiera disponen de este material.
- Evitar descargar archivos o entrar en enlaces sospechosos, ya que los correos fraudulentos y las webs no fiables son una de las principales causas de infección por *malware*. Los *spyware* son un tipo de malware especializado en hacer capturas y vídeos a través de webcams sin nuestro consentimiento.
- No revelar información personal a desconocidos, ni siquiera si creemos tener una relación especial con esta persona. Si no estamos seguros al cien por cien de sus intenciones, debemos evitar compartir fotografías, vídeos o información sensible sobre nosotros que pueda usarse en la *sextorsión*.
- Investigar a los usuarios nos ayudará a descartar a potenciales ciberdelincuentes. Por ejemplo, revisando sus perfiles, buscando su nombre de usuario o correo electrónico en la Red para ver si está registrado en más plataformas o está vinculado a algún fraude, etc.

## 5.21. Diapositiva 45. Cuestionario de evaluación 1

Lo que publicamos en Internet, fotos, vídeos, opiniones, etc., así como toda la información que existe en Internet sobre nosotros se conoce como:

- A. Identidad digital.
- B. Identidad social.
- C. Identidad online.

## 5.22. Diapositiva 46. Cuestionario de evaluación 2

¿Cuál de las siguientes informaciones no debemos compartir en redes sociales bajo ningún concepto?:

- A. Fotografía de un viaje.
- B. Opinión sobre una película.
- C. Dirección personal.



### 5.23. Diapositiva 47. Cuestionario de evaluación 3

Realizar una búsqueda en la red de nuestro nombre, teléfono o correo electrónico para ver qué se dice de nosotros, se conoce como:

- A. Autobúsqueda.
- B. *Egosearching*.
- C. *Egosurfing*.

### 5.24. Diapositiva 48 . Cuestionario de evaluación 4

Una de nuestras redes sociales nos ha enviado un correo avisándonos de una actividad sospechosa en nuestra cuenta. ¿Qué deberíamos hacer?:

- A. Configurar la privacidad de nuestra cuenta.
- B. Cambiar las contraseñas.
- C. Eliminar contactos.

### 5.25. Diapositiva 49 . Cuestionario de evaluación 5

¿Cómo podemos identificar perfiles falsos en una red social?:

- A. Revisando su información y contactos.
- B. Comprobando la fecha de creación y sus publicaciones.
- C. Ambas opciones.

### 5.26. Diapositiva 50 . Cuestionario de evaluación 6

Mientras navegamos por nuestra red social favorita, encontramos un anuncio sobre un producto que nos llama la atención. ¿Qué debemos hacer?:

- A. Analizar los comentarios.
- B. Comprobar la URL.
- C. Ambas opciones.

### 5.27. Diapositiva 51. Cuestionario de evaluación 7

Las noticias falsas son muy comunes hoy en día, ¿qué pasos debemos seguir para identificarlas?:

- A. Buscar la fuente, revisar la URL, ver el número de visitas.
- B. Buscar la fuente, revisar la URL, comprobar el titular y el formato.
- C. Analizar el contenido, los '*likes*' y el número de visitas.

### 5.28. Diapositiva 52. Cuestionario de evaluación 8

Imaginemos que un usuario con el que llevamos tiempo hablando por Internet, comienza a pedirnos imágenes de tipo íntimo o sexual. ¿A qué tipo de fraude nos estamos exponiendo?:

- A. *Sextorsión*.
- B. *Egosurfing*.
- C. *Phishing*.

### 5.29. Diapositiva 53. Cuestionario de evaluación 9

Algunas de las funciones que podemos activar desde la configuración de privacidad de nuestra cuenta en redes sociales, es:

- A. Modificar la contraseña de nuestra cuenta.
- B. Limitar la visibilidad de nuestro perfil.
- C. Activar la verificación en dos pasos.

### 5.30. Diapositiva 54. Cuestionario de evaluación 10

Una medida de seguridad muy recomendada es activar la función para recibir un código temporal en nuestro dispositivo móvil cada vez que queramos iniciar sesión. ¿Cómo se denomina esta función?:

- A. Doble inicio de sesión.
- B. Bloqueo en dos pasos.
- C. Autenticación en dos pasos.

### 5.31. Diapositiva 55. Final del taller

¡Gracias por vuestra atención!



## 6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller.** La participación del alumnado mediante dudas u otro tipo de aportaciones resulta de un gran valor evaluativo (10% de la evaluación final).
2. **Actividades.** Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u *feedback* directo sobre la evolución del alumnado (25% de la evaluación final).

- |   |  |
|---|--|
| 1 | Por muy concienciados que estemos, siempre podemos cometer un error o despistarnos. Para evitarlo, es conveniente que configuremos nuestras redes sociales de modo que estén lo más protegidas posibles contra fugas de información, protección de nuestras cuentas y para limitar la visibilidad de nuestro perfil. Dedica unos minutos para configurar correctamente tu red social favorita. |
| 2 | Ahora que ya sabemos en qué consiste el <i>egosurfing</i> , deberíamos ser capaces de llevarla a la práctica. Haz una búsqueda en Internet y en tus redes sociales sobre ti y apunta todo aquello que consideres importante, que contenga información personal o que no sabías que existía.  |

3. **Cuestionario de evaluación.** Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

**EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación**

## 6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test “opción múltiple” (3 opciones). La respuesta correcta está destacada en color verde.

1	Lo que publicamos en Internet, fotos, vídeos, opiniones, etc., así como toda la información que existe en Internet sobre nosotros se conoce como:	Identidad digital
		Identidad social
		Identidad online
	Feedback: Así es, la identidad digital es toda la información que podemos encontrar sobre nosotros en la red, así como lo que otros usuarios dicen de nosotros.	
2	¿Cuál de las siguientes informaciones no debemos compartir en redes sociales bajo ningún concepto?	Dirección personal
		Fotografía de un viaje
		Opinión sobre una película
	Feedback: Hay algunos datos personales, como nuestra dirección o número de teléfono que, si se publicase en la Red y llegase a malas manos podría traernos graves consecuencias de privacidad.	
3	Realizar una búsqueda en la red de nuestro nombre, teléfono o correo electrónico para ver que se dice de nosotros, se conoce como:	Egosurfing
		Autobúsqueda
		Egosearching
	Feedback: El término es conocido como <i>egosurfing</i> y nos permite obtener información muy interesante sobre nosotros que quizás no conocíamos, como una web donde se habla de nosotros, un usuario que publicó una foto donde aparecemos, etc.	
4	Una de nuestras redes sociales nos ha enviado un correo avisándonos de una actividad sospechosa en nuestra cuenta. ¿Qué deberíamos hacer?	Cambiar las contraseñas
		Configurar la privacidad de nuestra cuenta
		Eliminar contactos
	Feedback: En este caso lo más importante es que actualicemos la contraseña de nuestra cuenta a una más segura. Lo más probable es que nuestras credenciales se hayan podido filtrar y que nuestra cuenta corra peligro.	
5	¿Cómo podemos identificar perfiles falsos en una red social?	Ambas opciones
		Comprobando la fecha de creación y sus publicaciones
		Revisando su información y contactos
	Feedback: Un perfil falso tendrá todas sus fotografías copiadas de otra cuenta, así como su descripción y datos personales. Además, lo más probable es que siempre tenga el mismo tipo de publicaciones.	
6	Mientras navegamos por nuestra red social favorita, encontramos un anuncio sobre un producto que nos llama la atención. ¿Qué debemos hacer?	Ambas opciones
		Comprobar la URL
		Analizar los comentarios

	Feedback: Antes de decidir si entrar o no en un enlace o hacer clic en un anuncio, es fundamental que comprobemos primero la experiencia de otros usuarios con sus comentarios y valoraciones. Luego, deberemos asegurarnos que se trata de una web segura comprobando la URL (https y certificado de seguridad).	
7	Las noticias falsas son muy comunes hoy en día, ¿qué pasos debemos seguir para identificarlas?	Buscar la fuente, revisar la URL, comprobar el titular y el formato.
		Buscar la fuente, revisar la URL, ver el número de visitas.
		Analizar el contenido, los 'likes' y el número de visitas.
	Feedback: Las noticias falsas no son difíciles de identificar si nos fijamos en la fuente de la noticia y las fuentes utilizadas en su contenido, comprobamos la URL en busca de una web poco fiable, analizamos el titular para ver si es demasiado agresivo o si ataca directamente a alguien o una entidad y, finalmente, comprobando el formato en busca de errores ortográficos, mala traducción o mala calidad en sus imágenes, por ejemplo.	
8	Imaginemos que un usuario con el que llevamos tiempo hablando por Internet, comienza a pedirnos imágenes de tipo íntimo o sexual. ¿A qué tipo de fraude nos estamos exponiendo?	<i>Sextorsión.</i>
		<i>Egosurfing.</i>
		Phishing.
	Feedback: Se conoce como <i>sextorsión</i> , y es un fraude donde el ciberdelincuente afirma tener contenidos íntimos sobre nosotros que difundirá si no le pagamos o accedemos a sus condiciones. En ocasiones, se hacen con este material fingiendo ser un usuario en busca del amor por Internet.	
9	Algunas de las funciones que podemos activar desde la configuración de privacidad de nuestra cuenta en redes sociales, es:	Limitar la visibilidad de nuestro perfil.
		Modificar la contraseña de nuestra cuenta.
		Activar la verificación en dos pasos.
	Feedback: Dentro de las opciones de configuración de nuestra privacidad no es común encontrar las opciones de seguridad, como el cambio de contraseña o activar la verificación en dos pasos, pero sí podremos evitar que desconocidos puedan mandarnos mensajes, ver nuestras publicaciones o nuestro perfil.	
10	Una medida de seguridad muy recomendada es activar la función para recibir un código temporal en nuestro dispositivo móvil cada vez que queramos iniciar sesión. ¿Cómo se denomina esta función?	Autenticación en dos pasos
		Doble inicio de sesión
		Bloqueo en dos pasos
	Feedback: La autenticación en dos pasos es una medida de seguridad muy útil para proteger nuestras cuentas. Solo tendremos que especificar a dónde queremos que nos manden el código temporal de seguridad y utilizarlo cada vez que queramos iniciar sesión.	

## ANEXO

---

### RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- [¿Hacemos buen uso de las redes sociales?](#)
- [¿Sabías que las fake news preocupan al 86% de internautas españoles?](#)
- [Aprende a identificar fraudes online.](#)
- [Consideraciones a tener en cuenta al publicar en redes sociales.](#)
- [Deepfakes, ¿cómo se aprovechan de esta tecnología para engañarnos?](#)
- [Detecta el fraude.](#)
- [Guía para aprender a identificar fraudes online](#)
- [Muévete seguro por las redes sociales](#)
- [OnlyFans: la nueva red social para vender tu “privacidad”](#)
- [Piénsalo 2 veces antes de publicar](#)
- [TikTok, la nueva red social de moda](#)
- [Twitch: streaming, videojuegos y ¿fraudes?](#)
- [Un doble en la Red](#)