Junta de Castilla y León
Consejería de Educación

Seguridad en Internet

#Se_con_TIC

Seguridad en Internet

JUSTIFICACIÓN

Internet y las redes sociales se han convertido en herramientas que los alumnos utilizan de forma habitual, cada vez desde edades más tempranas. Sin embargo, en muchas ocasiones no tienen la formación necesaria para su uso de forma segura y no son conscientes de los riesgos que implican.
Esta unidad didáctica aborda contenidos relacionados con la seguridad en internet y ofrece ideas y actividades para que los alumnos puedan disfrutar de estos recursos de forma más segura.

COMPETENCIAS

- Competencia digital.
- Competencia en comunicación lingüística.
- Competencia de aprender a aprender.
- Competencia en sentido de la iniciativa y espíritu emprendedor.
- Competencia matemática y competencias básicas en ciencia y tecnología.
- Competencia social y cívica.

OBJETIVOS DIDÁCTICOS

- Conocer los riesgos de internet y estrategias para evitarlos.
- Aprender a proteger la identidad digital: contraseñas, visibilidad en la red ...
- Utilizar las redes sociales de forma respetuosa y segura.

CONTENIDOS

- Conocimientos previos sobre internet.
- Importancia del uso seguro de Internet.
- Contraseñas seguras.
- La identidad digital.
- Privacidad en Internet.
- Tratamiento de imágenes propias y de otros.
- Delitos en la red (usurpación de la identidad, *ciberbullying*, etc).
- Mecanismos de petición de ayuda ante abusos.

Seguridad en Internet

CRITERIOS DE EVALUACIÓN

- Conocer los riesgos de internet y estrategias para evitarlos.
- Proteger la identidad digital.
- Utilizar las redes sociales de forma respetuosa y segura.

ESTÁNDARES DE APRENDIZAJE EVALUABLES

- Conoce los riesgos de compartir datos personales propios y ajenos (dirección, fotos, ubicación, hábitos, gustos, aficiones, etc).
- Es consciente de los delitos que se pueden cometer en la red, sus consecuencias y medidas básicas de prevención.
- Sabe actuar en caso de convertirse en víctima o testigo de comportamientos inadecuados y/o delictivos.
- Conoce la forma de gestionar la seguridad de sus cuentas a través de la creación de contraseñas seguras y la configuración de la privacidad.
- Se comporta con corrección en el uso de las redes sociales *(netiqueta).*

METODOLOGÍA

- Metodología activa y participativa.
- Agrupaciones: trabajo individual, gran grupo, grupos reducidos y por parejas.
- Descubrimiento guiado.
- Resolución de problemas.

MATERIALES RECOMENDADOS

- Pizarra digital o proyector.
- Aula de informática, tablet o miniportátiles.
- Acceso a internet.
- Presentación PREZI:
  http://prezi.com/zbrqq4bhon0v

Seguridad en Internet

COMPETENCIA DIGITAL

- Conoce la importancia de garantizar la privacidad de datos en internet y actúa en consecuencia: genera contraseñas seguras, consulta términos y condiciones, etc.
- Conoce los peligros que presenta internet (ciberacoso, grooming, etc) y actúa en consecuencia: respeta la edad mínima en participación en redes sociales, hace uso responsable de imágenes y vídeos, etc).

COMPETENCIA EN COMUNICACIÓN LINGÜÍSTICA

- Expone oralmente ideas con orden y coherencia sin apoyo visual.
- Narra situaciones con orden, claridad y continuidad.
- Aprende y emplea de manera natural palabras técnicas del argot de la ciberseguridad.
- Entiende el mensaje global de textos en formato digital.

COMPETENCIA SOCIAL Y CÍVICA

- Participa en situaciones que implican trabajar en grupo en las actividades y pequeños proyectos respetando las normas básicas de convivencia.
- Participa activamente en la elaboración y el desarrollo de actividades que fomenten la *netiqueta* (normas de convivencia en Internet).

COMPETENCIA APRENDER A APRENDER

- Partiendo de conocimientos previos relacionados con las TIC se desarrollan habilidades que facilitan el uso de forma segura y respetuosa.

COMPETENCIA EN SENTIDO DE LA INICIATIVA Y ESPÍRITU EMPRENDEDOR

- Conoce y utiliza de manera autónoma todo tipo de fuentes de información (diccionario, biblioteca, internet, etc.)
- Participa activamente en el desarrollo de esta unidad didáctica.

COMPETENCIA MATEMÁTICA Y COMPETENCIAS BÁSICAS EN CIENCIA Y TECNOLOGÍA

- Resuelve situaciones lógicas a partir de datos procedentes de fuentes proporcionadas por el profesor: gráficos, diagramas y esquemas.

Seguridad en Internet - Índice de Sesiones

ÍNDICE DE SESIONES

* **¿Cuánto sabes de Internet?**
* **Tu contraseña segura.**
* **Protege tu identidad digital.**
* **¿Qué hago con mi móvil?**
* **Crea tu decálogo.**

* ¿CUÁNTO SABES DE INTERNET?

Realiza el cuestionario y utiliza las respuestas para establecer un debate sobre lo que podemos hacer y lo que no.

* TU CONTRASEÑA SEGURA

Conoce estrategias para crear contraseñas seguras.

* PROTEGE TU IDENTIDAD

La información sobre nosotros que publiquemos en Internet, irá conformando nuestra Identidad Digital . Veremos qué podemos hacer para proteger nuestra identidad.

* ¿QUÉ HAGO CON EL MÓVIL / TABLET?

Es importante conocer los riesgos de Internet y sabernos comportar de forma respetuosa en las redes sociales.

* CREA TU DECÁLOGO

Elabora con los alumnos un decálogo de consejos de uso de internet para el aula.

¿Cuánto sabes de Internet?

Resuelve el cuestionario de 15 preguntas de verdadero y falso. Las siguientes preguntas se puede realizar siguiendo el siguiente enlace a la web de Kahoot: http://bit.ly/2fVEyvU.

1. Un ordenador infectado siempre presenta algún síntoma para detectarlo.

- ☐ VERDADERO
- ☐ FALSO

2. Los únicos sitios que pueden infectar un dispositivo son las páginas de juegos de azar y páginas con contenidos ilegales.

- ☐ VERDADERO
- ☐ FALSO

3. Las faltas de ortografía son un indicio o sospecha de intento de fraude.

- ☐ VERDADERO
- ☐ FALSO

4. No es recomendable cambiar muchas veces tu contraseña pues se te puede olvidar.

- ☐ VERDADERO
- ☐ FALSO

5. Los delincuentes informáticos no solo atacan a las grandes empresas.

- ☐ VERDADERO
- ☐ FALSO

6. Tus fotos y comentarios de tus redes sociales solo las puede ver quien tú quieras.

- ☐ VERDADERO
- ☐ FALSO

7. Si la Policía Nacional "bloquea" tu ordenador por haber accedido a contenidos ilegales de Internet y te pide 100€ para solucionarlo, debes pagarlos lo antes posible para recuperar tu ordenador.

- ☐ VERDADERO
- ☐ FALSO

8. Reenviar fotos o vídeos que has recibido es delito, aunque tú no los hayas grabado.

- ☐ VERDADERO
- ☐ FALSO

9. Puedo mandar fotos mías por Internet con seguridad siempre que conozca la identidad de quien las recibe.

- ☐ VERDADERO
- ☐ FALSO

¿Cuánto sabes de Internet?

Resuelve el cuestionario de 15 preguntas de verdadero y falso. Las siguientes preguntas se puede realizar siguiendo el siguiente enlace a la web de Kahoot: http://bit.ly/2fVEyvU.

10. Es recomendable poner mi verdadero nombre en USUARIO, para que sea más fácil de recordar.

- ☐ VERDADERO
- ☐ FALSO

11. No pasa nada por decir mis contraseñas a mis mejores amigos.

- ☐ VERDADERO
- ☐ FALSO

12. Es conveniente que mis padres conozcan todo lo que hago en Internet.

- ☐ VERDADERO
- ☐ FALSO

13. Es recomendable tener actualizados todos los programas del ordenador.

- ☐ VERDADERO
- ☐ FALSO

14. Hay que tener tapada la webcam, porque desde otros dispositivos se puede acceder a ella y ver lo que hago, grabar...

- ☐ VERDADERO
- ☐ FALSO

15. No pasa nada por agregar a un amigo de un amigo mío en una red social, porque lo conoce él/ella.

- ☐ VERDADERO
- ☐ FALSO

Ahora se trata de establecer un debate partiendo de las respuestas de los alumnos y las respuestas correctas y, sobre todo, explicarles el porqué de las mismas.

¿Cuánto sabes de Internet? - RESPUESTAS

1. Un ordenador infectado siempre presenta algún síntoma para detectarlo.

[X] FALSO

2. Los únicos sitios que pueden infectar un dispositivo son las páginas de juegos de azar y páginas con contenidos ilegales.

[X] FALSO

3. Las faltas de ortografía son un indicio o sospecha de intento de fraude.

[X] VERDADERO

4. No es recomendable cambiar muchas veces tu contraseña pues se te puede olvidar.

[X] FALSO

5. Los delincuentes informáticos no solo atacan a las grandes empresas.

[X] VERDADERO

6. Tus fotos y comentarios de tus redes sociales solo las puede ver quien tú quieras.

[X] FALSO

7. Si la Policía Nacional "bloquea" tu ordenador por haber accedido a contenidos ilegales de Internet y te pide 100€ para solucionarlo, debes pagarlos lo antes posible para recuperar tu ordenador.

[X] FALSO

8. Reenviar fotos o vídeos que has recibido es delito, aunque tú no los hayas grabado.

[X] VERDADERO

9. Puedo mandar fotos mías por Internet con seguridad siempre que conozca la identidad de quien las recibe.

[X] FALSO

10. Es recomendable poner mi verdadero nombre en USUARIO, para que sea más fácil de recordar..

[X] FALSO

11. No pasa nada por decir mis contraseñas a mis mejores amigos.

[X] FALSO

12. Es conveniente que mis padres conozcan todo lo que hago en Internet.

[X] VERDADERO

13. Es recomendable tener actualizados todos los programas del ordenador, aunque me lleve tiempo cuando quiero hacer otra cosa.

[X] VERDADERO

14. Hay que tener tapada la webcam, porque desde otros dispositivos se puede acceder a ella y ver lo que hago, grabar...

[X] VERDADERO

15. No pasa nada por agregar a un amigo de un amigo mío en una red social, porque lo conoce él/ella.

[X] FALSO

¿Tu contraseña es segura?

En esta sesión abordamos el tema de las contraseñas, explicando a los alumnos la importancia de tener una contraseña segura, cómo crearla y no difundirla.

¿Por qué es necesaria una contraseña segura?

Establecemos un pequeño debate para fomentar la participación.

https://www.youtube.com/watch?v=NR279FIzD4s

¿Podéis crear una contraseña segura?

Proponemos un pequeño juego para ver quién es el alumno que crea la contraseña más segura o menos débil.

Video: ¿Cómo eleboramos contraseñas seguras?

https://www.youtube.com/watch?v=iV9CmN-g_go

¿Sabes cuáles son los 25 caracteres más usados en Internet y, por tanto, los más vulnerables?

¿Tu contraseña es segura?

Ejemplo para crear una contraseña segura.

1º - Pensamos una frase fácil de recordar.

Ej: "Más vale pájaro en mano que ciento volando"

2º - Usa la primera letra de cada palabra (o la última o la segunda...)

escribiendo las consonantes en mayúsculas y las vocales en minúsculas → **MVPeMQ100V**

3º - Sustituye o añade caracteres especiales como por ejemplo: **@#€¬|€%&%$ +-***

Contraseña: **+VPeMQ100V**

4º - Comprueba la contraseña en:

http://password.social-kaspersky.com/es

https://howsecureismypassword.net/

5º—Una vez creada la contraseña segura, añade la extensión a cada Web que visites, escogiendo, por ejemplo, la primera y la última letra.

+VPeMQ100V#tr→Twitter

+VPeMQ100V#fk→ Facebook

+VPeMQ100V#im→Instagram

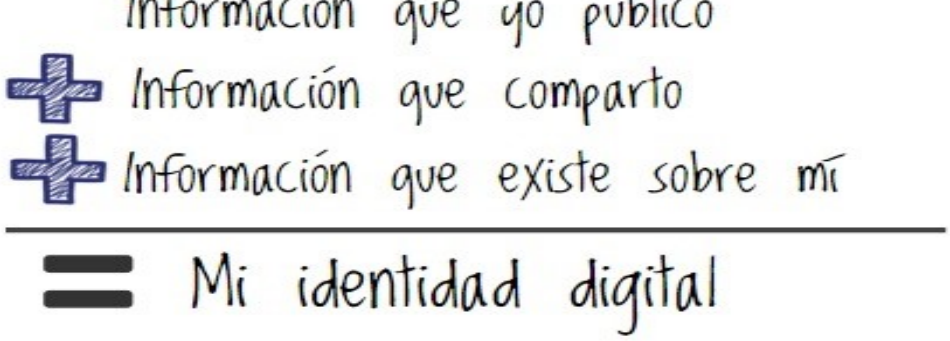
Protege tu identidad digital

Pequeño DEBATE con los alumnos. "Pistas sobre lo que los alumnos realizan en Internet"

¿Qué es identidad digital?

Es el rastro que cada usuario de Internet deja en la red como resultado de su interrelación con otros usuarios o con la elaboración de contenidos.

Vídeo:
https://www.youtube.com/watch?v=Zu2WDrErU20



Organizamos la clase en pequeños grupos. Cada grupo debe aportar cinco formas, medios, lugares, o páginas web, en los que su información personal pueda hacerse pública.

Concluimos estableciendo un debate en gran grupo favoreciendo la reflexión del alumnado sobre las graves consecuencias que puede tener la suplantación de identidad y cómo, preservando nuestra información y datos personales, podemos prevenir este riesgo. Si los demás no tienen nuestros datos, no pueden suplantarnos.

Protege tu identidad digital

La usurpación de la identidad es un delito que puede tener consecuencias penales o económicas en función de la gravedad.

1. ¿Cómo puedo proteger mi identidad digital?

- Cierra la sesión de tu cuenta al acabar.
- No respondas si ves un mensaje de correo electrónico sospechoso, un mensaje instantáneo o una página web que solicita tu información personal.
- Ten cuidado con las conexiones públicas y las redes WiFi gratis.
- Nunca ingreses tu contraseña cuando llegues a un sitio mediante un vínculo en un correo electrónico o un chat en el que no confías.
- No envíes tu contraseña por correo electrónico ni la compartas con otros.
- Si todo lo demás falla, desactiva tu cuenta.

2. ¿Cómo detecto que he sido víctima de una suplantación o usurpación de identidad en Internet?

Entendemos la suplantación de identidad como "el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio".

- No encuentro mensajes privados o emails en mi cuenta
- He descubierto una publicación o un comentario que yo no he realizado.
- Me encuentro con conversaciones de chats que no recuerdo haber mantenido.
- Mi lista de contactos ha crecido o se ha eliminado un seguidor sin saberlo.
- Recibo correos electrónicos indicando que se ha intentado recuperar la contraseña de mis cuentas.

3. ¿Qué puedo hacer si han suplantado o usurpado mi identidad?

- Denunciar ante la plataforma esta situación para solicitarles que tomen las medidas necesarias.
- Recopilar todas las pruebas necesarias.
- Denunciar el caso a la agencia de protección de datos.
- Cambiar todas las contraseñas y, en la medida de lo posible, tratar de deshacer lo que haya realizado el agresor en nuestro nombre.
- Si quieres denunciarlo ponente en contacto con la Policía Nacional o Guardia Civil.
- Denunciar las trampas y los correos electrónicos sospechosos.

¿Qué hago con el móvil / Tablet?

Utilizar las redes sociales de forma respetuosa y segura. Conocer los riesgos de internet.

PRESENTACIÓN

De noticias relacionadas con el *ciberbullying* y uso inadecuado de las redes sociales.

http://prezi.com/foykjduhnsig/

REFLEXIÓN:

¿A quién le ha ocurrido algo así?

¿Quién ha realizado algo así sin darse cuenta?

Trabajar en pequeños grupos:
En un folio escribir las edades mínimas para utilizar las redes sociales:

- Whatsapp
- Instagram
- Facebook
- Snapchat
- Cuentas de correo.

Exposición de las condiciones de uso de las redes sociales
http://prezi.com/2yy2ljl0nnuc/

Enfatizar el mensaje final:
¡Pide ayuda! email y teléfonos de ayuda

DEBATE:

¿Cómo se han creado esas cuentas?,
¿Conocen sus padres cómo lo habéis hecho?

¿Qué hago con el móvil / tablet?

Utilizar las redes sociales de forma respetuosa y segura. Conocer los riesgos de internet.

DEBATE

- **¿Qué es el *ciberbullying*?**
- **¿Conocéis algún caso?**
- **¿Qué se podría hacer para evitar el acoso escolar?**
- **¿Os habéis sentido alguna vez acosados?**
- **¿Pensáis que habéis acosado alguna vez?**

VÍDEOS DE APOYO:

Todos contra el acoso:
https://youtu.be/1XM0cr7CFCY

El acoso escolar es violencia:
https://www.youtube.com/watch?v=ovja5uA1JZg

Creación de mapa mental/infografía/póster/ sobre lo que se puede hacer o no en las redes sociales o la elaboración de lemas propios para evitar el acoso escolar.
(Ejemplo: (PDF): https://goo.gl/FYsa09)
Recursos para su realización:

- Popplet para mapas conceptuales.
- Genially para infografías, póster o presentaciones.
- Prezi: presentaciones.
- Padlet: muros virtuales.

Crea tu Decálogo #SE_con_TIC

Elaborar un decálogo de consejos de uso de internet para el aula.

1. #CONSEconTIC:

Investigación sobre **consejos** útiles a la hora de navegar en internet con seguridad.

2. #CreaTIC:

Creación de un Decálogo de seguridad digital, publicarlo en el aula virtual, blog, web escolar y difundirlo en las redes sociales del centro.

3. #EmprendeTIC:

Organización de un concurso de eslóganes, posters, vídeos o microrrelatos relacionados con la Seguridad con TIC en tu aula o para otro curso del centro.

Crea tu Decálogo #SE_con_TIC

1. #CONSEconTIC: .Presentación de consejos adaptados a la edad mediante la PDI.

Enlaces de ejemplo:

Ejemplo 1: http://bit.ly/2jFsHS2

Ejemplo 2: http://bit.ly/2ix2fwY

Ejemplo 3: http://bit.ly/2k0wkFi

Vídeo 1: https://www.youtube.com/watch?v=2TferQprZ0g&t=4s

Vídeo 2: https://youtu.be/Chi5Zcoczv0?list=PLHYL4-J_2mcbwNn_Zled7lRsaGEnbkR51

Consejos:

* Gestiona tu privacidad
* No reveles datos personales
* No necesitas miles de amigos
* No gastes en internet
* No compartas fotografías
* Piensa antes de publicar
* No a las citas a ciegas
* Evita la suplantación de identidad
* Ten cuidado con la webcam
* Respeta la privacidad

2. #CreaTIC:

Creación de un decálogo de seguridad digital con cualquiera de estas herramientas:

- https://www.genial.ly/es
- https://piktochart.com/
- http://www.toondoo.com/

3. #EmprendeTIC:

Los grupos eligen su trayectoria de emprendimiento para organizar, difundir y participar en concursos sobre Seguridad Digital a través de:

- Microrrelatos
- Eslóganes.
- Posters.
- Vídeos.