TICmenoRes

Programa para la prevención de riesgos y el uso adecuado de las TRIC

Comunidad de Madrid

TICmenoRes - Programa para la prevención de riesgos y el uso adecuado de las TRIC

Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor. Consejería de Presidencia, Justicia y Pordavocía del Gobierno. Comunidad de Madrid.

Comunidad de Madrid

CONSEJERÍA DE PRESIDENCIA,
JUSTICIA Y PORTAVOCÍA DEL GOBIERNO

Esta versión forma parte de la Biblioteca Virtual de la **Comunidad de Madrid** y las condiciones de su distribución y difusión se encuentran amparadas por el marco legal de la misma.

www.madrid.org/publicamadrid

Madrid, abril de 2016

Coordinación: Juan Fco. Franco Yagüe.

Maquetación y portada: Luis Ángel Suárez Tamayo.

Infografías: Raquel Rodríguez Castro.

Este documento es el resultado del trabajo y el compromiso de todos los profesionales del Área de Menores en Conflicto Social de la **Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor**, habiendo colaborado especialmente en su elaboración y redacción los siguientes responsables, educadores, psicólogos y técnicos de los Recursos y Programas de Medio Abierto: Irene Giménez Montero, Eduardo Cueto Hernández, Raquel Rodriguez Castro, Susana Pedraza Sánchez, Virginia López-Oliva Soria, Cristóbal Serrano Rodríguez, Alicia Martín Álvarez, Ana Rodríguez Gil, Tamara del Barrio Cantero, Ana Valdés Ortega, María Jesús Diago Gil, Alberto Aguilar González, Hermelinda González Núñez, Miguel Ángel López Sáez.

Presentación

La adaptación al avance y cambio constante de las Tecnologías y las Redes de la Información y Comunicación (TRICs), obliga a una actualización permanente de los profesionales que realizan su labor con adolescentes y jóvenes absolutamente implicados ya en estos sistemas (podríamos decir que viven “en” las tecnologías y las redes) y que, en nuestro caso, además cometen infracciones de la ley que, en muchas ocasiones, tienen un correlato directo en las TRICs.

Delitos como la violencia de género, las amenazas o el acoso escolar se acompañan e, incluso a veces, se producen exclusivamente a través de estos medios. Qué no decir de tipos penales tan diferentes como las estafas, las vejaciones o la venta de artículos robados que, en la actualidad, tienen su vertiente principal en las nuevas tecnologías.

La Comunidad de Madrid, a través de la Agencia para la Reeducación y Reinserción del Menor Infractor, es consciente de la necesidad de atender esta situación, anticipándonos en la medida de lo posible, para intervenir con los menores que cometen delitos a través de estos medios, haciendo especial hincapié en la prevención de estas actuaciones y brindando la oportunidad a todos aquellos que deben cumplir una medida judicial de conocer y formarse en un uso adecuado de los mismos.

Este enfoque preventivo viene especialmente motivado por la falta de conciencia que frecuentemente presentan estos menores sobre el hecho de poder estar cometiendo un delito en acciones que consideran “normales” o que creen que no tienen mayor trascendencia o repercusión.

Por todo ello, desde la Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor hemos desarrollado el programa que figura en el presente Manual. Cuando un trabajo se desarrolla con profesionalidad e interés por mejorar la situación de los menores surge un programa como éste. Un programa pensado y desarrollado para conseguir nuestro objetivo más preciado: la reinserción de los menores que por diversas causas, los jueces ponen bajo nuestra responsabilidad.

Además, a modo de característica singular, esta herramienta es fruto de la colaboración público-privada. De este modo, aunar conocimiento, experiencia y medios de diferentes ámbitos de la sociedad siempre resulta enriquecedor, por lo que es uno de nuestros ejes de actuación.

Reinsertar, colaborar con otros medios, y permanecer activo ante los cambios e innovaciones que se van operando en la sociedad es primordial para la Agencia. Sólo siendo proactivos y dinámicos en la intervención conseguiremos dar una nueva oportunidad a esos menores, en edades difíciles, y propiciar una sociedad más justa y segura.

En una sociedad como la nuestra tan vertiginosamente cambiante hay que estar alerta y conocer los pros y contras de todos los avances que marcan nuestra vida. Hay que estar "on" y saber en momentos hacer "off". Como con las TRICs, es necesario aprovechar lo bueno que tienen y lo mucho que nos pueden ayudar en nuestro desarrollo personal, en nuestro trabajo, en nuestras relaciones sociales, pero siempre desde el conocimiento a fondo de la herramienta que manejamos.

En definitiva, innovar sí pero con conocimiento, seguridad y respeto.

Madrid, 1 de abril de 2016

REGINA OTAOLA MUGUERZA
Directora de la Agencia de la Comunidad de Madrid
para la Reeducación y Reinserción del Menor Infractor

Índice

Introducción

La Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor, según la Ley 3/2004, de 10 de diciembre, de creación de este Organismo Autónomo adscrito a la Consejería competente en materia de Justicia de la Comunidad de Madrid, es la entidad a la que alude la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores, y su Reglamento de desarrollo [Real Decreto 1774/2004, de 30 de julio] cuando señala a la Entidad Pública de Protección y Reforma de Menores como la competente para dar cumplimiento a las medidas judiciales adoptadas por los jueces de menores en cada Comunidad Autónoma.

Junto a esta competencia, o mejor dicho para su desarrollo y aplicación, como contempla la letra z del citado art. 3 de la Ley 3/2004, le corresponde llevar a cabo "*todas aquellas [actuaciones] que, directa o indirectamente, coadyuven a la consecución de los objetivos básicos o al mejor desarrollo de las funciones que se atribuyen en la presente Ley*"; en definitiva, el desarrollo de programas e instrumentos eficaces para la evaluación, programación e intervención con los menores infractores.

En el año 2008 el documento *Programación de las actividades socioeducativas de los centros de día para menores y jóvenes con medidas judiciales de medio abierto*, al que se puede acceder en la página de la Agencia, recoge la visión y propuesta de los recursos especializados para la aplicación de las denominadas medidas de medio abierto y las reparaciones o soluciones extrajudiciales, así como las intervenciones socioeducativas previstas, a saber: Taller de Habilidades Sociales –ahora denominado de Desarrollo personal y Competencia social-, Educación en Valores, Actividades de Apoyo Escolar y Alfabetización, Educación para la Salud, Prevención del consumo de drogas, Educación y Seguridad Vial, Educación Afectiva-Sexual, Motivación y Orientación Sociolaboral, Actividades de Ocio y Tiempo Libre, y Reparaciones Extrajudiciales y Prestaciones en Beneficio a la Comunidad -Tareas Asistenciales y Medioambientales- y lo que denominamos Actividades de Tecnologías de la Información y la Comunicación -TICs-.

En las actividades relacionadas con las TICs se contempló un bloque de informática básica (ordenador, sistema operativo, procesador de texto, etc.), un segundo bloque para el tratamiento de Internet y el correo electrónico, y un tercero dedicado a los usos de las tecnologías de la información y la comunicación en el ocio creativo.

Posteriormente, en el mes de junio de 2014, esta programación se completa con el documento *Recursos didácticos y actividades socioeducativas para menores infractores con medidas en medio abierto*[1]. Si el primero responde a las necesidades de programación de los profesionales, este segundo adopta una mayor perspectiva didáctica, aportando materiales pensados para los menores y jóvenes participantes en los talleres y actividades que se llevan a cabo en estos recursos.

En este segundo documento se incluye los delitos relacionados con el mal uso de la redes

(1) Área de Menores en Conflicto Social de la Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor

sociales digitales, como los que atentan contra el derecho a la intimidad, al honor, de falsedades, contra las libertades… relacionándolos con aquellas actividades que muchas veces hacen los adolescentes sin ser conscientes del daño que producen, como acceder a los correos electrónicos o los perfiles de redes sociales sin el consentimiento del titular, difundir vídeos o imágenes íntimas, hacerse pasar por otro remitiendo infinidad de correos de suscripción, etcétera. Asimismo se abordan fenómenos actuales como el *ciberbullying*, *grooming* y *sexting-sextorsión*, facilitando la compresión de qué es, qué implica y qué hacer ante una agresión de este tipo.

A partir de la experiencia en el desarrollo de estas actividades, y si bien la incidencia en cuanto al número de casos en los que se adopta una medida judicial relacionada con el uso indebido de las tecnologías digitales o las redes sociales aún no es muy notable, pensamos que es creciente y sin duda tiene consecuencias e implicaciones directas en la vida cotidiana de muchos de los menores y jóvenes con medidas adoptadas por otras infracciones pues, como comprobamos día a día, las tecnologías digitales han dejado de ser para ellos meras herramientas de Información y Comunicación (TIC), pasando a convertirse en instrumentos para expandir sus espacios de Relación interpersonal (Tecnologías de la Relación, Información y Comunicación -TRIC-); espacios en donde lo *online* y lo *offline*, lo digital y lo físico, se fusiona. "*Son estos espacios de conversación, juego, recreación, interacción y construcción; risas y cotilleos; parodias y flirteos, los que generan [para los menores] un conjunto de oportunidades para aprender las denominadas habilidades para la vida, en su capacidad para sentir y emocionarse, socializarse y conocer, tal y como demuestran diferentes investigaciones en este ámbito*" [2].

Aun así, y pese a que se tiende a considerar a los adolescentes como nativos digitales, frecuentemente el uso que hacen de las redes sociales digitales es, cuando menos, inadecuada; asumiendo riesgos innecesarios en cuanto a su seguridad y protección, participando directa o indirectamente, consciente o inconscientemente, en conductas que perjudican a otras personas.

En consecuencia, consideramos que es el momento de sistematizar unas nuevas actuaciones que beneficien a los menores mediante el aprendizaje y la práctica del uso adecuado de Internet, de las redes sociales digitales, y la gestión de cuestiones fundamentales como la identidad digital, las contraseñas o la *netiqueta*. Junto a ello, también contemplamos el desarrollo de actividades encaminadas a fomentar la protección de los menores ante el riesgo de sufrir violencia a través de la comunicación *online*, la gestión de su privacidad e identidad digital, el acceso a páginas inapropiadas o la participación en comunidades peligrosas como las *hate-speech* o, en otro sentido, las tecnoadicciones.

Asimismo, no es inusual encontrarnos que algunos de los menores y jóvenes atendidos presentan comportamientos conflictivos en las relaciones de pareja. En la intervención cotidiana hemos detectado actitudes que podríamos calificar como micromachismos, al tiempo que observamos como, en ocasiones, mantienen relaciones de dominio que no están exentas de alguna forma de violencia. Si bien existen programas específicos de la Agencia, así como experiencia contrastada en el tratamiento de la violencia de género, tanto en Centros de internamiento -Programa VIOPAR- como en Medio Abierto, donde se ha puesto en marcha más recientemente el Programa Iguala2; también se ha constatado que estos comportamientos

(2) Gabelas, J. A., Lazo, C. M. y Aranda, D. (2009). Por qué las TRIC y no las TIC. *Revista de Estudios de Ciencias de la Información y de la Comunicación, 9*

lesivos se llevan a cabo, en muchas ocasiones, a través de las redes sociales virtuales o de mensajería instantánea, motivo por el que se incluye un apartado o unidad de trabajo dirigido específicamente a esta problemática, con una propuesta de abordaje y tratamiento de la misma que hemos llevado a cabo de manera eficaz y con resultados satisfactorios.

Por último, debemos tener presente que nuestro trabajo consiste también en la prevención de la conducta infractora de los menores y jóvenes con medidas judiciales, así como el cumplimiento de sus deberes relativos a su ámbito familiar, escolar y social, como recoge la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia; así como el desistimiento de posibles conductas acosadoras ejercidas a través de las tecnologías digitales y redes sociales como es el caso del conocido como *ciberbullying*, *sexting*, suplantación de identidad, con especial atención a la violencia de género.

Debemos finalizar esta introducción indicando que el documento que presentamos está basado tanto en los aspectos que hemos señalado, como en los objetivos y finalidades del trabajo con los menores infractores que llevan a cabo los profesionales de la Agencia, pretendiendo aportar una guía e instrumento que oriente y ayude en la programación de las actividades educativas que se lleven a cabo con los menores y jóvenes durante el cumplimiento de las medidas judiciales.

Menores, jóvenes y TRICs

En la página web del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información podemos acceder a distintos estudios y análisis del sector de las Telecomunicaciones y de la Sociedad de la información en España. Aquí sólo vamos a hacernos eco del análisis de datos del INE del año 2014 que se realiza en el *Perfil Sociodemográfico de los Internautas*[3]. En el mismo se señala que el grupo de edad de 16 y 24 años presenta los mayores porcentajes de acceso a Internet respecto a otros de mayor edad. De este grupo el 98.5% accede en alguna ocasión y el 96.2% con una frecuencia semanal. Sin lugar a dudas el uso de las TRICs tiene evidentes repercusiones en los menores y jóvenes en muchos aspectos, en cuanto a la configuración de identidades, en la propia personalidad del sujeto, en su proceso de socialización, etc.

Por otro lado, un incremento del número de adolescentes que reconocen que han sufrido situaciones de maltrato por parte de su pareja, podemos comprobarlo en la publicación de la Delegación del Gobierno para la Violencia de Género[4], en el que se da cuenta de las distintas formas que adopta como el control abusivo, la presión para actividades de tipo sexual, agresiones físicas.

Centrándonos en el acoso ejercido a través de mensajes de internet o móvil, evaluado a través de determinados indicadores, y siguiendo el mismo texto citado se aportan las siguientes resultados:

- "*He difundido mensajes de Internet o móvil que la insultaban, amenazaban, ofendían o asustaban*" es reconocido por el 1,6% de los chicos (el 1,1% en 2010). En 2013 el 2,6% de las chicas reconoce haber recibido este tipo de mensajes.

- "*He difundido por Internet o móvil insultos, mensajes o imágenes suyas, sin su permiso*": el 1,3% de los chicos responde que lo ha hecho (el 1,1% en 2010). En 2013 el 1% de las chicas reconoce haber sufrido dicha situación.

- "*He usado sus contraseñas, que ella me había dado confiadamente, para suplantar su identidad*", pregunta realizada solo en 2013, a la que responde afirmativamente el 1,6% de los chicos. Este porcentaje coincide con el del 1,6% de las chicas que reconoce haber sufrido dichas situaciones.

A partir de estos resultados, según los autores de la obra citada se desprende que:

- Insultar es reconocido como contenido de los mensajes por la mayoría de los adolescentes que los han enviado o sufrido. Los resultados obtenidos al preguntar a ellas y a ellos son bastante coincidentes, puesto que el 61,7% de las chicas y el 52,7% de los chicos lo reconocen como uno de los contenidos de los mensajes que han sufrido ellas y enviado ellos. En segundo lugar, destaca la frecuencia

(3) http://www.ontsi.red.es/ontsi/

(4) *La evolución de la adolescencia española en la igualdad y la prevención de la violencia de género*. Delegación del Gobierno para la Violencia de Género, 2014.

con la que dichos mensajes tratan de ridiculizar, en lo que también hay bastante coincidencia. El 39,3% de las chicas y el 36,4% de los chicos responden que dichos mensajes trataban de ridiculizarlas, a veces, a menudo o muchas veces.

- Hacer sentir miedo es reconocido por los chicos como objetivo de los mensajes que más han repetido. El 19% responde que éste era el contenido de los mensajes o las llamadas que han realizado, a menudo o muchas veces. El porcentaje de chicas que lo destaca como contenido frecuente de los mensajes es, en este caso, menor del 9,8%.

- Coacciones con amenazas (amenazar para que ella hiciera cosas que no quería hacer) y presiones para participar en actividades de tipo sexual, son reconocidas como el contenido de los mensajes bastante más frecuentemente por los chicos, que por las chicas. Cuando se consideran las dos categorías de más frecuencia se encuentra que, entre quienes han enviado o sufrido mensajes de maltrato, el 18,6% de los chicos y el 6,1% de las chicas, reconocen que incluían coacciones. Las presiones para que ella participara en actividades de tipo sexual en las que no quería, son reconocidas como contenido frecuente de los mensajes por el 16,3% de los chicos y el 4% de las chicas.

- Difundir imágenes de ella comprometidas o de carácter sexual sin su permiso, reconoce haberlo realizado frecuentemente el 15,9% de los chicos que han enviado mensajes de maltrato, y haberlo conocido con frecuencia, el 2,2% de las chicas que han sufrido dichos mensajes. La discrepancia en este contenido es máxima.

- Los medios a través de los cuales un mayor porcentaje de chicos han enviado los mensajes en situaciones de violencia de género son: Whatsapp, Tuenti y teléfono móvil, seguidos a cierta distancia de Twiter, SMS, Messenger, Skype, Facebook y Youtube. El resto de los medios son destacados por menos del 30% de los chicos que enviaron este tipo de mensajes. A partir de los datos proporcionados por las chicas, los medios de los mensajes de violencia de género que ellas han conocido con mayor frecuencia son, como sucedía en el caso de los chicos: Whatsapp, Tuenti y teléfono móvil, seguidos a cierta distancia de SMS; siendo el resto de los medios destacados por menos del 20% de las chicas que sufrieron dichos mensajes, mucho menos de los que los destacan los chicos que dicen haberlos enviado.

Menores: derechos y deberes

En la Observación General 13 (2011) del Comité de Derechos del Niño de Naciones Unidas sobre el Derecho del Niño a no ser objeto de ninguna violencia, se plantean distintas medidas protectoras, incluyendo la violencia a través de las TRICs. También desde Naciones Unidas se han postulado medidas de protección de víctimas y testigos a los que se reconocen los derechos a un trato digno y comprensivo, a la protección contra la discriminación, a ser informado, a ser oído y a expresar opiniones, a una asistencia eficaz, a la intimidad, a ser protegido de sufrimientos durante el proceso de justicia, a la seguridad, a la reparación y a medidas preventivas especiales (*Directrices sobre la justicia en asuntos concernientes a los niños víctimas y testigos de delitos*, aprobadas por el Consejo Económico y Social de Naciones Unidas el 10 de agosto de 2005).

Asimismo, respecto a los niños y adolescentes agresores se recomienda el estudio "caso a caso" para tomar las medidas sancionadoras y educativas más adecuado, dando preferencia a la rehabilitación y la justicia restitutiva que a la represión o la sanción.

En este sentido también es un importante objetivo de nuestro trabajo favorecer el cumplimiento de los deberes por parte de los menores, que según la legislación vigente[5] se sustancian en distintos ámbitos, y en concreto respecto al ámbito familiar: en el respeto a progenitores, hermanos y otros miembros de la familia, corresponsabilidad en el cuidado del hogar y las tareas de acuerdo a su edad, autonomía y capacidad; los relativos al ámbito escolar: respeto de las normas de convivencia, a los profesores, empleados y compañeros, "*evitando situaciones de conflicto y acoso escolar en cualquiera de sus formas, incluyendo el ciberacoso*", así como predisposición hacia estudio y hacia el aprendizaje; y en cuanto el ámbito social: respetando tanto a las personas con las que se relacionan como al entorno en el que se desenvuelven, concretándose estos deberes sociales particularmente en:

a) Respetar la dignidad, integridad e intimidad de todas las personas con las que se relacionen con independencia de su edad, nacionalidad, origen racial o étnico, religión, sexo, orientación e identidad sexual, discapacidad, características físicas o sociales o pertenencia a determinados grupos sociales, o cualquier otra circunstancia personal o social.

b) Respetar las leyes y normas que les sean aplicables y los derechos y libertades fundamentales de las otras personas, así como asumir una actitud responsable y constructiva en la sociedad.

c) Conservar y hacer un buen uso de los recursos e instalaciones y equipamientos públicos o privados, mobiliario urbano y cualesquiera otros en los que desarrollen su actividad.

d) Respetar y conocer el medio ambiente y los animales, y colaborar en su conservación dentro de un desarrollo sostenible.

(5) Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y adolescencia, Cap. III, Deberes de los menores.

El II Plan Estratégico Nacional de Infancia y Adolescencia 2013-2016 (PENIA II)[6] define "las grandes líneas estratégicas de desarrollo de las políticas de infancia con el objetivo final, de dar un efectivo cumplimiento a la Convención de Naciones Unidas sobre los Derechos del Niño teniendo en cuenta los derechos, pero también los deberes y responsabilidades de los menores de edad". Para ello se plantean ocho objetivos entre los que destacamos, en relación al tema que nos ocupa:

> OBJETIVO 3.- Medios y tecnologías de la comunicación: Impulsar los derechos y la protección de la infancia con relación a los medios de comunicación y a las tecnologías de la información en general.

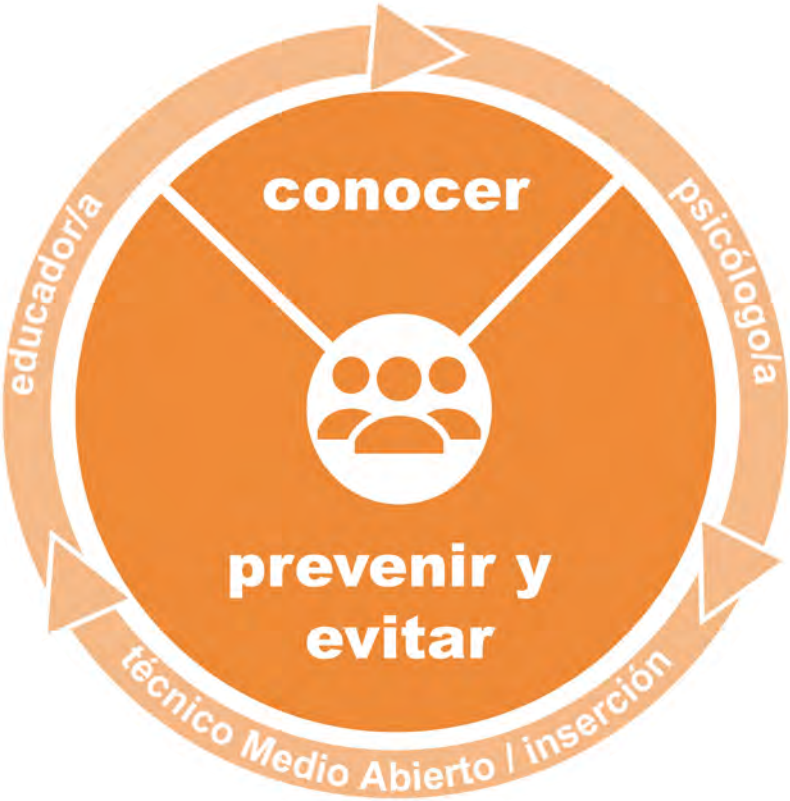
Para lo cual se proponen distintas medidas:

> 3.4.- Acceso a Internet: Fomentar acciones de sensibilización y formación dirigidas a la infancia y adolescencia, las familias y el profesorado, dirigidas a mejorar el acceso a Internet para todos y su buen uso con acciones como:
>
> > 3.4.1 - Formar a las familias y a los niños en el buen uso de Internet y sus posibilidades, teniendo en cuenta sus distintas capacidades, desarrollando las técnicas de apoyo para su accesibilidad y el diseño para todos.
> >
> > 3.4.2 - Difundir entre ellos el aprendizaje de los nuevos lenguajes de las tecnologías de la información y la comunicación e impulsar el acceso a contenidos educativos on-line basados en los principios de accesibilidad universal y diseño para todos los niños, (evitando cualquier tipo de exclusión digital o desigualdad género/ discapacidad) en el acceso y uso a las nuevas tecnologías que pudiera traducirse en una doble discriminación.
> >
> > 3.4.3 - Promover la prevención del abuso o la explotación sexual de niños y adolescentes a través de la red. Ofrecer formación a los niños y adolescentes sobre las actividades y conductas que pueden constituir delito (Ciberacoso, grooming, piratería…) o cualquier consecuencia no deseadas.
> >
> > 3.4.4.- Fomentar la accesibilidad a las tecnologías de comunicación, especialmente a Internet y a los medios audiovisuales, a todos los niños con cualquier tipo de discapacidad.
> >
> > 3.4.6.- Impulsar y desarrollar la presencia de la Delegación del Gobierno para el Plan Nacional sobre Drogas en las redes sociales, como forma de acceder a las poblaciones más jóvenes con el objetivo de dar a conocer los riesgos de las adicciones.

(6) Aprobado por acuerdo de Consejo de Ministros de 5 de abril de 2013 y dirigido a todos los menores de 18 años con la pretensión de constituir un marco de cooperación de todas las Administraciones Públicas, tanto la Administración General del Estado, como de la Autonómica y la Local, además de otros agentes sociales implicados en los derechos de la infancia, tales como la Plataforma de Organizaciones de Infancia.

El Proyecto TICmenoRes

Tenemos que conocer y transmitir las grandes posibilidades que nos da Internet, pero también prevenir los riesgos que implica. Para los adolecentes las relaciones sociales son fundamentales e Internet y las múltiples redes, aplicaciones y juegos online desarrolladas son una fuente constante de interacciones. Estas relaciones digitales pueden conducirnos a una cierta sensación de impunidad, descuidando la prevención necesaria y las posibles consecuencias negativas para otros, incluidos los amigos, de las acciones que llevamos a cabo en estas redes, teniendo en cuenta además el extraordinario eco que pueden llegar a tener las mismas. En consecuencia, como han señalado distintos autores, nosotros queremos recoger esa dimensión relacional, especialmente significativa para los adolescentes y su mundo de iguales, utilizando la perspectiva de las TRICs -Tecnologías de la Relación, Información y Comunicación-.



Este Proyecto se ha configurado con una estructura modular que, aunque tiene un planteamiento de secuencia y progresión, contempla dos posibles escenarios, pudiéndose llevar a cabo de manera independiente o de forma conjunta en función de las necesidades detectadas, las exigencias del cumplimiento de las medidas judiciales o las características de la persona o el grupo, siempre persiguiendo:

- Fomentar en los menores y jóvenes un uso adecuado de las TRICs, a la vez que se les *in-forma* de sus derechos y obligaciones.

- Trabajar la identificación de los potenciales riesgos del uso de las TRICs y las formas de protegerse, al tiempo que se les conciencia para que eviten o, en su caso, desistan de un uso inadecuado.

A la hora de diseñar las diferentes actividades, se ha tenido en cuenta también la posibilidad de que las mismas se puedan desarrollar tanto de forma individual como grupalmente, dando respuesta a las posibles necesidades de la actividad y de los participantes. Por ejemplo porque sea uno de los contenidos específicos que se haya programado en el cumplimiento de la medida de que se trate, o la posibilidad de creación de un grupo de menores con los sea conveniente el tratamiento de estos contenidos.

Además, constatando la problemática creciente, con el objetivo de abordar la prevención de la violencia de género especialmente en las primeras relaciones de pareja, en el Proyecto se han incluido también actividades específicas para trabajar el uso adecuado de las TRICs desde esta perspectiva.

Por último, atendiendo a la necesidad de información sobre las TRICs y sus distintos usos y prácticas por parte de padres, madres y otros adultos significativos para la vida del menor o el joven, el Proyecto contiene diversas propuestas con el fin de que sean capaces de fijar pautas adecuadas que contribuyan a que sus hijos utilicen dichas tecnologías evitando riesgos y otras contingencias.

En esta propuesta de conocer, prevenir y evitar el mal uso, los riesgos y peligros de las TRICs, lógicamente están implicados tanto los técnicos responsables de la ejecución de las medidas, como los educadores y otros profesionales de la intervención, así como los psicólogos y los técnicos de inserción sociolaboral.

En cuanto a la inclusión de un menor en un taller o actividad programada de las TRICs, dependerá en gran medida del recurso en el que se lleve a cabo, pero con carácter general el proceso inicial a llevar a cabo consiste en:

OBJETIVOS, METODOLOGÍA Y EVALUACIÓN

Cada una de las unidades tiene un planteamiento de objetivos más operativos con respecto a los aprendizajes a promover, pero en un plano general el conjunto de la programación busca el uso adecuado de las TRICs, la prevención y evitación de riesgos de los internautas, el descubrimiento de nuevas posibilidades y utilidades, y sobre todo las buenas prácticas.

USO ADECUADO DE LAS TRICs	
OBJETIVO GENERAL	**OBJETIVOS ESPECÍFICOS**
Favorecer la *alfabetización digital* y el uso de las redes sociales como instrumentos educativos para el desarrollo personal y la participación social.	• Conocer los derechos y deberes como internautas. • Aprender conceptos y aplicaciones básicas de informática, soportes digitales, Internet, cuentas de correo, perfiles… • Conocer las redes sociales, la navegación y las herramientas de uso práctico y cotidiano.
PREVENIR y EVITAR RIESGOS	
OBJETIVO GENERAL	**OBJETIVOS ESPECÍFICOS**
Tomar conciencia de los riesgos de la comunicación *online* y las redes sociales digitales, así como de los posibles delitos y sus consecuencias.	• Comprender qué es privacidad y los límites en el uso de la información personal y de imágenes obtenidas. • Conocer los riesgos más comunes de la comunicación en las redes. • Practicar con los usos adecuados de las contraseñas, barreras… • Motivar para favorecer la reducción o eliminación de comportamientos inadecuados, violentos e infractores.

NUEVOS USOS Y BUENAS PRÁCTICAS	
OBJETIVO GENERAL	**OBJETIVOS ESPECÍFICOS**
Realizar buenas prácticas y descubrir nuevas utilidades de las redes sociales digitales….	• Practicar las distintas posibilidades que las tecnologías digitales ofrecen como instrumento de ocio, videojuegos. • Conocer nuestra huella digital y las posibilidades de las redes digitales para la inserción sociolaboral. • Adquirir competencias que permitan mejorar las relaciones sociales.

En cuanto a la metodología, dado el carácter individualizado de la intervención, tendrá que ser necesariamente flexible y fundamentada en las características de cada menor, de su estilo de aprendizaje y de los conocimientos y demandas realizadas, así como del tipo de medida judicial y de las acciones a desarrollar durante la misma, también estará en función de la posible creación de un grupo ad hoc como apuntamos anteriormente.

Si bien la programación está diseñada para coincidir con los intereses y motivaciones de los menores y jóvenes, utilizando ejemplos y poniendo en práctica dinámicas relacionadas con sus experiencias, es prioritario crear un clima que favorezca la comunicación, la interacción y la confianza entre los participantes. Para ello se propone un cuestionario inicial que permita una autoevaluación de conocimientos y de actitudes de los propios menores hacia los temas a tratar, pero también un motivo para el diálogo e inicio motivado de la actividad.

Las actividades propuestas para cada sesión pretenden servir de apoyo al profesional responsable de la misma. Los contenidos asimismo pueden y deben ser adaptados a las necesidades y particularidades del grupo de adolescentes, teniendo presente que el éxito de la actividad se basa fundamentalmente en que ésta sea práctica y dinámica, ya que los adolescentes tienen que vivir este espacio, además de como propio, como oportunidad de adquirir nuevos conocimientos y desarrollar competencias mediante el manejo directo de las TRICs. Por otro lado, atendiendo al carácter cambiante y a la rápida evolución de las TRICs, en cada momento habrá que valorar siempre la necesidad de sustituir o actualizar las actividades y herramientas utilizadas, aprovechando las oportunidades que nos dan Internet y los instrumentos de acceso y navegación.

Tanto las unidades como las actividades programadas se pueden desarrollar de una manera consecutiva, pero también con una configuración modular, ya que cada unidad o partes de la misma pueden ser utilizadas para programar una actividad singular, sean con un solo menor o con un grupo determinado.

También hemos contemplado otras posibilidades complementarias, como las que se llevan a cabo con los padres y otros familiares, ya que es común que éstos participen más activamente en determinados momentos, bien porque ellos mismos soliciten ayuda respecto a un tema concreto, generalmente en referencia a la relación con sus hijos y a las pautas más eficaces a establecer desde su condición de adulto responsable, o bien porque acepten participar en un grupo de padres determinado. Frecuentemente las relaciones con las TRICs, su mejor conocimiento y sobretodo su comprensión y manejo es un tema de interés recurrente.

La *búsqueda de ayuda* que puede integrase perfectamente en las actividades tanto dirigidas a los padres y adultos como a los propios menores, y es un buen ejemplo de la conveniencia de realizar este diseño modular que comentamos. Y lo mismo podríamos decir de gran parte de los contenidos y actividades que se proponen en las distintas unidades.

Por último, tenemos que recordar nuevamente que toda la programación puede llevarse a cabo tanto de manera grupal como individualmente, en este último caso pensando más, pero no exclusivamente, en la medida de libertad vigilada en la que se producen frecuentes entrevistas de seguimiento con el técnico responsable de la ejecución de la medida, y en las que cada vez más se evidencian las lagunas, errores y riesgos innecesarios en los que incurren los menores como internautas, requiriendo en consecuencia su abordaje desde la perspectiva de resolución de conflictos pero también de prevención de otros posibles.

Como señalábamos anteriormente, algunas de las unidades contemplan la posibilidad de utilizar cuestionarios y otras herramientas para conocer el punto de partida respecto al tema y los contenidos a tratar en cada momento. Con ellos no sólo tendemos un mejor conocimiento de los participantes, sino fundamentalmente ayudaremos a que tomen conciencia de sus perspectivas, actitudes y competencias en estos temas, punto de partida para la motivación hacia la actividad o actividades a desarrollar en cada momento.

Consideramos también muy importante mantener un proceso de evaluación continua del taller o actividades que se lleven a cabo de cara a favorecer la participación de la persona o los miembros del grupo, así como para la adaptación de las distintas propuestas y su adecuación a los objetivos a conseguir.

El cuestionario de autoevaluación se adaptará a cada unas de las unidades tratadas por los conductores de la actividad, según su propia valoración y consideraciones. En el caso de la unidad Curriculum 2.0. por su singularidad, presenta el mismo cuestionario con las preguntas que se han considerado más adecuadas a los contenidos y propósito del mismo.

Por otro lado, se contempla también la posibilidad de implementar el cuestionario de satisfacción que es común a todas las actividades socioeducativas del AMCS, y que se viene utilizando tanto con los menores y jóvenes atendidos como con sus padres o familiares, cuando son éstos los que han participado en la actividad. Es un instrumento que se puso en marcha buscando un *feedback* directo para la mejora constante de los programas y los servicios desarrollados. Pensamos que es más adecuado para la unidad dirigida a los adultos, sean

padres, tutores u otros adultos significativos, pero también, como se hace con la gran mayoría de las actividades socioeducativas en medio abierto, tiene utilidad práctica para el grupo de menores o jóvenes participantes.

Conocer

1

módulo

INTRODUCCIÓN

Este módulo está dirigido fundamentalmente a fomentar y reforzar el uso adecuado de las tecnologías y redes sociales digitales. Consta de cuatro unidades cuyas actividades se plantean para la sensibilización, así como una posible formación inicial, sobre la necesidad de conocer los riesgos existentes, los instrumentos de protección y su aplicación.

Como hemos hecho hincapié anteriormente, las unidades y actividades propuestas pueden desarrollarse de manera consecutiva o compaginarse, en función de los objetivos que nos planteemos, con otras actividades según las necesidades detectadas o de las características de la persona o del grupo de trabajo.

COMPETENCIAS

En la actualidad, el uso de las tecnologías de la relación, la información y la comunicación está presente en la vida diaria de todos, formando parte fundamental de los distintos ámbitos de relación fundamentales para la personas: la vida social, la actividad económica y laboral, la cultural y también en el uso del tiempo libre y del ocio. Por ello, es fundamental desarrollar lo que podemos denominar como competencias digitales. Entre estas competencias destacan:

- El conocimiento digital: capacidad de comprensión el fenómeno digital y saber desenvolverse personal, social y laboralmente.
- La gestión de la información para saber compartir la información personal, así como buscar, evaluar y utilizar la información obtenida.
- La comunicación digital para aprender a relacionarse de manera apropiada y eficaz en los entornos y con las herramientas digitales.
- De relación en las redes sociales digitales, desarrollando las capacidades de colaboración y saber interactuar según las personas, los grupos o las actividades en las que nos integramos.
- El aprendizaje continuo y de gestión autónoma de los aprendizajes adquiridos y manejo de los recursos digitales.

Junto a ellas debemos tener presente otras competencias relacionadas con el trabajo que se desarrolla con los menores y jóvenes atendidos, y que tienen que ver más con los planteamientos y objetivos de otros talleres y actividades como el de *Desarrollo personal y Competencia social*:

- Competencias comunicación, verbal y no verbal, estilos de comunicación, asertividad…
- Competencias relacionadas con la expresión de emociones, inteligencia emocional, autoestima, aceptación y valores…

1.1. Inicio de la actividad

En los casos en los que se plantee como actividad grupal, la iniciaremos con una presentación de los miembros del grupo, favoreciendo la cohesión del mismo y la alianza con el responsable y conductor de la misma, generando un espacio de confianza, apoyo y motivación.

OBJETIVOS

- Conocer el uso de las TRICs que habitualmente hace la persona o el grupo de trabajo: cuáles son las tecnologías y redes sociales digitales que más usan y para qué.
- Comprender el concepto de ciudadanía digital, cómo se identifican habitualmente en la Red y descubrir los riesgos que existen.

ACTIVIDADES

Cuestionario inicial (FA-1)

Con el objetivo de conocer las prácticas más comunes de los menores de forma individual o grupal completarán la ficha de actividad FA-1.

Carta a mi tatarabuelo (FA-2)

Como dinámica inicial se propone la redacción en grupo de una carta imaginaria a una persona que desconoce completamente Internet, en ella comentarán a través de ejemplos de su vida cotidiana cómo se utiliza y para qué sirve.

Normalmente con esta actividad podemos obtener una amplia información sobre los aspectos positivos de Internet para los usuarios, mientras que los riesgos y los peligros suelen pasar desapercibidos.

Trabajo de grupo (FA-3)

Fuente: Programa Internet Sin Riesgos. Área de Juventud del Cabildo Insular de Tenerife.

Complementaria o alternativamente se puede plantear la actividad "¿Cuáles son las ventajas y las desventajas de Internet y las redes sociales?" según se propone en la pág. 24 de la Guía Didáctica *Navega en Positivo*, material elaborado por el Equipo Técnico de la Fundación General de la Universidad de La Laguna, para el Programa Internet Sin Riesgo.

Esta actividad de unos 20 minutos de duración nos ayuda a identificar las posibles ventajas y desventajas que nos ofrece el uso y manejo de Internet y las redes sociales en las diferentes esferas de la vida: personal, social, profesional, académica, y reflexionar con el grupo sobre el uso seguro y responsable de la Red.

Para su desarrollo se divide al grupo en pequeños equipos de trabajo de un máximo de 4 personas, intentando siempre que haya una representación equitativa de chicas y chicos, y se les entregará la ficha FA-3. El tiempo aproximado para que el equipo cumplimente la ficha será de diez minutos.

El resto del tiempo se ocupará en la realización de la puesta en común y el o la profesional que dirija la sesión deberá ir reforzando el uso de Internet y las redes sociales desde una óptica positiva.

Con el objetivo de reforzar los mensajes y en cierta medida de guía de actividad, a continuación se indican algunos aspectos que se pueden considerar como ventajas y desventajas:

- **Ventajas:** Comunicación e información inmediata, mantener contactos, entretenimiento, conocer gente nueva, rompe fronteras geográficas, facilita trámites burocráticos, búsqueda de empleo, nuevas formas de empleo, ligar, consulta de documentos públicos y de carácter personal, medio de socialización, compartir vivencias con familiares y amistades (fotos, etc.), comprar y vender artículos, denunciar injusticias, formación online, juegos, lecturas, acceso a idistintas informaciones fundamentales.

- **Desventajas:** Poca privacidad, violación de tu imagen, usurpación de identidad, fácil engaño, puede generar adicción, aislamiento y perdida de sociabilidad, virus, información no real, faltas de respeto, se encuentra información personal que no deseas mostrar, estafas, puede destruir relaciones, lo que subes a la red se queda en la red, quita tiempo y concentración, no se respetan los derechos de autor, falta de conocimientos sobre cómo utilizar internet y las redes sociales, vida sedentaria (en mayor o menor medida), problemas físicos como de espalda, vista..., mayor facilidad de distribución de pornografía infantil.

1.2. YO FÍSICO Y YO DIGITAL

Con estas primeras actividades pretendemos conocer las funciones de las TRICs en la vida social en general, así como los usos más frecuentes que hace el grupo de los participantes, buscando tanto resaltar los aspectos positivos de compartir información a través de Internet como aumentar la percepción de los riesgos asociados.

OBJETIVOS

- Identificar la vida *offline* y la *online* como "una única vida" y no como "partes diferenciadas de nuestra vida".
- Sensibilizar sobre la importancia de la privacidad, el uso seguro de Internet y las Redes Sociales (Adecuada gestión de la privacidad, identidad digital)
- Conocer los derechos y deberes acerca de la protección de la privacidad, el derecho a la intimidad y el secreto de las comunicaciones.

CONTENIDOS

Fuente: Oficina de Seguridad del Internauta (OSI).

Recogemos a continuación algunos aspectos básicos de los contenidos procedentes de las Unidades didácticas *Gestión de la privacidad e identidad digital Secundaria (13-17 años)* (www.red.es), que recomendamos revisar junto a la amplia documentación existente y de fácil acceso en Internet.

Qué es la identidad digital

"*La identidad digital, puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital*" (INTECO, 2012). Podemos tener una identidad digital aún sin haber usado nunca Internet, ya que es frecuente compartir con familiares, amigos y conocidos fotografías conmemorativas o simplemente por el mero hecho de compartirlas; estas fácilmente pueden llegar a ser compartidas con personas desconocidos.

Big Data. ¿Qué son?

Para la comprensión de las nuevas tecnologías relacionadas con la gestión de los datos generados por los internautas y sus posibles aplicaciones se recomienda la lectura del artículo del diario El País "¿Qué es eso del '*big data*'?"

Privacidad, derecho a la intimidad y el secreto de las comunicaciones

RAE: "*Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*" (Fuente: Real Academia Española. (2001). Privacidad. En Diccionario de la lengua española (22.a ed.)

Cuando se habla de protección de datos personales se hace referencia tanto a toda aquella información que identifica a la persona o que la puede hacer identificable, como a aquella que habla de ella misma. Es decir, gestionar la privacidad no sólo significa gestionar los datos personales de forma exclusiva sino que también debe abarcar aquella información que habla sobre las preferencias, gustos, comentarios, ideas, etc.

Confidencialidad

Implica que la información tan sólo podrá ser accesible a aquellas entidades o personas autorizadas a las que el usuario dé su consentimiento. Así, y especialmente en las redes sociales, este estándar resulta de vital importancia porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.

Integridad

La información que aparece en la red sólo puede ser modificada por las entidades o personas autorizadas.

Autenticación

Es necesario establecer mecanismos de verificación de la identidad digital de las personas y entidades en la red, para poder reconocer que el usuario sea realmente quién dice ser.

Riesgos de no proteger la privacidad.

Es importante conocer los riesgos de hacer públicos ciertos datos como los personales, el correo electrónico, los datos bancarios, la ubicación geográfica, las fotografías y vídeos.

¿Qué es la huella digital?

La huella digital en Internet es el rastro que se deja en aquellos lugares por los que navega y se va dejando información. Se debe ser consciente y trasladar a los menores la perdurabilidad de la información en Internet. Es muy sencillo subir fotografías, vídeos, comentarios… a Internet, pero no es tan fácil borrarlos. «En Internet, las huellas que se dejan son difíciles de borrar».

¿Qué es la reputación online?

La reputación *online* es el influjo, estima, prestigio, valoración…de una persona en Internet. "*La reputación online es la opinión o consideración social que otros usuarios tienen de la vivencia online de una persona o de una organización*".

VIDA SOCIAL
RELACIONES Y TRICs

DERECHO A LA INTIMIDAD

HUELLA DIGITAL

REPUTACIÓN ONLINE

PROTEGE TU PRIVACIDAD

AUTENTICACIÓN

INTEGRIDAD

CONFIDENCIALIDAD

ACTIVIDADES

Antes de iniciar la actividad, comprueba y en su caso actualiza los links de las propuestas que se hacen, ya que pueden no estar operativos, haber variado o existir otras propuestas más actuales y convenientes para trabajar los objetivos propuestos. En ocasiones también es necesario escribir directamente en el navegador la dirección del enlace.

Cuestionario Yo físico, Yo digital (FA-4)

Con el objetivo de conocer los conocimientos previos y las prácticas más comunes de los menores, estos, de forma individual o grupal, completarán la ficha de actividad FA-4.

Juego el simulador de privacidad

Fuente: Pantallas Amigas con la colaboración de EUKidsOnline y el apoyo de .Tuenti.

La importancia de la privacidad podemos tratarla a partir de las redes sociales donde se suelen subir fotografías (p.e. Tuenti y Facebook), con el fin de clarificar que la privacidad depende de diversos factores y, en ocasiones, no solamente depende de uno mismo, además de concienciar sobre la importancia de proteger la privacidad de terceras personas. Enlace: http://www.simuladordeprivacidad.com

Cuidar la privacidad es importante

Videos de animación didáctica que, tomando como referencia el uso de los teléfonos móviles, reflexionan acerca de la importancia de cuidar la privacidad y la identidad digital, tanto propia como de terceras personas:

- Tu celular, tu tesoro. Pantallas Amigas, 2015
- Amistades sin medida. Pantallas Amigas, 2015

¿Tienes privacidad de verdad en las redes sociales?

Fuente: Pantallas Amigas, 2010.

https://youtu.be/_VAgyuNjnoY

El peligro de las redes sociales

Fuente: Pantallas Amigas, 2012.

https://youtu.be/H_v0v70WFaA

Privial

Fuente: Pantallas Amigas

http://www.cuidatuimagenonline.com

Cómo hacer un buen uso de las tecnologías móviles

Fuente: Guía de Ciberbullyng y Privación, Centro de Seguridad en Internet Protégeles y Insafe, 2010.

https://youtu.be/ylh1zzeICDM

1.3. Uso responsable de las TRICs

Con esta unidad pretendemos analizar la forma en que utilizamos nuestros datos e imagen personal en la red, la importancia que tiene reservar información y cuidar el contenido de nuestras publicaciones y el respeto a la privacidad, que se traduce en el consentimiento del otro para usar o difundir su imagen, ideas, etc., en las redes sociales e Internet. También hablaremos de la necesidad de evitar riesgos a través de la protección de nuestra identidad digital y los datos de carácter personal.

OBJETIVOS

- Conocer las cuestiones básicas y fundamentales que determinan nuestra imagen y perfil en Internet, las buenas prácticas y la netiqueta.
- Aprender a crear contraseñas seguras y utilizar otras barreras de protección de la privacidad en las redes sociales digitales.

CONTENIDOS

Nuestra imagen en Internet

PRESTA ESPECIAL ATENCIÓN A...	
1. Aspecto físico y presencia, también en cuanto a lo profesional	Nuestra imagen *online* es muy importante para las relaciones y para nuestra vida. Antes de una reunión, cita o entrevista, nuestra información puede ser consultada en la Web
2. Comportamiento y comunicación no verbal	Conseguir nuestros objetivos, personales y también profesionales (un trabajo, un contrato, una recomendación…), no depende únicamente de nuestros conocimientos y méritos; también, y sobre todo, de nuestras capacidades sociales
3. Tus mensajes	Observa las palabras que usas, las frases que escribes o pronuncias
4. *Networking*	La traducción literal de este término es “trabajar tu red de contactos”

5. Tu presencia en Internet	Nadie duda de la importancia de tener presencia en Internet. Cuanto mejor sea tu información, y más fácil sea de encontrar, mayor serán las posibilidades de darte a conocer y de tener una buena imagen.
6. Tu presencia en las redes sociales	Casi el 80% de los internautas españoles utilizan las redes sociales, en consecuencia son una gran oportunidad de darse a conocer y de comunicarse. Las redes sociales acercan a las personas y permiten la interacción

Reputación *online*

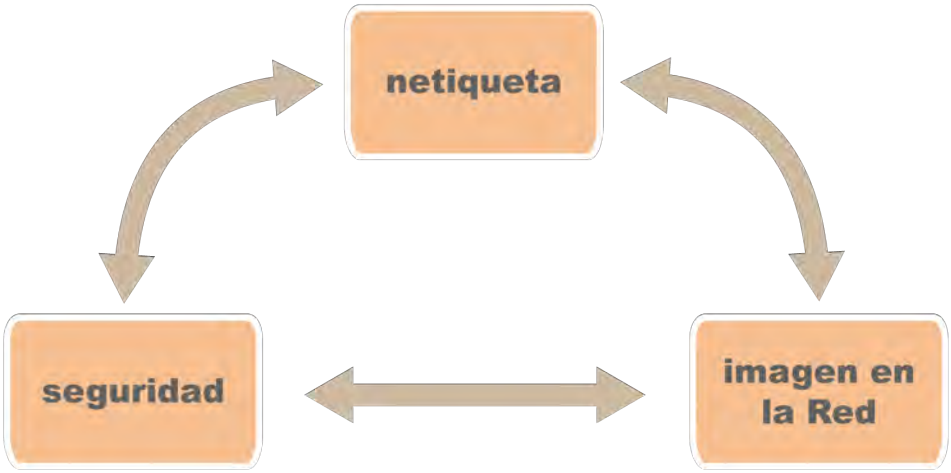
Un buen perfil requiere que sepamos proyectar la imagen que nosotros queremos, para ello tenemos que prestar atención al uso que hacemos de las redes, de lo contrario la imagen que creamos nos puede llegar a perjudicar.

Uso seguro de contraseñas

Uno de los problemas de utilizar claves demasiado simples es que existen programas diseñados para probar millones de contraseñas por minuto, por ello las contraseñas deben ser secretas, robustas y únicas. Para facilitar la tarea, podemos utilizar algunas sencillas reglas:

Cambiar las vocales por números
Por ejemplo: Mi familia es genial >>> M3 f1m3l3 2s g2n3ll
Utilizar reglas mnemotécnicas. Por ejemplo, elegir la primera letra de cada una de las palabras de una frase que sea fácil de recordar para nosotros
Con 10 cañones por banda… >>> C10cpb…
Para hacer más sencillo el trabajo, podemos utilizar claves basadas en un mismo patrón, introduciendo ligeras variaciones para cada servicio. Por ejemplo, tomando como base la contraseña anterior, añadir al final la última letra del servicio utilizado en mayúscula:
Facebook >>> C10cpb…K Twitter >>> C10cpb…R Gmail >>> C10cpb…L
Dependiendo del servicio y de su importancia podemos utilizar claves más robustas o menos, para facilitar su memorización. Para los servicios más sensibles, siempre podemos utilizar un generador aleatorio de contraseñas. La mayoría de los gestores de contraseñas ofrecen esta funcionalidad.

Para un uso responsable de las TRICs ten en cuenta:



ACTIVIDADES

Debemos insistir especialmente en la importancia de las contraseñas, barreras y medidas de protección primarias a las que generalmente no prestamos mucha atención, utilizando muy habitualmente claves que son demasiado simples.

Cuestionario uso responsable TRICs (FA-5)

Con el objetivo de conocer los conocimientos previos y las prácticas más comunes de los menores, estos, de forma individual o grupal, completarán la ficha de actividad FA-5.

Contraseñas seguras (FA-6)

Fuente: Oficina de Seguridad del Internauta

Para facilitar la comprensión de su importancia, podemos mostrar mediante la ficha de actividad FA-6 el tiempo que tarda un programa especializado en averiguar una contraseña en función de su longitud y los caracteres que utilicemos.

Configuración de privacidad. Facebook, Instagram, Twitter, WhatsApp

Fuente: Oficina de Seguridad del Internauta.

En la programación de estas actividades deberás tenerse presente la posible participación de algunas de las personas o el grupo de trabajo en el Módulo de Prevenir y Evitar, y en concreto en la Unidad 6.

OTRAS PROPUESTAS: BUENAS PRÁCTICAS EN EL USO DE TRIC Y NETIQUETA.

Para las buenas prácticas planteamos un conjunto de actividades propuestas en la mencionada Guía didáctica ISR, tales como:

No seas *NOOB*

Fuente: Programa Internet Sin Riesgos. Área de Juventud del Cabildo Insular de Tenerife, pág. 35

Con una duración estimada de 5 minutos, se pretende explicar lo que significa ser "*noob*", y recopilar información sobre los conocimientos que tiene el grupo en torno a las normas de netiqueta.

Podemos dar inicio a la actividad con preguntas tales como ¿qué significa ser una persona "*noob*"? y ¿qué son las "normas de *netiqueta*"? que nos permitirá saber los conocimientos que tienen sobre el tema. Tomamos nota de las respuestas posteriormente explicar el concepto "*noob*" tal y como se ha definido en las orientaciones metodológicas haciendo uso, en la medida de lo posible, de las respuestas dadas por el grupo. Así mismo se introducirá la idea que para no ser "*noob*" hay que cumplir con las "normas de *netiqueta*", las cuáles se explicarán en las actividades posteriores.

Normas de convivencia *offline* y *online* (FA-7)

Fuente: Programa Internet Sin Riesgos. Área de Juventud del Cabildo Insular de Tenerife, pág. 40

Con una duración estimada de 10 minutos, se pretende valorar el conocimiento que los adolescentes poseen sobre las normas de convivencia online.

Para el desarrollo de la actividad se entregará a cada grupo la ficha "Normas de convivencia *offline* y *online*" (FA-7) y se les explicará cómo cumplimentarla. En la columna de la izquierda deberán realizar un listado de aquellas normas sociales que facilitan que nuestras relaciones interpersonales y sociales sean adecuadas para el modelo cultural en el que vivimos. En la columna de la derecha deberán realizar un listado de aquellas normas sociales, que nos facilitan que nuestras relaciones a través de Internet sean vividas como experiencias placenteras, gratas y satisfactorias.

El tiempo para cumplimentar la ficha por parte de los grupos será de 4 minutos y el resto (6 minutos) se dedicarán a la puesta en común y aclaración de dudas en el caso de que surjan.

Con el objetivo de servir de guía a la persona que dirija al grupo para apoyar su discurso, se relacionan a continuación algunos ejemplos:

Normas que nos facilitan la vida *offline*	Normas que nos facilitan la vida *online*
• Saludar y despedirse cuando nos cruzamos con una persona conocida en la calle. • Seguir la conversación cuando estamos hablando. • No gritar, insultar, humillar, ridiculizar, avergonzar, ofender, etc. • Si no conocemos a una persona no actuamos con confianza como por ejemplo tocando en exceso, tener comportamientos cariñosos, decirles que no nos gusta la ropa que lleva, etc. • Si un amigo o amiga nos confía un secreto, lo debemos guardar y respetar su intimidad. • Si vamos a una casa que no es la nuestra, no entramos a todas las habitaciones, ni abrimos la nevera sin permiso, ni abrimos cajones, etc. • Por la calle no vamos chillando, ni en un examen nos ponemos a bailar, ni en un autobus le contamos nuestra vida y nuestros secretos a la persona que se sienta a nuestro lado, etc. • Cuando una puerta está cerrada llamamos antes de entrar.	• Saludar y despedirse. • Contestar a los mensajes. • Poner asunto en los correos electrónicos. • Ser amable. • No utilizar mayúsculas. • Poner emoticonos. • Control de faltas de ortografía y signos de puntuación. • Contestar en redes sociales a quien te habla y conozcas. • No utilizar abreviaturas para que el lenguaje sea comprensible. • Acompañar los emoticonos de palabras, onomatopeyas... para reforzar el lensaje. • No utilizar códigos personales en una conversación grupal para que las personas que no lo entienden no se sientan excluidas. • No insultar, mentir, humillar, dañar... • Pedir las cosas por favor y dar las gracias. • Revisar lo que has escrito por si tienes el corrector activado y cambia el sentido de tu frase.

¿Cuáles son las normas de netiqueta?”

Fuente: Programa Internet Sin Riesgos. Área de Juventud del Cabildo Insular de Tenerife, pág. 41

Con una duración estimada de 15 minutos, se busca conocer cuáles son alguna de las normas de netiqueta.

Esta actividad se puede realizar tanto *online* (http://www.netiquetate.com) con las imágenes interactivas, como imprimiendo las fichas que hay en esa web.

Es probable que en la actividad anterior se hayan tratado las normas que contienen las fichas y ya se hayan citado, por ello se considera oportuno rescatar todas aquellas normas que han verbalizado los grupos en la puesta en común para incidir en el correcto conocimiento de cómo hay que comportarse para disfrutar de experiencias online positivas.

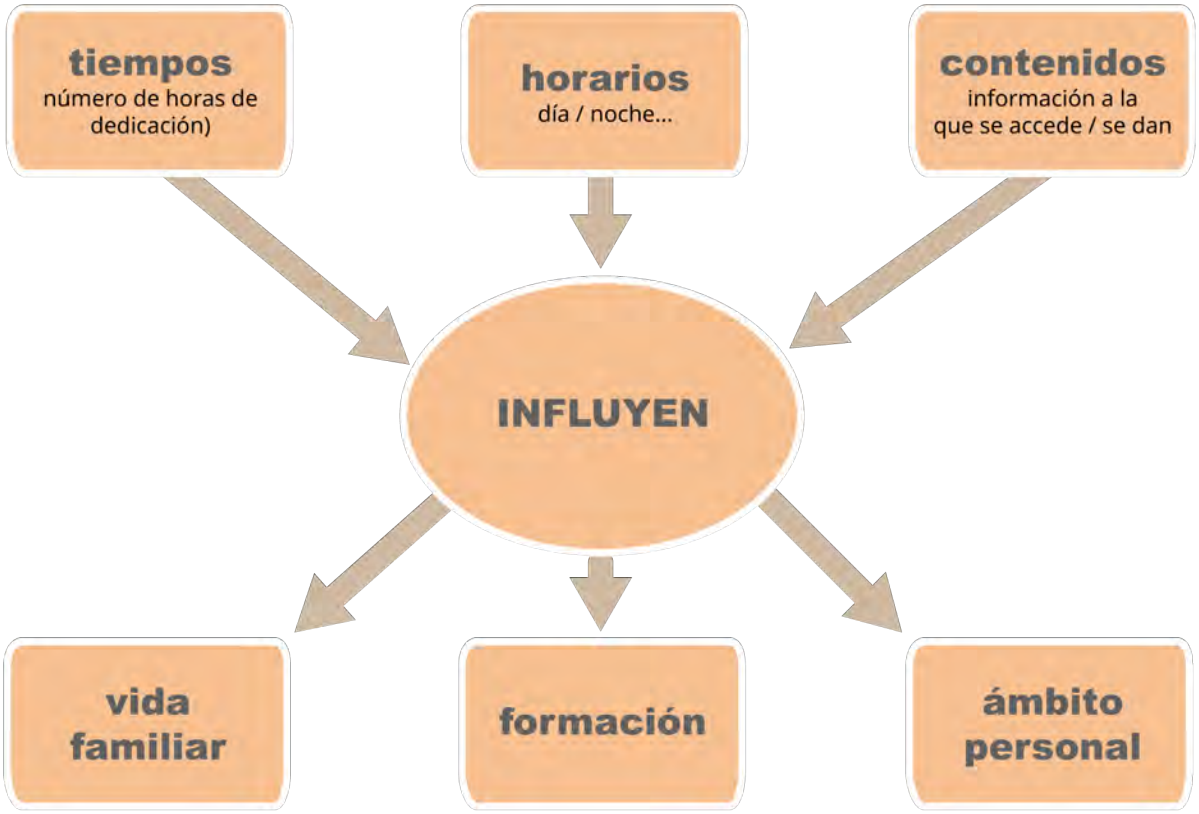
Así mismo se fomentará la reflexión sobre la idea de que Internet y las redes sociales al permitirnos en muchas ocasiones el anonimato y facilitar la evasión de la responsabilidad, se convierte en un espacio en el que podemos llegar a creer que todo vale sin pensar en las consecuencias que nuestros actos tendrán en otras personas.

En Internet hay que tener en cuenta la viralidad, es decir, la rápida difusión de la información. Muchas veces reenviamos contenidos sin pensar en el uso que le pueden dar otras personas y, aunque nuestra actuación no sea de mala fe, cuando esa broma, foto, video, comentario, mentira, cotilleo... sale de nuestro dispositivo ya no tenemos el control sobre lo que otros y otras puedan hacer. Hay que concienciar a los y las adolescentes de que es importante valorar los riesgos y consecuencias que puede tener cualquier actuación no solo para otras personas sino también para ellos mismos.

OTRAS PROPUESTAS: PUBLICACIÓN Y DIFUSIÓN DE CONTENIDOS EN LA RED ¿CONTROLAS O TE CONTROLAN?

La importancia del equilibrio entre dedicación y horarios de uso de las TRICs y otras actividades fundamentales de la vida cotidiana, que se contempla en la unidad dedicada a los padres, puede estar justificada en esta unidad en función del menor o grupo con el que se lleve a cabo.

Si hablamos de un uso responsable de las TRICs hay que tener en cuenta varios factores, como son el tiempo de dedicación y los contenidos a los que se encuentran expuestos. Ambas cuestiones influyen en los ámbitos familiar, formativo y personal de los menores, teniendo en cuenta que el desarrollo social de éstos en el entorno digital transcurre en paralelo a su desarrollo social en el entorno físico.



I forgot my phone **(FA-8)**

Visionado, reflexión y posterior debate sobre el contenido del video "I Forgot My Phone" (CharstarleneTV, 2013), para lo cual se pueden encontar algunas propuestas en la ficha de actividad FA-8. Duración aproximada de la actividad: 30 minutos.

https://youtu.be/OINa46HeWg8

Desconectar para conectar **(FA-9)**

Visionado, reflexión y posterior debate sobre el contenido del video "Desconectar para conectar" (Linddrops, 2011), para lo cual se pueden encontar algunas propuestas en la ficha de actividad FA-9. Duración aproximada de la actividad: 30 minutos.

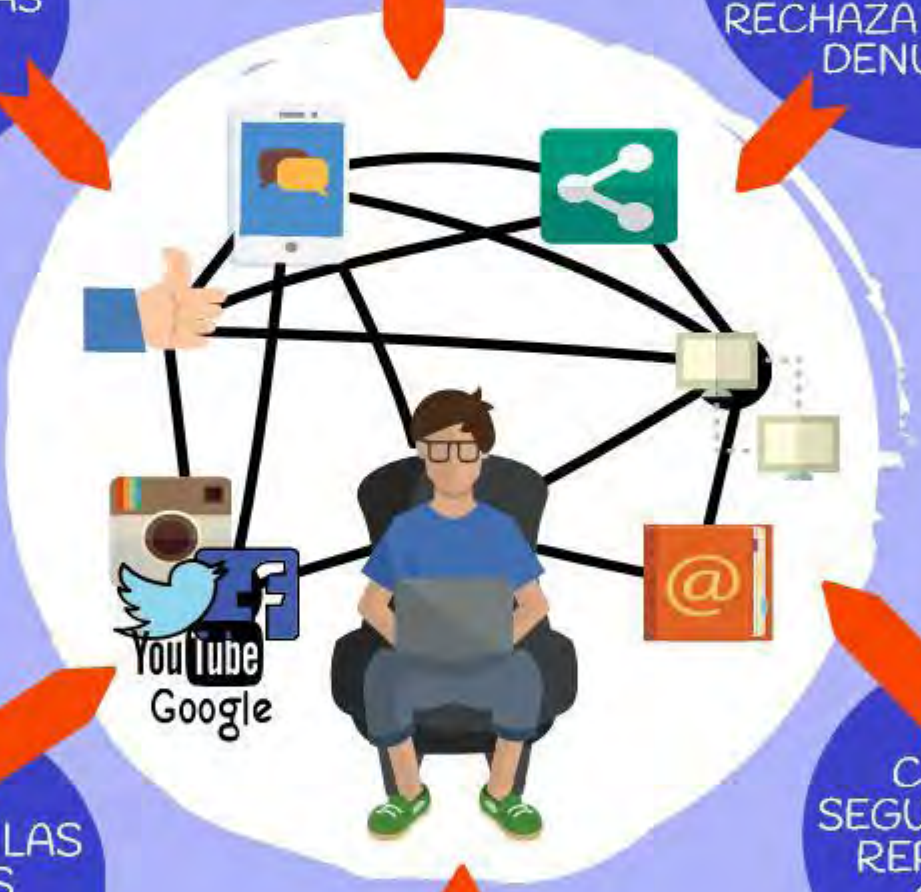
https://youtu.be/Ag7OHQJPBRw

USO ADECUADO DE LAS NUEVAS TECNOLOGIAS

CONOCE Y MANEJA LAS POSIBILIDADES QUE OFRECE LA WEB

SE RESPONSABLE, INDIVIDUAL Y SOCIALMENTE. TEN ACTITUD CRÍTICA RECHAZA EL ABUSO. DENUNCIA

ADQUIERE COMPETENCIAS DIGITALES



RESPETA A LAS NORMAS NETIQUETA

CUIDA LA SEGURIDAD Y TU REPUTACIÓN ONLINE

CUIDA TU PRIVACIDAD: DATOS, IMAGENES, IDEAS..

1.4. Cierre y generalización

La sesión de cierre debe programarse como un resumen de los usos adecuados de los perfiles y las redes sociales online, así como hacer referencia a los otros posibles usos relacionados con el ocio y otras actividades, y la búsqueda de ayuda…

OBJETIVOS

- Repasar mediante material didáctico adaptado los contenidos fundamentales trabajados.
- Aprender a comprobar nuestra imagen y perfil en Internet, estableciendo hábitos de revisión y mejora continuada.

CONTENIDOS

UNO

Las TRICs son una importante herramienta para el conocimiento, la comunicación y las relaciones. **Tienen muchas ventajas pero también algunos peligros si no hacemos UN USO RESPONSABLE**. Algunos usos de Internet pueden resultar muy dañinos para ti y/o para otras personas de tu entorno, también estos malos usos pueden llegar a constituir una infracción legal con graves consecuencias.

DOS

Por ello: **TOMA TUS PRECAUCIONES** en la información personal que aportas, ya que no sabes a quién le puede llegar finalmente, ni el uso que pueden hacer de la misma, en el presente o en el futuro. **NO publiques en la red información privada** (teléfono, dirección, DNI, datos bancarios, contraseñas……) **NO compartas las contraseñas con otras personas**… **UTILIZA siempre el botón de salir o de cerrar sesión**.

TRES

UTILIZA CONTRASEÑAS SÓLIDAS Y SEGURAS (de un mínimo de 8 caracteres, mezcla mayúsculas y minúsculas, caracteres especiales (@ # *) y números. **CÁMBIALA CON REGULARIDAD**.

CUATRO

Elige a tus **AMIGOS DE LA RED social digital entre las personas que conozcas**, rechaza solicitudes de amistades de un desconocido.

CINCO

CUIDA TU IMAGEN Y TU REPUTACIÓN DIGITAL, ES TU DERECHO. Tú decides qué información aportas sobre ti, a quién y cómo usarlos, pero no olvides que una vez que los subes a la red pierdes el control de su uso y su divulgación. Todo deja huella y perdura en el tiempo, afectando a la identidad y a la reputación digital. Lo divertido en un momento, lo que

te genera popularidad en la red en un momento, puede pesar en un futuro sobre tu reputación o sobre la de otra persona que confió en ti.

SEIS
Reconoce el derecho del otro a proteger su imagen y su reputación LOS OTROS TAMBIÉN MERECEN RESPETO.

SIETE
COMPÓRTATE **CON LOS DEMÁS COMO QUIERES QUE LOS DEMÁS SE COMPORTEN CONTIGO**. No actúes online como no lo harías en la vida real o en la relación cara a cara con la otra persona.

OCHO
ANTES DE ACTUAR: **PIENSA Y REFLEXIONA** sobre el posible daño o perjuicio que puedas causar a otro o a ti mismo con los contenidos o comentarios que vayas a enviar o reproducir en la red. "Lo que se cuelga en la red queda en la red"

NUEVE
Si estás siendo objeto de acoso, humillación, amenazas o chantaje por la red, NO TENGAS MIEDO, sé valiente y pide ayuda a un adulto en el que confíes –padres, profesores, educadores...-. **CUÉNTALO y DEJATE AYUDAR** juntos el problema se resolverá mejor.

DIEZ
MUESTRA TU RECHAZO si conoces o eres testigo de ciberacoso y no actúas acabas contribuyendo con la situación, NO te quedes parado: ACTÚA. DA UN PASO ADELANTE, seguro que muchos otros te seguirán: comunícaselo a un adulto de confianza, a la persona víctima y/o a sus padres, bloquea y borra el contenido.

ACTIVIDADES COMPLEMENTARIAS

Búscate en la red, actualiza tus perfiles (FA-10)

Al igual que las empresas se preocupan por lo que dicen sus clientes de ellos en Internet, las personas deben interesarse por lo que dice y aparece de ellos en buscadores y redes sociales, por lo que el primer paso será pedir a los menores que busquen su nombre en un buscador como Google, revisando las dos primeras páginas de resultados y comprobar si aparece algo malo de ellos, alguna foto o vídeo que consideres que puede manchar tu imagen personal o profesional.

Deben tener en cuenta que las opiniones de los demás sobre ellos conforman su identidad digital y ésta puede afectar directamente a la decisión que un contratador puede tomar sobre ellos.

Despues de realizar la búsqueda, en el caso que los menores encuentren información que crean afecta negativamente a su imagen, deberán procurar eliminarla o pensar en los pasos que debes de dar para ello.

Cómo crear gratis nuestro blog en WordPress

Fuente: Ciudadano 2.0, 2013.

https://youtu.be/2l4IRjpOtiI

Cuestionario de autoevaluación (FA-11 y FA-12)

El cuestionario que se propone pretende ser un instrumento de evaluación pero también de reflexión personal acerca del trabajo realizado en una determinada sesión, a lo largo de las sesiones o al finalizar una unidad o el taller programado, en función de las necesidades educativas percibidas por responsable de la actividad.

Otros usos

2

módulo

Además de para la comunicación y las relaciones sociales, Internet tiene muchas otras posibilidades y utilidades. Es por ello, que este segundo módulo se enfoca a conocer otras posibilidades que ofrecen las TRICs para un ocio satisfactorio que responda a las expectativas, aficiones y el desarrollo personal y cultural.

Asimismo, se hace una propuesta de actividades relacionadas con la inserción sociolaboral, dada la importancia de Internet y las redes digitales, no sólo para la formación, información y búsqueda de empleo, sino en cuanto a las consecuencias directas que tiene nuestra huella digital.

La última unidad, que no necesariamente tiene que realizarse al finalizar las otras, se dirige a establecer las bases para pedir ayuda en caso de dificultades del internauta y los recursos disponibles para ello.

2.1. LAS TRICS COMO INSTRUMENTOS DE OCIO

OBJETIVOS

- Fomentar el uso responsable de las nuevas tecnologías y los videojuegos.
- Conocer el sistema de clasificación PEGI, y tomar conciencia de la importancia de cumplir con las directrices de la normativa para las edades mínimas.
- Tomar conciencia de los riesgos del uso de las tecnologías y los videojuegos.

CONTENIDOS

¿Qué es el sistema de clasificación PEGI?[7]

PEGI es un sistema para clasificar el contenido de los videojuegos y otro tipo de software de entretenimiento que se aplica en 25 países europeos. El sistema es independiente, pues no tiene relación alguna con la Unión Europea, aunque cuenta con su respaldo y se considera un modelo de armonización Europea en materia de protección de la infancia. En los últimos años ha sido también adoptado por Amazón, Apple y Google para clasificar las diferentes aplicaciones y juegos que venden a través de sus tiendas on-line.

Dentro del sistema PEGI existen dos formas de clasificación para cualquier software; una de edad sugerida y otra sobre seis descripciones de contenido, tales como el uso de lenguaje indecente, violencia, etc.. De esta forma, se orienta a los consumidores (especialmente a los padres) y se les ayuda a tomar una decisión sobre si deben comprar o no un producto concreto.

Se puede encontrar toda la información relativa a la clasificación PEGI por edades y por descriptores en la web de la Pan European Game Information.

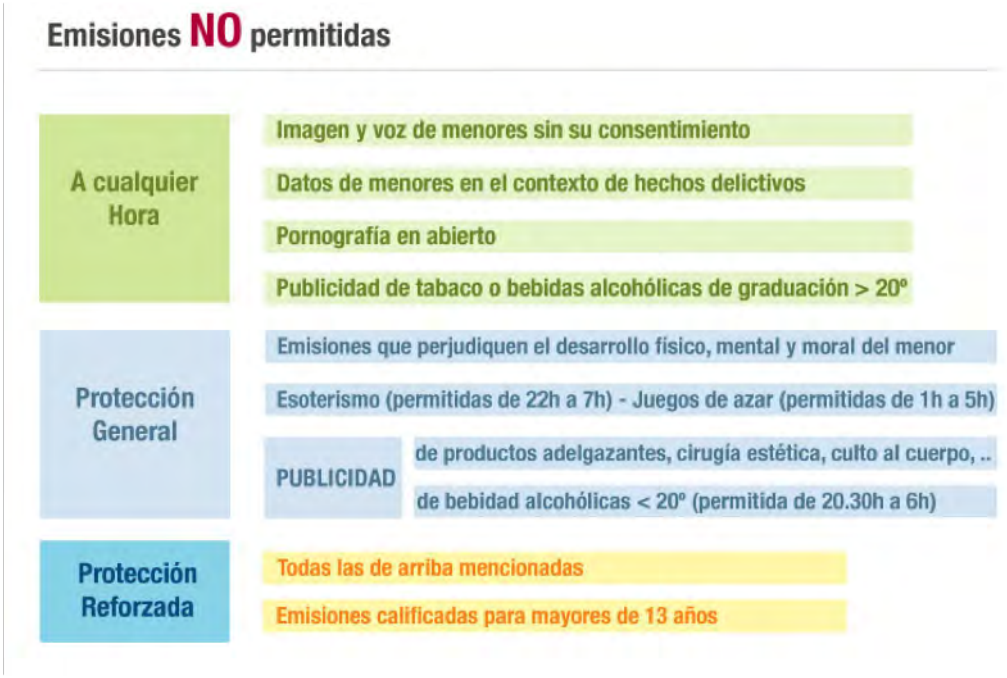
(7) Fuente: Wikipedia.

LEYENDAS							
							
Lenguaje soez	Discrimi-nación	Drogas	Miedo	Apuestas	Sexo	Violencia	Juego en red

Códigos de clasificación por edades en la TV en España

Hasta 2011 sólo se mostraban al principio del programa, pero ahora se muestran durante toda la duración del mismo, en la mayoría de cadenas.

Programa no clasificado	SC
Para todos los públicos	TP
No recomendado para menores de 7 años	7
No recomendado para menores de 10 años	10
No recomendado para menores de 12 años	12
No recomendado para menores de 13 años	13
No recomendado para menores de 16 años	16
No recomendado para menores de 18 años	18



ACTIVIDADES

Sobre videojuegos y TV (FA-13)

Con el objetivo de conocer las ideas previas y las prácticas más comunes de los menores, estos, de forma individual o grupal, completarán la ficha de actividad FA-13.

¿A qué edad...? (FA-14)

Los menores deberan averiguar la edad mínima que se necesita para usar cada una de las app y servicios listados. Pueden ayudarse de cualquier motor de búsqueda para ello (Google, Bing, etc.).

Sistema PEGI (FA-15)

De forma individual o grupal y ayudándose de un motor de búsqueda, o de la la propia página de la Pan European Game Information, los menores deberán explicar el significado de los distintos códigos PEGI que aparecen en la ficha de actividad FA-15.

Videojuegos (FA-16)

Accediendo a la base de datos de PEGI, averigurar tanto la edad como el pictograma de descripción de contenido que corresponde a cada juego listado en la ficha de actividad FA-16.

La clasificación de la TV (FA-17)

Una vez vista la normativa y las restricciones de contenidos en los diferentes horarios televisivos, los menores deberán hacer su propia valoración de si se cumplen o no las normas.

Aislados

Fuente: Asociación Servicio Interdisciplinar de Atención a las Drogodependencias

Aislados es un proyecto, dirigido a adolescentes, para la prevención de drogodependencias y otros comportamientos de riesgo. Elaborado por la Asociación Servicio Interdisciplinar de Atención a las Drogodependencias (SIAD), tiene por objetivo los menores aprendan mientras juegan. O que jueguen mientras aprenden. Para ello, proponen herramientas innovadoras y cercanas al adolescente (el videojuego y el juego de rol), como plataforma para el aprendizaje global, activo y lúdico de habilidades sociales, cognitivas y emocionales ("Habilidades para la vida").

http://www.aislados.es

2.2. Curriculum 2.0

La inserción sociolaboral hoy en día requiere también de la actualización de los instrumentos convencionales, entre otras razones porque los currículos digitales también tiene una dimensión mayor que los tradicionales, al mejorar, o todo lo contrario, la imagen que proyectamos en Internet y en unas redes sociales que llegan a todas partes y están alcance de la mayoría de las personas.

Dada la especificidad de esta unidad, que además forma parte de los nuevos instrumentos para implementar las actuaciones de inserción sociolaboral, se hace una propuesta más completa de los contenidos a desarrollar.

OBJETIVOS

Con esta unidad pretendemos:

- Dar a conocer las posibilidades que se encuentran en la red para trabajar nuestro currículum digital.
- Comprender qué es un currículum vitae (CV), cómo se estructura e iniciar la creación de nuestro CV.
- Comprender y prevenir los riesgos para nuestra inserción sociolaboral de la información, imágenes, etc. que aportamos en la red.

Antes de introducir los contenidos e ir tratando cada uno de los aspectos que se van desarrollar, en función de la persona o grupo y de la dinámica que se haya desarrollado hasta el momento, es conveniente iniciar la actividad conociendo la idea que tienen y las posibilidades que da Internet para la inserción laboral, mediante preguntas tales como:

- ¿Tienes hecho un curriculum vitae?
- ¿Has usado alguna vez, o usas habitualmente, internet y las redes sociales para buscar empleo?
- ¿Conoces las diferentes herramientas para crear tu Currículum 2.0.?
- ¿Has pensado alguna vez en los riesgos que supone el uso de Internet en la búsqueda y mantenimiento de empleo?
- ¿Alguna vez has tenido un problema relacionado con el uso de las redes sociales? ¿Crees que ha perjudicado tu imagen laboral?

CONTENIDOS

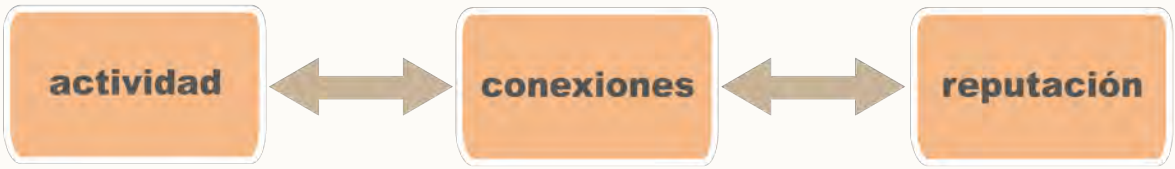
Elaborar nuestro curriculum

A la hora de hacer nuestro currículum 2.0. nos encontramos con amplio abanico de posibilidades, muchas de ellas con características comunes, entre las que encontramos la opción de incluir la información que hemos dado en redes como Facebook, Twitter o LinkedIn, unas redes sociales a través de las cuales también podremos difundir nuestro curriculum.

También debemos de ser conscientes de nuestra marca personal y tener muy presente nuestro curriculum social, la imagen que damos a las empresas a través de las redes sociales.

CURRICULUM SOCIAL

- Recoge información que no aparece en el CV.
- Ayuda al responsable de selección a decidir entre usuarios con currículos similares.
- Es la Huella Digital que dejamos en internet.



Somos lo que hacemos, pero también lo que decimos y compartimos en la red.

No publiques cosas que puedan dañar tu imagen

CONEXIONES: amplia tu círculo de contactos.

REPUTACIÓN: lo que decimos y lo que dicen de nosotros

Contamos con distintas herramientas 2.0.: Facebook, Twitter, LinkedIn, YouTube, Instagram, SlideShare, Pinterest, Google+, web y blog.

- **Crear un Blog:** Blogspot y WordPress son buenas herramienta para la creación de su marca personal y el eje central en torno al cual gira todo lo demás.
- **LinkedIn:** La red social profesional por excelencia al ser mucho más que un CV online. Un consejo: se debe explora especialmente el concepto de los grupos y sus debates profesionales, así como las aplicaciones, las respuestas y la búsqueda avanzada de profesionales y empresas.
- **Twitter:** Es la herramienta más dinámica de todas, una herramienta magnífica para mantener un contacto permanente con una comunidad de seguidores y seguidos,

fuente de ideas, herramienta de difusión de información e infinitas cosas más que serve para potenciar la marca personal.

En un momento como este, es importante distinguirse de los demás, señalando las competencias profesionales que se han desarrollado. Todos tenemos una marca personal, algo que nos diferencia de los demás. Sin quererlo todos desarrollamos nuestra propia marca: con los gestos, la manera de actuar, de vestir, de sentarnos, de escribir… todo influye y desarrolla una huella personal.

Cada vez más, las empresas utilizan las redes sociales para buscar candidatos (LinkedIn, Facebook, Twitter). Por eso es importante saber cómo crear un perfil profesional.

DEBEMOS TENER EN CUENTA

- **Foto de perfil inadecuada:** Fotografías en poses inadecuadas o en momentos inoportunos, pueden ser causa de que los usuarios que miren tu perfil, tengan una mala imagen de ti. Si deseas dar una imagen profesional, es preferible elegir una foto acorde. Otro aspecto que debes considerar es las fotos que circulan por la web, algunas de las cuales quedan indexadas en los buscadores con tu nombre y apellido.

- **Post vergonzosos:** Evita que otra persona te etiquete en una publicación, video o foto vergonzosa. Para ello, configura tu perfil de modo que puedas administrar los post donde te etiquetan, antes de publicarse en tu muro. También puedes configurar los permisos de privacidad para evitar que todos tus contactos puedan ver este tipo de contenidos.

- **Cuida tus contactos:** Algo importante a considerar es que tu imagen está muy ligada a la imagen que presentan tus contactos más cercanos en redes sociales. Por lo que es necesario evitar ser etiquetado en algún comentario incorrecto o en una foto equivocada.

- **Comentarios fuera de lugar:** Aunque algunos comentarios puede resultar graciosos, para ciertos contactos, debes valorar que tanto pueden repercutir en tu imagen como profesional.

- **Exprésate de forma correcta:** Considera que Facebook es una red social, no es lugar adecuado para lamentarte o expresar tu rebeldía. Recuerda que la forma en que escribe una persona puede revelar mucho de su identidad.

ACTIVIDADES

Realiza tu curriculum digital (FA-18)

Se les propondrá a los participantes que realicen su curriculum digital a través de alguno de los recursos que aparecen en la ficha de actividad FA-18.

Redes Sociales y empleo

Los participantes deben conocer las existencia de las diferentes redes sociales profesionales, y como les pueden ayudar a conseguir empleo: Xing, LinkedIn, Viadeo.

Del mismo modo se les enseñará como las redes sociales personales pueden ser utilizadas como nuevos motores de empleo:

https://es-es.facebook.com/InfoJobs

https://es-la.facebook.com/Infoempleo

https://es-es.facebook.com/RandstadEs

Incluso para buscar trabajo en sectores concretos como el de hostelería:

https://www.facebook.com/hosteleo.empleoenhosteleria

https://www.facebook.com/centresdeturisme/

Debilidades, amenazas, fortalezas y oportunidades (FA-19)

Se pedirá a los participantes que respondan a las preguntas que aparecen en la ficha de actividad FA-19 y que plasmen sus cualidades en el cuadro “DAFO” (Debilidades, Amenazas, fortalezas y Oportunidades).

Recursos para encontrar trabajo

Fuente: Entrevista a Juan Merodio en “Para Todos La 2” de TVE, 2013.

https://youtu.be/_u50RUjnABM

También podemos recurrir en estos momentos a programas televisivos como el que emite en estos momentos TV2, de lunes a viernes a partir de las 8/9 hs.

DEBES TENER EN CUENTA

1

NO USES FOTOS DE PERFIL INADECUADAS

2

NO HAGAS COMENTARIOS FUERA DE LUGAR

3

EVITA LOS POST VERGONZOSOS

4

CUIDA TUS CONTACTOS

5

EXPRÉSATE DE FORMA CORRECTA

Cuestionario de autoevaluación **(FA-20)**

El cuestionario que se propone pretende ser un instrumento de evaluación pero también de reflexión personal acerca del trabajo realizado en esta Unidad. Para alcanzar este objetivo, se propondrá a los participantes que realizan los cuestionarios contenidos en la ficha de actividad FA-20.

2.3. La búsqueda de ayuda

Esta unidad no tiene por que plantearse de manera consecutiva respecto a las anteriores. Puede desarrollarse en cualquier momento que se considere oportuno según las necesidades y temas que surjan en la dinámica grupal o en la relación con el profesional. Un aspecto fundamental, que no desarrollamos aquí por razones obvias, es establecer las condiciones para una relación de confianza con el adulto, y por supuesto con el profesional, que verdaderamente posibilite la consulta o solicitud de ayuda por parte de los menores o jóvenes respecto a un posible uso inadecuado de las nuevas tecnologías, o las posibles consecuencias adversas que pudiera estar sufriendo.

OBJETIVOS

Esta unidad puede desarrollarse de manera independiente o como parte de otra/s unidad/es o sesiones determinadas, en función de las personas o del grupo de participantes.

Es primordial transmitir, sobretodo en el caso de los menores, que en determinadas situaciones hay que superar las reservas o resistencias a pedir ayuda a los adultos, sean padres, tutores, educadores, etc., así como que existen determinadas páginas en Internet, que nos pueden ofrecer una importante orientación sobre los pasos a seguir en aquellas situaciones que requieren de ayuda externa, como la de iniciar una actuación para paliar o denunciar una información maliciosa sobre nuestra identidad.

CONTENIDOS

Pedir y dar ayuda

En primer lugar debemos tener presente que para conseguir que el menor o joven pida ayuda -a un adulto- deben existir unas condiciones que lo favorezca (así como un marco, incluso un espacio físico y un tiempo propicio para ello). Para favorecer esta relación positiva con el profesional, debemos partir de la aceptación de la persona -basada en el aprecio y la resonancia empática- y la autenticidad; generando confianza –cumplimiento de compromisos que favorezca el aprendizaje- desde la discreción que implica la confidencialidad, la proyección de expectativas positivas; y, en muchas ocasiones, ayudar al manejo de las emociones y el desarrollo del autocontrol.

En gran medida también estos planteamientos son válidos cuando son los padres los que solicitan esta ayuda. En ambos casos es necesario explorar alternativas y facilitar la búsqueda de soluciones, así como retroalimentar -dar *feedback*- animando a avanzar paso a paso y apoyando los logros.

Páginas especializadas

Existen multitud de organizaciones, entidades y foros que nos pueden llegar a ser útiles, entre otras páginas destacamos las siguientes. Una buena actividad es visitar alguna de ellas, descubriendo juntos sus contenidos y propuestas

- http://www.pantallasamigas.net/ es una iniciativa para fomentar el uso seguro y responsable de las TRICs y la ciudadanía digital enfocado especialmente a la infancia y la adolescencia, para la prevención del *ciberbullying*, el *grooming*, el *sexting*, la *sextorsión* y la protección de la privacidad en las redes sociales. También cuenta con una línea de ayuda directa a niños y adolescentes ante situaciones de peligro en Internet.

- http://www.anar.org. La Fundación ANAR para la promoción y defensa de los derechos de los niños y adolescentes en situaciones de riesgo social y de desamparo, lleva a cabo un servicio de ayuda sobre aspectos psicológicos, sociales y jurídicos tanto a los menores y como a las familias.

- http://www.alia2.org. La Fundación Alia2 también se ocupa especialmente del uso seguro y responsable de la red, de la protección de los derechos de los menores en Internet, asimismo desarrolla una línea de ayuda para niños y adolescentes víctimas de abusos en la Red.

- http://www.deaquinopasas.org de Save the Children ayuda, entre otras cuestiones de interés, en la configuración de privacidad de las principales redes sociales de Internet.

- http://www.padres20.org es una organización dedicada a la defensa de la infancia frente a los problemas de Internet, entre otras cuestiones frente al ciberacoso, la adicción a Internet y al juego *online*. Ofrece también recursos de sensibilización y formación, así como una línea ayuda para la mediación y la asistencia psicológica y jurídica.

- http://e-legales.net. Portal web de referencia e información complementaria para todos los asuntos relacionados con los delitos cometidos por medio de las TRIC, principalmente Internet y telefonía móvil. En él nos dan a conocer algunos conceptos necesarios y para estar al día sobre las últimas noticias relacionadas.

- http://www.chaval.es desarrollada por Red.es, del Ministerio de Industria, Energía y Turismo, aporta numerosos recursos, también didácticos, tanto para la sensibilización de padres, educadores, etc. como de formación.

- http://www.osi.es. Oficina de Seguridad del Internauta, proporciona información y soporte para evitar y resolver los problema de seguridad que surjan en Internet.

- http://www.agpd.es. La Agencia Española de Protección de Datos tiene como objeto velar por el cumplimiento de la legislación sobre protección de datos y controla su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos

- http://www.incibe.es. El Instituto Nacional de Ciberseguridad, sociedad dependiente del (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). Es la entidad de referencia para el desarrollo de la Ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores del Ministerio de Industria, Energía y Turismo.

- http://www.seguridadenlared.org. Asociación de internautas es una asociación de ámbito nacional fundada en 1998 que ofrece información y herramientas para la protección de menores, confianza en la red, seguridad y agujeros en la red (*bugs*), *malware* y *cineware*, etcétera.

- *Guía pedagógica para trabajar la educación en las nuevas tecnologías: uso responsable, preventivo y educativo* (Gobierno Vasco, 2016): Encaminada a que los jóvenes tomen conciencia de la dimensión que ofrece la Web 2.0 (sensibilizar al alumnado), la posibilidades que ofrece y los peligros que podemos encontrarnos si no realizamos un uso responsable de ésta.

Instituciones

Determinas conductas pueden ser constitutivas de delito. En estos casos hay que conocer los grupos especializados tanto de la Policía Nacional como de la Guardia Civil:

- **Policía Nacional** (Brigada de Investigación Tecnológica)
  Correo electrónico (consultas genéricas) delitos.tecnologicos@policia.es
  Correo electrónico (pornografía infantil): denuncias.pornografia.infantil@policia.es
  Teléfonos: 915.822.751 / 752 / 753 / 754 / 755

- **Guardia Civil** (Grupo de Delitos Telemáticos)
  Teléfono: 900.101.062 (Oficina de atención al ciudadano)

ACTIVIDADES

Entre las distintas actividades para el fomento de la búsqueda y petición de ayuda, que necesariamente tendremos que adaptar a la persona o el grupo de participantes, podemos extraerlas de:

- http://www.incibe.es. Guía para usuarios sobre identidad digital y reputación online (INTECO) Guía que analiza los conceptos de identidad digital y reputación online desde el punto de vista de la privacidad y la seguridad. Nos describe situaciones que preocupan a los usuarios, como la suplantación de identidad, las amenazas a la privacidad o los impactos derivados de publicaciones falsas o descontextualizadas. Asimismo, analiza las implicaciones jurídicas de estas categorías de riesgo y se aportan una serie de pautas de actuación.

- http://www.cuidatuimagenonline.com. Recurso educativo online sobre cuestiones relativas al manejo en Internet y con la telefonía móvil de la imagen y la privacidad por parte de niños, niñas y adolescentes.

- http://www.proteccionprivacidad.com. Portal web de sensibilización y formación para la protección de la privacidad y los datos personales en redes sociales y *smartphones*. Aportan también una serie de recursos didácticos.

- http://www.simuladordeprivacidad.com. Recurso que ayuda a entender que la privacidad de uno no depende solamente de uno mismo y la importancia de proteger la privacidad de terceros que aparecen en las imágenes.

SEXTING

CIBERACOSO

GROOMING

SUPLANTACION DE INDENTIDAD

QUIÉN DÓNDE CUÁNDO!!

A ADULTOS

PADRES, MADRES, TUTORES

EDUCADORES

A TRAVÉS DE PAGINAS DE INTERNET

www.pantallas amigas.net
www.anar.org
http://e-legales.net
www.chaval.es ...

Nos ayudan a denunciar una actuación maliciosa

Nos ofrecen orientación y pasos a seguir si necesitamos ayuda

CONDICIONES QUE FAVORECEN QUE SE PIDA AYUDA A UN ADULTO

DISPONER DE UN ESPACIO FISICO APROPIADO

TIEMPO PROPICIO

Favorecer una relación positiva, basada en la aceptación y la resonancia empática.

Fomentar una relación de confianza, con compromiso y discrección

Prevenir y Evitar

3

módulo

INTRODUCCIÓN

El tercero y último módulo se enfoca a conocer, identificar y aprender a protegerse de los riesgos existentes en el uso de las TRICs y las redes sociales digitales, así como evitar y en su caso desistir de un posible mal uso, desde la perspectiva de la responsabilidad personal y el autocontrol.

COMPETENCIAS

Además de las competencias recogidas en el Módulo I (Conocer) consideramos que ahora debemos contemplar nuevas competencias como:

- Comunicación y expresión a través de conceptos y términos relacionados con gestión de la privacidad, identidad digital y huella digital. Incluyendo el uso del lenguaje para hacer un buen uso de datos e información personal propios y de terceros.

- Gestión de la información y datos personales en la Red, preservando su privacidad, así como con la información y datos personales procedentes de terceros.

- Para configurar la privacidad, saber evitar y saber protegerse de los riesgos y no contribuir activa o pasivamente con conductas de manipulación de la información o que produzcan un daño a la identidad digital de otros…

- De conocimiento y asunción de las consecuencias legales y penales del mal uso de la información, acoso, suplantación de identidad…en Internet.

Asimismo, las competencias relacionadas con:

- Habilidades de interacción a través de diversos dispositivos y aplicaciones digitales, con el objetivo de entender cómo se distribuye, presenta y gestiona la comunicación digital, siendo crítico con la información que encuentre sobre la vulneración de la privacidad y la falta de protección de datos de carácter personal.

- De competencia social y ciudadana: reflexión sobre la realidad social en la que vivimos, empleando el juicio ético basado en valores y buenas prácticas.

- Competencia de autonomía e iniciativa personal: capacidad para desenvolverse adecuadamente y de forma independiente para actuar frente a los riesgos provocados por una inadecuada gestión de la privacidad.

CONTENIDOS

Responsabilidad en el uso de las TRICs

Como señalábamos al inicio de este documento, pensamos que el tratamiento que debemos dar, tanto al planteamiento y programación de las actividades como a su implementación, debe basarse principalmente en la educación mediante la práctica, así como con el fortalecimiento

y el refuerzo del uso adecuado de las TRICs con la perspectiva de favorecer unas relaciones adecuadas en las redes sociales digitales. Para ello debemos transmitir también los marcos reguladores de la convivencia para unas relaciones sociales respetuosas. En este sentido, señalábamos en apartados iniciales de este documento los deberes referidos a distintos ámbitos[8].

Estos deberes, en cuanto al ámbito escolar se concretan en evitar "*situaciones de conflicto y acoso escolar en cualquiera de sus formas, incluyendo el ciberacoso*". El fenómeno del acoso a través de Internet y sus medios hacen referencia al *ciberbullying*, *grooming* y *sexting*, que tratamos en este documento, pero también al acoso realizado sobre los profesores, conocido como ciberbaiting. Desde una perspectiva de la responsabilidad, nuestra actuación debe enfocarse hacia fomentar el establecimiento de relaciones sociales basadas en "*Respetar la dignidad, integridad e intimidad de todas las personas con las que se relacionen con independencia de su edad, nacionalidad, origen racial o étnico, religión, sexo, orientación e identidad sexual, discapacidad, características físicas o sociales o pertenencia a determinados grupos sociales, o cualquier otra circunstancia personal o social.*"

No debemos olvidar que estos deberes son también para garantizar sus derechos, como reconoce expresamente la Constitución Española de 1978, cuando en su artículo 18 de los Derechos y Libertades fundamentales, y más en concreto el punto 4 se establece, en alusión directa con el tema de las TRICs, que: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*"

El derecho a la privacidad está amparado por normas internacionales, como la Declaración Universal de los Derechos Humanos en cuyo art. 12 se recoge que "*Nadie será objeto de inferencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación*". El Convenio Europeo de Derechos Humanos también se ocupa en el artículo 8 sobre el Derecho al respeto a la vida privada y familiar "*1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*".

Por otro lado, en función de las personas, el grupo de participantes y la dinámica establecida puede ser conveniente tratar las consecuencias de la vulneración de estos derechos, que pueden llegar a ser muy lesivas, como la humillación y el ensañamiento público que pudiera tener afecciones psicológicas, e incluso riesgos físicos propiciados por la geolocalización que permiten determinados documentos subidos a la Red.

Además de la búsqueda de ayuda cuando sea necesario, cuestión que se aborda en una unidad específica de este documento de trabajo, es conveniente el tratamiento de las posibles denuncias de estas situaciones. En primer lugar, promoviendo un papel activo que evite una posible colaboración, tanto directa como indirectamente, con las situaciones de acoso en general; pero también enseñando a superar aquellas barreras, como el miedo, la vergüenza, el temor a no ser escuchados o ser creídos, a que la denuncia no servirá de nada…

(8) Según establece la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y adolescencia.

Internet es una gran herramienta, pero tiene sus riesgos, la denuncia de acosos o abusos, servirá para parar la agresión pero también para prevenir otras posibles a nosotros mismos o a otras personas. Hay un primer nivel de actuación, a través de la propia denuncia de la situación a los responsables de la aplicación en donde se produce, y en función de la gravedad o la posible constitución de un delito la denuncia tendrá que interponerse ante las Fuerzas y Cuerpos de Seguridad del Estado: Policía (https://denuncias.policia.es/OVD/) o Guardia Civil (https://gdt.guardiacivil.es/webgdt/pinformar.php)

Consecuencias legales

Junto al daño producido por la conducta infractora, debemos contemplar por otro lado las consecuencias civiles y también penales para el infractor, sean las establecidas en el Código Penal para los adultos o en la Ley Orgánica Reguladora de la Responsabilidad Penal para los Menores que tengan entre 14 y 17 años de edad, que pudiera conllevar incluso medidas de internamiento (privativas de libertad). En el caso de los menores de 14 años, que son inimputables, pueden tener otras respuestas administrativas, además de consecuencias en cuanto a la responsabilidad civil de los padres o tutores por los perjuicios causados por la conducta del menor.

Los tipos de delitos que puede llevarse a cabo a través de Internet, tanto por los menores como por los adultos, no sólo son los relativos a la intromisión en la intimidad, también pueden ser de incitación al odio y a la violencia, delitos de odio, control de la propiedad intelectual e industrial…Entre otras actividades delictivas encontramos:[9]

- *"Delitos de amenazas: cuando se amenaza a una persona o a alguien de su familia o con el que esté íntimamente relacionado con causarle un mal, constituya delito o no, por ejemplo, de revelar o difundir hechos referentes a la vida privada del amenazado o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés. Puede implicar una pena de privación de libertad que oscila entre los tres meses y los cinco años, dependiendo de las circunstancias de la amenaza.*

- *Delitos de acoso (coacciones). El artículo 172 ter del Código Penal castiga con prisión de tres meses a dos años o multa[10] de seis a veinticuatro meses al que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, de manera que altere gravemente el desarrollo de su vida cotidiana, entre otras las siguientes acciones:*

    - *La vigilancia, la persecución o la búsqueda de cercanía física.*

    - *El establecimiento o el intento de establecer contacto con la persona acosada a través de cualquier medio de comunicación.*

    - *La adquisición de productos o mercancías, o la contratación de servicios, o hacer que terceras personas se pongan en contacto con la persona acosada mediante el uso indebido de sus datos personales.*

    - *Atentar contra su libertad.*

(9) Agencia Española de Protección de Datos, Enséñales a ser legales en internet, Guía para familiares y padres. 2016: http://www.tudecideseninternet.es/agpd1/images/guias/Guia_formadores2016.pdf.

(10) La multa, junto a otras penas como las privativas de libertad, es una sanción pecuniaria establecida en el Código Penal para delitos menos graves. Debe contemplar una duración, número de cuotas diarias, semanal o mensual, y una cuantía económica de las mismas.

Cuando la víctima sea una persona especialmente vulnerable por razón de edad, enfermedad o situación se impondrá la pena de prisión de seis meses a dos años.

- *Delito contra la integridad moral: el artículo 173.1, párrafo primero, del CP: el que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.*

- *Delito de calumnias: achacar a una persona la comisión de un delito, sabiendo que no es cierto. Está castigado con pena de prisión de seis meses a dos años o multa de doce a veinticuatro meses si es con publicidad y, en otro caso multa, de seis a doce meses e indemnización por daños y perjuicios.*

- *Delito de injurias: consiste en humillar, insultar, ofender a un tercero de manera que lesione su dignidad, menoscabando su fama o atentando contra la propia estima. Se castiga con multa de tres a siete meses y de seis a catorce si se realiza con publicidad.*

- *Delitos de descubrimiento y revelación de secretos: Se castiga con la pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Pena que se impondrá en su mitad superior cuando la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección o los hechos se hubieran cometido con una finalidad lucrativa (sexting).*

- *Delito de inducción al suicidio, castigado con pena de prisión de cuatro a ocho años."*

Además, según el art. 183 ter del Código Penal[11] son conductas delictivas: *"1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189 (abusos y agresiones sexuales a menores de 16 años), siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. 2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años"*.

Para finalizar, debemos tener presente que existen materiales pedagógicos y guías especialmente elaboradas para su uso con menores que nos pueden ayudar a complementar

(11) L.O. 1/2015, de 30 de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 31 marzo).

las actividades que proponemos aquí, y que en todo caso es conveniente consultar previamente, también por ser recursos didácticos muy válidos para nuestra actividad como los proporcionados por la Agencia Española de Protección de Datos: *Sé Legal en Internet, guía para jóvenes:* http://www.tudecideseninternet.es/agpd1/images/guias/Guia_menores2016.pdf

CUESTIONARIO INICIAL **(FA-21)**

Con el objetivo de conocer los conocimientos previos y las prácticas más comunes utilizaremos la ficha de actividad FA-21.

3.1. Robo de identidad

Uno de los riesgos existentes en Internet es la suplantación de nuestra identidad digital, que se produce cuando otra persona accede a una cuenta que tengamos en una red social. En el momento que esta persona interactúa con nuestra identidad o perfil, se está produciendo una usurpación de identidad que generalmente tiene como fin obtener algún beneficio, por ejemplo económico cuando se accede a cuentas bancarias, pero también con otras finalidades como cuando se produce esta usurpación en video juegos.

OBJETIVOS

- Saber qué es y cómo se produce el robo, suplantación y usurpación de identidad, y sus consecuencias.
- Aprender las principales estrategias de prevención ante la suplantación de la identidad.
- Adquirir pautas de protección ante un caso de suplantación de la identidad.

CONTENIDOS

Definición y descripción de la suplantación de identidad

La suplantación de identidad consiste en el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio. Normalmente este beneficio genera un perjuicio a la persona que sufre dicha suplantación de identidad. Debemos distinguir entre suplantación de identidad y usurpación de la identidad.

Motivaciones para la suplantación de identidad

La suplantación de identidad en los menores o jóvenes se produce principalmente por mera diversión, para “burlarse” de un compañero/a o con motivos de venganza. Normalmente la excusa para engañar en los juegos online se encuentra relacionada con fallos de seguridad en la plataforma del juego o en la cuenta de los usuarios.

Servicios y Técnicas más comunes de suplantación de identidad

Bancos y cajas, pasarelas de pago *online* (PayPal, MasterCard, Visa, etc.), redes sociales (Facebook, Twitter, .Tuenti, Instagram, LinkedIn, etc.), páginas de compra/venta y subastas (Amazon, eBay, etc.), juegos *online*, soporte técnico y de ayuda (*helpdesk*) de empresas y servicios (Outlook, Yahoo!, Apple, Gmail, etc.), servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.), *phishing* a servicios o empresas públicas, *phishing* a servicios de mensajería, falsas ofertas de empleo…

Indicios para detectar la posibilidad de que hayamos sufrido suplantación de identidad:

- Accesos o usos anómalos de las cuentas. Por ejemplo, si nuestros contactos reciben mensajes de nuestra cuenta sin que nosotros los hubiéramos enviado.
- Inminente desactivación de algún servicio que tuviéramos activado sin que hayamos procedido a ello.
- Cambios en el estado de los juegos online sin que los haya realizado por sí mismo.

RECOMENDACIONES

1. Nunca des tus contraseñas a NADIE. Y evita que cuando las introduzcas te miren.
2. Utiliza contraseñas seguras.
3. Gestiona correctamente las sesiones (sobre todo en ordenadores públicos):
   - No almacenes las contraseñas.
   - Cierra las sesiones.
4. Si descubres que han entrado a tu cuenta, cambia rápido la contraseña. Si ya no puedes: denúncialo.
5. Si alguien se hace pasar por ti creando una cuenta similar a la tuya: denúncialo.

ROBO DE IDENTIDAD

SUPLANTACIÓN DE IDENTIDAD

Uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio. Normalmente este beneficio genera un perjuicio a la persona que sufre dicha suplantación de identidad

(por ejemplo, acceder sin consentimiento a la cuenta de una red social)

USURPACIÓN DE IDENTIDAD

Una vez suplantada la identidad se empieza a interactuar como si realmente fuera propietario de los derechos y facultades (por ejemplo, realizar comentarios o subir fotografías desde la cuenta suplantada).

POR QUÉ SE HACE

BURLA O VENGANZA

COMO DETECTAR LA SUPLANTACIÓN

1. Accesos o usos anómalos de las cuentas. Por ejemplo, si nuestros contactos reciben mensajes de nuestra cuenta sin que nosotros los hubiéramos enviado.
2. Inminente desactivación de algún servicio que tuvierass activado sin que hayas procedido a ello.
3. Cambios en el estado de los juegos online sin que los hayaS realizado por Tí mismo.

ACTIVIDADES

La fuente de las actividades propuestas es, fundamentamente, la Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Seguridad.

Suplantación de identidad

Podemos iniciar la unidad con el vídeo "Así de fácil es robar tu identidad en internet" (Febelfin y Safeinternetbanking.be, 2013), para continuar con un debate sobre el mismo y una lluvia de ideas sobre qué hacer para evitar que suplanten nuestra identidad por Internet. Aquellas propuestas que sean relevantes para el grupo se escriben en cartulinas y se exponen en un lugar visible del aula.

https://youtu.be/PAvbYdsiNl8

Comentario de noticias reales sobre usurpación de identidad por Internet

Existen múltiples noticias relacionadas con casos de suplantación de la identidad, aportamos algunos ejemplos que pueden ser debatidos en el grupo:

- *Dos años de cárcel por suplantar la identidad de un menor en Tuenti*. Diario El País, 10 de febrero de 2015.
- Kleinman, Z. *El curioso caso de la ladrona de perfiles*. BBC, 8 de marzo de 2015.
- *Un año de cárcel y multa por entrar en el correo electrónico de una conocida*. El Comercio.es, 11 de diciembre de 2011.
- Martín, A. *Dos chicas multadas con 12.400 euros por crear un perfil falso de otra en Tuenti*. Diario El País, 30 de mayo de 2011.
- *Detenida una joven de 18 años por usurpar el perfil de otra persona en una red social*. Cadena Ser, 18 de noviembre de 2010.

Qué hacer en caso de detección de la suplantación de identidad.

Vídeo *¿Qué se hace ante una suplantación de identidad en las Redes Sociales?* (Legálitas Abogados, 2014).

Otras propuestas

Fuente: Noelia Ramírez. *8 películas que muestran el "lado oscuro" de las redes sociales.* Diario El Pais, 17 de julio 2015.

8 películas que muestran el "*lado oscuro*" de las redes sociales:

- *Eliminado*. Dirigida por Levan Gabriadze, 2014.
- *Puedes confiar en mí (Trust)*. Dirigida por David Schwimmer, 2010.
- *Desconexión (Disconnect)*. Dirigida por Henry Alex Rubin, 2012.
- *Catfish*. Dirigida por Henry Joost, Ariel Schulman, 2010.
- *Cyberbully*. Dirigida por Ben Chanan, David Lobatto, 2015.
- *Uwantme2killhim?* Dirigida por Andrew Douglas, 2013.
- *Hard Candy*. Dirigida por David Slade, 2005.
- *Hombres, mujeres y niños*. Dirigida por Jason Reitman, 2014.

3.2. Contraseñas, protección de la privacidad y reputación *online*

Está unidad está pensada para el tratamiento de temas relativos a la configuración de la privacidad en Facebook, Instagram, Twitter o Whatsapp fundamentalmente, y gran medida se fundamenta en las propuestas y materiales de la citada Oficina de Seguridad del Internauta. En su planificación y desarrollo hay que tener presente la posibilidad de que la persona o el grupo hayan participado anteriormente en las actividades de la Unidad sobre Uso responsable de las TRICs, especialmente en lo referente a contraseñas.

OBJETIVOS

- Conocer la importancia de proteger nuestra privacidad.
- Adquirir conocimientos sobre la privacidad y la identidad digital en Internet.
- Comprender las características y las consecuencias del riesgo asociado a una mala gestión de la privacidad y gestión de la identidad en la red.
- Aprender a utilizar los recursos y herramientas necesarias para poder proteger nuestra privacidad y reputación on-line mediante un uso seguro de Internet.

CONTENIDOS

Privacidad

"*Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*". La privacidad en Internet se refiere al control de la información personal que posee un usuario que se conecta a la Red, interactuando por medio de diversos servicios en línea con los que intercambia datos durante la navegación. Son datos personales: el DNI, una fotografía, la dirección, el número de teléfono, la voz...

Todo ello influye de forma directa y negativa en la creación de nuestra identidad digital y reputación personal. Por ello, se debe insistir en la importancia que tiene «pensar antes de publicar» y en las posibles consecuencias que pueda tener en un nuestro futuro.

Elementos para la gestión de la privacidad

ELEMENTOS PARA LA GESTIÓN DE LA PRIVACIDAD
Confidencialidad: Implica que la información tan sólo podrá ser accesible a aquellas entidades o personas autorizadas.

Integridad: La información que aparece en la red sólo puede ser modificada por las entidades o personas autorizadas.

Autenticación: Es necesario establecer mecanismos de verificación para poder controlar que el usuario sea realmente quién dice ser.

Privacidad y anonimato de la identidad digital: Existen espacios donde poder actuar bajo un *nick* y otros donde se requieren de una identificación real del usuario. Es importante valorar, teniendo en cuenta el entorno donde se encuentre la persona, qué forma de identificación se va a usar: anónima o personal, ya que esto influirá en la identidad digital y en la interacción con el resto de usuarios de la Red.

Privacidad de nuestros datos personales: Antes de facilitar los datos o dejar abierto nuestro perfil, se debería valorar quién va a tener acceso a ellos y cuál podría ser el uso que se hiciera de los mismos.

Huella digital

La huella digital en Internet es el rastro que se deja en aquellos lugares por los que navega y se va dejando información. «*En Internet, las huellas que se dejan son difíciles de borrar*». Cuidar nuestra imagen o reputación en Internet es cuidar nuestra imagen en nuestra vida real, ya que Internet no es más que una extensión misma de la realidad.

La reputación *online*

Entendida como la influencia, el prestigio y la consideración de una persona en Internet. En el caso de los adolescentes la reputación *online* es muy importante, sobre todo si se quiere ser popular o "respetado", para ello se puede hacer comentarios o subir fotos para llamar la atención, que se hable de uno… en un foro que difícilmente es controlable ya que depende de la opinión de otros y en consecuencia puede ser fuente de conflicto.

Riesgos por la vulneración de la privacidad en los menores

Cuando se realiza un registro en una web o red social digital, se ofrece la posibilidad de agregar mucha información sobre la persona, sus gustos, preferencias… y se debe recordar que cualquier información que se *cuelgue* en Internet permanecerá mucho tiempo, a veces para siempre, lo que se ha llamado la huella digital, y si no se configura bien la privacidad, puede haber consecuencias a causa de comentarios o fotografías comprometidas.

PRINCIPALES PELIGROS O RIESGOS PARA LOS MENORES

- Publicación por parte del menor de información sensible (imágenes, videos, comentarios) que conlleven un impacto negativo en la construcción de su identidad y reputación. La difusión de imágenes propias de carácter sexual se conoce como *sexting*.

- Uso malintencionado de su información privada por parte de terceros: o menores que utilizan imágenes, videos, confesiones…con la intención de hacer daño y atormentar a otros menores, lo que se conoce como *ciberbullying*.
- Adultos que buscan información (gustos, preferencias, hábitos de uso) para establecer lazos de amistad con menores con una finalidad sexual, lo que se denomina como *grooming*. Puede implicar el uso de información sensible (confesiones, imágenes subidas de tono) para extorsionarles y que accedan a sus peticiones.
- Suplantación de la identidad de los menores para cometer fraudes. También puede estar vinculado con los riesgos antes descritos (*ciberbullying* y *grooming*).
- Uso comercial de la información personal.

Configurar la privacidad

Normalmente, en la mayoría de blogs, redes sociales, webs, etc., se debe indicar un perfil de protección de la privacidad, es decir, con quien comparto y quien puede ver mi información. La configuración de la privacidad puede resultar complicada y engorrosa, todo dependerá de la Web y de los parámetros que se quieran o puedan configurar, aunque hay dos perfiles que se encontrarán en casi toda:

- Un perfil público, toda la información es visible por todo usuario.
- Un perfil privado, sólo comparte la información con las personas que tienen permiso para ello.

Se pueden utilizar dos páginas de referencia para obtener información sobre como configurar la privacidad en cada una de las redes sociales más utilizadas en España:

- Página de la Oficina de Seguridad del Internauta.
- Página publicada por Save the Children bajo el nombre "*De aquí no pasas*".

ALGUNOS CONSEJOS A TENER EN CUENTA PARA PROTEGER TU PRIVACIDAD

- Seleccionar los contactos.
- Revisar los ajustes periódicamente.

- Examinar lo que otros publican.
- Proteger la información delicada.
- Controlar desde dónde y cómo conectarse.
- No entrar en páginas Web sospechosas.
- No facilitar las contraseñas a nadie y modificarlas periódicamente.
- Controlar el uso de la Webcams y cuando no estén en uso, taparlas o quitarlas pues pueden ser encendidas por control remoto sin darnos cuenta.
- No compartir libremente los datos de geolocalización pues todos sabrán dónde estás y dónde no.

Características de las contraseñas seguras

RECOMENDACIONES PARA UNA BUENA GESTIÓN DE NUESTRAS CLAVES

- No compartas tu clave con otras personas. Una vez la compartes, deja de ser secreta.
- Utiliza una clave robusta y segura. Hay muchas formas de tener una clave robusta fácil de memorizar.
- No utilices la misma clave en diferentes servicios. Siempre claves diferentes para servicios diferentes.
- Cuidado con las preguntas de seguridad. Si las utilizas, que sólo tú y nadie más sepa las respuestas.
- Utiliza gestores de contraseñas. Si te cuesta memorizar o utilizas muchos servicios, utiliza uno de estos programas. Son muy útiles y sencillos de usar.

ACTIVIDADES

El día que Carlos descubrió el testamento de su abuelo (FA-22 y FA-23)

Lectura reflexiva y posterior comentario de texto de la narración contenida en la ficha de actividad FA-22.

Posteriormente, se trabajará con los participantes el resumen de las medidas de seguridad a adoptar para establecer una contraseña segura, contenidad en la ficha de actividad FA-23 (Oficina de Seguridad del Internauta (OSI)). Pueden darse copias en papel o utilizar un proyector para facilitar el repaso de contraseñas errónea.

Configura tu nivel de privacidad

Una actividad práctica y muy útil es configurar la privacidad en distintas redes como Facebook, Instagram, Twitter, WhatsApp…

Complementariamente

En función de los tiempos y necesidades del grupo, se puede plantear la exposición o lectura para su análisis, debate y reflexión de noticias de actualidad que tengan que ver con casos reales y conocidos de robo y mal uso de contraseñas…También, como en el resto de las unidades, exponer y trabajar una infografía como la que proponemos a continuación, o bien, a partir de la misma, elaborar una propia del grupo de trabajo.

CUIDA TU PRIVACIDAD

- Reputación online
- Redes Sociales
- Huella digital

CONOCE LOS RIESGOS

- SEXTING
- CIBERBULLYING
- GROOMING
- SUPLANTACION DE INDENTIDAD

PROTÉGETE

PERFIL PÚBLICO

CONFIGURACIÓN DE PRIVACIDAD

PERFIL PRIVADO

CONTRASEÑAS Y CLAVES

Contraseñas secretas, seguras, robustas y únicas

Preguntas de Seguridad.

Utiliza Gestores de contraseñas

3.3. Ciberacoso

El ciberacoso es un fenómeno que puede producirse de distintas maneras, con esta unidad pretendemos conocer y ser conscientes de sus distintas formas, sobre todo cuando se produce entre adolescentes, tanto para prevenirlas como para evitarlas, sobre todo estando alertas con una posible participación, incluso cuando esta se produce de manera pasiva cuando somos testigos de las mismas y están afectando a otras personas de nuestro entorno.

OBJETIVOS

- Aprender qué es el ciberacoso y las consecuencias que sufren las personas acosadas.
- Conocer los comportamientos activos y pasivos que producen ciberacoso y sus consecuencias.
- Aprender a prevenir los riesgos y a evitar participar en el ciberacoso.

CONTENIDOS

"*El ciberacoso es un fenómeno que puede producirse de distintas maneras. Con esta unidad pretendemos conocer y ser conscientes de sus distintas formas, sobre todo cuando se produce entre adolescentes, tanto para prevenirlas como para evitarlas. Estando alerta ante una posible participación, incluso cuando se produce de manera pasiva, cuando somos testigos de las mismas y están afectando a otras personas de nuestro entorno.*"[12]

Algunas de sus manifestaciones características son: colgar en Internet una imagen comprometida (real o efectuada mediante fotomontajes), datos delicados, cosas que pueden perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones; dar de alta, con foto incluida, a la víctima en un web donde se trata de votar a la persona más fea, a la menos inteligente… y cargarle de puntos o votos para que aparezca en los primeros lugares; crear un perfil o espacio falso en nombre de la víctima; dejar comentarios ofensivos en foros o participar agresivamente en chats haciéndose pasar por la víctima; hacer circular rumores en los cuales a la víctima se le suponga un comportamiento reprochable, ofensivo o desleal; enviar menajes amenazantes por e-mail o SMS, perseguir y acechar a la víctima en los lugares de Internet en los se relaciona de manera habitual provocándole una sensación de completo agobio….

(12) Matos, A & Cuevas, V. (2014). Identidad Digital y Redes Sociales con menores. 1 de marzo de 2016, de Sitio web: https://sites.google.com/site/talleridi1/

UN DECÁLOGO SOBRE ALGUNAS LAS FORMAS EN LAS QUE SE PUEDE EXPRESAR EL CIBERACOSO (sin pretender ser exhaustivos)

- Distribuir en Internet una imagen (*sexting*) o datos comprometidos de contenido sexual (reales o falsos)
- Dar de alta a la víctima en un sitio web donde puede estigmatizarse o ridiculizar a una persona.
- Crear un perfil falso en nombre de la víctima para, por ejemplo, realizar demandas u ofertas sexuales.
- Usurpar la identidad de la víctima para, por ejemplo, hacer comentarios ofensivos sobre terceros.
- Divulgar por Internet grabaciones con móviles en las que se intimida, agrede, persigue, etcétera, a una persona.
- Dar de alta el email de la víctima para convertirla en blanco de spam, contactos con desconocidos, etc.
- Acceder digitalmente al ordenador de la víctima para controlar sus comunicaciones con terceros.
- Hacer correr en las redes sociales rumores sobre un comportamiento reprochable atribuido a la víctima.
- Perseguir e incomodar a la víctima en los espacios de Internet que frecuenta de manera habitual.
- Presentarse en un perfil falso ante la víctima con el fin de concertar un encuentro digital para llevar a cabo algún tipo de chantaje *online* como, por ejemplo, *grooming* (acoso sexual a menores)

En cuanto a las pautas y recomendaciones a seguir podemos utilizar las propuestas por la Asociación Protégeles:

- 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.

ACTIVIDADES

Cuestionario ciberacoso (FA-24)

Con el objetivo de conocer los conocimientos previos y las prácticas más comunes de los participantes, se completará la ficha de actividad FA-24 de forma individual o en grupo.

Dinámica de inicio de actividad

Para esta dinámica es conveniente que los participantes estén de pie y se puedan mover por el aula. El responsable 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 responsable de la actividad realizará una explicación sobre las mismas. Si es necesario se aclararán conceptos.

El *ciberbullying* es un delito	No es una broma ni algo gracioso. Se trata de un delito que puede tener consecuencias legales para quien lo realiza.	**VERDADERO**

Si alguien te está molestando o insultando, puedes bloquear al remitente como no deseado y no recibirás más mensajes	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.	**VERDADERO**
Si el *ciberbullying* se realiza de forma anónima es imposible saber quien lo realiza.	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 envíen desde ciber-cafés o los ordenadores del instituto, sigue resultando fácil reconocer a la persona que está detrás, puesto que siempre se piden datos reales para utilizar los ordenadores públicos.	**FALSO**
Si alguien te insulta o amenaza por Internet, lo mejor que haces es contestarle o borrar los mensajes.	Pautas recomendadas por la Asociación Protégeles	**FALSO**

El *ciberbullying* termina con el paso del tiempo, si denuncias será peor.	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.	**FALSO**
El *ciberbuying* tiene consecuencias para el agresor y la victima	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, hay estudios que demuestran que el agresor también puede sufrir ansiedad, trastornos de conducta y baja autoestima.	**VERDADERO**

No lo digas por Internet

Visionado y posterior comentario del vídeo *No lo digas en Internet* (Inetsegura, 2008).

Amanda Todd's story

Visionado y posterior comentario de este vídeo sobre un caso real de *ciberbullying:*

https://youtu.be/NaVoR5IDIsU

Create No Hate

Visionado y posterios comentario del vídeo *Create No Hate* (Luke Culhane, 2016).

Tras el visionado se puede realizar la siguiente actividad. Formados dos grupos diferenciados según los roles de víctima y de acosador, cada uno de ellos con funciones distintas. Víctima: debatir sobre las emociones de la víctima y análisis de los motivos por los que se ha dejado engañar por el acosador; Acosador: pensar en estrategias que se le ocurrirían a un acosador imaginario para contactar con la víctima.

Noticias reales sobre *ciberbullying*

- Gosálvez, P. *Condenadas dos menores por acosar a otra que se suicidó*. Diario El País, 30 de diciembre de 2014.
- Simón, P. *Agresión escolar y salto al vacio*. Diario El Mudo, 23 de marzo de 2014.
- Martín, M. *Condenadas a 550 euros por llamar puta y gorda a una chica en Tuenti*. Diario Sur, 30 de mayo del 2012.

Algunas propuestas para la actividades de generalización **(FA-25)**

Con el apoyo del la ficha de actividad FA-25, trabajar en grupo los consejos y formas de actuar para evitar ser víctima de *ciberbulling.*

Cómo pasar de "espectador" a luchar contra el *ciberbullying* **(FA-26)**

Fuente: Curso "Seguridad TIC y menores de edad para educadores" de Red.es, Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). Más información.

Un "espectador" es alguien que ve lo que está ocurriendo entre acosador y víctima, pero que no participa directamente en el acoso. El papel de los "espectadores" es clave en el desenlace de la situación: pueden animar al acosador para que continúe con sus abusos; no implicarse en la acción, mirar para otro lado y, por lo tanto, consentirla; o ayudar a la víctima a salir de la situación.

En la ficha de actividad FA-26 se dan algunas pautas, para trabajar con el grupo de participantes, para que estos pasen de espectadores a luchar activamente contra el ciberacoso.

CIBERBULLYING

MENSAJES INTIMIDATORIOS E INSULTANTES

USURPACIÓN DE IDENTIDAD

HACER CIRCULAR IMÁGENES, COMENTARIOS

COLGAR IMÁGENES COMPROMETIDAS O MANIPULADAS

QUÉ PUEDES HACER

PIDE AYUDA

No respondas a provocaciones

Revisa tu privacidad online

Bloquea remitentes no deseados

Guarda las pruebas del acoso

3.4. *Sexting y sextorsión*

Es frecuente que por falta de atención o muchas otras veces por cierto atrevimiento, subamos fotos personales a las redes sociales digitales que pueden llegar a ser utilizadas por terceras personas con fines ilegítimos, ilícitos e ilegales. Conocer esta realidad y las formas de prevenir sus fatales consecuencias es fundamental para evitar ser acosados o colaborar indirectamente con los acosadores.

OBJETIVOS

- Conocer que es el *sexting* y cuando se produce la *sextorsión*.
- Desarrollar pautas eficaces de protección y saber como actuar.

CONTENIDOS

En la guía del Instituto Nacional de Tecnologías de la Comunicación INTECO[13] sobre la Adolescencia y *Sexting*, encontramos las siguiente definición: el *sexting* consiste en la difusión o publicación de contenidos (principalmente fotografías o videos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico, caracterizando este fenómeno como:

Voluntariedad inicial: por norma general estos contenidos son generados por los protagonistas de los mismos o con su consentimiento. Normalmente se realiza como regalo para su pareja o como herramienta de flirteo. Habitualmente el propio protagonista es el productor de los contenidos y el que da el primer paso para la difusión.
Dispositivos tecnológicos: para la existencia y difusión del *sexting*, es necesaria la utilización de dispositivos tecnológicos, que al facilitar su envío a otras personas también hacen incontrolables su uso y redifusión a partir de ese momento. Hablando tanto de teléfonos móviles como otros dispositivos así como la webcam de los ordenadores.
Lo sexual frente a lo atrevido: en la consideración de una situación de *sexting*, el protagonista posa en situación erótica o sexual. Quedarían fuera del ámbito del sexting, las fotografías que simplemente resultan atrevidas o sugerentes, pero no tienen un contenido sexual explicito. Aunque es difícil diferenciarlas.
La importancia de la edad: no solo pasa en los menores/jóvenes, dentro de los adultos también se produce.

(13) En octubre de 2014 pasó a denominarse Instituto Nacional de Ciberseguridad (INCIBE) y es un organismo dependiente de Red.es y del Ministerio de Industria, Energía y Turismo de España.

Relacionado con el *sexting* se encuentra el *sex-casting*. Con ese término se identifica la grabación de contenidos sexuales a través de la *webcam* y difusión de los mismos por e-mail, redes sociales o cualquier canal que permitan las tecnologías digitales.

La *sextorsión*, inglés como muchos otros términos utilizados en las TRICs, es una forma de chantajear a una persona por medio de una imagen de sí misma que ha compartido a través de Internet mediante *sexting*.

La sextorsión puede ser:[14]

- A menores de edad o a adultos.
- Por medio de imágenes obtenidas mediante webcam, email, mensajería instantánea, teléfonos u otros dispositivos móviles: es decir, por todos los medios que sirven para realizar sexting.
- Por medio de imágenes obtenidas en el contexto de una relación sentimental.
- Con objeto de un abuso sexual, una explotación pornográfica para uso privado, para redes pedófilas o comercial, una extorsión económica o cualquier otro tipo de coacción.
- Puntual o continuada.
- Realizada por conocidos, anteriores relaciones o personas desconocidas.

En consecuencia hay que reforzar las decisiones y actitudes que eviten ser víctima o colaborador de las mismas:

Conocer el nivel de seguridad y privacidad de los dispositivos y aplicarlo de manera responsable. La seguridad y la privacidad en las nuevas tecnologías a veces pueden ser vulneradas de las formas más simples. La pérdida del teléfono móvil (si no está protegido) puede poner a disposición pública nuestra información, pero también existen vulnerabilidades e infracciones con virus informáticos. Si no se está seguro de no poder proteger información sensible, mejor no guardarla en el dispositivo.
No ceder ante la presión ni el chantaje. Si se reciben solicitudes insistentes para que proporcionemos una imagen por parte de una persona querida o de confianza o se sufren amenazas de alguien desconocido, la única decisión acertada es no ceder a las peticiones bajo ningún concepto. Si se trata de alguien malintencionado, habría que solicitar el apoyo de un adulto responsable.
No ser partícipe del *sexting*: ni creándolo, ni reenviándolo, ni fomentándolo. Cuando se reenvía a otras personas una imagen de sexting, se está participando activamente en el juego. Se recomienda al menor/joven que no participen ni en su creación ni en su difusión y que elimine de su terminal las imágenes de este estilo que le pueden llegar para evitar riesgos asociados.

(14) Fuente: Pantallas Amigas

ACTIVIDADES

Cuestionario *sexting* y *sextorsión* (FA-27)

Al objeto de conocer los conocimientos previos y las prácticas más comunes utilizaremos la ficha de actividad FA-27, de forma individual o en grupo.

Riesgos y implicaciones del *sexting*

Explicar y debatir sobre los riesgos y las implicaciones asociadas al *sexting* con la ayuda del visionado de los siguientes vídeos:

- *Qué es sexting*. Protección Online, 2011.
- *No lo produzcas*. Pantallas Amigas, 2009.
- *No lo provoques*. Pantallas Amigas, 2009.
- *No lo transmitas*. Pantallas Amigas, 2009.

Noticias sobre casos reales

- *En prisión por amenazar por Internet a menores para grabarlas desnudas*. Diario La Vanguardia, 18 de enero de 2011.
- Fernández, M. *«Conecta la 'webcam', desnúdate y métete en la cama»*. Diadio El Correo, 4 de marzo de 2011.
- Tomé, M. J. *Detenido tras captar por internet fotos de 600 menores desnudas, entre ellas varias vascas*. Diadio El Correo, 7 de marzo de 2011.
- Garcés, L. *Alarma por la 'sextorsión'*. Diario Las Provincias, 11 de mayo de 2011.

SEXTING
SEXTORSIÓN

Prevenirlo es cosa de todos

Sex + texting = sexting

Difusión o publicación de imágenes o videos de tipo sexual, producidos por el propio remitente, principalmente a través del teléfono móvil, o por otros dispositivos tecnológicos

«sexting pasivo»
Acto de recibir las imágenes

RIESGOS

Una vez que el contenido es enviado, se pierde el control del mismo

El contenido puede tener difusión pública (grupo de amigos, en el entorno escolar, en páginas web de carácter pornográfico)

Puede ser utilizado como un elemento para extorsionar o chantajear

Tiene repercusiones sociales y emocionales

PREVEN EL CHANTAJE SEXUAL

Antes de enviar: PIENSA
Ninguna app de fotos es 100% segura

Evita tener imagenes privadas en tu dispositivo.
¡CUIDA TU SEGURIDAD!

Puede que esa relación de pareja o de amistad, no sea para toda la vida
Protege tu imagen

No cedas al chantaje.
PIDE AYUDA. NO LO DEJES PASAR

Si reenvias, comentas, das al me gusta... estas fomentando el acoso
Recuerda, la victima sufre

3.5. *Grooming*

Suelen ser los adultos quienes, haciéndose pasar por menor, buscan captar la atención y la confianza de éste para conseguir concesiones en temas de índole sexual. También hay algunos casos protagonizados por menores. Debemos conocer sus formas de proceder y las fases en las que las desarrollan para poder protegernos y en su caso denunciarlas.

OBJETIVOS

- Saber qué es *grooming* o acoso sexual a menores, sus características y posibles manifestaciones.
- Aprender a detectar el *grooming*, las técnicas usadas por los *groomers* y cómo defendernos de ellas.
- Conocer los cauces manejar una situación de *grooming*, las recomendaciones para prevenirlas y las opciones que existen para denunciar un caso de *grooming*.

CONTENIDOS

Para el tratamiento del concepto y los contenidos relacionados con el *grooming* nos basamos en el curso de "Seguridad TIC y menores de edad para educadores" que se enmarca dentro del programa de "Capacitación en materia de Seguridad TIC para padres, madres, tutores y educadores de menores de edad" puesto en marcha por Red.es.

Definición:

Grooming, *Child grooming* o Internet *grooming* se puede definir como «el ciberacoso ejercido deliberadamente por un adulto para establecer una relación y un control emocional sobre un menor con el fin de preparar el terreno para su abuso sexual». Supone el conjunto de técnicas de engaño y persuasión que utiliza un adulto para ganarse la confianza y disminuir las inhibiciones del menor y obtener de él un beneficio de índole sexual, que es la finalidad que persigue (*grooming* es una palabra inglesa que significa "engatusamiento").

Las acciones realizadas pueden comprender delitos de corrupción y prostitución infantil, abusos sexuales, o embaucar al menor para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca dicho menor. Así, el grooming se encuentra muy relacionado con los términos pederastia y pedofilia (que son patologías distintas).

Fases del *grooming*

Se diferencian varios elementos o fases de acoso por las que el groomer consigue hacerse con la confianza del menor y consumar el abuso. El conocimiento de este proceso y su identificación permitirá la detección y por tanto la protección de los menores:

- Fase de amistad: premio o pago, y engaño. Una vez consolidada la relación, lo que al principio eran inofensivas conversaciones sobre temas infantiles o de adolescentes, irán derivando hacia la obtención de datos personales: nombre y apellidos de familiares y amigos, direcciones, teléfonos, direcciones, email, lugar de trabajo, etc.;

- Fase de relación

- Fase de inicio del abuso.

- Fase de abuso y agresiones sexuales.

Modos más utilizados por el groomer para contactar y acosar al menor[15]

Los principales modos que utilizan los acosadores para contactar y acosar a menores son:

Redes sociales: Son un medio en el que el grooming se hace especialmente evidente. Al ser uno de los servicios en Internet más utilizados por los menores, incluso por debajo de las edades legales permitidas, el riesgo de que sean utilizados por los *groomers* para este tipo de acosos y prácticas es alto.
Foros y chat: Son medios abiertos de exposición de información empleados con frecuencia por los ciberacosadores para contactar con las víctimas.
Plataformas de juegos en línea: Los especialistas en FBI advierten a través de su programa IINI (Innocent Images National Inititaive) del aumento del uso de los juegos *online* por los *groomers*.
Teléfono móvil: Es un método más inmediato e íntimo de contacto entre el acosador y su víctima, siendo los servicios más utilizados los de mensajería instantánea tipo Whatsapp.
***Webcam*:** Algunos *groomers* se valen de la *webcam* de los dispositivos que usamos para conectarnos a Internet para practicar el *grooming*. Es importante destacar el uso de la *webcam* tanto para la obtención de material para el chantaje y la extorsión como para la realización de concesiones al acosador.

Decir no, protegerse de manera asertiva

En el documento del curso de Red.es en el que nos basamos fundamentalmente para el planteamiento de esta unidad, así como de partes fundamentales de otras unidades, encontramos también justificación y argumentación suficiente para exponer e incidir en la necesidad de decir “NO” como forma y estrategia más eficaz de evitar estos conflictos.

(15) “Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad” Red.es Ministerio de Industria, Energía y Turismo.

ACTIVIDADES

Cuestionario *grooming* (FA-28)

Al objeto de conocer los conocimientos previos y las prácticas más comunes utilizaremos la ficha de actividad FA-28, de forma individual o en grupo.

Vídeos sobre *grooming*

Siguiendo las propuestas de la web "Identidad Digital y Redes Sociales con Menores". Visionado y debate de los siguientes videos:

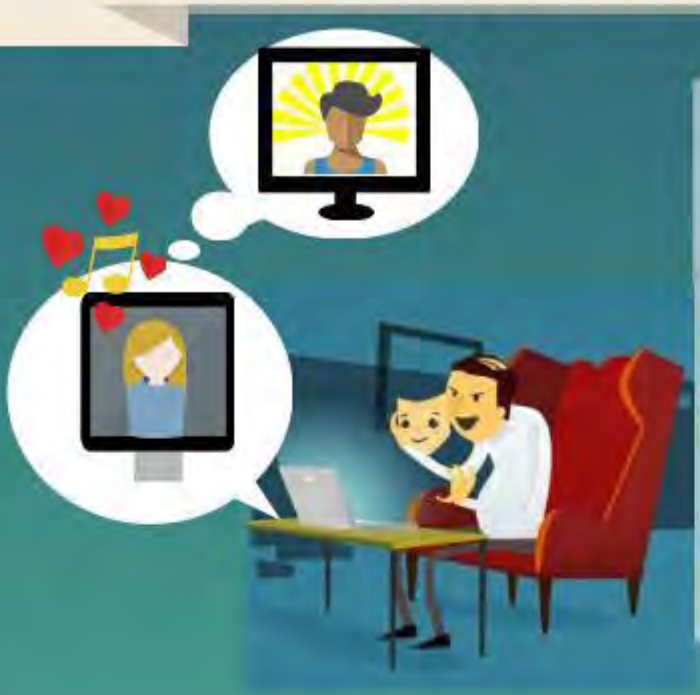
- *El Grooming*. Pantallas Amigas, 2011.
- *Campaña PDI grooming*. Policía de Investigaciones de Chile, 2015.
- *Internet segura grooming*. Ministerio de Educación de Chile, 2013.
- *El peligro de las redes sociales*. The Child Exploitation and Online Protection Center (CEOP), 2013.

Noticias sobre *grooming*

Debate sobre noticias tales como:

- Romero, R. *Detenido en Conil tras violar a una menor en Chiclana*. Diario de Sevilla, 9 de febrero de 2010.
- García, S. *Atrapada en la Red de su agresor*. Diario El Correo, 27 de febrero de 2011.

GROOMING



"Ciberacoso ejercido deliberadamente por un adulto, para establecer una relación y un control emocional sobre un menor, con el fin de preparar el terreno para su abuso sexual"

HACE USO DE:

Intercambio de imágenes
Video chats
Correos electrónicos
Redes Sociales

CONOCE SUS ETAPAS

BUSCANDO A LA VICTIMA

A través de redes sociales y foros

Vulnerabilidad: poca supervisión parental

ENGANCHE

Recaba información sobre gustos personales. Afianza amistad

"tenemos cosas en común, podemos ser amigos...

FIDELIZACIÓN

El acosador se muestra amable con el menor. Intenta estrechar amistad

AISLAMIENTO

El acosador intenta separar al menor de sus padres o de otros amigos..

"Yo nunca haría algo así...

SEDUCCIÓN

El acosador recurre a regalos para generar en el menor un sentimiento de deuda

ACOSO

El acosador está cerca de su objetivo. Recurre a chantajes, amenazas y extorsiones

3.6. *Phishing* y *hoax* (estafas *online*)

Saber qué métodos y procedimientos se usan más frecuentemente, pero sobretodo acostumbrarse a las buenas prácticas, es fundamental para evitar estas nuevas formas de bulos y estafas.

OBJETIVOS

- Conocer los conceptos y consecuencias del *hoax* y *phishing*, y aprender a reconocerlos mediante el estudio de casos reales.
- Conocer y utilizar algunas herramientas y estrategias para afrontar el *phishing* y el *hoax*.
- Entender que la evolución tecnológica es rápida y requiere de una actualización permanente de conceptos, herramientas y estrategias.

CONTENIDOS

Bulos y estafas

Generalmente entendemos por bulo aquella notica falsa que se crea de una manera intencionada; mientras que la estafa es el engaño intencionado que busca obtener un beneficio económico. *Hoax* y el *Phishing* es en el mundo digital lo que bulo y la estafa es en el "analógico".

Hoax es un bulo virtual, que se transmite con nuevas tecnologías y tiene un fin premeditado, que por lo general es malintencionado. Se trata de mensajes con falsas advertencias de virus, o cualquier otro tipo de alerta o cadena (incluidas las solidarias…) o de algún tipo de denuncia, distribuida por las redes generalmente pidiendo se distribuya a nuestros contactos.

Del *phising* diremos que es la estafa llevada a cabo a través de la obtención de los datos personales, como los números de cuentas bancarias, las contraseñas, etc…

Reconocer *Hoax*	Reconocer *Phishing*
• Pide casi siempre el reenvío de la información o posteo en el muro de la red social.	• Mensajes con faltas de ortografía o de redacción por la utilización de programas de traducción automática que construyen frases incoherentes o incomprensibles.

• No suele aparecer una fecha concreta, sólo aproximaciones: la próxima semana, el viernes, etc.. • Apela a sentimientos y por lo general a la responsabilidad del usuario ante el no reenvío: desde consecuencias para terceros como para sí mismo. Son impactantes y sorprendentes. • No proporcionan la fuente de información, ni enlaces válidos, se firman con nombres falsos o usurpando identidades, se presenta lo que tiene apariencia de verdad absoluta a través de un pretendido argumento de autoridad.	• Piden datos innecesarios para la tramitación, como pines de tarjeta o cuenta. • Mensajes con faltas de ortografía o fácilmente detectables, traducidos con programas debido a la construcción de las frases sean incoherentes. • Las web, a través de su url presentan una dirección no reconocida, pero que contiene palabras relacionadas para tratar de engañarnos: la marca, el nombre de la entidad, etc… Muchas veces se omite la “s” en el protocolo http, pudiendo redirigirnos a páginas inseguras o de pago.

Protegerse del *hoax*	**Protegerse del *phishing***
• Buscando siempre la fuente oficial: si hace un llamamiento a una administración, buscar en los elementos oficiales que tenga como cuentas oficiales en redes sociales. • Evitando actuar con visceralidad e inmediatez sin haber comprobado si es cierto. • Googleando el texto. Desde cualquier buscador, podemos comprobar que muchos de los mensajes que recibimos llevan años en las redes sociales. • Verificando en cuentas oficiales de los cuerpos del estado y entidades referidas sobre la información pertinente.	• Entrando siempre desde la url de la entidad, escribiéndola en la barra del navegador e ignorando el enlace del mensaje. • Con programas antivirus y antispam. • Poniéndonos en contacto con la entidad correspondiente ante la duda de fraude. • Verificando en cuentas oficiales de los cuerpos del estado y empresas de seguridad sobre las alertas de phisingactules. • Usando programas antispam, que eviten que nos salten “pantallazos” no deseados. • Descargando aplicaciones de las tiendas oficiales.

• Si hay elementos de ataque personal sensibles a ser un delito, a través de una captura de pantalla y denunciando estos hechos, ante el portal o red social que lo muestra y a los cuerpos de seguridad del Estado.	• Usando las tarjetas de coordenadas, activación y aviso de pago por SMS y revisando las cuentas y pagos frecuentemente. • Y en el caso que pensemos que hemos sufrido este delito, poniéndonos en contacto con la entidad y recopilando pruebas como capturas de pantalla para posterior reenvío ante la tramitación de denuncia a la entidad para que bloquee nuevos pagos y a la autoridad competente.

Fuentes: www.red.es, www.chaval.es, www.policia.es/consejos/internet.html, www.incibe.es, www.elblogdeangelucho.com.

ACTIVIDADES

Cuestionario *phishing* y *hoax* (FA-29)

Como en las unidades anteriores, al objeto de conocer los conocimientos previos y las prácticas más comunes utilizaremos la ficha de actividad FA-29, de forma individual o en grupo.

Jugando a detectives (FA-30)

Los participantes analizarán la captura de pantalla representada en la ficha de actividad FA-30, para determinar si se trata de un posible caso de *phishing*. Se les animará a fijarse en los siguientes detalles:

- Lo sospechoso de los caracteres de la parte de abajo, que aparecen como palabras incompletas o mal escritas.
- Es un claro indicio de que algo no está bien cuando habiendo configurado el navegador para que las aplicaciones aparezcan en un determinado idioma, el texto se presenta en otro distinto al elegido.
- Además, si pudiéramos interactuar con la página nos daríamos cuenta de que la mayoría de elementos son captaciones de pantalla y por tanto una foto de la original.
- Y por último la URL no corresponde al sitio en concreto, por lo que está claro que nos encontramos ante una suplantación de identidad con el fin de robarnos la cuenta.

¿Cuál de las imágenes es real? (FA-31)

Los participantes analizarán las dos imágenes representada en la ficha de actividad FA-31, para determinar si son o no reales.

> *La primera foto es el resultado de un montaje fotográfico muy famoso por la viralidad con la que se transmitió entre usuarios hace ya años y a pesar de ello, continua apareciendo de manera cíclica en los mensajes.*
>
> *La segunda es una imagen retocada también que trata de sugerirnos un caballo. Usa el efecto de la pareidolia para ello pero también es una foto retocada.*

Robando a un labron

Visionado del vídeo *Hackear Facebook en 1 minuto con mi chiringuito* (El Lado del Mal, 2015), sobre ejemplos de páginas web que pretenden *hackear* Facebook y que realmente están estafando a los usuarios.

Buscando mensajes sospechosos (FA-32)

Se propondrá a los participantes que busquen un mensaje digital en su móvil, correo electrónico o muro de red social sospechoso de ser un *hoax*. Despues, deberán buscar información acerca del mismo para contrastar su verosimilitud.

Para ampliar la información y conocimientos

- El Lado del Mal.
- Asociación de Internautas.
- El Blog de Angelucho.
- Capacitación en materia de Seguridad TIC para padres, madres, tutores, educadores de menores de edad.
- Policía Nacional Española.

HOAX

PHISHING

CÓMO RECONOCERLOS

Podría estar firmado con nombre falso

No proporcionan fuente, ni enlaces

No suele aparecer la fecha completa

Suele pedir reenvío de la información, apelando a tus sentimientos de responsabilidad, si no lo haces

Te piden datos innecesarios como pin de cuenta

Lanzan mensajes apremiantes a abrir enlaces o rellenar datos

Contienen mensajes con faltas de ortografía o mal traducidos

La web presenta una dirección no reconocida de url, o no aparece la "s" en el protocolo http, siendo segura htpps

COMO PROTEGERSE

Evitando actuar con visceralidad e inmediatez

Buscando siempre la fuente oficial

GOOGLEANDO EL TEXTO

Verificando en cuentas de la policia y entidades referidas

Si hay elementos de ataque personal: denuncia los hechos usando una captura de pantalla

descarga de tienda oficial

usa antivirus y antispam

accede dede url de la entidad

contacta con la entidad en caso de fraude

Usa tarjetas de coordenadas, aviso de pago por SMS. Revisa cuentas y pagos frecuentemente

Verificando en cuentas de la policia y empresas de seguridad, sobre alertas de phising actuales

3.7. VIRUS Y *MALWARE*

OBJETIVOS

- Conocer que son y como actúan los virus informáticos y software malintencionado, así como los riesgos que implican.
- Aprender a detectar y evitar los virus informáticos y los programas maliciosos.

CONTENIDOS

Virus[16]

Se pueden definir los virus informáticos como programas que buscan alterar el funcionamiento de los dispositivos (ordenadores, tabletas, teléfonos móviles, etc.) y en muchos casos, robar información del usuario. Existen muchos tipos de programas maliciosos (virus, gusanos, troyanos) con diferentes objetivos, todos ellos perjudiciales. Estos programas maliciosos han ido evolucionando, volviéndose más sofisticados, más peligrosos, y más difíciles de detectar y combatir.

También existen muchos programas maliciosos que permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin conocimiento del usuario, como por ejemplo la suplantación de identidad y el envío de correos electrónicos en nombre de la víctima, utilizar el ordenador de la víctima para realizar ataques a otros ordenadores, infectar a otros ordenadores para obtener información de sus usuarios, realizar estafas en las que figurará el ordenador de la víctima (y su IP) como origen del delito, enviar publicidad.

El riesgo es aún mayor en los dispositivos móviles, ya que estos virus pueden escuchar y grabar llamadas realizadas y recibidas en los teléfonos móviles, enviar mensajes SMS Premium que incrementarán el coste de la factura, obtener información de la posición geográfica del dispositivo mediante GPS, hacer grabaciones con la cámara y tomar fotos sin conocimiento del usuario.

Cómo se infectan nuestros dispositivos

Correo electrónico / Dispositivos de almacenamiento externos (memorias USB, discos duros, tarjetas de memoria, etc.) / Descarga de ficheros / Páginas web maliciosas / Redes sociales / Vulnerabilidades / Fallos de seguridad.

Tipos de virus[17]

Existen multitud de clases de virus, cada uno de los cuales puede realizar acciones diferentes.

(16) Fuente: *Monográfico Protección ante virus y fraudes*. Red.es, 2015.
(17) Fuente: *Fauna y flora del mundo de los virus*. Oficina de Seguridad del Internauta (OSI), 2014.

Dos tipos de virus muy comunes son los falsos antivirus y los programas rescate:

- **Antivirus falsos:** son programas visualmente muy parecidos a un antivirus legítimo, aunque tienen el mismo comportamiento que un virus. Su intención es obligar al usuario al pago de la versión completa del programa malicioso y realizar otras acciones con el ordenador. El acceso a nuestro ordenador es a través de banners que advierten de infecciones inexistentes dentro de un archivo.

- **Programas rescate o ransomware:** son virus que impiden utilizar el equipo, mientras no paguemos una cierta cantidad de dinero, bloqueándolo o cifrando nuestra información. Para resultar más convincentes, en ocasiones utilizan los logos de autoridades u organismos oficiales para intimidar a las víctimas. De esta forma nos hacen creer que hemos sido sancionados por alguna acción ilegal. Algunos ejemplos de este tipo de malware: Virus de la Policía y "Virus de Correos".

RECOMENDACIONES PARA EVITAR INFECCIONES DE VIRUS
Mantener actualizado todo el *software* instalado, el sistema operativo, el navegador de Internet y antivirus. Es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
Utilizar cuentas de usuario limitadas. Es aconsejable utilizar un usuario con permisos restringidos que no pueda instalar programas. De ese modo, si se cuela un virus, será más difícil que pueda instalarse. Las cuentas de usuario con permisos de administración sólo deben utilizarse para instalar aplicaciones, o para cambiar la configuración del equipo.
Verificar los enlaces cortos antes de acceder a ellos. Los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de phishing, ya que el usuario no sabe hacia dónde apunta el enlace. Para poder prevenir este tipo de riesgos, es interesante que conozcas algunos servicios que permiten previsualizar el enlace antes de acceder al mismo y saber así, previamente, si es el correcto.

Evitar la navegación por páginas web sospechosas. (Programas gratis, juegos gratis, fotos de famosas, etc.).
Descargar los programas solo de las páginas oficiales. Para evitar la instalación de programas manipulados maliciosamente se recomienda descargarlos únicamente de sus páginas oficiales.
Ten cuidado con las preguntas de seguridad: Algunos servicios ofrecen la opción de utilizar preguntas de seguridad para que, en caso de olvido, sea posible recuperar la contraseña. No obstante, algunas respuestas a estas preguntas pueden ser conocidas por personas del entorno. Por ejemplo: ¿Cómo se llama tu mascota? Por esta razón, no es recomendable utilizar preguntas de seguridad con respuestas obvias. Es conveniente establecer respuestas complejas que no puedan ser averiguadas por personas cercanas.
Evitar introducir en los equipos medios de almacenamiento extraíbles de dudosa procedencia. Estos dispositivos se conectan vía USB y pueden ser una puerta de entrada para los virus.

PREVENCIÓN EN CASA
Descargar aplicaciones sólo desde fuentes confiables: Google Play para Android; Apple Store para iOS; Marketplace para Windows Phone.
Sospechar ante un número bajo de descargas.
Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes -> Seguridad -> Orígenes desconocidos.
Instalar un antivirus para dispositivos móviles.
No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

Fuente: *Unidad didáctica de Protección ante virus y fraudes*. Red.es, 2015.

ACTIVIDADES

Medidas de protección ante virus y *malware* (FA-33)

Repasar con el grupo las diferentes medidas de protección, a partir del cartel de la Oficina de Seguridad del Internauta (OSI) reproducido en la ficha de actividad FA-33.

Investigando un poco (FA-34 y FA-35)

En grupo o individualmente, se propondrá a los participantes que busquen ejemplos en Internet de cada uno de los virus o *software* malintencionados descritos durante esta unidad, que intenten averiguar cómo se han transmitido y que propongan de qué manera se podrían haber solucionado o evitado, atendiendo a las medidas de seguridad y recomendaciones vistas.

Para facilitar el trabajo, se puede proporcionar como guía la infografía de la Oficina de Seguridad del Internauta (OSI) reproducida en la ficha de actividad FA-35.

Triviral

Actividad repaso sobre lo abordado hasta ahora en relación a los virus y el *software* malicioso, a través del siguiente juego interactivo del Instituto Nacional de Ciberseguridad (incibe_):

Triviral: http://www.navegacionsegura.es/

VIRUS Y MALWERE

TIPOS DE VIRUS

SPYWERE

Cojo información de tu ordenador y la envio a mi dueño

ROGUE WERE

Soy Antivirus falso. Te bloqueo el ordenador si no me pagas.

VIRUS

molesto a los usuarios de ordenadores y demuestro lo listo que soy

GUSANO

Me multiplico y me propago por la red

TROYANO

No soy lo que parezco

ACCEDEN A TRAVÉS DE ...

CORREO ELECTRÓNICO

DESCARGA DE FICHEROS

REDES SOCIALES

ALMACENAMIENTO EXTERNO: USB, DISCO DURO TARJETA DE MEMEORIA...

PAGINAS WEB MALICIOSAS

FALLOS DE SEGURIDAD

MEDIDAS DE PROTECCIÓN

3.8. Actividad de cierre y evaluación

Cuestionario de autoevaluación (FA-10)

El cuestionario que se propone pretende ser un instrumento de evaluación pero también de reflexión personal acerca del trabajo realizado en una determinada sesión, a lo largo de las sesiones o al finalizar una unidad o el taller programado, en función de las necesidades educativas percibidas por el responsable de la actividad.

RIESGO EN EL USO DE LAS TRICs

GROOMING | SEXTING Y SEXTORSIÓN | CIBERBULLIYNG | ROBO DE IDENTIDAD | HOAX Y PHISHIING | VIRUS Y MALWERE

VICTIMA o VICTIMARIO

PREVENIR

CUIDA Y CONFIGURA TU PRIVACIDAD
NO publiques en la red información privada
NO compartas las contraseñas con otras personas

¡Piensa antes de publicar!

TOMA MEDIDAS DE SEGURIDAD:
ANTIVIRUS. CORTAFUEGOS
COPIAS DE SEGURIDAD
CONTRASEÑAS SEGURAS.
¡SENTIDO COMÚN!

Elige a tus AMIGOS DE LA RED
rechaza solicitudes de amistades de un desconocido

CUIDA TU REPUTACIÓN ONLINE

CUIDA TU HUELLA DIGITAL

HELP!

CUÉNTALO y DEJATE AYUDAR
Si estás siendo objeto de acoso, humillación, amenazas pide ayuda a un adulto en el que confíes padres, profesores, educadores

DESISTIR

COMPÓRTATE CON LOS DEMÁS COMO QUIERES QUE LOS DEMÁS SE COMPORTEN CONTIGO.

respeto

CONSECUENCIAS PERSONALES, SOCIALES Y LEGALES.

¡¡NO CONDICIONES TU FUTURO!!

NO LO COMPARTAS NO LO DIVULGUES, NO LO CONSIENTAS

Otras propuestas de trabajo

4

módulo

4.1. Orientaciones para adultos

OBJETIVOS

- Sensibilizar a los adultos, responsables de la educación de los menores, sobre la importancia de su implicación en la educación digital de estos.
- Ampliar el conocimiento de los adultos sobre las herramientas y recursos a su alcance para la educación digital de los menores.
- Conocer pautas y normas de prevención y seguridad en el uso de las TRICs.
- Adquirir conocimientos sobre cómo debe ser una actuación adecuada frente a un incidente relacionado con las TRICs en el que se vea implicado un menor.

COMPETENCIAS

- De relación, educación y parentalidad positiva.
- En comunicación lingüística, conociendo el lenguaje específico relacionado con las TRICs.
- De comprensión de diferentes usos de las TRICs y especialmente de los riesgos asociados a un uso inadecuado o a su abuso.
- Para fomentar un uso responsable en el manejo de las TRICs de los menores y adolescentes a su cargo.
- De apertura y formación continua para iniciarse en su propio aprendizaje y que sea capaz de continuar aprendiendo autónomamente.

CONTENIDOS Y ACTIVIDADES

Las TRICs, como herramienta para el Desarrollo Personal y Social

Para iniciar este tema con los padres, madres, tutores u otros adultos significativos para el menor o joven, en primer lugar es conveniente transmitir la verdadera importancia que tiene para el desarrollo de la identidad tanto personal como grupal de los adolescentes, su participación en las redes sociales e internet. Para ello podemos hacer un análisis conjunto de un texto, que se ocupa de este tema con suficiencia:

Lectura y análisis conjunto del artículo *El papel de las redes sociales en el desarrollo de la identidad de los adolescentes* (Kidsandteensonline, 2014):

Aunque a los menores se les consideren nativos digitales esto no quiere decir que sean competentes digitales.

> *"La competencia digital se refiere a las capacidades y habilidades para interactuar con las herramientas tecnológicas, con la finalidad de sacarles el máximo provecho y hacerlo de una forma segura"*

Riesgos asociados al mal uso de las TRIC. Infractores, víctimas, adictos...

En cuanto al conocimiento de las posibles infracciones que pueden cometer los menores y jóvenes por medio de las TRICs y las redes sociales virtuales, podemos proponer el análisis de algunos fragmentos del artículo *Adolescente ciberdelincuente ¿un accidente?* (Jorge Fernández Flores y Ofelia Tejerina Rodríguez), con los siguientes aspectos clave a tratar:

- Delitos al alcance de golpe de CLIC
- ¿Están los adultos preparados para orientar a los menores en un uso adecuado de las TICs?
- El desconocimiento de la ley y sus consecuencias por parte de los menores, características propias de la edad, y de la propia Red, como facilitadores de la comisión de los delitos.

¿Qué podemos hacer? El papel de los padres

En función de los padres o grupo de padres participantes quizás sea conveniente abordar algunas cuestiones previas tales como:

- Comunicación y relaciones familiares.
- Estilos educativos y de supervisión parental.
- Disciplina familiar, apoyo, refuerzo y corrección educativa.

Normas, límites y control parental

Siguiendo las pautas anteriores, antes de abordar estos aspectos es conveniente ver el vídeo *"Tú le conoces", acoso en la red* (Estrella García Alburquerque, 2015).

Tras el mismo podemos tratar más adecuadamente el sentido y propósito de las normas y límites del uso de las redes sociales virtuales por parte de los menores, y del papel de los padres y responsables a la hora de establecer pautas en este sentido.

- **Establecer horarios y situaciones en las que el menor se conecte a Internet**. Evitar horarios en los que se pueda afectar a su descanso, a su rendimiento académico, a la realización de otras actividades familiares y de ocio, o simplemente por educación. **Limitar o acotar la cantidad de horas de conexión** (se recomienda una hora seguida como máximo).
- **Establecer edades a las que el menor podrá accederá la Red o tener su primer móvil.** La tecnología no es un entretenimiento más. Los padres deben usarlas con ellos para que éstos sean capaces de emplearlas de forma segura y competente.
- **Limitar programas, aplicaciones, webs y servicios en función de la edad**. Debemos informarnos de las condiciones de uso, edad recomendada, como con las películas o videojuegos.
- **Limitar** la **"subida" de datos personales y de imágenes** a la Red.
- Educar a los menores en la sensibilidad y el respeto. No hagamos a otros lo que no queremos que nos hagan a nosotros. Tenemos derechos, también en la red.
- Enseñar a los menores a **no responder a las provocaciones** y a los malos modos de otros.
- Educar para desarrollar un **ocio saludable**. Será necesario ofrecer alternativas de ocio a los menores con el fin de evitar el uso abusivo de las TRIC.

Fuente: Monográfico mediación parental del curso *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad* (Red.es, 2013)

Denominamos **Control Parental** a cualquier herramienta o programa tecnológico que permita a los padres controlar y/o limitar el uso que un menor pueda hacer de un dispositivo o de Internet. Existen herramientas sencillas y gratuitas como Qustodio que es importante conocer, así como las amplias posibilidades que tienen en cuanto a bloqueo de información, seguimiento de páginas visitadas, control de tiempo de uso, restricción de acceso, etcétera, pero lo fundamental es tener una visión adecuada, un plan de acción respecto a su aplicación y sobretodo un diálogo constructivo respecto al ejercicio de la función supervisora parental.

La privacidad y la importancia de los datos personales

Tras el visionado de un video sobre gestión de la privacidad *¿Tienes privacidad de verdad en las redes sociales?* (PantallasAmigas, 2010) podemos tratar el tema de la de vulnerabilidad y

sus consecuencias, así como otros riesgos mayores que pueden implicar las TRICs, como el ciberacoso, *grooming*, fraudes o *sexting*… (ver unidades correspondientes), para finalizar con la exposición y el tratamiento en grupo de:

RECOMENDACIONES

- No compartir imágenes propias, o imágenes de la familia o de terceros sin el permiso de ellos, ni tampoco etiquetar a otros sin su consentimiento.
- Avisar a los amigos de que no compartan fotos o vídeos en los que salga él/ella sin su conocimiento.
- No divulgar información personal sobre los horarios, el lugar de residencia, el teléfono, el colegio o instituto, los hábitos diarios, las amistades...
- Diferenciar los conceptos de íntimo (aquello que a lo mejor puede compartir con su grupo de amigos cercanos) y privado (aquello que no se debe compartir).
- Enseñarles a configurar la privacidad de aquellos servicios web que utilicen y que lo permiten, como por ejemplo las redes sociales.
- A informar a los padres y a denunciar todos los atentados contra su privacidad y contra la de su familia.
- A desconfiar en Internet de quien está al otro lado, nunca se tiene el 100 % de seguridad de con quien se está hablando, así que no se deben facilitar datos personales.

Fuente: Monográfico mediación parental del curso *Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad* (Red.es, 2013)

La infografía de esta unidad puede ayudarnos a revisar y tratar con la persona o el grupo los aspectos claves de lo que llamamos educación digital.

Comunidades peligrosas en línea y tecnoadicciones

El tratamiento de estos temas requiere de una valoración previa sobre su oportunidad, así como una elaboración específica en función de las demandas planteadas y las características de la persona o el grupo de trabajo.

Existen distintas fuentes de información para la programación de esta posible actividad, o en su caso la orientación a los padres sobre el tema. Además de lo recogido en la unidad de búsqueda de ayuda, es recomendable consultar los materiales del curso *Capacitación en materia de seguridad TRIC para padres, madres, tutores y educadores de menores de edad* (Red.es, 2013) y en concreto para el tratamiento de las comunidades peligrosas en línea.

Por otro lado, en el caso de los adultos, para abordaje a través de algunas actividades sencillas podemos utilizar recursos como el visionado del video *The phonbies* (CAM, Protegeles, Fundación Smilestone y MovilFest Awards, 2014) que, con estética hollywoodiense y en clave de humor, se acerca al uso abusivo que los menores hacen de los móviles.

También podemos hacer una lectura y comentario de un caso real como el de Lucía, adolescente de 14 años; este caso lo encontramos en el monográfico Tecnoadicciones del curso "Seguridad TIC y menores de edad para educadores", acción formativa enmarcada dentro del programa de "Capacitación en materia de Seguridad TIC para padres, madres, tutores y educadores de menores de edad" puesto en marcha por Red.es.

Otros recursos

Un recurso útil, como referencia para padres y madres de adolescentes y jóvenes, es la guía *Internet y Nuevas Tecnologías, ¿hablamos en familia?* (Gobierno Vasco, 2016), donde se resume mucho de lo tratado en este apartado, así como los doce consejos que esta institución ha incorporado por temas y de forma resumida en su página web recursos para trabajar la educación en el uso seguro y responsable de las herramientas digitales.

Para saber más sobre ciberdelitos y comportamientos en la Red castigados por la Ley, la iniciativa de PantallasAmigas e-Legales puede ser un buen punto de partida.

Cuestionario de autoevaluación

Para estos grupos y actividades es más conveniente utilizar el cuestionario de satisfacción.

EDUCACIÓN DIGITAL

DEBEMOS CONOCER DE LAS TRIC

Comunicar relacionarse

Uso irresponsable Riesgos

CADA VEZ MAS FUSIONADOS

DEBEMOS SABER PARA EDUCAR Y PREVENIR

educaciòn digital

Desde una relación de confianza

CON UN ESTILO EDUCATIVO DEMOCRÁTICO

Imagen en la red

Huella digital

Curriculum social

REPUTACIÓN ONLINE

"Pensar antes de publicar

Proteger la privacidad

Seguridad:
contraseñas
claves
configurar privacidad

Riesgos:
Suplantación de identidad, grooming, ciberbullying, sexting

Netiqueta

TENGAMOS en CUENTA

Normas y Limites en...

programas de control parental

Tiempos

Horarios

contenidos (PEGI)

Edad de inicio

USO RESPONSABLE Y SEGURO DE LAS TRIC

4.2. TRICs, ADOLESCENTES Y RELACIONES DE PAREJA

En la actualidad cuando hablamos de violencia de género, pensamos principalmente en una violencia física entre adultos. Es más, si hacemos un repaso de la publicidad institucional para la prevención de la violencia de género, la mayoría de las campañas hacen referencia a ese perfil. Pero hay otra prevalencia de violencia contra la mujer, contra mujeres adolescentes, en la que no sólo hay agresiones físicas.

Los datos nos indican que la violencia contra la mujer ocurre desde la juventud, aunque en muchas ocasiones esa violencia no es concebida como tal o no se considera tan grave como para denunciar y/o considerarse víctima. Los últimos estudios "*Jóvenes y Género: Estado de la cuestión*" (2014) y "*¿Fuerte como papá? ¿Sensible como mamá? Identidades de género en la adolescencia*" (2015) del Centro Reina Sofía, muestran la tolerancia y normalización a la violencia de género entre jóvenes. De igual manera, los datos de la Delegación del Gobierno para la Violencia de Género (2013), en el estudio "*La evolución de la adolescencia española sobre la igualdad y la prevención de la violencia de género*", exponen que la violencia machista no se encuentra superada, en la misma línea los estudios sobre igualdad y prevención de la violencia de género en la adolescencia.

En todos ellos se indica como el control es un elemento clave de la violencia ejercida por los adolescentes, y sufrida por las adolescentes. Es importante remarcar este aspecto porque no es una violencia bidireccional, es una violencia primordialmente ejercida por ellos, contra ellas. Además, cabe destacar que cuando la violencia machista es ejercida por ellas, es un ejemplo de la agresión estructural en la que tiene profundamente asumida la opresión (por ejemplo, con la asunción de estereotipos de género tradicionales). En cambio, son los varones agresores los que pretenden perpetuar sus privilegios, tal y como se muestra al asumir desigualdades en el discurso entre chicos y chicas adolescentes en el estudio "*¿Sensible como mamá? Identidades de género en la adolescencia*".

Asimismo es necesario señalar la importancia que juegan las tecnologías digitales en las formas de ejercer la violencia, ya que tal y como muestran los datos, el control se realiza mediante smartphones, accediendo a redes sociales ajenas u observándolas.

Además de los preceptos y finalidad de la LORROM, debemos tener presentes otras Leyes Orgánicas, como la L.O. 1/2004, de 28 de diciembre, de Medidas de Prevención y Protección Integral Contra la Violencia de Género" y la L.O. 2/2006, de 3 de mayo, de Educación que recogen también la necesidad de incorporar una educación que fomente la igualdad efectiva de oportunidades entre hombres y mujeres.

Es aquí, donde enmarcamos el capítulo de TRICS y violencia de género, para dar algunas pautas que nos permitan trabajar la prevención de estas conductas e invitar a reflexionar a nuestros y nuestras jóvenes y adolescentes para permitir un cambio de paradigma conceptual sobre lo que implica ser hombre y ser mujer de forma sana y saludable.

OBJETIVOS

- Aprender a identificar las situaciones de violencia explícita e implícita, reconociendo las concepciones machistas, nuestras conductas inapropiadas, así como las agresiones sufridas.
- Modificar conductas y actitudes que son generadoras de violencia contra la mujer y todo lo que es considerado femenino.
- Cambiar la perspectiva de minusvaloración y de "normalidad" de los casos de violencia de género a través de las tecnologías digitales.

ACTIVIDADES

Con el vídeo "Conversaciones de WhatsApp" trabajaremos la identificación, características y consecuencias de los casos de violencia de género entre adolescentes, proponiendo la siguiente secuencia:

a) En primer lugar visualizaremos el vídeo propuesto.

b) Al acabar plantearemos al grupo una serie cuestiones con las que pretendemos identificar estas situaciones, así como reflexionar y reconocer la idea que tenemos de la violencia y como se ejerce. Podemos utilizar preguntas como ¿te has sentido identificado con el grupo o algunas de las personas?, ¿conoces alguna situación parecida?

c) Esta puesta en común puede tener continuidad con la exposición de cómo se sitúa cada joven y adolescente participante ante situaciones similares, ¿cómo crees que continuará la historia? ¿se irá o debería irse Carol del grupo de WhatsApp? ¿por qué?...

d) En la misma sesión o en otra posterior, trataremos las violencias ejercidas contra las mujeres, sus diferentes tipos (física, sexual, psicológica, económica y social). Para guiarnos usaremos la infografía *Violencia contra las mujeres* (ONU Mujeres, 2015) contenida el la ficha de actividad FA-36.

ACTIVIDADES COMPLEMENTARIAS

Crear un *avatar*

Iniciamos la actividad explicando que vamos a crear un "*avatar*" de un hombre y de una mujer, poniendo todos los detalles posibles, para ello usaremos la web http://crearunavatar.com/

A continuación en la pizarra, mejor si disponemos de una pizarra digital, iremos escribiendo los *avatares* creados y pedimos al grupo que vaya definiendo en dos columnas las características de un hombre y una mujer, según los avatares que hemos creado. A continuación, intercambiaremos hombre-mujer en las columnas que hemos creado.

Con ello confrontaremos la idea que tenemos de hombre y de mujer, explicaremos que hay diferencias biológicas, pero que estas no implican limitaciones, que las limitaciones son construidas culturalmente por eso que llamamos género.

Identificando la violencia

Para trabajar en la cuestión de la identificación de la violencia, podemos usar la aplicación del Instituto Canario de Igualdad, a partir de los botones de "¿y mi relación funciona?" y el de "Verdad o mentira".

El amor y sus mitos

A través de la aplicación "Detecamor" de la Junta de Andalucía, usando el botón "test del amor".

Rompe tópicos

A través de la aplicación "Detecamor" de la Junta de Andalucía, usando con el botón "test detecta" podemos trabajar los estereotipos e ideas erróneas sobre la violencia contra la mujer.

Otro recurso interesante es la guía para la prevención de la violencia de género en parejas jóvenes *Rompe tópicos* (Ayuntamiento de Logroño, 2011). Es sencilla, directa contra los prototipos dañinos y proporciona claves fundamentales para unas relaciones igualitarias

y satisfactorias. Además, su contenido se puede usar como infografía, para ir tratando los diferentes mitos de uno en uno.

Violencia sexual digital

Para tratar la violencia sexual digital podemos recurrir a una serie de cortos disponibles en diferentes páginas web, como por ejemplo la iniciativa de PantallasAmigas.

En función del grupo y de su participación en otras unidades o sesiones anteriores, trataremos el fenómeno *sexting* centrándonos en actitudes para prevenir la violencia mediante propuestas como la que podemos encontrar en http://www.sexting.es/

Fichas de actividades

FA

módulo

FA-I

Cuestionario inicial

¿Eres usuario de las redes sociales digitales? Escribe las que usas más frecuentemente:

¿Para qué te conectas? ¿Con cuánta frecuencia lo haces?

¿Crees que haces un buen uso de las mismas? ¿Cuáles son los riesgos para tu seguridad como internauta?

FA-2

CARTA A MI TATARABUELO

FA-3

Las ventajas de Internet

VENTAJAS ¿Qué aspectos positivos tiene el uso de internet y las redes sociales?	DESVENTAJAS ¿Qué aspectos negativos tiene el uso de internet y las redes sociales?

FA-4

CUESTIONARIO YO FÍSICO, YO DIGITAL

Puedo sacar una foto desde mi móvil a quien quiera y sin permiso:

- ☐ a) SÍ, siempre que les conozca.
- ☐ b) NO, siempre he de pedir permiso.

Puedo publicar las fotos que saqué desde mi móvil a mis amigos en Internet:

- ☐ a) SÍ, puede que alguno no quiera que suba su imagen en Internet.
- ☐ b) NO, si me han dejado sacar una foto, yo puedo hacer con ella lo que quiera.

Tener fotos guardadas en mi móvil, ¿es seguro?

- ☐ a) SÍ, mi móvil sólo lo veo yo.
- ☐ b) Depende del tipo de foto.
- ☐ c) No es del todo seguro porque si me roban el móvil o lo pierdo, cualquier persona accedería a esta información. También es peligro si me conecto a redes wifi públicas.

Si te llega un mms (vídeo) donde han hecho una broma pesada a un compañero de clase, ¿qué haces?

- ☐ a) Lo reenvío al resto de mis compañeros porque es muy gracioso.
- ☐ b) Lo borro de inmediato.
- ☐ c) Aviso a mi profesor/padres para que puedan ayudar a ese compañero.

Al cambiar de móvil (aparato) por otro nuevo he de asegurarme de:

- ☐ a) Quitar la tarjeta de memoria.
- ☐ b) Borrar la información almacenada en el teléfono y quitar la tarjeta.
- ☐ c) La opción “b” y llevar el móvil a un punto de reciclaje.

Si te llega un mensaje de un contacto que no conoces para que te descargues un archivo...

- ☐ a) Lo abro para ver qué es.
- ☐ b) Paso de abrirlo, porque no sé si es seguro.

FA-5

CUESTIONARIO USO RESPONSABLE TRICs

¿Cuáles de estos dispositivos electrónicos tienes en casa?:

PC / Portátil / Tablet / DVD / Smartphone / Videoconsola / Otros: _____

¿Tienes conexión a Internet en casa?

¿Y conexión a datos en tu teléfono móvil?

¿A qué redes sociales perteneces?

¿Usas las TRICs de manera segura y responsable? ¿Y las redes sociales?

¿Sabes lo que es la Netiqueta? Enumera alguna de sus normas:

¿Cuánto tiempo dedicas a navegar por la Red durante el día?

¿Y durante la noche?

Valora con una palabra el tiempo que dedicas a Internet y redes sociales:

FA-6

Contraseñas seguras

Longitud	Todos los caracteres	Solo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

Fuente: Oficina de Seguridad del Internauta

FA-7

NORMAS DE CONVIVENCIA *ONLINE* Y *OFFLINE*

Normas que nos facilitan la vida *offline*	Normas que nos facilitan la vida *online*

FA-8

I FORGOT MY PHONE

Elije una de las situaciones que aparecen en el video que hayas vivido alguna vez. Describe el rol que tú cumplías:

Elije una situación que te parezca impactante o inusual. ¿Crees que podría pasarte?

¿Te parece que están viviendo el momento al 100%? Explícate:

¿Qué sensación te ha generado el vídeo?

¿Qué impresión tienes sobre nuestro comportamiento hoy en día?

FA-9

Desconectar para conectar

Reflexiona sobre el titulo del vídeo. ¿Te parece apropiado?

Describe en 3 palabras qué te sugiere el vídeo (por ejemplo: aislamiento)

¿Te parece prescindible el móvil en alguna de las situaciones del video?

¿En cuál y por qué?

¿Y tú, eres capaz de desconectar?

FA-10

Búscate en la red, actualiza tu perfil

Al igual que las empresas se preocupan por lo que dicen sus clientes de ellos en Internet, tú debes interesarte de lo que dicen y aparece de ti en buscadores y redes sociales, por lo que el primer paso es:

> **Busca tu nombre en un buscador como Google, revisar las dos primeras páginas de resultados. Si aparece algo malo de ti, alguna foto o vídeo que consideres que puede manchar tu imagen profesional, procura eliminarla o piensa en los pasos que debes de dar para ello.**

Ten en cuenta que las opiniones de los demás sobre ti conforman la identidad digital y ésta puede afectar directamente a la decisión que un contratador pueda tomar sobre ti.

Recuerda también que dedicaste un tiempo a crear tus perfiles para ser tú quien explique a los demás quién eres. Cuidar tu propia imagen es una buena medida para tener una buena carta de presentación. Visita de vez en cuando tus perfiles para ver si hay algo que te gustaría cambiar o actualizar, y muy especialmente si cambias de trabajo, terminas un programa de formación relevante o si hay cualquier otro cambio importante en tus circunstancias profesionales.

FA-II

Cuestionario de autoevaluación

Haz un breve resumen con tus palabras de las ideas principales de la sesión/es:

Propón dos formas para prevenir los riesgos analizados en el módulo:

¿Qué te ha parecido la unidad/sesión/módulo, qué aspectos destacarías y cuáles mejorarías?

Algo que añadir….

Autovaloración del dominio de las competencias adquiridas en el Módulo (FA-12)	Nada	Algo	Normal	Mucho
Actitudinal				
Ha cambiado mi forma de entender _____				
Considero que soy más responsable ante _____				
Mi actitud ante _____ ahora es más crítica				
Ha despertado mi curiosidad por aprender más sobre _____				
Cuando me hablen de _____ intentaré buscar información de otras fuentes				
El tema me resulta útil				
El tema me ha interesado				
He mantenido una buena actitud				
Procedimental				
He trabajado de forma activa y participativa				
Considero que ahora depende de mí la forma de entender los contenidos				
He trabajado de forma autónoma la información				
Simplemente he recibido la información sin aportar nada de mi parte				
Creo que he realizado las tareas asignadas				
Conceptual				
He entendido lo trabajado				
Considero que he aprendido los contenidos de _____				
Considero que he aprendido los contenidos de _____				
Considero que he aprendido los contenidos de _____				

FA-13

Sobre videojuegos y TV

¿Conoces que tipos de limitaciones tienen los juegos, app y programas de TV?

¿Conoces juegos y app para mayores de 14 años? ¿Y mayores de 16?

¿Qué juegos usas más frecuentemente y por qué?

¿Qué programas de TV son los que más ves? ¿Qué es lo que más te gusta de ellos?

¿Cuántas horas le dedicas al uso del móvil?, ¿a los juegos? y ¿a ver la TV?

¿Qué aplicaciones tienes? ¿Cuáles usas más frecuentemente?

FA-14

¿A QUÉ EDAD...?

¿Sabrías decir la edad mínima que se necesita para usar cada una de las app y servicios siguentes? Puedes ayudarte con cualquier motor de búsqueda (Google, Bing, etc.).

App / servicio / juego		Edad
	Para registrarse en Facebook.	
	Para tener Whatsapp	
	Para tener cuenta en play store	
Disponible en el App Store	Tener un ID de Apple Store.	
FIFA	Jugar al FIFA	
	Vine	
grand theft auto	Grand Thef Auto	
	Para tener cuenta en Twitter	
	Para tener cuenta en Tuenti	
	Crear cuenta en Gmail	
	Usar Instagram	
	Registrarse en Snapchat	
	Edad para registrarse en Youtube	
	Comprar o vender por internet	

FA-15

SISTEMA PEGI

¿Cuál es el significado de los siguientes códigos PEGI?

CÓDIGO	SIGNIFICADO
	
	
	
	
	
	

FA-16

VIDEOJUEGOS

Juego									¿Edad?
Metal Gear solid									
Assasin´s Creed									
Fifa 2016									
Grand Theft Auto									
Elige uno...									
Elige uno...									
Elige uno...									

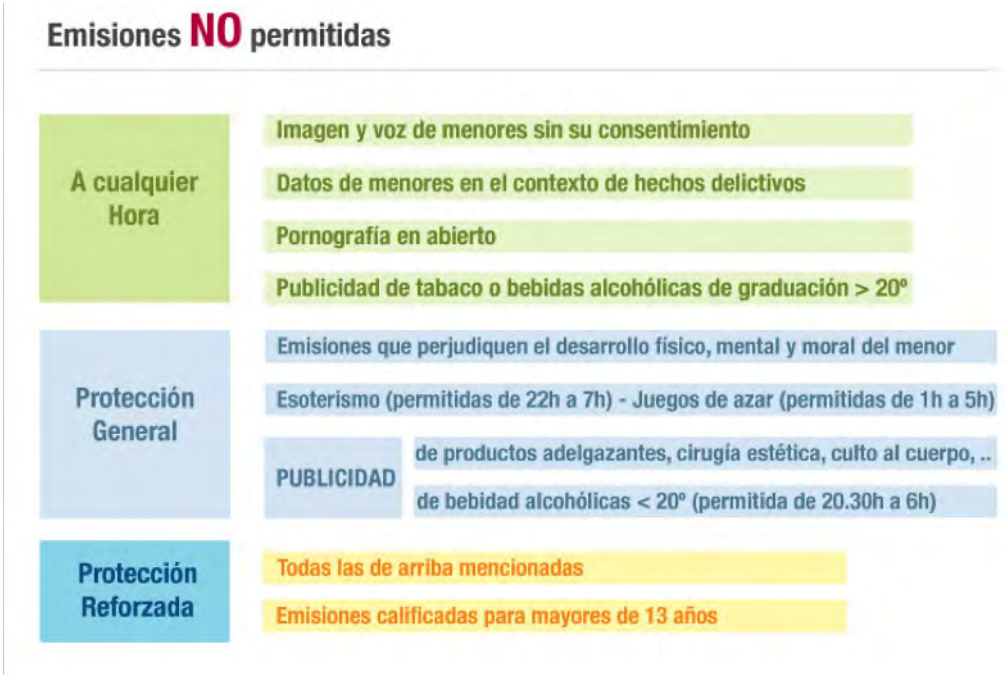
LEYENDAS							
							
Lenguaje soez	Discrimi-nación	Drogas	Miedo	Apuestas	Sexo	Violencia	Juego en red

FA-17

La clasificación de la TV

Haz una lectura del siguiente artículo:

"*La ley ha establecido una franja horaria de protección –entre las 6.00 y las 22.00- durante la cual, las televisiones no pueden emitir contenidos que perjudiquen el desarrollo de los menores de 18 años. Esta franja se ha reforzado entre las 8.00 y las 9.00 de la mañana, y entre 17.00 y las 20.00 horas, los días laborables. Durante los fines de semana y festivos de ámbito nacional, la franja de protección reforzada empieza a las 9.00 de la mañana y se prolonga hasta las 12.00 del mediodía. En estos tramos horarios tan solo se pueden emitir contenidos aptos para menores de 13 años.*"



Una vez vistos los códigos para la protección a la infancia que se establece para la TV, haz tu propia valoración sobre si se cumplen estas normativas:

FA-18

REALIZA TU CURRICULUM DIGITAL

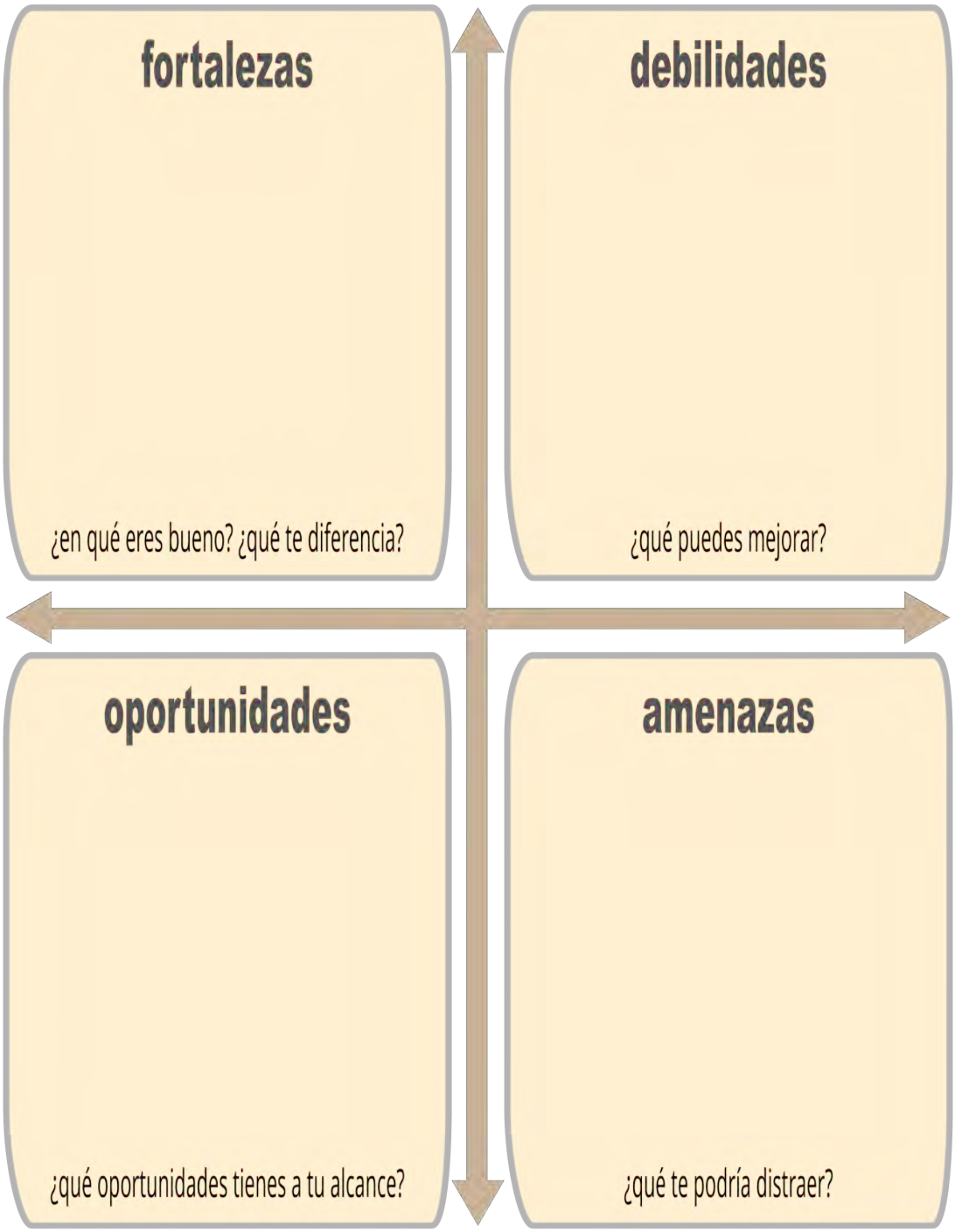
Entre las muchas posibilidades que encontramos en la red para hacer un currículum digital, estas son algunas de las más destacadas:

about.me (https://about.me)	Es uno de los más simples. Nos permite crear una tarjeta de presentación a la que se pueden añadir datos de redes sociales, blogs o páginas web personales.
Flavors (http://flavors.me)	Es muy parecida, solo que funciona más como red social.
CV Maker (https://cvmkr.com)	Tiene seis plantillas para rellenar con los datos de un currículum (información personal, formación, experiencia, etc.). El resultado es un currículum en pdf, html o documento de texto.
Visualize.me (http://vizualize.me)	También crea un currículum en forma de infografía a partir de los datos de LinkedIn. Es muy importante haberlos rellenado bien antes de importarlos a la aplicación.
Comoto (http://www.comoto.com)	Ofrece varias plantillas para importar datos de LinkedIn. Uno de sus puntos fuertes es que lo encontramos en varios idiomas y puede integrarse en el formato Europass. El resultado estará en pdf, doc y también recibiremos la url.
EuroPassMaker (http://www.europassmaker.com)	Con esta aplicación podemos hacer un currículum digital en formato Europass, un modelo cada vez más solicitado. Se crea y almacén un currículum que se puede actualizar y compartir en papel, de forma electrónico e incluso con un código QR.
tumeves.com (http://www.tumeves.com)	Es otra de las muchas aplicaciones que nos permiten hacer un videocurrículum o una presentación personal y compartirla en la red.

FA-19

Debilidades, amenazas, fortalezas y oportunidades

Tómate unos minutos y responde a las siguientes preguntas que aparecen a continuación. Plasma tus cualidades en el siguiente cuadro de "DAFO" (Debilidades, Amenazas, Fortalezas y Oportunidades)



FA-20

CUESTIONARIO DE AUTOEVALUACIÓN

Haz un breve resumen con tus palabras de las ideas principales de la sesión/es:

Indica los riesgos que tienen las Redes sociales para tu Currículum 2.0:

Autovaloración del dominio de las competencias adquiridas	Nada	Algo	Normal	Mucho
Actitudinal				
Ha cambiado mi forma de entender el uso de las nuevas tecnologías y redes sociales para la búsqueda de empleo				
Mi actitud ante la búsqueda de empleo se ha vuelto más crítica				
Considero que soy más responsable ante el uso de las nuevas tecnologías y redes sociales en materia de búsqueda de empleo				
Mi actitud ante el uso de las redes sociales ahora es más crítica				
Ha despertado mi curiosidad por aprender más sobre las redes sociales				
Cuando me hablen de redes sociales intentaré buscar información de otras fuentes				
El tema me resulta útil				

El tema me ha interesado				
He mantenido una buena actitud				
Procedimental				
He trabajado la búsqueda de empleo de forma activa y participativa				
Considero que ahora depende de mí la forma de entender los contenidos				
He trabajado de forma autónoma la información				
Simplemente he recibido la información sin aportar nada de mi parte				
Creo que he realizado las tareas asignadas				
Conceptual				
He entendido lo trabajado				
Considero que he aprendido los contenidos de la actividad 1				
Considero que he aprendido los contenidos de la actividad 2				
Considero que he aprendido los contenidos de actividad 3				
Considero que he aprendido los contenidos de actividad 4				
Otros…				

¿Qué te ha parecido la unidad/sesión/módulo, qué aspectos destacarías y cuáles mejorarías?

Algo que añadir….

FA-21

CUESTIONARIO INICIAL

¿Eres usuario de las redes sociales digitales? Por favor, indica cuáles usas:

¿Sabes cómo proteger tu privacidad?

¿Consideras que tus cuentas y perfil online está bien protegidos?

Medidas que aplicas habitualmente:

¿Qué reputación/imagen dirías que tienes en las Redes Sociales?

¿Crees que tiene riesgos utilizar de manera inadecuada las Redes Sociales? ¿Cuáles?

FA-22

El día que Carlos descubrió el testamento de su abuelo

Leonardo siempre ha tenido bastante mala memoria. Nunca se acordaba de las fechas señaladas como cumpleaños, aniversarios, etc. y no iba a ser menos con las contraseñas. Para Leonardo resultaba mucho más sencillo apuntar en un papel o en un documento de texto sus contraseñas. De esa forma, no las tenía que recordar y las podía consultar siempre que se le olvidaran.

Leo recordó que su nieta Eva le había enseñado cómo poner contraseña a un fichero de texto y decidió guardar ahí todas sus contraseñas a salvo de ojos curiosos. Sin embargo, aquella mañana tuvo la mala suerte de que Carlos encontró ese documento.

La verdad es que a su nieto le llamo la atención ver un documento llamado "Contraseñas" en el ordenador, pero cuando intentó abrirlo no pudo. Al más puro estilo de las películas de *hackers* que tanto le gustaban a Carlos, se puso a intentar averiguar la contraseña del documento.

Sospechando que ese documento era de él, intentó averiguar la contraseña con las cosas que conocía de su abuelo. Lo intentó con Leonardo, Leo, leo… hasta que dio con la contraseña correcta: davinci.

Si alguien conoce nuestro usuario y contraseña tendrá acceso a toda nuestra información: podrá publicar en nuestro nombre en las redes sociales, leer y contestar a correos electrónicos o ver el saldo de nuestra cuenta bancaria, entre otras cosas.

FA-23

EJEMPLOS DE CONTRASEÑAS QUE NO DEBEMOS UTILIZAR

Fuente: Oficina de Seguridad del Internauta (OSI).

FA-24

Cuestionario ciberacoso

¿Conoces que significa ciberacoso o *ciberbullying*?

¿Conoces algún caso de alguien que lo sufra o haya sufrido?

¿Cómo crees que debería actuar una víctima de ciberacoso?

¿Y tú? ¿Cómo crees que deberías actuar si presencias actos de ciberacoso?

FA-25

10 CONSEJOS BÁSICOS PARA EVITAR EL *CIBERBULLING*

- No contestes a las provocaciones, ignóralas. Cuenta hasta cien y piensa en otra cosa.
- Compórtate con educación en la Red. Usa la *netiqueta*.
- Si te molestan, abandona la conexión y pide ayuda.
- No facilites datos personales. Te sentirás más protegido/a.
- No hagas en la Red lo que no harías a la cara.
- Si te acosan, guarda las pruebas.
- Cuando te molesten al usar un servicio online, pide ayuda a su gestor/a.
- No pienses que estás del todo seguro/a al otro lado de la pantalla.
- Advierte a quien abusa de que está cometiendo un delito.
- Si hay amenazas graves pide ayuda con urgencia.

FA-26

Cómo pasar de "espectador" a luchar contra el *ciberbullying*

Muestra tu rechazo: Algunas personas realizan ciberacoso porque creen que la gente aprueba lo que están haciendo o porque piensan que les resulta gracioso. Criticar lo que está pasando, decir que no es divertido y que se trata de un abuso, puede ser suficiente para que el acosador pierda la motivación y deje de hacerlo.
Alguien tiene que ser el primero: Si das un paso al frente es probable que veas que no estás solo. A la mayoría de la gente joven le desagrada el *ciberbullying*, solo están esperando a que alguien tome la iniciativa para apoyarle.
Denuncia los contenidos abusivos: La mayoría de servicios en la red (redes sociales, mensajería instantánea, etc.) permiten denunciar contenidos (fotografías, comentarios, incluso perfiles) que resulten ofensivos. Denuncia para construir una red más respetuosa.
Rompe la cadena: Si te envían comentarios o imágenes humillantes sobre otra persona es el momento de ponerle freno. Si te sientes cómodo haciéndolo, responde diciendo que no te parece bien, que no quieres fomentarlo, y que animas a otras personas a hacer lo mismo.
Ofrece tu ayuda: Si eres amigo de la persona afectada pregúntale por lo que está pasando y muéstrale tu apoyo. Hazle saber que no apruebas lo que le están haciendo y que no se lo merece. Aunque no seas su amigo también puedes hacerlo, seguro que te lo agradecerá. Si ves que la cosa se complica y va a más, busca la ayuda de un profesor.
No seas un espectador y lucha activamente contra el *ciberbullying*.

Fuente: Curso "Seguridad TIC y menores de edad para educadores" de Red.es, Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). Más información.

FA-27

CUESTIONARIO *SEXTING* Y *SEXTORSIÓN*

¿Sabes qué es *sexting*? Haz una breve descripción:

¿Has conocido algún caso de *sexting* aunque haya sido por los medios de comunicación?

¿Crees que el *sexting* es un delito?

¿Cómo crees que podría evitarse?

FA-28

CUESTIONARIO *GROOMING*

¿Crees que Internet es un medio seguro para conocer amigos?

¿Tienes agregado a tus redes sociales a alguien que no conoces personalmente?

¿Alguna vez has recibido la propuesta de quedar con alguien que solamente conocías por Internet?

¿Sabes lo que es el Grooming? ¿Conoces algún caso aunque sea a través de los medios de comunicación?

FA-29

CUESTIONARIO *PHISHING* Y *HOAX*

¿Son lo mismo *phising* y *hoax*? ☐ Sí ☐ No

Define cada uno de ellos brevemente con tus palabras:

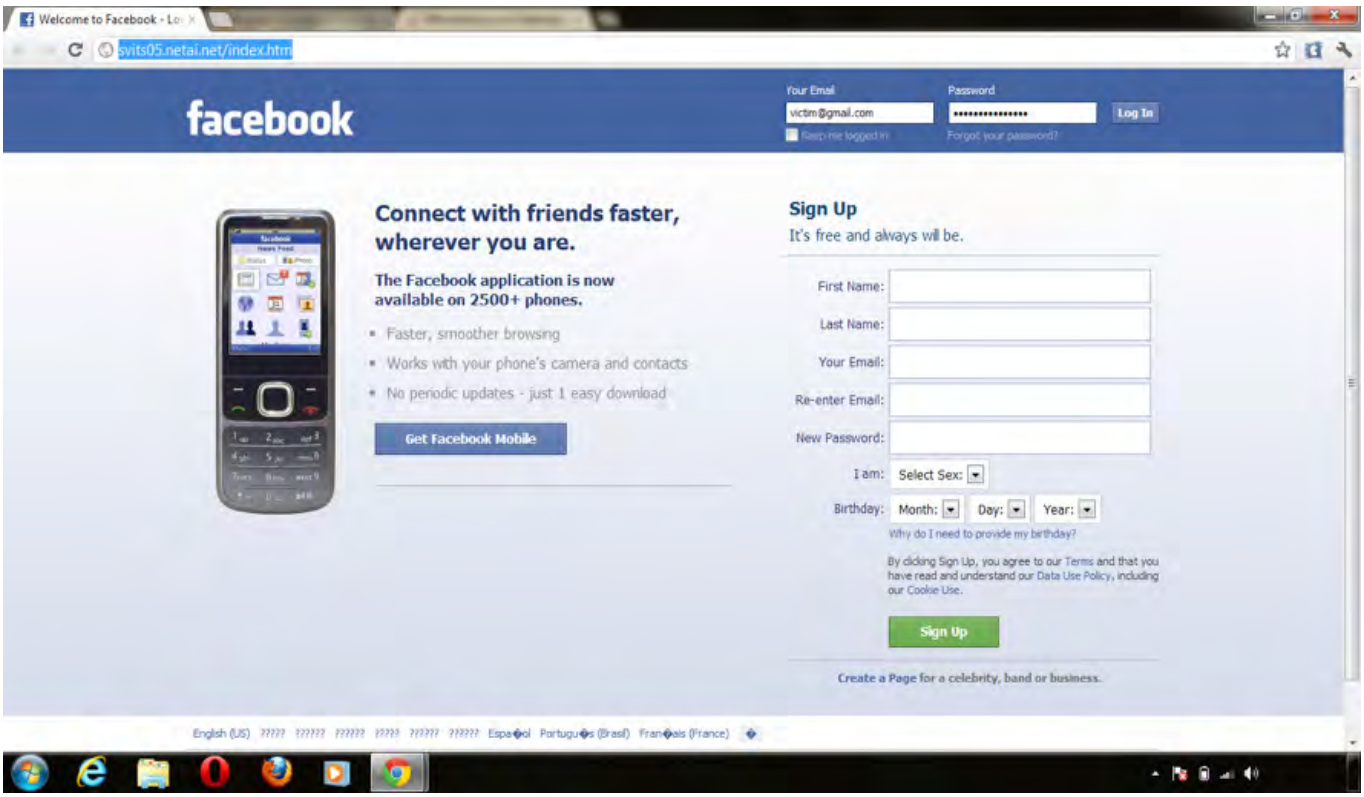
¿Te has sentido víctima de *phising* o *hoax* en alguna ocasión o conoces a alguien que le haya ocurrido?

¿Crees que puede prevenirse? ☐ Sí ☐ No

En caso de que creas que se puede prevenir indica cómo hacer:

FA-30

JUGANDO A DETECTIVES



¿Dirías que esta página es un posible *phishing*? ¿Por qué?

FA-31

¿Cuál de las imágenes es real?

FA-32

Bajo sospecha

Busca un mensaje digital en tu móvil, correo electrónico o muro de red social sospechoso de ser un *hoax*. Después busca información acerca del mismo para contrastar su verosimilitud.

Mensaje:

Información sobre el mensaje encontrado:

FA-33

MEDIDAS DE PROTECCIÓN ANTE VIRUS Y *MALWARE*

Repasar as diferentes medidas de protección, a partir de este cartel de la Oficina de Seguridad del Internauta (OSI).

FA-34

INVESTIGANDO UN POCO

Busca ejemplos en Internet de cada uno de los virus o *software* malintencionado descrito durante esta unidad. Intenta averiguar cómo se han transmitido. Propón de qué manera se podrían haber solucionado o evitado atendiendo a las medidas de seguridad y recomendaciones vistas.

VIRUS / *MALWARE*	SOLUCIÓN

FA-35

oficina de seguridad del internauta

TIPOS DE VIRUS

BichosNet

BICHOSNET ES UNA RED SOCIAL QUE PONE EN CONTACTO A TODO TIPO DE VIRUS CON SUS AMIGOS Y SU ENTORNO

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Gripe
Resfriado

VIRUS

Información del perfil

Información Básica
Soy el más viejo de todos mis malvados compañeros y he sido programado para molestar a los usuarios de ordenadores y demostrar lo listos que son mis creadores. Además, si puedo hacerles ganar algo de dinero, ¡mejor!

Aficiones
- Fastidiarte
- Destrozar la información de los ordenadores
- Hacer que tu equipo vaya lento

Lugares de Residencia
Suelo estar ubicado en los programas que tu ordenador cree que son de fiar y así pasar desapercibido hasta que llegue el momento de hacer el mal

Tiene una relación
Con todo el malware que existe. Para eso soy su predecesor…

No Me Gusta
- Las actualizaciones de seguridad
- Los antivirus
- La cautela y las precauciones de los usuarios en Internet

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Hipica
Troya
Caballos

TROYANO

Información del perfil

Información Básica
Soy un malware eficaz y muy usado. Mi gran arma es que no soy lo que parezco ser

Aficiones
- Me gusta la leyenda del caballo de Troya
- Darle el control de tu ordenador a mi amo
- Cada vez me gustan más los móviles. Puedo acceder a toda su información.
- Juntarme con otros troyanos y hacer fiestas en las botnets

Lugares de Residencia
Aplicaciones y archivos del sistema operativo.

Orígenes
Provengo de adjuntos de correos y programas que parecen inofensivos

Tiene una relación
Con puertas traseras (backdoors) y otros troyanos en botnets

No Me Gusta
- Los antivirus y anti-troyanos
- Que no se fíen de adjuntos sospechosos
- El software legítimo. Yo prefiero programas piratas

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Mariposas

GUSANO

Información del perfil

Información Básica
Mi misión principal es multiplicarme y propagarme por las redes. Solo necesito tu ayuda para arrancar. ¡Luego nadie puede pararme!

Aficiones
- Molestar saturando y colapsando las redes inútilmente
- Replicarme y extenderme por otros ordenadores

Lugares de Residencia
En la memoria RAM de tu ordenador. No necesito infectar otros ficheros

Orígenes
Provengo de otros ordenadores de tu red o directamente desde Internet. Mi pariente más famoso es El Gusano de Morris

Tiene una relación
Con internet y las redes de ordenadores

No Me Gusta
- Los cortafuegos (firewalls) que no me dejan expandirme por las redes
- Los antimalware en general
- Los chats seguros

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Espionaje
Escondite
Navegador
Adware

SPYWARE (PROGRAMAS ESPÍA)

Información del perfil

Información Básica
Soy el James Bond del malware. Busco y recopilo información de tu ordenador y se la envío a mi dueño para que saque beneficio de ella. Todo sin tu consentimiento, claro

Aficiones
- Esconderme en tu ordenador y reinstalarme cuando arranca
- Buscar y recopilar información para luego ser vendida al mejor postor
- Cambiar tu buscador por defecto
- Añadir barras de herramientas a tus navegadores web

Lugares de Residencia
Oculto en el sistema operativo. En aplicaciones shareware (gratuitas con limitaciones)

Orígenes
Llego a tu ordenador a través de adjuntos al correo electrónico. También suelo acompañar a programas gratuitos (freeware)

Tiene una relación
Con barras de herramientas de los navegadores y adware (anuncios) en general

No Me Gusta
- Los antivirus web y de correo electrónico
- Los navegadores actualizados
- Los complementos de seguridad de los navegadores Web

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Troyanos
Antivirus
Infecciones

ROGUEWARE (FALSOS ANTIVIRUS)

Información del perfil

Información Básica
Simulo ser un antivirus que detecta una infección en tu ordenador. Intento sacarte dinero vendiendo soluciones o suscripciones a servicios. Si no ¡te infecto de verdad!

Aficiones
- Simular que hago un escáner del ordenador
- Infectar cuando piensan que estoy desinfectando

Lugares de Residencia
En cualquier parte de tu ordenador, como te crees que soy bueno...

Orígenes
Los programas "gratuitos" como falsos códecs o plugins. Páginas web de dudosa reputación: descargas ilegales, contenidos de adultos, etc

Tiene una relación
Con troyanos y páginas Web fraudulentas o infectadas

No Me Gusta
- Los navegadores actualizados
- Los complementos de seguridad de los navegadores web
- Los antivirus de verdad
- Los sistemas operativos actualizados
- Los usuarios que se informan antes de hacer una compra online

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Policia
Malware

RANSOMWARE (SECUESTRADORES)

Información del perfil

Información Básica
Bloqueo tu ordenador para que no lo puedas usar hasta que no hagas lo que yo digo. Normalmente: ¡pagarme!

Aficiones
- Apoderarme de tu ordenador y no dejarte usarlo hasta que pagues
- Cifrar tus ficheros importantes y chantajearte con su contraseña
- Hacerme pasar por policía o jueces para engañarte

Lugares de Residencia
En cualquier parte de tu ordenador esperando a que me ejecutes o me ejecute mi amo

Orígenes
Troyanos y gusanos con forma de programas gratuitos, pirateados o adjuntos de correos electrónicos. Mi mayor orgullo es el "Virus de la Policía"

Tiene una relación
Los cryptolockers, malware que cifra ficheros y que chantajea al usuario con la contraseña de desbloqueo

No Me Gusta
- Los sistemas actualizados
- Los antimalware
- Los usuarios que se informan y denuncian antes que pagar a ciberdelincuentes

BichosNet | Busca | Inicio | Perfil | Amigos | Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Teclados

KEYLOGGER (REGISTRADOR DE TECLAS)

Información del perfil

Información Básica
Capturo y recopilo todo aquello que escribes en tu ordenador sin que te enteres. Puedo ser un programa oculto en tu ordenador o un pequeño acople camuflado en tu teclado

Aficiones
- Obtener tus contraseñas: banco, correo electrónico, redes sociales...
- Chantajearte con la información recopilada

Lugares de Residencia
Instalado o conectado a tu ordenador

Orígenes
Suelo venir con mis amigos los troyanos. Los de tipo "físico" somos enchufados por nuestros amos en la parte trasera de los ordenadores

Tiene una relación
Con troyanos que me instalan y permiten que me comunique con mi amo.

No Me Gusta
- Los usuarios que están atentos y vigilan su ordenador
- Los antimalware en general

www.inteco.es www.osi.es

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO Instituto Nacional de Tecnologías de la Comunicación

Comunidad de Madrid

Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor
CONSEJERÍA DE PRESIDENCIA, JUSTICIA Y PORTAVOCÍA DEL GOBIERNO - **COMUNIDAD DE MADRID**

FA-36

ONU MUJERES

onumujeres.org

@UN_Women

facebook.com /onumujeres

gplus.to /unwomen

FUENTES

Estadísticas: Estimaciones mundiales y regionales de la violencia contra la mujer, OMS, 2013; Estudio mundial sobre el homicidio, UNODC, 2013; El Progreso de las Mujeres en el mundo, ONU Mujeres, 2011-2012; Informe mundial sobre la violencia en el mundo, OMS, 2002; Estimación Mundial sobre el Trabajo Forzoso de la OIT, OIT, 2012; Fondo de las Naciones Unidas para la Infancia, *Female Genital Mutilation/Cutting: What might the future hold?*, UNICEF, 2014.

Citas: "6 Brave Personal Stories of Domestic Abuse, "TedX, 2013; Half the Sky, Turning Oppression into Opportunity for Women, Sheryl Wu Dunn, Nicholas Kristof, 2009; "Historias de sobrevivientes ÚNETE", ÚNETE para poner fin a la violencia contra las mujeres, 2012; "My battle against female genital cutting", The Guardian, 2012; I Am Nujood, Age 10 and Divorced, Nujood Ali, Delphine Minoui, 2010.

VIOLENCIA CONTRA LAS MUJERES

UNA PANDEMIA MUNDIAL QUE ADOPTA MUCHAS FORMAS

Ya sea en el hogar, en la calle o en los conflictos armados, la violencia contra las mujeres es una PANDEMIA MUNDIAL que ocurre en espacios PÚBLICOS y PRIVADOS.

FORMAS DE VIOLENCIA

Física

Sexual

Psicológica

Examinemos más detenidamente algunas de estas formas de violencia

VIOLENCIA POR UN COMPAÑERO SENTIMENTAL

> "En realidad, soy una víctima muy corriente de maltrato doméstico... La violencia doméstica le ocurre a todo el mundo. En todas las razas, en todas las religiones, en todos los niveles económicos y educativos".
>
> — **Leslie Morgan Steiner,** *licenciada de Harvard, empresaria editora de una revista, en el pasado sufrió una relación de maltrato*

Datos básicos

En todo el mundo, una de cada tres mujeres ha sufrido violencia física o sexual, principalmente por parte de un compañero sentimental.

En 2012, en uno de cada dos casos de mujeres asesinadas el autor era su compañero sentimental o un miembro de la familia. En el caso de los hombres, estas circunstancias únicamente se dieron en uno de cada 20 hombres asesinados.

¿Existen leyes para proteger a las mujeres?

Dos terceras partes de los países han prohibido la violencia doméstica

Sólo 52

países han penalizado explícitamente la violación al interior del matrimonio

De hecho,

2.600 millones

de mujeres y niñas viven en países en los que la violación conyugal no está explícitamente penalizada

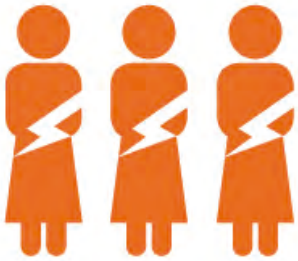
VIOLENCIA SEXUAL

"No importa el empeño que pongan en aniquilar todo lo que llevamos dentro; dentro de mí no consiguieron aniquilar nada. No me rendiré. Mientras pueda seguir andando, resistiré. Encontraré la fuerza dentro de mí".

— **Enisa,** *sobreviviente de una violación en la guerra de Bosnia*

¿QUÉ ES LA VIOLENCIA SEXUAL?

La violencia sexual es todo acto sexual, la tentativa de consumar un acto sexual, los comentarios o insinuaciones sexuales no deseados, o el uso de la sexualidad de una persona mediante coacción por otra persona, sea cual fuere su relación con la víctima y sea cuales fueren las circunstancias.



Los actos de violencia sexual pueden ocurrir en distintas circunstancias y entornos. Entre ellos:

- Violación (al interior del matrimonio u otro tipo de relaciones, por parte de extraños, y durante un conflicto armado)
- Avances sexuales no deseados o acoso sexual, incluido el hecho de pedir sexo a cambio de favores
- Abusos sexuales a niñas y niños
- Convivencia o matrimonio forzados, incluido el matrimonio infantil

En la mayoría de países, los datos de investigación sobre este problema son escasos.

Datos básicos

En algunos países, hasta una tercera parte de las adolescentes afirma que su primera relación sexual fue forzada.

En la Unión Europea, del 45 por ciento al 55 por ciento de las mujeres han sufrido acoso sexual desde los 15 años de edad.

Contenidos y programación de las actividades desarrolladas por la Agencia de la Comunidad de Madrid para la Reeducación y Reinserción del Menor Infractor para la Prevención y Formación en el uso adecuado de las Tecnologías de la información y la Comunicación de los menores y jóvenes atendidos.

Agencia
de la Comunidad de Madrid
para la Reeducación y Reinserción
del Menor Infractor

Comunidad
de Madrid

CONSEJERÍA DE PRESIDENCIA,
JUSTICIA Y PORTAVOCÍA DEL GOBIERNO