

Líderes Digitales en el Aula

Edición número 4



Tema 1

Uso de internet y ciberseguridad



¿Qué vamos a aprender hoy?



1. ¿Qué es internet?



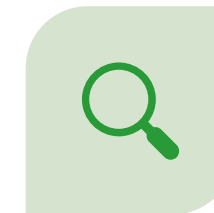
2. ¿Para qué puedes usar internet?



3. Beneficios y peligros de internet



4. ¿Qué es la ciberseguridad?



5. ¿Cómo descubrir los peligros de internet?

1. ¿Qué es internet?



— ¿Qué es internet?



- Internet es una gran red de ordenadores conectados entre sí.
- Esta gran red conecta los ordenadores y móviles de todo el mundo.
- La palabra Internet viene de las palabras en inglés Interconnected Networks. Interconnected Networks significa **redes interconectadas**.

2. ¿Para qué puedes usar internet?



___ ¿Para qué puedes usar internet?

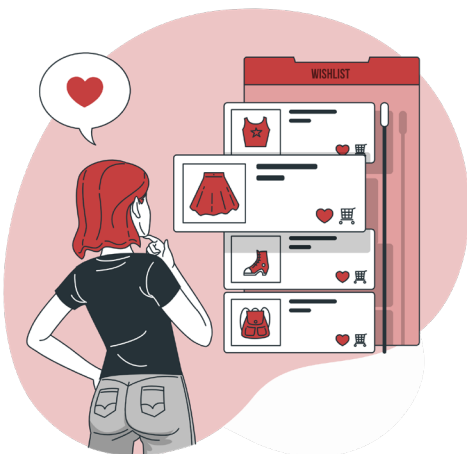


- Puedes usar internet para buscar información de todo tipo.

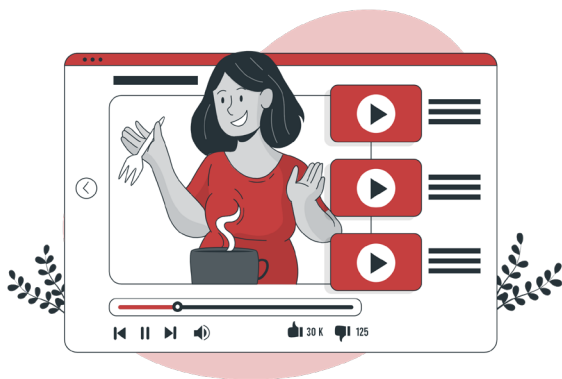


- Puedes usar internet para comunicarte con tus amigos, amigas y familia.

___ ¿Para qué puedes usar internet?



- Puedes usar internet para hacer compras sin salir de casa.



- Puedes usar internet para ver videos y películas. También escuchar música y jugar.

3. Beneficios y peligros de internet



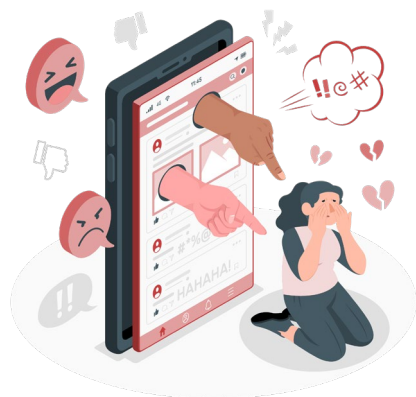
— Beneficios de Internet



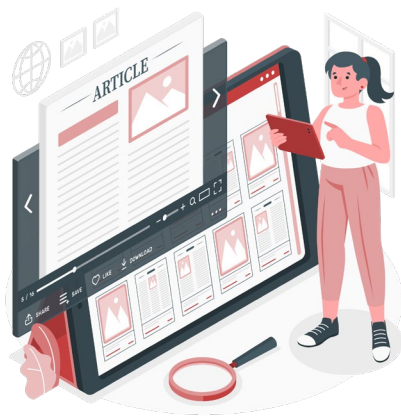
- Con internet, puedes comunicarte con amigos, amigas y familiares que están lejos.
- Con internet, puedes buscar información de manera rápida y sencilla.
- Con internet, puedes aprender cosas nuevas que te interesan.
- Con internet, puedes entretenerte. Puedes ver vídeos, escuchar música o jugar.



Peligros de Internet



- En Internet puedes ser víctima de **ciberacoso**. Algunas personas pueden utilizar internet para molestarte y hacerte daño.



- En Internet puedes encontrar **información falsa**. No toda la información en internet es verdadera.

Peligros de Internet



- En internet,
las personas pueden **robar tus datos personales**.
Las personas pueden robar tus datos personales
para hacerte daño
o para robarte tu dinero o tus cosas.
- En Internet existen **virus**
que pueden dañar tu ordenador
o robar tus datos.

— Peligros de Internet



- Si pasas mucho tiempo en internet en tu ordenador o en tu móvil puedes crear una **adicción a internet**.

La adicción a internet significa que quieres estar siempre en internet y dejas de hacer cosas importantes de tu vida.

— Actividad 1

Ordena los beneficios y peligros de Internet.

Para hacer esta actividad
pulsas la tecla Control o Ctrl de tu ordenador
y pinchas en el siguiente enlace:

[Beneficios y Peligros \(genially.com\)](https://genially.com)

4. ¿Qué es la ciberseguridad?



— ¿Qué es la ciberseguridad?



- Son las acciones que podemos poner en marcha para protegernos de los peligros de internet.
- Estas acciones protegen nuestros ordenadores, nuestros móviles y a nosotros mismos.

— ¿Cómo puedes protegerte en internet?



- No compartas mucha información en tus redes sociales.
- No publiques o compartas datos personales, por ejemplo, tu teléfono, tu dirección o fotos que no quieres que nadie vea.
- Revisa la privacidad de tus cuentas.
Por ejemplo, puedes decidir qué personas ven tu información.

— ¿Cómo puedes protegerte en internet?



- Usa conexiones seguras de internet.
Las conexiones seguras son las que tienen contraseña o la conexión de internet de tu casa.
No uses conexiones wifi públicas.
- Intenta tener tu ordenador y móvil actualizados.
- Usa Antivirus.
Un antivirus es un programa que protege tu ordenador o tu móvil de los virus de internet.
- Usa contraseñas seguras.
Una contraseña segura es una contraseña difícil de adivinar, con letras, números y símbolos.

— Privacidad



- La privacidad es el derecho a proteger tu información personal y las actividades que haces en internet.

¿Para qué es importante tener privacidad en internet?

- Para que otras personas no puedan utilizar tus datos personales. Por ejemplo, tu nombre, tus fotos o tu tarjeta de crédito.
- Para proteger tus cuentas de correo y tus redes sociales.
- Para usar internet como tu quieras y de manera segura.



— Contraseñas

Contraseñas seguras:

Una contraseña segura es una contraseña difícil de adivinar.

Tiene que ser una contraseña larga,
con números, letras y símbolos.

¿Por qué necesitas usar contraseñas seguras?

- Las contraseñas seguras te ayudan a proteger tu información personal.
- Las contraseñas seguras también te ayudan a que no te roben tu identidad.

Si alguien consigue tu contraseña puede hacerse pasar por ti.



— ¿Cómo puedes crear una contraseña segura?

Paso 1. Piensa una frase con 8 letras o más.
Vamos crear una contraseña de 12 letras.

Por ejemplo: un globo verde

¿Cómo puedes crear una contraseña segura?

Paso 2. Pon en mayúscula la primera letra de cada palabra y une las palabras.

Por ejemplo: UnGloboVerde

¿Cómo puedes crear una contraseña segura?

Paso 3. Cambia algunas letras por números.
Puedes cambiar las letras vocales por números.
Por ejemplo, la letra **u** por el número 1,
la letra **e** por el número 3,
o la letra **o** por el número 0.

Por ejemplo: 1nGl0b0V3rd3

— ¿Cómo puedes crear una contraseña segura?

Paso 4. Añade símbolos

Por ejemplo: 1nGl0b0V3rd3!%

— ¿Cómo puedes crear una contraseña segura?

Paso 5. Debes tener una contraseña para cada cosa.

Por ejemplo, puedes poner una **I** a la contraseña y usarla para Instagram.

I1nGl0b0V3rd3!%

Después puedes poner una **F** a la contraseña y usarla para Facebook.

F1nGl0b0V3rd3!%

— Actividad 2

Juego ¿Cuál es la contraseña más segura?

Para hacer esta actividad
pulsas la tecla Control o Ctrl de tu ordenador
y pinchas en el siguiente enlace:

[Contraseñas \(genially.com\)](https://genially.com)

5. ¿Cómo descubrir los peligros de internet?



— ¿Cómo descubrir los peligros de internet?

Phishing

- El phishing significa que una persona intenta engañarte para que le des tu información personal.
- La persona que te hace phishing te pide tus contraseñas, tu nombre, tus teléfonos o tus números de tarjetas de crédito.
- Las personas que hacen phishing te mandan correos electrónicos y mensajes falsos para intentar conseguir tu información personal.



— ¿Cómo descubrir el phishing?

- Las personas que hacen phishing te mandan correos y mensajes para pedirte información personal. También te piden que respondas de forma urgente.
- En estos correos o mensajes te piden que pinches en un enlace.
- La mayoría de las veces estos correos o mensajes te los mandan desde correos electrónicos y contactos desconocidos o falsos.
- La mayoría de las veces estos correos o mensajes están mal escritos.



— Ejemplos de correos de phishing



**BANCO CAJAMAR CIF.
A-044655**



Estimado/a cliente,
Le enviamos este mensaje para informarle que su "Tarjeta", infortunadamente ha sido desactivada debido a una actividad sospechosa en su cuenta.
Le informamos que a partir de la fecha indicada, no se puede realizar ninguna operacion.
Para reactivar su acceso:
[=> haga clic aqui](#)
Atención al cliente.
Seguridad Banca Online - Cajamar



**RE//:Aviso de seguridad
ref-11092020**

Bankia

Estimado/a cliente,

Le enviamos este mensaje para informarle que su "Tarjeta", infortunadamente ha sido desactivada debido a una actividad sospechosa en su cuenta.

Le informamos que a partir de la fecha indicada, no se puede realizar ninguna operacion.

Para reactivar su acceso :

[haga clic aqui](#)

Atención al cliente.

Bankia Banco Seguridad.

— Actividad 3

Descubre mensajes de Phishing.

Para hacer esta actividad
pulsa la tecla Control o Ctrl de tu ordenador
y pincha en el siguiente enlace:

[Phishing \(genially.com\)](https://genially.com)

— ¿Cómo descubrir los peligros de internet?



Virus

Un virus es un programa informático que puede estropear tu ordenador, móvil o tablet y robar tu información personal

¿Qué puedes hacer para evitar los virus?

- No descargues archivos o programas de páginas web que no son seguras.
- No pinches en enlaces que te parecen sospechosos.

— ¿Cómo descubrir los peligros de internet?

Ciberacoso

El ciberacoso significa que una persona te acosa por internet, redes sociales o mensajes.



¿Cómo puedes descubrir el ciberacoso?

- Una persona te acosa en internet cuando te manda mensajes negativos, insultos o amenazas.
- La persona te envía los mensajes negativos varias veces.



info@plenainclusion.org

www.plenainclusion.org