¡Ciberprotégete! Taller de prevención de riesgos digitales y para la protección de l@s usuari@s de la web 2.0

Laura Bécares Rodríguez[1]
becaresespalabraesdrujula@gmail.com

Abstract

En el siguiente artículo se propone un taller de actuación directa con el colectivo adolescente para prevenirles de los principales peligros de internet y proporcionarles herramientas para ser consumidores conscientes de las nuevas tecnologías. Este colectivo es el principal usuario de los recursos digitales, y por ello son muy vulnerables a los riesgos que entraña la web (estafas, acoso o violación de la privacidad). A través de esta propuesta de taller se busca sensibilizar tanto a jóvenes como adultos de la cotidianeidad de dichas amenazas y la necesidad de tomar precauciones en el uso de Internet.

Palabras clave: *Prevención, didáctica, educación, nuevas tecnologías*

Hurrengo artikuluan nerabeen kolektiboari zuzendutako jokaera zuzeneko tailer bat proposatzen da, interneten arrisku nagusiak prebenitzeko eta teknologia berrien kontsumitzaile zentzudunak izateko tresnak eskaini asmoz. Talde hau baliabide digitalen kontsumitzaile nagusia da beraz oso kaltebera webak berarekin dituen arriskuekiko (maulak, jazarpena eta intimitatearen urratzea). Tailer proposamen honen bidez bai gazteak zein helduak mehatxu hauen ohikotasunez, eta internet erabiltzean ardurak hartzearen premiaz sentsibilizatzea bilatzen da.

Introducción:

El propósito de este artículo es aportar un recurso a profesores, monitores, educadores y formadores. Se trata de un modelo de taller para realizar actividades sobre concienciación digital con usuarios adolescentes. Considero esta contribución un ejemplo moldeable que permite adaptaciones y modificaciones, tanto en las actividades o duración, como en objetivos. Por esta razón este artículo está estructurado como una programación didáctica para facilitar su uso en el aula.

[1] Becaría Predoctoral Severo Ochoa en la Universidad de Oviedo

Colectivo destinatario

En mi opinión veo recomendable iniciar este tipo de talleres en las edades comprendidas entre los 14 y los 18 años por los siguientes motivos. A partir de esta franja de edad, el consumo de contenidos digitales aumenta y se generaliza respecto a etapas anteriores.

Además, a la hora de desarrollar las actividades, esta etapa de desarrollo cognitivo nos permite trabajar una serie de contenidos que tal vez, sean demasiado complejos para etapas anteriores. Esto es debido a que, a partir de los 14 años se posee una estructura de pensamiento formal, lo que permite al adolescente abordar conocimientos de forma organizada y formular cuestiones más abstractas y jerarquizadas. A la hora de elaborar este taller se tienen en cuenta las aportaciones de Piaget que nos señalan el estadio evolutivo que atraviesan: la etapa de pensamiento formal.

También se tiene en cuenta para la metodología la importancia de un aprendizaje social cooperativo que subraya Vigotzky[2] y, sobre todo, la relevancia del aprendizaje significativo que manifiesta Ausubel y los requisitos que se necesitan para su consecución: funcionalidad, motivación, conocimientos previos, significatividad lógica y psicológica de los contenidos.

Por ello, este colectivo es capaz, de realizar razonamientos abstractos básicos para comprender el desarrollo de las nuevas tecnologías y se fomentará la metodología que permita promover los tipos de aprendizaje resaltados anteriormente.

Objetivos

1. Concienciar a los usuarios del peligro que entraña el uso de las nuevas tecnologías.
2. Disminuir la vulnerabilidad de los adolescentes ante las nuevas tecnologías.
3. Sensibilizar a los jóvenes sobre las consecuencias del ciberbulliyng.
4. Estimular la búsqueda de ayuda cuando los usuarios se encuentren en una situación digital comprometida o incómoda.

[2] CASTILLO, A (1997, 45).

Duración

El tiempo indicado para desarrollar los contenidos del taller será de cuatro sesiones de dos horas cada una. En total, contamos con ocho horas de trabajo para poder asimilar los contenidos y poder tener una evaluación positiva.

Contenidos

Cada sesión plantea el desarrollo de un tema principal a trabajar durante dos horas.

- El principal contenido de la primera sesión sería la navegación segura en la web. El objetivo será trabajar el tema de las estafas por Internet, la exposición a contenidos inadecuados y el grado de exposición de los datos personales que publican en la red.
- En la segunda sesión se tratará el tema del ciberbullying, como identificarlo y actuar frente a él.
- La tercera sesión se denomina protege tu equipo, en el que se tratará la protección de los datos privados del ordenador personal y la identidad digital.
- En la cuarta sesión, se hará un repaso a los temas tratados para asegurar los conceptos clave desarrollados en las sesiones anteriores del taller. También se realizará una dinámica final global, junto con un cuestionario de satisfacción de los usuarios para autoevaluar nuestro propio trabajo.

Recursos a utilizar

1. Guía del taller
2. Encerado convencional/ pizarra digital.
3. Ordenadores con conexión a Internet.
4. Ordenador conectado a un cañón de proyección.
5. Presentaciones del tipo PowerPoint.
6. Cartulinas y folios.
7. Rotuladores y bolígrafos.

Actividades

- **Presentación del taller, de los encargados y los usuarios (primera sesión)**

Existen múltiples dinámicas de presentación en Internet, su elección es libre para los encargados del taller. Aquí se sugiere una muy sencilla cuyo objetivo principal es romper el hielo inicial en el aula:

Dinámica de presentación: Se pide a cada usuario que, alternativamente, diga su nombre, una afición y algo que no le guste. El monitor o monitora del taller también debe participar.

Dinámica de introducción: Carta a mi tío abuelo[3]

Se trata de que individualmente, cada usuario redacte una carta explicando que es Internet a una persona que desconoce completamente el tema. También deben comentar cómo se utiliza y para que sirve a través de ejemplos de su vida cotidiana. Uno de las principales resultados que se tienen de esta actividad es que, los usuarios, suelen resaltar lo positivo de la web como lugar de acercamiento, recopilación de información etc. Mientras que los peligros que entraña su uso suelen pasar desapercibidos.

- **Navegar en la web (primera sesión)**

Dinámica 1- Timos, estafas y engaños

Uno de los mayores peligros que existen en Internet es ser víctima de una estafa. A partir de esta actividad se intentará identificar el mayor número posible de timos que circulan por la web. Dependiendo un poco de los recursos del centro donde nos encontremos, se puede realizar una búsqueda conjunta de fraudes o la exposición del monitor con la ayuda de un PowerPoint de los principales "sablazos" y sus consecuencias. A continuación inserto varios timos:

Cheque-regalo- Se presentan como una oportunidad para ganar un cheque de 300 euros para gastos de una conocido marca, H&M, Hipercor etc. Para ello había que contestar a una preguntar para posteriormente insertar tu número de teléfono. Al realizar esto se daba de alta al usuario en un servicio de descarga de contenidos para móviles. Cada mensaje que envían tendría un coste de 65 céntimos de euro. Para dejar de recibir estos mensajes tendrás que darte de baja en un número de teléfono, pero seguramente ya habrán robado entre 10 y 20 euros.

Test- se presentan como test de inteligencia. En principio tú realizas el test sin coste alguno, pero cuando llega el momento de darte el resultado, te piden que insertes tu número de teléfono. Como mínimo tendrá un gasto de 1´25 euros y como máximo te darán de alta en un servicio de descargas de contenidos para móviles con las mismas consecuencias que la anterior, pudiendo llegar a facturas de más de 600 euros si no te das de baja del servicio.

[3] Recurso encontrado en http://coleccion.educ.ar/coleccion/CD27/datos/carta-a-mi-tio-abuelo-que-vive-en-la-montana.html Consultada el 10/07/2013

Ilustración 1 Ejemplo de test gratuito que finalmente es de pago

¡Gratis! – bajo este título quiero aglutinar todas las ofertas que existen en Internet que se califican sin cargo para el usuario pero realmente no lo son.

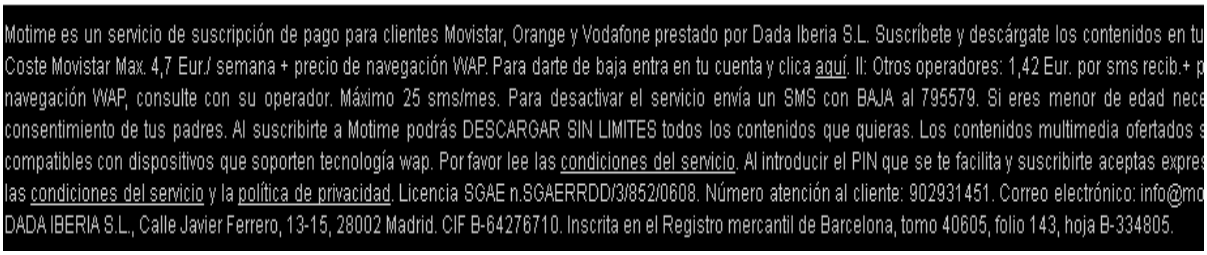
Motime es un servicio de suscripción de pago para clientes Movistar, Orange y Vodafone prestado por Dada Iberia S.L. Suscríbete y descárgate los contenidos en tu Coste Movistar Max. 4,7 Eur./ semana + precio de navegación WAP. Para darte de baja entra en tu cuenta y clica aquí. II: Otros operadores: 1,42 Eur. por sms recib.+ p navegación WAP, consulte con su operador. Máximo 25 sms/mes. Para desactivar el servicio envía un SMS con BAJA al 795579. Si eres menor de edad nece consentimiento de tus padres. Al suscribirte a Motime podrás DESCARGAR SIN LIMITES todos los contenidos que quieras. Los contenidos multimedia ofertados s compatibles con dispositivos que soporten tecnología wap. Por favor lee las condiciones del servicio. Al introducir el PIN que se te facilita y suscribirte aceptas expres las condiciones del servicio y la política de privacidad. Licencia SGAE n.SGAERRDD/3/852/0608. Número atención al cliente: 902931451. Correo electrónico: info@mo DADA IBERIA S.L., Calle Javier Ferrero, 13-15, 28002 Madrid. CIF B-64276710. Inscrita en el Registro mercantil de Barcelona, tomo 40605, folio 143, hoja B-334805.

Ilustración 2

Si vemos las condiciones del servicio (ilustración 2) podemos observar que de gratis tiene poco. Por tanto, debemos fomentar a nuestros usuarios que antes de insertar su número de teléfono en una página web, se informen de las condiciones y de las consecuencias que les podría acarrear. Leer las condiciones del servicio es aburrido, pero fundamental para no llevarse a sorpresas en la factura telefónica.

Emails- los estafadores hacen llegar al correo electrónico ofertas de trabajo, cheques, loterías, curas milagrosas, pérdidas de peso, alquiler de pisos falsos etc. Como en todo, la prevención es la mejor manera de evitar el robo. Por ello, si no se conoce la identidad del email se debe borrar inmediatamente. Es importante crear un filtro de spam y reenviar los emails sospechosos a spam@uce.org

Dinámica 2- La lista Robinson

La lista Robinson es un recurso muy interesante para evitar las estafas y el abuso publicitario. Esta gestionado por la Asociación Española de Economía Digital. Cualquier persona puede inscribirse en el Servicio de Lista Robinson de forma gratuita. Para ello es necesario indicar, de acuerdo con lo señalado en el Reglamento del Servicio, el medio a través del cual no desea recibir publicidad de entidades con las cuales no mantenga ni haya mantenido algún tipo de relación.

Para inscribirse es necesario ser mayor de 14 años, por tanto, nuestros usuarios podrían usarlo. Además es un buen ejercicio para leer conjuntamente las condiciones y el reglamento para darse de alta para evitar la recepción de publicidad a sus celulares.

Es muy útil para evitar el envío masivo de publicidad, engañosa o no, de manera telefónica, postal y digital (a través del correo electrónico) No obstante, esto no evita que si se dan de alta en un servicio de envío de mensajes, como los citados anteriormente, sean estafados.

La dinámica consistirá en conocer la página de la lista Robinson y los recursos que les ofrece https://www.listarobinson.es.

Dinámica 3- ¿Soy un personaje público?

Para esta actividad plantearemos a los usuarios que pongan su nombre y apellidos en el metabuscador Google. La finalidad es que observen que la mayoría de los contenidos que publican en Internet son de dominio publico. Por tanto, es muy fácil que cualquier usuario de la red pueda llegar a verlo, no solo sus amigos y sus conocidos.

Dinámica 4: **Decálogo de buenas prácticas**

A través de esta actividad, en grupos de cuatro, nuestros usuarios redactarán 10 consejos para un uso seguro de Internet y para prevenir las estafas. Para ello se les facilitará una cartulina. Posteriormente se pondrá en común el resultado y se debatirá en el caso de no estar de acuerdo con alguno de los consejos. Finalmente se colgarán en el sala/aula las cartulinas con la intención de que puedan consultarlas frecuentemente.

- **Acoso en la red (segunda sesión)**

Dinámica 5: Definición de ciberbullying

Se pide a los usuarios que formen grupos de cuatro y que intenten realizar una definición del término ciberbullying. Posteriormente se pondrán en común y el monitor o monitora realizará una definición global a partir de las creadas por los grupos. Es recomendable que tenga unas características similares a esta:

> *"El ciberacoso o ciberbullying puede ser definido como la intimidación psicológica u hostigamiento que se produce entre pares, frecuentemente dentro del ámbito escolar, pero no exclusivamente, sostenida en el tiempo y cometida con cierta regularidad, utilizando como medio las tecnologías de la información y la comunicación. Se brindan aquí algunas claves que contribuyen a reconocer la existencia de esta problemática y cómo proceder frente a ella.*[4]*"*

Dinámica 6: Mitos sobre el ciberbullying

Esta dinámica necesita que los usuarios estén de pie y se puedan mover por el aula. El monitor debe decir una frase sobre el ciberbullying y éstos se colocarán en el lado izquierdo de la clase si están de acuerdo o al lado derecho si piensan que la afirmación es falsa. Se deben justificar las respuestas y el o la responsable de la actividad realizará una explicación sobre las mismas. Si es necesario se aclararán conceptos.

- **El ciberbullying es un delito**

Verdadero, no es una broma ni algo gracioso. Se trata de un delito que puede tener consecuencias legales para quien lo realiza.

- **Si alguien te esta molestando o insultando, puedes bloquear al remitente como no deseado y no recibirás más mensajes.**

Verdadero, hay que actuar cuanto antes. No se debe aguantar este tipo de conductas. Tanto las redes sociales como los Chats tienen dispositivos de bloqueo para evitar usuarios molestos.

- ***Si el ciberbullying se realiza de forma anónima es imposible saber quien lo realiza.***

---

4 *María José Edreira(2003)* Fenomenología del acoso moral en http://revistas.ucm.es/index.php/ASEM/article/view/ASEM0303110131A/16177 (Consultada el 03/05/2013).

Falso. Es cierto que en Internet muchas personas utilizan nicks y muchas veces, "inventan" perfiles y características personales falsas.

A veces, este anonimato puede favorecer las actitudes agresivas por parte de las personas que se creen anónimas. No obstante es bastante fácil identificar la dirección desde donde se envían los mensajes. La dirección I.P. de nuestro ordenador es como nuestro DNI. Además aunque los mensajes se envien desde ciber-cafés o los ordenadores del instituto, sigue resultando fácil reconocer a la persona que esta detrás, puesto que siempre se piden datos reales para utilizar los ordenadores públicos.

- **Si alguien te insulta o amenaza por Internet, lo mejor que haces es contestarle o borrar los mensajes.**

Falso. La asociación Protégeles recomienda seguir las siguientes pautas[5]:

- No contestes a mensajes que traten de intimidarte o hacerte sentir mal. Con ello probablemente conseguirías animar al acosador.
- Guarda el mensaje: no tienes por qué leerlo, pero guárdalo como prueba del hostigamiento. Es vital tener registro del incidente en caso de que busques ayuda o tengas intención de denunciarlo.
- Cuéntaselo a alguien en quien confíes. El hablar con tus padres, amigos, un profesor, el celador de la escuela, el delegado del curso o a alguna organización que te pueda ayudar, es el primer paso que deberías dar.
- Bloquea al remitente. No tienes que aguantar a alguien que te está hostigando.
- Bloquea a los remitentes no deseados.
- Denuncia los problemas a la gente que pueda hacer algo al respecto. Puedes tomar el control de la situación no soportando contenidos ofensivos.
- Respeta a los demás y respétate a ti mismo, el estar conectado en la Red supone que estas en un lugar donde la información se hace pública, aunque no siempre parezca así. Conoce tus derechos.

- **El ciberbullying termina con el paso del tiempo. Si denuncias será peor.**

Falso, es la falta de denuncia la que facilita que el agresor mantenga el acoso. La manera más eficaz de acabar con el ciberbulliyng es contándoselo a alguien que te pueda ayudar. No se trata de una broma pesada de la que el agresor de cansará al cabo de un tiempo.

- **El ciberbulliyng tiene consecuencias para el agresor y la víctima.**

Verdadero. No solo nos referimos a las consecuencias legales de cometer un delito. La víctima puede padecer enfermedades psíquicas y físicas tales como depresión, fobia escolar, ansiedad, trastornos de aprendizaje, cefalea, dolor abdominal, etc. Pero además,

[5] Esta información ha sido extraída de http://www.protegeles.com/es_linea8.asp

hay estudios que demuestran que el agresor también puede sufrir ansiedad, trastornos de conducta y baja autoestima.

Dinámica 7- ¿Qué harías tú?

Se dividirá al grupo principal en equipos de 4 ó 5 personas. Se presentarán varios supuestos de ciber-acoso. A partir de los cuales los usuarios tendrán que ponerse en la piel de la persona que escribe y establecer unas pautas de actuación. La dinámica se debe encaminar hacia la importancia que tiene la comunicación con personas que les pueden ayudar, padres, familiares, profesores o asociaciones. Debemos recordar a los usuarios que:

> "Nadie está libre de ser el objeto de una campaña de ciberbullying, pero las posibilidades son casi nulas si se siguen unas pautas preventivas. Comportarse con respeto en la Red, reaccionar de forma inteligente y calmada, controlar qué tipo de información se proporciona y rastrear los propios datos son muy buenas medidas de protección"[6]

Supuesto número 1:

"Me llamo Manuel y tengo 15 años. Hace cuatro meses me hice una cuenta de Facebook. Enseguida me empezó a agregar gente del "insti", incluso chavales con los que no tenía apenas trato. La verdad es que me daba palo no agregarles. Sin embargo enseguida empezaron a ponerse pesados, me insultaban el mis fotos, me llamaban maricón, gordo, nenaza. He dejado de subir fotos.

Ahora se dedican a coger mis fotos y subirlas retocadas, me ponen lazos en el pelo o dibujan un vestido. La verdad es que no aguanto más, no se que hacer, me da miedo conectarme y he pensado en borrar mi facebook. ¿Tú que harías?".

Supuesto número 2:

"Mi nombre es Silvia. Hace tres meses empecé a salir con un chico guapo y supermajo. Todo nos va genial, salvo por una cosa, su ex Carmen. Antes éramos amigas, pero desde que sabe que salgo con Jonathan no me deja en paz. Es muy raro porque a la cara no me dice ni "mu", pero me tiene amargada en el Tuenti. No para de poner de estado que le he robado a "su" Jonathan, que soy una zorra y que me voy a enterar. Hay gente que pone "me gusta" y le da la razón a través de comentarios.

Jon me dice que no me preocupe que se le pasará pero yo tengo miedo de que un día se le crucen los cables y me haga algo."

Supuesto número 3:

[6] Guía de prevención del ciberbulliyng, http://www.pantallasamigas.net/recursos-educativos-materiales-didacticos/guia-ciberbullying/index.htm

"Creo que la he liado parda. Yo solo quería gastarle una broma a Miguel pero creo que se me ha ido de las manos. El otro día estábamos de borrachera y Miguel vomitó. Me pareció simpático grabarle un vídeo. No debí subirlo al Youtube. Todo el instituto le llama "el aspersor humano", al principio a Miguel le hacía gracia pero ahora además de que la gente se ría, se ha enterado el instituto y sus padres. Está cabizbajo, casi no habla y evita venir a clase. No me atrevo a ir a hablar con él, seguro que me odia."

Dinámica 8- ¡Infórmate!

Por último, para cerrar la sesión sería interesante informar a los usuarios de la existencia de recursos para ayudar contra el ciberbullying.

Como complemento a la Línea de ayuda sobre Acoso Escolar (http://www.acosoescolar.info) creada por Protégeles en 2005. Siguiendo este ejemplo, se crea en 2009 la Línea de Ayuda contra el Ciber-bullying o acoso a través de las nuevas tecnologías http://www.internetsinacoso.com

Incluyo también esta página donde se pueden descargar varias guías en pdf contra el acoso escolar, para docentes, alumnado y familias.

http://www.defensordelmenor.org/documentacion/publicaciones_detalle.php?id_agrupacion=1&agrupacion=EDUCACI%D3N%20Y%20CULTURA

- **Protege a tu equipo (tercera sesión)**

Dinámica 9- "El Ciberglosario Malicioso"

Existen muchos términos que definen programas que pueden destruir o dar problemas en nuestro ordenador se denominan "malware".

Esta dinámica consistiría en un concurso. El monitor o monitora deberá decir la definición de un término de la siguiente lista[7] y los usuarios repartidos en dos grandes grupos, deberán acertar a que palabra se refiere. Al ser términos complejos y confusos, se pueden escribir en la pizarra para facilitar la dinámica.

 Email-bombing: consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando la casilla de correo del destinatario.

 Los virus: programas que generalmente requieren alguna interacción por parte del usuario (por ejemplo, abrir un archivo adjunto que recibimos por correo electrónico). Hoy también existen los que afectan los teléfonos celulares, como Cabir (que se

[7] Definiciones extraídas de: http://coleccion.educ.ar/coleccion/CD27/datos/amenazas_en_la_web.html

desplaza a través del bluetooth y que permite sustraer mensajes, contactos y escuchar nuestras conversaciones, entre otros).

 Los "caballos de Troya" o "troyanos": son programas que tienen una funcionalidad conocida (por ejemplo, un juego) pero además tienen una función oculta (como ser capturar las claves que escribe el usuario y mandarlas en un mensaje de correo electrónico a otra persona).

 Los "gusanos": programas que se reproducen sin necesidad de interacción de los usuarios, por ejemplo atacando servicios de red vulnerables.

 Keyloggers: es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computadora. Algunos registran además otro tipo de información útil, como ser imágenes de pantalla.

 Spyware: son aplicaciones que recogen y envían información sobre las páginas web más visitadas por un usuario, su tiempo de conexión, los datos relativos al equipo donde se encuentran instalados (sistema operativo, tipo de procesador, memoria, etcétera) e, incluso, hay algunos diseñados para informar si el software que utiliza el equipo es original o no.

 Spam: mensajes de correo no solicitados suelen incluir publicidad, y muchas veces contienen información falsa o engañosa.

 Hoax: mensajes fraudulentos con información falsa o inexacta, que nos inducen a reenviar el mensaje, a fin de difundir su contenido o a realizar acciones que muy probablemente nos ocasionarán problemas (Ejemplo: "borre el archivo x"; con consecuencias negativas para el ordenador y pérdida de información para nosotros.).

Dinámica 10- Del otro lado del clic

A partir del siguiente vídeo, se trabajará la prevención frente a mecanismos maliciosos que pueden vulnerar la seguridad de nuestros datos y equipos.

http://coleccion.educ.ar/coleccion/CD27/datos/del_otro_lado_del_clic.html

Se realizará una lista con las medidas que los usuarios vean convenientes para evitar este tipo de virus. El monitor o monitora puede ayudarles, por ejemplo:

1. No abrir correos de desconocidos.
2. Tener activado siempre el antivirus.
3. Actualizar el antivirus y el firewall cuando sea necesario.
4. Realizar descargas en sitios oficiales y de confianza.
5. No abrir datos adjuntos si se tiene la más mínima sospecha.

6. Ante cualquier duda, desconfía y consulta en un megabuscador si es una estafa o un virus.

Dinámica 11- Protegiendo nuestra identidad digital

Para esta actividad se plantea que cada usuario realice un autorretrato de su identidad digital, dibujando como cree él o ella que los demás le ven en Internet. Probablemente se dibujen tal y como se ven en la realidad. No obstante a partir de aquí se harán unas preguntas y contestar según la siguiente tabla:

- ¿Eres vergonzos@?
- ¿Consideras como amigos a personas que acabas de conocer?
- ¿Hablas con desconocid@s?
- ¿Le darías a una persona que no conoces tus datos o número de teléfono?
- ¿Te has hecho pasar por algún amig@ o conocid@?
- ¿La gente te felicita el cumpleaños?

En la calle	En las redes sociales

El objetivo de este ejercicio sería reflexionar sobre la identidad digital. Aceptar que son la misma persona en Internet que en la vida real y que en Internet, no deberíamos hacer cosas que no nos atreviésemos a hacer cara a cara.

Dinámica 12: Piénsalo antes de publicarlo

En la actualidad existen múltiples campañas para concienciar a los jóvenes sobre el peligro de divulgar aspectos de la vida cotidiana en Internet.

Sería interesante ver este vídeo: http://www.youtube.com/watch?v=-L93JZc-Kgo&feature=related. Su duración es de 1:05 y esta subtitulado. Por otra parte, en youtube existen varias reproducciones que podrían ser tan aptas como esta.

A continuación se reflexionaría sobre el mismo y la necesidad de mantener nuestra privacidad en Internet.

- **El casting (cuarta sesión)**

Dinámica 13: el Casting[8]

El objetivo principal de este ejercicio es reflexionar sobre la identidad digital de cada usuario en la red y sensibilizar sobre las consecuencias sociales y profesionales de sus acciones en Internet.

Para ello necesitamos un ordenador conectado a Internet y un cañón de proyección.

En primer lugar, cuatro alumnos escogidos al azar o voluntarios, junto al monitor actuarán de jurado del casting al que se presentan el resto de miembros del grupo. La prueba costará de una ronda de selección. Los participantes deberán proyectar con el ordenador su perfil de una red social. Los miembros del tribunal tienen derecho a preguntar lo que consideren oportuno.

El jurado deberá buscar el perfil que más se base en el respeto a sí mismo y a los demás, que resultará ganador de la prueba.

Una vez finalizada la parte del concurso se realizarán las siguientes cuestiones:

1. ¿Cómo se valora la imagen que das a través de la red social?
2. ¿Te has sentido avergonzado de alguna de las cosas que has mostrado?
3. ¿Piensas alguna vez en la imagen que das de ti mismo en las redes sociales?
4. ¿Crees que esta imagen puede tener repercusiones laborales?
5. ¿Crees que los perfiles que has visto reflejan la personalidad de su usuario?
6. ¿Habría alguna cosa que borrarías de tu perfil? ¿recomendarías eliminar algún elemento del perfil de un compañero?
7. ¿Has observado aspectos positivos en perfiles que te gustaría destacar?

Una vez finalizado el ejercicio se recomienda resaltar de manera más general la necesidad de construir una identidad digital basada en el respeto a uno mismo y hacia los demás.

[8] Reelaborada a partir de http://sites.google.com/site/tallerid11/actividades-de-aula/dinamicas-de-aula

Actividad final:

En último lugar, es aconsejable hacer una síntesis final de manera informal y breve. Se trata de recordar los aspectos más importantes del taller y su valor en la vida cotidiana. Es útil animar a los usuarios a poner en práctica las habilidades trabajadas en el taller.

Sería un buen momento para pasar el cuestionario final y agradecer la implicación, los esfuerzos realizados y desearles lo mejor para el futuro.

Criterios de evaluación

- Identificar los riesgos que existen en la navegación por Internet.
- Saber actuar ante los abusos y estafas que puedan encontrar.
- Reconocer situaciones de ciberbulliyng
- Ser capaces de buscar de ayuda cuando se encuentren en una situación comprometida o que les incomode.

La evaluación del proceso será en dos direcciones: por un lado se va a evaluar el proceso de enseñanza, es decir, que los métodos utilizados por los monitores son efectivos para cumplir con los objetivos, por otro lado, se evaluará el cumplimiento de los objetivos marcados para el taller.

El proceso de evaluación será realizado a través de la observación en el aula por parte de los responsables. También se realizará un cuestionario final para analizar el grado de satisfacción con los contenidos.

Por otro lado los monitores o monitoras también realizarán un pequeño test para autoevaluar el desarrollo del taller.

Bibliografía

Castillo, A (1997). *Apuntes sobre Vygotsky y el aprendizaje colaborativo*. *Lev Vygotsky: sus aportaciones para el siglo XXI*, Publicaciones UCAB, Caracas. Pp. 4251.

Coll, C. (1991). *Psicología y currículo. Una aproximación psicológica a la elaboración del currículo*. Paidós, Barcelona.

Coll, Marchesi y Palacios (1990). *Desarrollo psicológico y educación*. Alianza, Madrid.

Morris, C. y Maisto, A. (2005). *Introducción a la psicología*, duodécima edición, Pearson Educación, México.

Sampascual, G. (2001). *Psicología de la Educación*, UNED, Madrid.

Bibliografía de los recursos digitales

FTC, agencia nacional de protección del consumidor de EEUU http://alertaenlinea.gov/articulos/s0002estafascomuneseninternet, (04102013)

http://ciberbullying.wordpress.com/

Antonio Omatos Soria, http://sites.google.com/site/tallerid11/actividadesdeaula/dinamicasdeaula#TOCElcastingdegranhermanodeLinda (10112013)

Centro de seguridad de Internet para menores en España, http://www.protegeles.com/ (04102013)

Iniciativa Pantallas Amigas, http://www.pantallasamigas.net/, (1111.2013)

Centro de seguridad de Internet para menores en España, http://www.portaldelmenor.es/, (04102013)

Minetur, http://chaval.es/chavales/page?p=index (04102013)

Consejería de Innovación, Ciencia y Empresa de la Junta de Andalucía. http://www.kiddia.org/ (17012014)