Curso
Ciudadanía Digital

Unidad 3:
Promoción de prácticas seguras y responsables en entornos virtuales desde el rol mediador del docente

Sesión 1
Rol del docente en la promoción de prácticas seguras y responsables en entornos virtuales

mejor educación mejores peruan@s
PERÚ Ministerio de Educación
El Perú Primero

Sesión 1

Rol del docente en la promoción de prácticas seguras y responsables en entornos virtuales

Esta unidad busca que los docentes reconozcan, a partir de gestionar la información en redes y entornos virtuales de manera crítica y responsable para un uso seguro de internet, la importancia de su rol como mediadores en la construcción de la ciudadanía digital, poniendo énfasis en la promoción de la responsabilidad, empatía y respeto.

Identifica

Para iniciar, te invitamos a observar el siguiente video:

Principio del formulario

Final del formulario

Empecemos por observar este video de PantallasAmigas, en el cual se propone 10 claves para usar internet con seguridad:

PantallasAmigas (2020). Las 10 claves para usar Internet con seguridad [Video]. YouTube.

https://www.pantallasamigas.net/las-diez-claves/

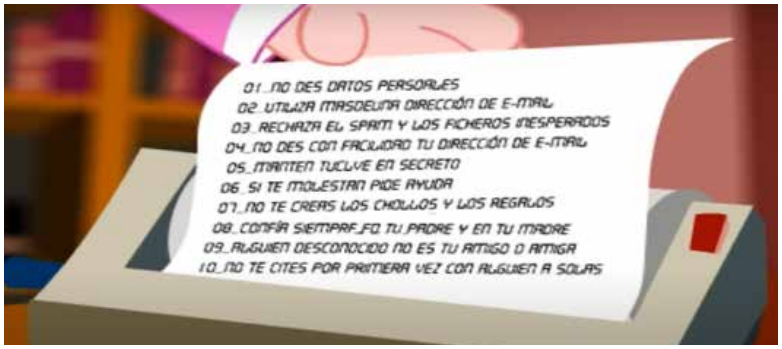
Resumen del video

PantallasAmigas plantea que la red es un extraordinario recurso y, por ello, sostiene que prohibir su uso es una equivocación. De la misma manera, también es un error mirar hacia otro lado, pensar que no existen ciertos riesgos o que no se puede hacer nada para evitarlos.

En consecuencia, es la responsabilidad de docentes, padres y madres tomar cartas en el asunto, poner los medios para que las niñas, niños y adolescentes hagan un uso seguro y saludable de internet. Y cuanto antes lo hagan, mejor.

Figura 1.1

Las 10 claves para usar Internet con seguridad



Nota. De PantallasAmigas (2020). Las 10 claves para usar Internet con seguridad [Video]. YouTube.

https://www.pantallasamigas.net/las-diez-claves/

1. No des tus datos personales.
2. Utiliza más de una dirección de email.
3. Rechaza el spam y los mensajes inesperados.
4. No des con facilidad tu dirección de email.
5. Mantén tu clave en secreto, y cámbiala de vez en cuando.
6. No creas en ofertas o grandes regalos, primero averigua más y consulta con un adulto de confianza.
7. Alguien desconocido no es tu amiga o amigo, por mucho que lo parezca.
8. Nunca te cites por primera vez con alguien a solas.
9. Confía siempre en tu padre y en tu madre.
10. Si te molestan, pide ayuda.

Te invitamos a reflexionar en base a las siguientes preguntas:

1. ¿Consideras que enseñar habilidades para que tus estudiantes gestionen la seguridad de manera autónoma en su interacción en internet es mejor que otros métodos para lograr la seguridad?
2. Si tuvieras que aplicar un cuestionario a tus estudiantes acerca de si han compartido su contraseña, o publicado alguna vez información de otra persona o fotos sin su consentimiento, rellenado formularios sin investigar la fuente, instalado algún software en la computadora de casa sin aprobación de sus padres, o chateado con gente que usa contenido sobre temas sexuales o de violencia, ¿cómo lo harías?

Analiza

Te invitamos a observar este video:

Sulmont, L. (octubre de 2020). Mensaje a los docentes del Perú sobre la ciudadanía digital [Video]. Google Drive. **https://drive.google.com/file/d/1h5T1cuBrYZ2ISrDTZdOd2M7ph5DdPszD/view?usp=sharing**

Resumen del video

Lea Sulmont, experta educativa peruana dedicada a desarrollar propuestas didácticas para la práctica docente durante los tiempos de transformación digital, envía un mensaje a los docentes del Perú para pedirles que promuevan el cuidado de la salud, la seguridad, el bienestar y el derecho a participar activamente como ciudadanos en entornos digitales, y es a esto, según la especialista, a lo que se llama competencia de la ciudadanía digital, la cual hay que seguir cultivándola

como docentes, no solo cuidando la identidad digital, la privacidad, mi imagen, lo que publico, sino también interesarme por acceder a sitios de fuentes confiables, para formar a otros como personas responsables, pero también creativas en el mundo digital.

1.1 gestión de la ciudadanía digital responsable y segura

La gestión de la ciudadanía digital responsable y segura, acorde a los niveles educativos, se estructura de la siguiente manera:

A. **En nivel primaria:** La construcción de ciudadanía empieza por buscar que el estudiante encuentre un equilibro entre las actividades de la vida diaria, y aquellas en las que está conectado a dispositivos digitales o en línea, y cuando están conectados virtualmente, que sepan distinguir entre los sitios que son seguros y los que no; reconocer que el respeto en línea es tan importante como el respeto en entornos de la vida en general, y reflexionar acerca de lo que siente cuando interactúa con las tecnologías.

Ejemplo de actividad para primaria

ACTIVIDAD: ¿Mi información vuela? Aprendiendo a gestionar mi privacidad

Descripción de la actividad

La pregunta inicial: ¿Cómo funciona internet? Esta red interconectada entre millones de computadoras de todo el mundo, con teléfonos conectados por wifi, o cables y alambres, funciona con servidores con dirección de internet única, llamada Internet Protocol (IP). Ahí puedes subir fotos, videos y todo tipo de información. ¿Alguna vez has publicado fotos personales en una página de internet o app en donde desconocidos la pudieran ver, o has aceptado una invitación de alguien en medios sociales que nunca habías conocido en persona? Comparte tu experiencia.

Segunda pregunta: ¿Cómo te comunicas con tus amigos y familiares usando internet?

Las redes sociales. Las redes sociales han cambiado la forma en que las personas se comunican en la vida. Permiten interactuar con gente de todas partes del mundo, crear contenido, compartirlo y difundirlo a gran escala. Puede ser que las personas que interactúan en las redes sociales no se conozcan, pero comparten un interés común.

Las principales redes sociales son:

- Facebook
- Twitter
- Instagram
- YouTube
- LinkedIn
- Pinterest
- WhatsApp
- Snapchat

Para que las redes sociales sean útiles en la vida, es necesario estar consciente de los riesgos y saber cómo utilizarlas para crear una identidad digital íntegra. No todo contenido tiene que ser compartido en todas partes, y no todo contenido es pertinente para todas las redes sociales.

Cuando la gente quiere:

- Contactar a la familia y amigos, usan Facebook.
- Compartir fotos, usan Instagram.
- Compartir un video para aprender a hacer algo, van a YouTube.
- Comunicarse con profesionales, ingresan a LinkedIn.

Tercera pregunta: ¿Crees que te pueden espiar y conseguir tus datos usando las redes sociales o internet?

Las redes sociales y tu información: En redes sociales hay personas a las que les gusta espiar las páginas que estás visitando. Tenemos que aprender a identificar cómo es que pueden sacar tu información o la de tus amigos y qué tipo de información es la que les interesa extraer.

¡Ideas para prevenir antes que lamentar! La información personal se colecta en sitios de redes sociales (YouTube, Facebook, Instagram, etc.). ¿Quién puede ver tu perfil en internet? Mientras estás en estos sitios, puedes:

1. Cambiar las configuraciones de privacidad para evitar que ingresen desconocidos.
2. Rechazar la solicitud de amistad de desconocidos.
3. Cubrir tu cámara (webcam) cuando no la estés usando.
4. Aprender a identificar cuando aparecen mensajes basura (de ofertas gratis, que son falsas).
5. Consultar con algún adulto sobre alguna información que te parezca inapropiada, antes de compartirla.

Aprende la importancia de proteger la información personal de otros, incluyendo lo que necesitan preguntar y decir antes de publicar fotos, videos y otros artículos. Es importante obtener permiso de amigos cuando vas a publicar información, fotos o videos de ellos. Los amigos pueden ser víctimas de ataques en línea por algo que publicaste, aun cuando lo hayas hecho sin ninguna mala intención.

Técnica de protección: Cuando vas a publicar algo personal, contarás antes:

1. ¿Qué voy a publicar? (Un video, una foto o información personal)
2. ¿Por qué lo quieres publicar? (¿Por diversión? ¿Por otra razón?)
3. ¿Dónde lo quisieras publicar? (¿YouTube? ¿En otro lugar?)

Y aunque tengas que tomarte unos minutos, debes pedir permiso a cada amigo incluido en la foto/video/otro artículo.

B. En secundaria: Se debe buscar que el estudiante sea consciente de la importancia de balancear su tiempo en entornos virtuales con sus interacciones con el mundo real, e idee estrategias para conseguirlo. También se busca que interactúe de manera segura en los chats y forme relaciones de amistad por redes sociales de manera sana; reconozca la importancia de la privacidad de sus datos y cómo ciertas organizaciones recolectan y usan su información; que reconozca los peligros de la suplantación de identidad y de la violación de la privacidad; sepa actuar ante el acoso y el hostigamiento sexual; que desarrolle el pensamiento crítico para distinguir entre la información creíble y de fuentes confiables, reconociendo los fake new (noticias que aparentan ser verdaderas pero no lo son); sepa pronunciarse ante actitudes xenofóbicas, homofóbicas u otro tipo de paradigma mental; comprenda que sus interacciones en el mundo digital dejan una huella digital y que esta sirve para establecer su identidad digital; que reconozca sus derechos y obligaciones como ciudadano en el mundo real y su símil en el mundo digital; y reconozca y aproveche las oportunidades que le ofrece la red para desarrollarse como ser humano.

Ejemplo de actividad para secundaria

ACTIVIDAD: El ciudadano digital del Perú del siglo XXI

Descripción de la actividad

Invita a tus estudiantes a imaginar un día típico en internet: empiezas revisando textos y correos electrónicos, luego chequeas Twitter en el bus, publicas una foto en Instagram. A la hora de almuerzo, revisas el horario de una película que un amigo te recomendó en Facebook y ves un anuncio de un videojuego que estabas queriendo tenerlo. Esos son algunos sitios web, pero cada vez que estás en internet, dejas rastros de tu actividad. Tras bambalinas, un montón de empresas "externas" —entidades separadas de los sitios web que visitaste— pueden rastrear tu actividad y recopilar tus datos mientras se mueven por la web. Más tarde, ese mismo día, empiezas a ver anuncios recomendando la película por la que consultaste el horario, y anuncios de ofertas para comprar ese videojuego. No es coincidencia, es el rastreo de datos en acción.

Comparte con tus estudiantes este artículo para discutir en la clase siguiente sobre el mismo.

Nombre del artículo: "El lado bueno, malo y feo del rastreo de datos" (extraído de https://internethealthreport.org/2018/el-lado-bueno-feo-y-malo-del-rastreo-de-datos/?lang=es)

"No toda la recopilación de datos es mala. Los sitios web a menudo guardan tus datos para personalizar y mejorar tus experiencias para cuando los uses. Utilizan cookies 'de origen' —pequeños archivos de datos colocados en nuestros navegadores— para recordar tu idioma, tus preferencias o el contenido que usaste y te lo guardan ahí. Al otro lado de la moneda, hay quienes trabajan con algunos sitios web para insertar métodos de rastreo adicionales —como sus

propias cookies— para registrar qué leíste, dónde hiciste clic y qué visitaste en la web. Esta recopilación de datos tú no la podrás ver, pero revela más sobre ti, como dónde has estado. Crea una imagen total de ti, desde tus preferencias hasta tu identidad. Los anunciantes usan esos datos para dirigirte anuncios y contenidos mientras navegas en tus dispositivos, aunque tú estés en desacuerdo".

Indica a tus estudiantes que no se pueden escapar de la publicidad en internet, sobre todo en redes sociales y en sitios de medios digitales. Hay una lógica en esto: es la principal manera por la cual la mayoría de las empresas digitales y las publicaciones de internet se sostienen de dicha publicidad. Entonces, eso de ser "sitios gratuitos" no es exactamente cierto. Los medios de noticias y de entretenimiento también dependen de la publicidad para apoyar el periodismo y la creación de contenidos.

¿El lado bueno? No toda la publicidad en internet es mala. En el lado bueno, el rastreo en línea debería hacer que te llegaran avisos más útiles y relevantes.

¿El lado malo?, muchos anunciantes no ofrecen a los usuarios opciones verdaderas y controlan qué datos se recopilan sobre ellos. A veces, tus movimientos en la web los recopilan intermediarios de datos que pueden combinar datos anónimos con información personal identificable (información que puedes haber completado en un formulario, una aplicación o que se recopiló fuera de la web) para elaborar un perfil sorprendentemente detallado de ti.

A medida que más publicidad se va a los celulares, todos deberían tomar en cuenta los datos que difunden con sus dispositivos móviles. Investigaciones han mostrado que la capacidad de seguimiento de las redes publicitarias móviles se puede manipular para lograr una vigilancia que sea altamente específica.

Para combatir la publicidad invasiva y eludir a los rastreadores que invaden la privacidad (y también para aumentar la velocidad y la capacidad de almacenamiento de datos), más personas están recurriendo a navegadores privados y a técnicas de bloqueo de anuncios. Pero mientras los bloqueadores de anuncios dan a los usuarios lo que quieren en términos de menos anuncios, también plantean un dilema porque recortan los ingresos de los creadores de contenidos.

La compleja relación que existe entre las preferencias de privacidad de los usuarios y los anuncios no invasivos y la necesidad de las entidades de internet de prosperar seguirá siendo una negociación en los próximos años, mientras los creadores de contenidos y los consumidores se ponen de acuerdo sobre qué es un internet vibrante y saludable para todos.

EJERCICIO

A partir de la lectura de estos textos, los estudiantes elegirán de una lista de recursos en línea, que usarán para explorar y analizar el tema.

1. Pregunta al grupo: ¿Qué tipo de información sobre ustedes mismos comparten en línea?

   Invita a los alumnos a responder

2. Pregunta, también: ¿Con quién comparten esta información? ¿Quién la ve? Los estudiantes pueden decir sus amigos y familiares, o cualquier persona que vea sus publicaciones. Has un seguimiento, y pregunta: ¿Qué pasa con las personas y empresas propietarias de las aplicaciones o sitios web en los que publican? Invita a tus alumnos a responder. Explica que las empresas recopilan la información que comparten y mucho más. Empresas como Facebook, Google y otras también rastrean y recopilan la ubicación, hábitos de navegación, búsquedas, compras, etc.

3. Explica que cuando las empresas hacen esto, se denomina seguimiento en línea, que significa que las aplicaciones, los sitios web o los terceros recopilan información sobre su actividad en línea (otros sitios que visitan, enlaces en los que hacen clic, cuánto tiempo se quedan, etc.).

4. ¿De qué otras formas las empresas pueden utilizar los datos que recopilan sobre ustedes?

   Invita a los alumnos a responder. Explica que las empresas también utilizan los datos que recopilan para proporcionarles contenido personalizado, que es información en línea que ha sido adaptada para cada uno por sitios web y aplicaciones, basada en datos que se han recopilado sobre ellos. Por ejemplo, Netflix recomienda películas y programas para que los vea según lo que ha visto anteriormente y lo que le ha "gustado". Spotify hace algo similar con la música.

5. Pregunta: ¿Qué piensan del seguimiento y la orientación? ¿Creen que está bien que las empresas recopilen información sobre ustedes? Las opiniones variarán. Explica que deberán investigar sobre el tema y tomar una posición al respecto.

6. Exploren entre grupos de estudiantes cuáles son **los beneficios y los inconvenientes** del seguimiento en línea para las empresas, así como para las personas que usan sus sitios y aplicaciones. Por ejemplo, una empresa como Amazon podría rastrear el comportamiento del usuario en su sitio, de modo que pueda anunciar productos en los que es más probable que las personas estén interesadas. Dependiendo de cómo se sientan acerca de la publicidad dirigida, pueden ver esto como un beneficio o una desventaja. Dependiendo de cómo reaccionen, podría terminar siendo un beneficio o un inconveniente para Amazon. Y desde el lado del usuario, esto puede

repercutir en la creación de necesidades en forma inconsciente, que incita a consumir algo que, si bien puede ser atractivo, no era algo requerido.

7. Invita a los estudiantes a trabajar en grupos pequeños para reflexionar sobre posibles ventajas e inconvenientes que pueden generarse cuando la información es rastreada.

Recursos educativos para promover prácticas saludables y seguras en internet

Para promover prácticas seguras y responsables en entornos virtuales en los estudiantes, en tu quehacer cotidiano como docente te presentamos un conjunto de consejos, actividades y recursos educativos que te servirán como complemento al CNEB para orientar tu trabajo en el aula:

Consejos para el uso de las tecnologías e internet para lograr ciudadanía

Docentes

La y el docente debe considerar (Junta de Extremadura, 2015, p.5)

- Realizar un control del tiempo que los estudiantes se conectan a internet en clase. Proponer y hacer cumplir horarios.
- Colaborar en el mantenimiento de todos los dispositivos tecnológicos del aula.
- Fomentar la utilización de una posición correcta para el cuerpo frente al ordenador.
- Fomentar el respeto y tolerancia a otros usuarios, evitando las burlas, difamaciones y agresiones.
- Enseñar a navegar por internet de forma segura y accediendo solo a contenidos aptos para su edad.
- Crear un espíritu crítico sobre la información que aparece en la red y explicar que no todas las webs tienen la misma credibilidad, que es importante filtrar y evaluar su calidad.
- Enseñar el uso de los motores de búsqueda y contrastar varias fuentes sobre un mismo campo, evitando el “cortar y pegar” y los plagios.
- Advertir del derecho a la privacidad de la información personal de sus compañeros y que no sea difundida sin su consentimiento por la red.
- Enseñar que siempre es aconsejable evitar publicar detalles o imágenes privadas.
- Demostrar el uso adecuado de la privacidad en las redes sociales.
- Enseñar el uso responsable del correo electrónico y otros medios de comunicación.
- Enseñar la diferencia entre contenidos apropiados e inapropiados.

Estudiantes

Las alumnas y alumnos deben conocer y tener presentes los siguientes principios (Junta de Extremadura, 2015, p.5)

- Controlar el tiempo que se conecta
- Cuidar su correcta posición corporal
- Tener prudencia y no concertar encuentros con personas que no conocen
- Tener respeto a los otros, evitar las burlas, difamaciones, humillaciones y agresiones.
- No suplantar la identidad de nadie en la red.
- Aprender a navegar por internet de forma segura, accediendo solo a contenidos aptos para su edad.
- Saber que tienen derecho a la privacidad de su información personal al cuidar los datos que comparten tanto en chat, redes sociales, email u otro canal.
- Entender que no se puede publicar información de otra persona sin su consentimiento.

Después de haber leído y reflexionado sobre lo presentado, te invitamos a resolver el cuestionario de autoevaluación.

1. ¿Cuál de estas opciones se recomendaría a los estudiantes para denunciar la acción ejecutada por algunos de ellos en redes sociales?

Marcar todas las opciones que apliquen.

a. Un estudiante publica una foto grupal en una cuenta pública, pero a una de sus compañeras no le gusta cómo salió en la foto.

b. Se creó una cuenta falsa de un estudiante del que se conoce su nombre y foto de perfil. Dibujaron un bigote y otros rasgos faciales raros en la foto, y la convirtieron en meme de burla.

c. Un estudiante crea una cuenta usando el nombre de la escuela como usuario y publica fotos de los alumnos con comentarios de los que se entera todo el mundo. Algunos son comentarios crueles sobre los estudiantes.

d. Están publicando muchos comentarios crueles sobre un estudiante de la escuela, y se sospecha de uno de ellos como el autor.

2. En una clase de ciudadanía digital se indica a los estudiantes que los secretos son un tipo de información personal que es preferible mantener en privado o solo compartir con familiares o amigos de confianza. Tras compartir un secreto, no se controlará quién más lo sepa. ¿Qué tipo de información no es necesario proteger?

a. La dirección particular y número de teléfono

b. La dirección de correo electrónico

c. Las contraseñas

d. El nombre de usuario

e. El nombre al registrarse en un foro educativo

3. Se puede encontrar cantidad de datos personales en internet. Cuando se lee parte de esa información, puede pensarse cosas que no son ciertas. ¿Qué información encontrada sobre una persona, es la que se sabe con certeza?

a. La que ella publica como su información personal, sin control de privacidad.

b. La que se supone que es de ella a partir de la información personal y de comentarios de terceros.

c. La que se ha recopilado en una búsqueda en varias redes sociales, sin identificar la fuente.

d. La que está publicada en sitios oficiales, como la web del RENIEC y otros.

4. ¿Cuáles de estas opciones no son maneras apropiadas de enseñar a los estudiantes sobre habilidades de ciudadanía digital?

a. Cómo aprender a tomar buenas decisiones en entornos digitales.

b. Cómo hacer de internet un espacio seguro para uno y los demás.

c. Memorizar y practicar esta lista larga de lo que no puede hacerse.

d. Reconocer el propósito de la información y sus sesgos.

5. Los estudiantes comparten en redes sociales distinto tipo de información. Cuando se dialoga con ellos sobre la información que comparten y la que no deben compartir, ¿qué tipo de reflexiones deben hacerse ellos?

a. Distinguir entre compartir algo indebido accidentalmente que no se debería, y algo con una intención que perjudique a terceros.

b. ¿Será que se está compartiendo información en forma compulsiva?

c. ¿Debe modificarse la manera en la que se comparte el contenido?

d. Identificar posibles consecuencias negativas de compartir contenido públicamente en lugar de hacerlo solo con los amigos.

e. Todas las anteriores

Referencias

Aula Siena (2020). 7 buenas prácticas para el uso responsable y seguro de internet en los colegios. Grupo Siena. **https://aulasiena.com/7-buenas-practicas-para-el-uso-responsable-y-seguro-de-internet-en-los-colegios/**

Common Sense Education (2020). Guía de implementación de la ciudadanía digital. **https://www.commonsense.org/education/digital-citizenship-implementation-guide**

Common Sense Media (2020). 5 consejos para hablar con tus hijos sobre las elecciones. [Video]. Common Sense. **https://www.commonsensemedia.org/videos/5-consejos-para-hablar-con-tus-hijos-sobre-las-elecciones**

DQ Institute (2019). Movimiento Global de Ciudadanía Digital para 8-12 Años. DQ Every Child. **https://www.dqinstitute.org/dqeverychild/**

ISTE (2020). Ciudadanía digital en educación. https://www.iste.org/learn/digital-citizenship

Junta de Extremadura (2015). Guía buen uso educativo de las TIC. **https://saludextremadura.ses.es/filescms/ventanafamilia/uploaded_files/CustomContentResources/guia%20buen%20uso%20educativo%20de%20las%20tic.pdf**

Mozilla (2020). El lado bueno, malo y feo del rastreo de datos. **https://internethealthreport.org/2018/el-lado-bueno-feo-y-malo-del-rastreo-de-datos/?lang=es**

PantallasAmigas (2020). Las Diez Claves. **https://www.pantallasamigas.net/las-diez-claves/**

Sulmont, L. (2020). Mensaje a los docentes del Perú sobre la gestión de la Internet segura, sana y responsable.

Universidad de Newcastle (22 de enero de 2015). La mejor huella digital. **https://www.newcastle.edu.au/newsroom/faculty-of-education-and-arts/best-footprint-forward**