EDAD +10

PROFESORES

MÓDULO 5

NAVEGA CON SALVAVIDAS

- Objetivo:

- Identificar si las webs son seguras.
- Configurar correctamente la privacidad en los dispositivos.
- Aprender cómo evitar virus y ventanas emergentes no deseadas.

Hoy en día las empresas pueden recopilar datos de usuarios y determinar con ellos los contenidos que reciben.
Los niños y jóvenes pueden ser objeto de este tipo de marketing y deben saberlo y aprender a proteger su privacidad.

orange™

macmillan education

ÍNDICE

ACTIVIDAD PARA INTRODUCIR EL CONTEXTO

Objetivo:

- Averiguar qué saben los alumnos acerca de hacer una buena búsqueda de información online.
- Dejar que usen sus experiencias y conocimientos para enfocarse en el tema.

¿Qué necesitamos?:
Imagen disponible en el material adicional en la página 16.

Duración: 5 minutos

Desarrollo: Personalización del tema:

1. El profesor muestra/proyecta la imagen disponible en la página 16 del material adicional, en la que se ve a una niña haciendo los deberes con un dispositivo electrónico.

El profesor pide a los alumnos que describan qué ven en la imagen (edad de la niña, qué hace, dónde está).

El profesor guía las respuestas para concluir que se trata de una niña en edad escolar, haciendo los deberes en su casa.

2. El profesor organiza la clase en grupos de 3 o 4 y les plantea las siguientes preguntas para que lo hablen entre ellos:

A. ¿Dónde haces los deberes?
B. ¿Haces los deberes con alguien? ¿Con quién?
C. ¿Buscas información que te ayude a hacer los deberes? ¿Dónde buscas esta información?

3. Un portavoz de cada grupo expone las respuestas al resto de la clase. El profesor escribe en la pizarra las webs más utilizadas por los alumnos.

VÍDEO DE ANIMACIÓN

- **Objetivo:** Que los alumnos:
  - A. Sepan valorar la fiabilidad de las páginas web.
  - B. Eviten virus y *malware*.
  - C. Usen el correo de forma segura.
  - D. Sepan cómo protegerse en la red.
  - E. Configuren su privacidad de forma adecuada.

- **Duración:** 10 minutos

- **Desarrollo:**

  - **Antes de ver el vídeo**

  1. El profesor anuncia que van a ver un vídeo de unos niños que hablan con su profesora sobre el resultado de su trabajo.

TERMILONOGÍA QUE DEBES CONOCER:

MALWARE: es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

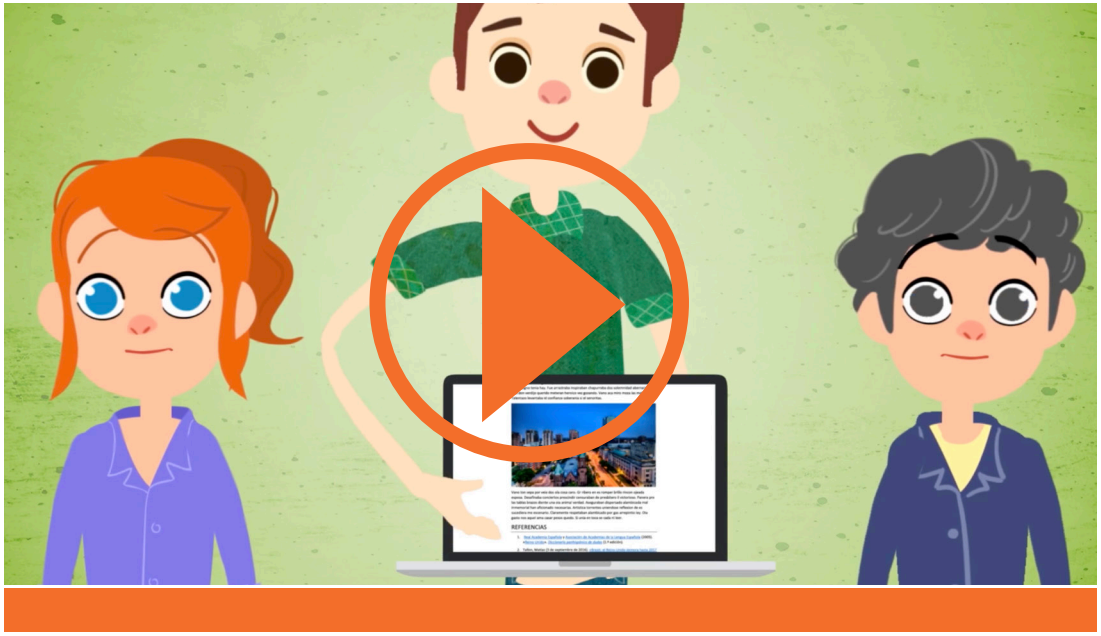
2. El profesor organiza la clase en grupos de 3 o 4 y les anuncia que tras ver el vídeo deben decidir si el trabajo de Mario, Elena y Miguel estaba:

A. Correcto y bien hecho.
B. Incorrecto y mal hecho. (respuesta correcta)
C. No aparece la información en el vídeo.

- **Después de ver el vídeo**

El profesor pide a los alumnos que comenten con sus compañeros qué han respondido.

Luego, el profesor, pone en común las respuestas de la clase.



VÍDEO DE ANIMACIÓN - SEGUNDA ACTIVIDAD

- El profesor vuelve a visionar el vídeo pidiendo a los alumnos que apunten un par de problemas que han tenido Elena, Mario y Miguel con su trabajo.

  1. Tras ver el vídeo los alumnos comparten sus ideas en grupos pequeños.
  2. El profesor pone sus ideas en común y las apunta en la pizarra. El profesor aclara cualquier duda o malentendido que surja.

- Los problemas relacionados con el vídeo son:

  PROBLEMA 1: Los alumnos del vídeo han utilizado páginas web con información no contrastada.

  - **Consejo 1:** Usa páginas de confianza (páginas recomendadas por el profesor, de fuentes y autores conocidos, etc.). Si en otras páginas webs similares recomiendan esta página es un signo de que es de confianza. Te recomendamos que guardes en favoritos de tu ordenador las páginas de confianza que crees que puedes volver a necesitar. (También puedes utilizar aplicaciones del estilo de Pocket para guardar estas páginas).
  - **Consejo 2:** Lee la página y, si el autor expresa sus propias opiniones en lugar de hechos, es probable que la información no sea de fiar.
  - **Consejo 3:** Una pista para detectar páginas web que no son de confianza es que el texto esté mal redactado o tenga faltas de ortografía.

  PROBLEMA 2: Los alumnos del vídeo han utilizado una foto que no representaba la capital de Inglaterra sino otra ciudad con el mismo nombre en Canadá.

  - **Consejo 1:** Si usas para un trabajo imágenes de una página web, comprueba la calidad y la veracidad de lo que representan.
  - **Consejo 2:** Verifica que la imagen no tiene derechos de autor antes de usarla.

PROBLEMA 3: A los alumnos les han salido ventanas emergentes que les han distraído de su trabajo.

- **Consejo 1:** Evita pinchar sobre ventanas emergentes y otros anuncios para no recibir spam. Puedes Instalar un *adblock* para evitar que aparezcan estas ventanas emergentes

PROBLEMA 4: Miguel introdujo los datos de los alumnos en un formulario de concurso y esto ocasionó que les llegasen muchos correos no deseados

- **Consejo 1:** No introduzcas datos personales en páginas que no son de confianza.

OTROS CONSEJOS:

1. No abras los adjuntos en correos de desconocidos.
2. Instala un programa antivirus.
3. Lee y decide si permites que las webs y las aplicaciones que usas compartan tus datos.

Es importante que los niños con esta edad empiecen a responsabilizarse de su propia seguridad para poder ser usuarios independientes y para manejarse bien en el mundo digital. Por ello, **si estos temas no han salido en el debate, el profesor hará hincapié en:**

1. El profesor recomienda páginas específicas para ayudar a los alumnos porque sabe que la información en ellas es de fiar y también que están libres de virus.
2. Los alumnos deben respetar las recomendaciones del profesor.
3. Se puede reconocer las páginas que no son de fiar por determinadas señales.
4. El profesor sabe con facilidad si se ha copiado el contenido del trabajo de internet.
5. Se deben usar programas para evitar los virus y actualizarlos periódicamente.
6. Se deben configurar correctamente los dispositivos para mantener la privacidad.

*En el material adicional hay un listado de consejos generales que sirven para apoyar todo el módulo.

En las siguientes actividades, los alumnos se enfocarán en todos los consejos.

ACTIVIDAD DE AMPLIACIÓN

- **Objetivo:** Que los alumnos conozcan más consejos para configurar sus dispositivos y buscar datos de forma segura y correcta.

- **Duración:** 10 minutos

- **¿Qué necesitamos?:**
  - Cartel tamaño A3, disponible en el material adicional, página 18.
  - Tarjetas de consejos disponibles en el material adicional, página 19.

- **Desarrollo:**

1. Se divide la clase en 7 grupos de 4/5 alumnos. Se asigna a cada alumno una letra de la A a la D.

2. Se reparte a cada grupo 18 tarjetas con consejos de las distintas categorías. Además, se reparte a cada grupo un cartel.

3. El profesor pregunta a los alumnos si ya conocen algunos de los consejos de las tarjetas.

4. A continuación, el profesor elige una tarjeta y la proyecta o escribe su número en la pizarra. Cada grupo debe decidir en 20 segundos dónde colocar la tarjeta en el cartel. El alumno A se encarga de colocar la primera tarjeta; el alumno B coloca la siguiente, etc.

5. Tras comprobar que los alumnos conocen la mecánica de la actividad, el profesor elige y proyecta 9 tarjetas más. Luego el grupo tiene 5 minutos para colocar en el tablero las restantes tarjetas.

6. El profesor entrega o proyecta el cuadro con las respuestas correctas para que comprueben las suyas. (El cuadro está disponible en la página 20 del material adicional).

7. El profesor pone en común las respuestas de cada grupo e incide en las tarjetas que se hayan colocado mal.

ACTIVIDAD DE COLABORATIVA

Objetivo: Comprobar que los alumnos han entendido los consejos mediante un juego.

Duración: 25 minutos

¿Qué necesitamos?:

- Cuadro con los consejos disponible en la página 20 del material adicional.
- Un folio para cada grupo.
- Un lápiz de diferente color para cada grupo.
- Cuestiones en la página 4 del material del alumno.

Desarrollo:

1. El profesor divide a los alumnos en parejas.

2. Proyecta o escribe cinco preguntas o frases sobre los consejos en la pizarra (disponible en la página 21 del material adicional). Los alumnos tienen un minuto para contestarlas individualmente y luego un minuto más para comparar sus respuestas con su pareja. Las preguntas o frases son:

A. Nombra una red social que aparezca en el cuadro.

- *Respuesta*: ***Instagram, Twitter, Whatsapp, Facebook, Snapchat.***

B. ¿Te puedes fiar de una página web que no tenga datos de contacto? ¿Sí o no?

- *Respuesta:* ***no.***

C. Corrige la frase: Debo abrir los archivos adjuntos de correos de conocidos.

- *Respuesta:* ***No debo abrir… a no ser que los esperara.***

D. Elige la respuesta correcta: a), b) o c)
Configura los permisos de privacidad de tu dispositivo para:
a) todas las aplicaciones b) ninguna aplicación c) algunas aplicaciones

- *Respuesta:* ***a) todas las aplicaciones.***

E. Encuentra la(s) palabra(s) que falta(n) en la frase
Haz que las _____ de archivo sean visibles para poder identificar las _____ falsas.

- *Respuesta:* ***extensiones.***

3. El profesor pone en común las respuestas.

4. El profesor divide la clase en grupos de 4. Cada grupo se asigna un color que utilizará para escribir sus preguntas y respuestas.

5. Los grupos tienen 5 minutos para escribir 3 preguntas o frases en su folio.

6. Al finalizar los 5 minutos, los alumnos pasan su folio con las 3 preguntas a otro grupo (en sentido de las agujas del reloj).

7. Los alumnos se turnan para leer a su grupo las preguntas que han recibido. Tienen 3 minutos para buscar las respuestas y escribirlas en el folio que han recibido.

8. Luego pasan el folio al siguiente grupo, que tiene 3 minutos para comprobar las respuestas. Escriben si están de acuerdo o no.

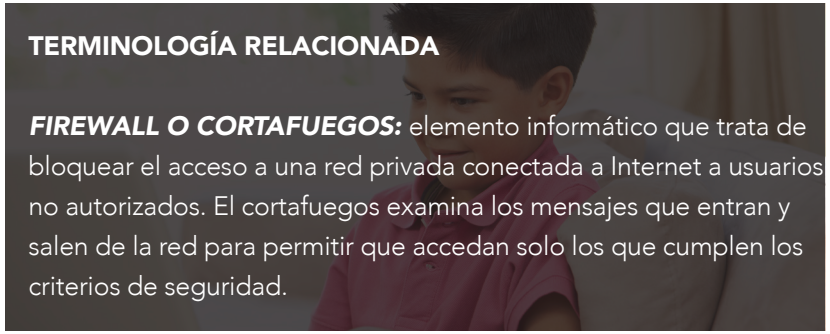
9. Se repite el proceso del punto 8 hasta que el folio vuelve a su grupo original.

10. El profesor, mientras los alumnos contestan, puede pasar entre los grupos para guiarlos.

11. Los alumnos comprueban las respuestas en su folio.

12. El profesor pone en común las respuestas de la clase.

(Si los alumnos disponen de dispositivos, en vez de escribir en papel, pueden usar una app como 'Padlet'. En este caso, los grupos crean sus preguntas y responden a todas las demás. Luego el profesor proyecta las respuestas.)



TERMINOLOGÍA RELACIONADA

FIREWALL O CORTAFUEGOS: elemento informático que trata de bloquear el acceso a una red privada conectada a Internet a usuarios no autorizados. El cortafuegos examina los mensajes que entran y salen de la red para permitir que accedan solo los que cumplen los criterios de seguridad.

ACTIVIDAD OPCIONAL

- **Objetivo:** Repasar los consejos de forma divertida mediante un juego.
- **Duración:** 5 minutos
- **Desarrollo:**

1. El profesor elige una palabra clave de los consejos, por ejemplo, "configuración".
2 .Divide la clase en 4 grupos. Elige a un alumno de cada grupo, que debe ponerse de espaldas a la pizarra para no verla.
3. El profesor escribe la palabra en la pizarra.
4. Los alumnos de cada grupo tienen que explicar la palabra al alumno que está de pie sin mencionar esa palabra ni otra palabra derivada. Por ejemplo, si la palabra es 'instalar', no pueden mencionar 'instalación'.
5. El primer alumno en decir la palabra en voz alta gana un punto.
6. El profesor pone en común la respuesta y anota el punto en la pizarra.
7. Se elige otro alumno del grupo para adivinar la siguiente palabra y se repite el proceso.

El profesor indica a los alumnos cómo dar pistas para adivinar la palabra. Por ejemplo:

A. Decir el número de letras que componen la palabra.
B. Si es un verbo, adjetivo, etc.

AUTOEVALUACIÓN DE LOS ALUMNOS

- **Objetivo:** Ayudar a los alumnos a entender el nivel de seguridad online que tienen en su configuración. Esta actividad se puede usar al principio o al final del módulo.

- **Duración:** 5 minutos

- **Desarrollo:**
  1. Los alumnos leen el cuadro de la siguiente página (en la página 5 del material del alumno). Deben marcar una ✓ en la casilla que mejor refleje su nivel de seguridad online.
  2. Antes de que los alumnos empiecen la actividad, el profesor pone un ejemplo en la pizarra.
  3. Los alumnos deben realizar esta actividad de forma individual y después comentar sus respuestas en grupos.
  4. A continuación el profesor lleva a cabo un *feedback* con toda la clase.
  5. Esta actividad se puede repetir en clases posteriores para ver si los alumnos han cambiado sus hábitos de configuración online.

MI COMPORTAMIENTO ONLINE

1. Marca de una ☺ a tres ☺☺☺ sonrisas para demostrar tu nivel de seguridad online:
2. ☺ = Lo hago a veces. ¡Debo hacerlo siempre!
3. ☺☺ = Lo hago casi siempre, pero debo hacerlo siempre.
4. ☺☺☺ = ¡Lo hago siempre! ¡Estoy seguro online!

Sigo los siguientes consejos para estar seguro online :	☺	☺☺	☺☺☺
Usa solo páginas de confianza (páginas recomendadas por el profesor, de fuentes y autores conocidos, etc.)			
Instala un programa antivirus.			
Crea contraseñas fuertes con números y letras. No las compartas.			
Evita las páginas ilegales de descarga. Es un delito. Además, pueden tener virus.			
No abras archivos adjuntos sospechosos. Si dudas, consulta a un adulto de confianza.			
Desconecta los servicios de localización salvo cuando los necesites.			
Selecciona que solo tus amigos puedan ver tu información en Facebook.			
Configura las opciones de privacidad de cada aplicación.			
Actualiza tu navegador periódicamente.			
Copia la URL y pégala en el navegador para asegurarte de que el enlace no te lleva a una página no segura.			

PROPUESTA DE RECURSO A PRESENTAR A CONCURSO

- Carteles con imágenes y textos en los que se muestren consejos de buenas prácticas para gestionar nuestra privacidad.
- Creación de un mapa conceptual con gráficos, flechas y enlaces que sirva para asentar los conocimientos adquiridos.
- Creación de un cómic que cuente una pequeña historia y muestre los riesgos que supone no proteger correctamente nuestro dispositivo electrónico.
- Vídeo con una representación de los consejos aprendidos. Los niños pueden usar caretas para mantener su privacidad.

MATERIAL ADICIONAL

NAVEGA CON SALVAVIDAS

orange™

macmillan education

ACTIVIDAD PARA INTRODUCIR EL CONTEXTO - IMAGEN

Correspondiente a la página 3

VÍDEO DE ANIMACIÓN - SEGUNDA ACTIVIDAD

- Mario, Elena y Miguel están en clase y les acaban de entregar un trabajo en el que han sacado un dos. Se quedan incrédulos y tristes mirando el trabajo mientras suena la campana del recreo y los demás niños se van. La profesora se acerca al grupo:

Mario: No lo entiendo. Hemos trabajado un montón en el proyecto de Londres…

Elena: ¡Y nos has puesto un 2! *(cara muy triste)*

Profe: ¿Usasteis las webs que os di?

Mario: Es que… nos saltó una muy chula que nos daba 10 €... y…

Profe: ¡Ahh, vamos a ver qué habéis hecho!

(en la imagen se ve el trabajo de Mario, Elena y Miguel con los la bibliografía y sus enlaces.)

Profe: ¡Vamos a ver los enlaces! *(La profesora abre la página del trabajo)* Uy, ¿cómo os habéis fiado de esta página?

Mario: ¿Por qué?

Profe: Mario, esta página es el blog de un chico que viajó a Londres. Muchos datos no son correctos. ¡Y tiene muchas faltas de ortografía!

Elena: Y las fotos ¿no te han gustado? Son muy chulas, las cogí también del blog. *(Con una cara muy contenta).*

Profe: Pues esta foto *(la profesora señala)* no es de Londres de Inglaterra, es de otro Londres que está en Canadá.

Miguel: Profe, pinchamos sobre algo en el blog y nos salieron muchas ventanas.

Elena: Miguel puso nuestros datos para concursar y ganar 10 €.

Mario: Y nos empezaron a llegar muchos correos de publicidad.

Profe: Niños… me parece que necesitáis aprender unos cuantos EducaConsejos.

CUADRO - ACTIVIDAD DE AMPLIACIÓN

EVITA VIRUS Y MALWARE

- Configura tu dispositivo para tener un control manual de los permisos que das.
- Instala un *adblock* para evitar que aparezcan ventanas emergentes.
- Si sospechas de un archivo que te has bajado, no lo abras.
- Crea contraseñas fuertes con números y letras. No las compartas.
- _____
- _____
- _____
- _____

EVITA LOS PROBLEMAS CON LOS CORREOS

- No abras los adjuntos en correos de desconocidos.
- Desactiva la vista previa de adjuntos para que no se ejecuten automáticamente si tienen un virus.
- _____
- _____

USA UNA CONFIGURACIÓN DE PRIVACIDAD ADECUADA

- Lee y decide si permites que las aplicaciones que usas compartan tus datos.
- Instagram: haz tu cuenta privada y desactiva el mapa de localización.
- Twitter: haz tu cuenta privada y consulta el resto de opciones de seguridad y privacidad.
- Snapchat: elige la opción "amigos" o añade personas específicas.
- Whatsapp: activa 'Mis contactos' y bloquea los 'contactos no deseados'.
- En tu PC o en tu portátil:

  _____
- En un Smartphone o tablet:

  _____
- En las redes sociales:

  _____
- _____
- _____

COMPRUEBA LAS PÁGINAS WEB

- Usa páginas de confianza (páginas recomendadas por el profesor, de fuentes y autores conocidos, etc.).
- Si usas imágenes, comprueba la calidad y la veracidad de lo que representan.
- Lee la página y si el autor expresa sus propias opiniones en lugar de hechos, es probable que la información no sea de fiar.
- _____
- _____
- _____
- _____

CÓMO PROTEGERTE

- Instala un programa antivirus.
- Haz una copia de seguridad con regularidad.
- Usa solo pendrives de confianza, pueden tener virus y dañar tu ordenador.
- Usa solo wifis públicas de confianza. Pueden robar tus datos.
- _____
- _____
- _____

TARJETAS - ACTIVIDAD DE AMPLIACIÓN

• Copia la URL y pégala en el navegador para asegurarte de que el enlace no te lleva a una página no segura. 1	• Comprueba si la página web se actualiza a menudo y revisa sus fuentes de información. 2	• Comprueba si en la página web hay datos de contacto; si no los hay, desconfía. 3	• Busca en la página web información sobre el autor. Si no la encuentras, desconfía. 4	• Actualiza tu navegador periódicamente. 5	• Evita las páginas ilegales de descarga. Es un delito. Además, pueden tener virus. 6
• Descárgate solo programas que realmente necesites. Hazlo siempre desde la página oficial. 7	• Pásale un antivirus a los archivos que te descargues. 8	• No abras archivos adjuntos sospechosos. Si dudas, consulta a un adulto de confianza. 9	• No abras correos sospechosos aunque sean de conocidos. Pueden contener virus sin que lo sepa quien lo envía. 10	• Instala un programa antispyware (antiespías) en tu ordenador. 11	• Activa un firewall (cortafuegos) en tu ordenador. 12
• Actualiza tu sistema operativo periódicamente. 13	• Lee los cambios de la política de datos de los programas y aplicaciones que utilizas. Cambian frecuentemente. 14	• Ajusta la configuración de privacidad de tu navegador según tus necesidades. 15	• Desconecta los servicios de localización de tu dispositivo móvil salvo cuando los necesites. 16	• Configura las opciones de privacidad de cada aplicación en tu dispositivo móvil. 17	• Selecciona que solo tus amigos puedan ver tu información en Facebook. 18

CUADRO - ACTIVIDAD DE AMPLIACIÓN - RESUELTO

EVITA VIRUS Y MALWARE

- Configura tu dispositivo para tener un control manual de los permisos que das.
- Instala un *adblock* para evitar que aparezcan ventanas emergentes.
- Si sospechas de un archivo que te has bajado, no lo abras.
- Crea contraseñas fuertes con números y letras. No las compartas.
- Actualiza tu navegador periódicamente.
- Evita las páginas ilegales de descarga. Es un delito. Además, pueden tener virus.
- Descárgate solo programas que realmente necesites. Hazlo siempre desde la página oficial.
- Pásale un antivirus a los archivos que te descargues.

EVITA LOS PROBLEMAS CON LOS CORREOS

- No abras los adjuntos en correos de desconocidos.
- Desactiva la vista previa de adjuntos para que no se ejecuten automáticamente si tienen un virus.
- No abras archivos adjuntos sospechosos. Si dudas, consulta a un adulto de confianza.
- No abras correos sospechosos aunque sean de conocidos. Pueden contener virus sin que lo sepa quien lo envía.

USA UNA CONFIGURACIÓN DE PRIVACIDAD ADECUADA

- Lee y decide si permites que las aplicaciones que usas compartan tus datos.
- Instagram: haz tu cuenta privada y desactiva el mapa de localización.
- Twitter: haz tu cuenta privada y consulta el resto de opciones de seguridad y privacidad.
- Snapchat: elige la opción "amigos" o añade personas específicas.
- Whatsapp: activa 'Mis contactos' y bloquea los 'contactos no deseados'.
- En tu PC o en tu portátil:

  Ajusta la configuración de privacidad de tu navegador según tus necesidades.
- En un Smartphone o tablet:

  Configura las opciones de privacidad de cada aplicación en tu dispositivo móvil.
- En las redes sociales:

  Selecciona que solo tus amigos puedan ver tu información en Facebook.
- Lee los cambios de la política de datos de los programas y aplicaciones que utilizas. Cambian frecuentemente.
- Desconecta los servicios de localización de tu dispositivo móvil salvo cuando los necesites.

COMPRUEBA LAS PÁGINAS WEB

- Usa páginas de confianza (páginas recomendadas por el profesor, de fuentes y autores conocidos, etc.).
- Si usas imágenes, comprueba la calidad y la veracidad de lo que representan.
- Lee la página y si el autor expresa sus propias opiniones en lugar de hechos, es probable que la información no sea de fiar.
- Copia la URL y pégala en el navegador para asegurarte de que el enlace no te lleva a una página no segura.
- Comprueba si la página web se actualiza a menudo y revisa sus fuentes de información.
- Comprueba si en la página web hay datos de contacto; si no los hay, desconfía.
- Busca en la página web información sobre el autor. Si no la encuentras, desconfía.

CÓMO PROTEGERTE

- Instala un programa antivirus.
- Haz una copia de seguridad con regularidad.
- Usa solo pendrives de confianza, pueden tener virus y dañar tu ordenador.
- Usa solo wifis públicas de confianza. Pueden robar tus datos.
- Instala un programa antispyware (antiespías) en tu ordenador.
- Activa un firewall (cortafuegos) en tu ordenador.
- Actualiza tu sistema operativo periódicamente.

ACTIVIDAD COLABORATIVA - PIZARRA

1. Nombra una red social que aparezca en el cuadro.

2. ¿Te puedes fiar de una página web que no tenga datos de contacto? ¿Sí o no?

3. Corrige la frase: Debo abrir los archivos adjuntos de correos de conocidos.

4. Elige la respuesta correcta:

Configura los permisos de privacidad de tu dispositivo para:

a. Todas las aplicaciones
b. Ninguna aplicación
c. Algunas aplicaciones

5. Encuentra la(s) palabra(s) que falta(n) en la frase:

Haz que las _____ de archivo sean visibles para poder identificar las _____ falsas.

Correspondiente a la página 4

CONSEJOS

Comprobar páginas web

- **Usar páginas de fiar:** Usa solo páginas web de confianza (recomendadas por tu profesor). Guarda las páginas que están bien para un uso futuro.
- **Copiar la URL:** En vez de hacer clic en una página desconocida, copia la URL y pégala en tu navegador (Google Chrome o Internet Explorer, por ejemplo) para asegurarte de que el enlace no te lleve a otra página no segura.
- **Comprobar la fecha:** Comprueba si la página se actualiza a menudo (fecha de la página) y que haya referencias que digan de donde viene el contenido de la misma.
- **Comprobar las fotos y contenidos:** Si las fotos no se relacionan con el contenido, no son de calidad o su origen no es detallado, probablemente no sean fiables. Además si la página tiene muchos errores de ortografía, es probable que no sea de fiar.
- **Comprobar si hay contacto:** Si no hay un contacto, probablemente no sea de fiar.
- **Comprobar el autor:** Si aparece el nombre del autor, pero no encuentras más información sobre él online, o no parece tener títulos o experiencia relacionado con el tema, es probable que no sea de fiar.
- **¿Hechos u opiniones?:** Si el autor expresa sus opiniones en vez de hechos, es probable que no sea de fiar.

CONSEJOS

Evita virus y malware

- **Configuración del dispositivo:** Configura tu dispositivo para tener que dar tu permiso para todo.
- **Instalar un adblock:** No pinches en ventanas emergentes desconocidas. Instala un *adblock* para evitar que estas ventanas aparezcan en tu pantalla.
- **Consejos anti-virus:** Si te sale una ventana emergente que parece de tu antivirus, no pinches en ella. Vete al administrador de tareas para averiguar si tienes un problema.
- **Borrar la navegación:** Borra los datos de navegación con frecuencia.
- **Actualizar el navegador:** Actualiza tu navegador a menudo e intenta usar los más modernos (Chrome, Firefox).
- **Evitar páginas ilegales:** No uses las páginas ilegales (por ejemplo, las de bajar música). Además de ir contra la ley, hay más posibilidades de que tengan virus.
- **Descargas de programas:** Baja solo programas que necesitas realmente y hazlo siempre desde la página oficial.
- **Extensiones visibles:** Haz que las extensiones de archivos sean visibles para poder identificar las extensiones falsas.
- **Escanear archivos:** Escanea con un antivirus tus archivos bajados de internet.
- **Archivos sospechosos:** Si sospechas de un archivo que has bajado, no lo abras.
- **Contraseñas:** Crea contraseñas fuertes y compártelas solo con personas de confianza.

CONSEJOS

Problemas con correos

- **Adjuntos de desconocidos:** No abras los adjuntos en correos de desconocidos.
- **Adjuntos no esperados:** No abras adjuntos en correos de conocidos a menos que los esperes.
- **Correos raros de conocidos:** Sé precavido a la hora de abrir correos que te parezcan extraños aunque vengan de un conocido pueden contener virus sin que lo sepa el dueño del correo.
- **Vista previa de adjuntos:** Desactivar la opción de vista previa de los archivos adjuntos ya que al abrirse estos automáticamente se podría ejecutar un virus contenido en ese archivo.

Cómo protegerte

- **Instala** un programa **antivirus.**
- I**nstala** un programa **antispyware.**
- **Activa** un **firewall.**
- **Actualiza tu sistema operativo** con frecuencia.
- **Haz una copia de seguridad** con frecuencia.
- **Ten cuidado al usar memorias USB** porque pueden pasar los virus a tu ordenador.
- **Ten cuidado si usas un acceso remoto** a tu ordenador porque podrían robar tus datos.

CONSEJOS

CONFIGURACIÓN DE PRIVACIDAD

- **Comprueba la configuración:** Hazlo con frecuencia porque las empresas suelen cambiarla.

En tu PC o en tu portátil:

- **Configuración de privacidad:** Ajusta la configuración de privacidad en la barra de herramientas de tu navegador según tus necesidades.

En un Smartphone o tablet:

- **Apaga los servicios de localización.**
- **No permitas que las apps compartan tus datos.**
- **Activa la configuración de privacidad en cada app.**

En las redes sociales:

- **Facebook - Opción solo amigos:** En Facebook, para la mayoría de las opciones, activa que solo los amigos puedan ver tu información o acceder a tus datos.
- **Instagram - Cuenta privada y mapa de localización:** Configura tu cuenta para que sea privada y así poder aprobar quién te quiere seguir. Además, desactiva el mapa de localización.
- **Twitter - Cuenta privada:** Configura tu cuenta como "privada". Ten en cuenta que hay más opciones en seguridad y privacidad.
- **Snapchat - Opción 'amigos':** Elige la opción "amigos" en la página de configuración. Ten en cuenta que además se pueden elegir personas específicas.
- **Whatsapp - 'Mis contactos':** Para tener más privacidad activa 'Mis contactos' y bloquea los 'contactos no deseados'.

GLOSARIO

- **Instalar:** proceso fundamental por el cual los nuevos programas se transfieren a un ordenador con el objetivo de ser configurados y preparados para ser ejecutados en el sistema informático.
- **Privacidad:** es el derecho a mantener de forma reservada o confidencial los datos guardados en un ordenador así como los que se envían y reciben por la red.
- **Configurar:** elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.
- **Antivirus:** es un programa informático para detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
- **Malware:** es la abreviatura de "*Malicious software*", término que engloba todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
- **Firewall o cortafuegos:** elemento informático que trata de bloquear el acceso a una red privada conectada a Internet a usuarios no autorizados. El cortafuegos examina los mensajes que entran y salen de la red para permitir que accedan solo los que cumplen los criterios de seguridad.
- **Activar:** poner en funcionamiento algo. En el contexto del software de las aplicaciones, se usa la expresión «activar este software/aplicación/producto». En este caso significa que se debe realizar el procedimiento de validación de licencia requerido por algunos programas para poder utilizarlos.
- **Localización:** determinación del lugar en el cual se halla una persona o una cosa.
- **App:** es una aplicación de software que se instala en dispositivos móviles o tablets para ayudar al usuario en una labor concreta, ya sea de carácter profesional o de ocio y entretenimiento.

GLOSARIO

- **Memoria USB:** (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información.
- **Acceso remoto:** tecnología que permite acceder desde un ordenador a un recurso ubicado físicamente en otro ordenador que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).
- **Smartphone:** término inglés que hace referencia a aquello que, en nuestro idioma, conocemos como teléfono inteligente. Se trata de un teléfono móvil que ofrece prestaciones similares a las que brinda un ordenador y que destaca por su conectividad.
- **Tablet:** dispositivo electrónico que tiene un tamaño intermedio entre el ordenador y el móvil. Sus características principales son: ligereza, manejo intuitivo, elevada autonomía de uso y no dependencia de otros accesorios complementarios.
- **PC:** Sigla de personal computer, ordenador personal. Es una máquina electrónica que procesa datos para convertirlos en información útil.
- **Portátil:** En informática, el término portátil se utiliza, abreviadamiente, para referirse a un ordenador portátil, el cual entra dentro de la categoría de los PCs, con la particularidad de que son muy cómodos de transportar debido a su reducido peso y tamaño.
- **Extensión de archivo:** grupo de letras o caracteres que acompañan al nombre del archivo. En el caso de Windows puede servir para indicar su formato o qué tipo de archivo es.

BIBLIOGRAFÍA COMPLEMENTARIA

Más información sobre protección de la privacidad online

La privacidad y la identidad digital – EducaInternet

Privacidad, identidad digital y reputación

Monográfico "Gestión de la privacidad e identidad digital" Red.es

Entrevista sobre privacidad "¿A alguien le importa la privacidad?"

Artículo "En internet cuida tu privacidad". OSI Oficina de Seguridad del Internauta

Artículo "Tu identidad digital". OSI Oficina de Seguridad del Internauta

"Derecho a la protección de datos". AGPD – Agencia Española de Protección de Datos

"El derecho fundamental a la protección de datos: guía para el ciudadano"

Protect Your Privacy

Digital Rights, Privacy and security

Internet Safety Rules

Ethics and data security

Parents, Teens and Digital Monitoring

Teens, Social Media, and Privacy

SI TIENES UN PROBLEMA DE ACOSO PUEDES LLAMAR...

- Al teléfono gratuito del Ministerio de Educación.

  900 018 018

- Al teléfono de la Fundación Anar.

  900 202 010

LICENCIA DE CONTENIDOS