UNIVERSIDAD POLITÉCNICA DE VALENCIA.

UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

Escola Tècnica
Superior d'Enginyeria
Informàtica

INTERNET Y ADOLESCENCIA:
GUIA ON LINE PARA EDUCADORES.

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA,

ESPECIALIDAD: SISTEMAS DE INFORMACIÓN.

ALUMNA: M. PILAR PUCHADES PARDO

DIRECTOR: JUAN VICENTE OLTRA GUTIERREZ.
DEPARTAMENTO: DEPARTAMENTO DE ORGANIZACIÓN DE EMPRESAS, ECONOMIA FINANCIERA Y CONTABILIDAD.

SEPTIEMBRE 2013

A mis sobrinos,
que han participado como modelos en
las fotos y me han servido de inspiración
en la realización de este proyecto

http://adolescentesinternet.wordpress.com/

Índice

INDICE

Introducción al PFC

INTRODUCCION PFC

Objetivo del proyecto

La popularización de internet ha conseguido que la mayoría de los hogares españoles ya dispongan de ordenadores conectados a la red.

Los jóvenes adolescentes que se conectan a internet, lo realizan a través de los diferentes dispositivos que disponemos hoy en día, tales como: tabletas, móviles, ordenadores portátiles, ordenadores de sobremesa, conexiones inalámbricas en Smart TV, etc.

Estos medios forman parte de las llamadas "nuevas tecnologías de la información/comunicación" (TIC), que se crearon con el objetivo de mejorar las comunicaciones entre personas, para agilizar la comunicación y el intercambio de información.

Cada día somos más los usuarios que nos sentimos atraídos por esta forma de comunicación. Somos iniciados voluntaria u obligatoriamente, puesto que incluimos esta herramienta dentro de nuestra actividad laboral o simplemente necesitamos un reconocimiento social en general que nos incita a ser activos en la red de internet.

No es raro, el cambio de actitud que experimentamos cuando una mañana comenzamos el día averiguando que hay una incidencia en

nuestro teléfono móvil (por ejemplo) y no podemos conectarnos a internet, enseguida nos ponemos en contacto con la operadora que nos facilita el acceso y realizamos la reclamación correspondiente en aras de poder recuperar cuanto antes la ansiada conectividad. Nos traumatizamos por la carencia de esta facilidad y bajo un estado de espera y resignación, tenemos que recurrir a otros "rudimentarios" sistemas de búsqueda manual de información.

Cuando sufrimos esta incidencia, se produce un grave trastorno en nuestra rutina diaria, se deja patente la estrecha dependencia de las tecnologías en la actividad laboral, personal, social de los seres humanos.

Figura 1: Nuestros niños y adolescentes son la generación de las nuevas tecnologías.

Las nuevas tecnologías están a la orden del día entre los más pequeños. Tal es así, que no nos sorprendemos al ver a niños enseñando a sus mayores a utilizar el DVD, la cámara digital, su nuevo móvil o incluso a navegar por la Red sin que aparentemente nadie les haya enseñado previamente..

La invasión de estas nuevas formas de comunicación en nuestra sociedad, pueden actuar como medio facilitador potencial de posibilidades de perpetrar acciones delictivas incluso a miles de kilómetros, basándose en la suplantación de identidad o identidad falsificada y en técnicas de navegación anónima, lo que se convertiría en un grave problema cuando participa un menor como receptor de esta actividad delictiva y es nuestro deber como padres o educadores, tomar las medidas necesarias para combatir o minimizar este tipo de delitos.

Los adolescentes van a ser el sector de la población más vulnerable a este tipo de riesgos, por lo que prestaremos nuestra atención en resaltar estos peligros que puede suponer para el menor, ya que pueden ser contactados con facilidad a través de internet por parte de los "*depredadores sexuales*".

Por ello, **la motivación de este estudio** ha sido en centrarnos en el adolescente en internet, la influencia de su uso en aspectos muy importantes de sus vidas, como por ejemplo, el ámbito escolar, el entorno familiar, tiempo de uso de pantallas y la valoración de los posibles peligros que puede entrañar. Ya el hecho, de lo que podríamos

en un principio suponer una simple conexión y que resulta no ser lo inocente que esperábamos.

Asimismo, miraremos el código penal español, observaremos que defensas y castigos se pueden obtener al respecto y qué podemos hacer nosotros como padres y educadores para protegerlo de estas posibles amenazas.

Brecha digital

BRECHA DIGITAL. DEFINICION DE PARTICIPANTES.

Brecha digital

La inclusión de las llamadas tecnologías de la información y de la comunicación (TICs) en todos los sectores de nuestra sociedad, ha supuesto para el ser humano, un esfuerzo de adaptación a las mismas, ya que estas van evolucionando cada día.

Las TICs cada día van evolucionando, y es el ser humano el que de forma individualizada realiza constantemente dicha adaptación, para asimilar el constante bombardeo de información y comunicación.

El grado en que las personas tienen acceso a los instrumentos y herramientas de la información y asimilan su mensaje, va propiciando marcadas diferencias, ya sea entre género, países, generaciones, niveles socioeconómicos, niveles educativos, etcétera. Entonces, estamos hablando de brecha digital o 'digital divide'.

El término "brecha digital" recoge las diferencias entre dos mundos que por la estructura de nuestra sociedad cada vez más separados entre sí, puesto que está relacionado con la idea de tener acceso a internet y la capacidad de usar dicha tecnología en cualquiera de los dispositivos que en la actualidad se dispone para asegurar un acceso a la red, tales como el teléfono móvil, tabletas, televisión,… etcétera.

> *La brecha digital se define como la separación que existe entre las personas (comunidades, estados, países…) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas.*

Serrano, Arturo, Martínez, Evelio (2003) "La Brecha Digital: Mitos y Realidades",
México, Editorial UABC ISBN 970-9051-89
http://www.labrechadigital.org

No nos parece raro cuando pensamos en la brecha digital que se relaciona entre las ciudades y las zonas rurales, puesto que, entre otros motivos, el cableado telefónico es más accesible y económico en la metrópolis que en zonas rurales o aisladas.

Si un futuro usuario de una zona rural quiere disponer de tecnología para conectarse a internet, tiene que salvar las distintas trabas o inconvenientes que le puedan surgir, tales como disponer de cobertura en su zona, numeración telefónica disponible en su central, tener una infraestructura necesaria existente,… es decir, la mayoría de las veces no solo depende del usuario que quiera o no conectarse a internet, sino también entra en la ecuación terceras partes tales como las actuales compañías telefónicas.

Las mismas empresas que ofrecen el cable telefónico dictaminan si es viable para su economía el invertir en la instalación o no, de un nuevo

tendido telefónico (bien sea tecnología DSL o fibra óptica) así como dar cobertura por sistemas de ondas de radio.

Pese a estos inconvenientes, el alta de nuevas líneas para acceder a internet en zona rural, continúa creciendo aunque a un ritmo más moderado que en la ciudad, pero gracias al empeño de nuestros gobiernos a favor de la conectividad en el máximo territorio posible, va propiciando que poco a poco el número de zonas aisladas vaya siendo cada vez menor.

Todo ello, lo ha favorecido el nuevo sistema de conexión a internet vía satélite que en vez de depender de ondas de radio o el cableado telefónico, ahora utiliza el cielo abierto como medio de enlace hacia un satélite, este sistema es recomendable a aquellos lugares donde no puede llegar el ADSL o cable.

En cuanto a la zona metropolitana, el número de inconvenientes se reduce considerablemente, puesto que las distintas empresas telefónicas ya han realizado la inversión de la instalación de la infraestructura necesaria para la conectividad y el interés de dichas compañías pasará por preocuparse de obtener el máximo número de usuarios en la línea, para recuperar cuanto antes el capital invertido en la zona. Por lo tanto, el usuario de la ciudad tan solo se debe de preocupar de aspectos básicos tales como elegir la compañía telefónica que le facilitará la conexión y a lo sumo, con qué ordenador o dispositivo se va a conectar, y en qué momento.

El número de conexiones a Internet en núcleos urbanos es mayor que en ámbito rural. Y cuanto más grande sea la ciudad, mayor número de comunicaciones por la red. Este hecho no es de extrañar, puesto que las empresas utilizan la red como vía principal de comunicación y forma indispensable de hacer negocios. Por lo tanto, la brecha digital también está presente incluso en cada núcleo urbano, si lo elevamos a otras escalas, podríamos decir que existe entre clases económicas, y si lo miráramos a nivel mundial, la diferencia también estaría entre los países más o menos desarrollados industrialmente.

> *"Las TIC incluyen las tecnologías de redes, telecomunicaciones e informática (teléfono, televisión, radio, internet, computadoras etc.) que de manera directa o indirecta, influyen en nuestras actividades socioeconómicas, educativas y culturales."*
>
> *Martínez, Evelio, Serrano, Arturo, (2007)*
> *Artículo "La evolución hacia la nueva brecha digital" publicado en la revista NOVÁTICA: Revista de la Asociación de Técnicos de informática ISSN 0211-2124 nª 186, 2007 págs. 71-74.*

Desafortunadamente, no todos tenemos acceso a la tecnología de manera equitativa. Podemos afirmar que todavía, en el mundo, hay poblaciones que no tienen acceso al teléfono, ni siquiera a los servicios básicos fundamentales como son el agua y la electricidad. Por lo tanto, la diferencia entre los que acceden y los que no acceden a dicha tecnología en este aspecto, representarían el punto más amplio de separación de la brecha digital.

En el aspecto social de una misma comunidad, la brecha digital también existe entre las clases sociales de acuerdo con el nivel de ingresos de la población, clases con mayor o menor nivel académico. Incluso las búsquedas en este aspecto son diferentes, por ejemplo, en las clases menos escolarizadas, los intereses en internet van más referenciados al deporte, ocio y relaciones sociales la mayoría del tiempo de conexión, mientras que el sector más académico o universitario realizan las consultas más relacionadas a intereses de negocios, documentación, didácticos, así como también de ocio pero como tiempo de evasión.

El aspecto económico también influirá para potenciar o moderar el índice de la brecha digital dentro de una misma sociedad, ya que será necesario tener el sustento económico suficiente para contratar los servicios ofrecidos y poder favorecer un tiempo de conexión más amplio que cuando se carece de los recursos económicos para tener conexión propia, y el usuario tiene que recurrir a las opciones de wifi compartido tales como bibliotecas públicas, cibercafés, … donde las conexiones son esporádicas. Además también se deberá tener las habilidades suficientes para utilizar dichos servicios. Por ejemplo, la habilidad de utilizar una computadora y navegar por internet, leer un correo electrónico, generar contenidos con valor educativo o cultural, mantener conversaciones entre usuarios a distancia, etc. Dichas habilidades estarán marcadas también por la clase de usuario que acceda a internet, pudiéndolos clasificar en analfabetos digitales, inmigrantes o nativos digitales, como veremos detallados en los puntos siguientes.

Analfabeto digital

> *"Sin educación, no podemos ver más allá de nosotros mismos y nuestro estrecho entorno y comprender la realidad de la interdependencia mundial. Sin educación, no podemos comprender cómo las personas de otras razas y religiones comparten nuestros mismos sueños y esperanzas. Sin educación, no podemos reconocer la universalidad de los objetivos y las aspiraciones humanas."*
>
> *Kofi Annan, Secretario General de las Naciones Unidas.*
>
> *Fuente: http://www.educacionenvalores.org/objetivosdelmilenio/objetivo2/index2.htm.*

Un analfabeta digital es el individuo que desarrolla prácticamente todas las actividades diarias, tanto personales, como educativas, profesionales,… sin vincularse con las TICs, realizando sus quehaceres mediante métodos tradicionales, tales como apuntar una cita en un dietario en vez de utilizar alguna herramienta digital para ello.

No nos referimos a las personas que no han logrado aprender a leer y escribir, estas más bien son analfabetos, pero con el concepto de digital, nos queremos referir a las personas que con la aparición de las nuevas tecnologías, no han querido interactuar en el mundo digital, no entienden de redes sociales, si necesitan buscar una información,

prefieren utilizar un libro, enciclopedia o algún elemento ya escrito a papel en el que localizar la información, es decir, no llegan a entender, como poniendo unas palabras claves en un momento dado en un ordenador conectado a la red, puede localizar en fracciones de segundos la información requerida.

El desconocimiento y la falta de habilidades y destrezas para acceder a estas tecnologías, potencian más el rechazo a querer utilizarlas, por lo que dichas personas cada vez se sienten más aisladas y desinformadas. Se siente marginado por el mundo digital, lo que según los expertos en economía, al relacionar la información con el poder, la riqueza, aparece el concepto de info-pobre, frente al info-rico que será la persona que comprende y maneja la información obtenida de internet para fines de desarrollo socio-económico o personal.

El analfabetismo digital está presente en las personas adultas y de la tercera edad, que no ven la importancia ni las bondades que ofrece el empleo de estas nuevas tecnologías o medios de comunicación, aún prefieren seguir escribiendo en sus viejas máquinas de escribir, no se plantean que el uso de una computadora le pueda ofrecer múltiples alternativas para crear, publicar e intercambiar mensajes y documentos con rapidez y prontitud. Se informan sobre todo a través de libros, revistas o diarios impresos. Se suelen comunicar solo mediante el teléfono fijo, no quieren aprender a utilizar un móvil para comunicarse. Y si llegara el caso que necesitan información o requieran hacer uso de las TICs por algún motivo, lo harían mediante la colaboración de algún inmigrante o nativo digital. Hoy en día, no nos sorprende la imagen de ver a un adolescente buscando información para un anciano.

Además de las personas mayores, también podemos encontrar analfabetos digitales tanto en la ciudad como en los barrios marginales y que no necesariamente tiene relación con los recursos económicos para comprar un ordenador para acceder a internet, sino que más bien se trata de una actitud de rechazo a lo novedoso, porque lo nuevo crea incertidumbre, temor a cometer errores. Son del pensamiento de "si hasta ahora, con los años que tengo, he sobrevivido sin esta tecnología, ¿Por qué no puedo continuar así al menos un par de años más?".

Y en cuanto al área rural, tal y como hemos indicado en el apartado de la brecha digital, en los pueblos aislados será donde exista mayor presencia de analfabetos digitales, debido a diversas razones tales como la falta de infraestructura, ausencia de ofertas de acceso a internet, bajo poder adquisitivo, falta de cobertura en la zona,... en definitiva, una brecha digital muy difícil de superar, pero que poco a poco se va reduciendo dicho índice, tal y como lo podemos observar en la siguiente tabla que hemos compuesto gracias a la base de datos estadísticos que recoge la página de la comisión europea de estadística:
http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home

Individuals who have never used a computer by NUTS 2 regions
Last update: 31.07.13
Source of data: Eurostat

INDIC_IS: Computer use: never **UNIT:** Percentage of individuals

TIME / GEO	2008	2009	2010	2011	2012
Spain	33	31	27	26	22
Noroeste (ES)	38	37	32	30	27
Noreste (ES)	30	28	25	23	19
Centro (ES)	37	36	30	30	26
Este (ES)	30	27	24	24	21
Sur (ES)	39	34	30	29	26

Figura 2: personas que nunca han usado una computadora en España. Fuente EUROSTAT.

En la figura 2 podemos analizar que hay ciertas comunidades en la que el porcentaje de personas que nunca han usado una computadora está por debajo de la media española.

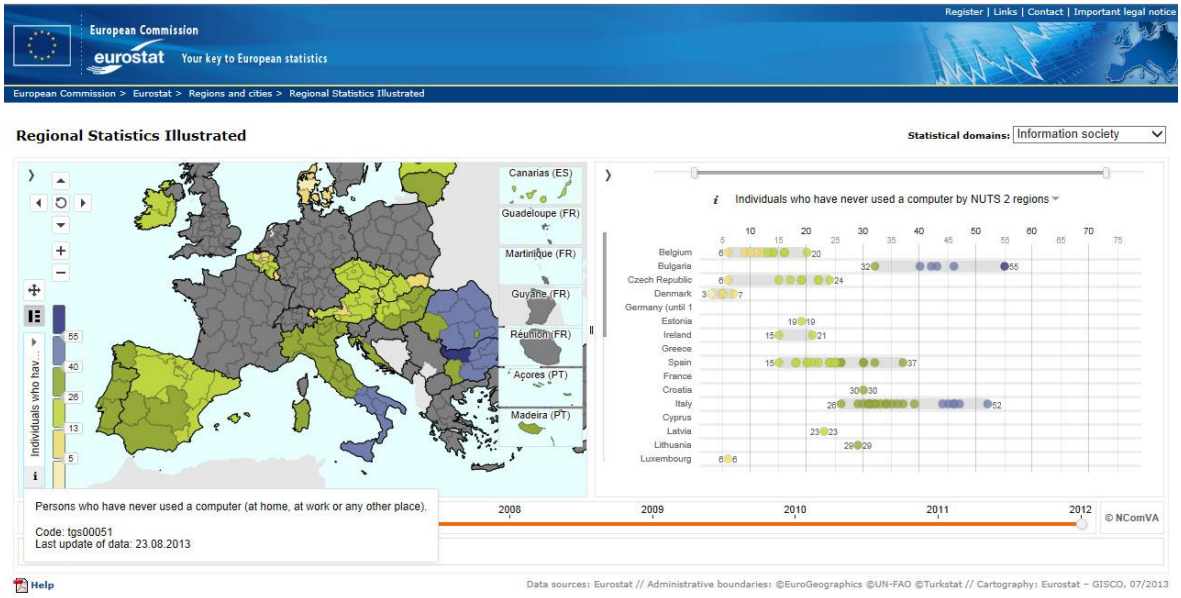


Figura 3: personas que nunca han usado una computadora en Europa. Fuente: EUROSTAT. http://epp.eurostat.ec.europa.eu/cache/RSI/

En la figura 3 podremos observar que España se encuentra en la media europea de personas que nunca han utilizado internet, destacando tres países en los que todavía no usan ningún tipo de tecnología llegando incluso a ser casi la mitad de la población de dicho país como lo son Bulgaria, Italia y Rumania.

El analfabetismo es una consecuencia directa de la no escolarización, y supone, con todas sus secuelas una enorme barrera para salir de la

pobreza. Por ello, la campaña internacional *"Educación para Todos"* desarrollada por UNESCO trata de concienciar y dar respuesta a las necesidades educativas urgentes que tienen los países menos desarrollados. Además, trata de comprometer a los gobiernos en la aplicación de programas en sus países y en el desarrollo de programas de cooperación internacional con el objetivo de alcanzar el Objetivo 2 del Milenio: la universalización de la enseñanza primaria en el año 2015. Para ampliar información sobre los objetivos del milenio, podemos acceder a la siguiente dirección:

http://www.educacionenvalores.org/objetivosdelmilenio/objetivo2/index2.htm

Inmigrante digital

Los migrantes o **inmigrantes digitales** nacieron en la década de los 60-70, por lo que sus edades circulan entre los 35 y los 55 años de edad.

Son aquellos que han tenido que adaptarse a una sociedad cada vez más técnica o digital gracias al progresivo y constante desarrollo de las TICs.

Se adaptan a su manera, como pueden a la tecnología a su propio ritmo, obligados por la rutina diaria y/o profesional en estos últimos años.

La educación y/o formación de estas personas también fue mediante el apoyo de grandes enciclopedias y elementos gráficos principalmente soporte a papel. Incluso en la actualidad, si hubiera oportunidad de presentar sus trabajos en soporte escrito, no lo pensarían dos veces, y preferirían dicha opción, eso sí, previamente elaborada con la ayuda de la computadora.

Salvo en casos en los que la presentación de trabajos requiera más uso de la tecnología, como por ejemplo, presentaciones animadas o "PowerPoint", el inmigrante optará por la opción de papel, dando el falso sentimiento como dicen nuestros mayores "lo que está escrito permanece en el tiempo, mientras que las palabras se las lleva el viento".

Pese a la preferencia de los métodos tradicionales, el inmigrante digital también hace uso de las tablets, laptops, iPod, iPad, netbooks, móviles, etcétera.

En cuanto al aspecto comunicativo, son los que mayor uso del móvil realizan, entendiendo el móvil como un instrumento para hacer y recibir llamadas de voz, desaprovechando mayoritariamente las distintas actividades que podemos realizar en la actualidad gracias a la fuerte inclusión del Smartphone.

Una tarde cualquiera, sentados en una terraza de un café, observando la gente de alrededor paseando o sentadas en la misma terraza, nos

fijáramos en sus móviles, podríamos fácilmente adivinar si un inmigrante digital está más próximo al grado de adaptación de un nativo o por el contrario casi podríamos considerarlo más cercano al grupo de analfabetos digitales. Por ejemplo, un señor en edad de merecer que lleva un móvil de los de "tipo concha" (los que se pliegan por un eje, cerrándose como una caja), nos daría pistas acerca de su actitud o grado de adaptación a la nueva tecnología, este seguramente sería un iniciado, pero más bien, poco adaptado.

Mientras, si observáramos una señora, con un Smartphone táctil contestando un mensaje recibido por alguna aplicación de mensajería instantánea, nos atreveríamos a pensar en esta ocasión que se trataría de un inmigrante digital de grado medio/avanzado de adaptación a las nuevas tecnologías.

La presencia del inmigrante digital en las redes sociales, se reduce a un número reducido de aplicaciones destacando principalmente el Facebook o el Twitter.

Son usuarios de estas redes sociales, sólo por el hecho "de que hay que estar", porque "no eres nadie si no estás en las redes sociales".

Otros motivos, por los que el migrante digital se introduce en el mundo de las redes sociales, atiende más bien al instinto expiatorio que tenemos todos, porque nos gusta ver, como le va a nuestro vecino o amigo de la infancia, si ha triunfado en la vida,….

En la red social, hablamos cordialmente con alguna persona, incluso comentamos las fotos que expone en su muro personal, mientras que si ese mismo sujeto, nos lo encontramos por la calle, ni le dirigimos la mirada.

En cuanto a la obtención de información se refiere, los grandes tomos de enciclopedias que usaban cuando eran niños, ya no tienen cabida en los hogares actuales (ocupan espacio y sólo sirven para almacenar polvo o hacer bonito en la repisa del mueble del comedor).

Actualmente, hacen uso de la tecnología, y se han convertido en los principales usuarios de las llamadas "wikis" o "foros", donde satisfacen muchas necesidades de información. A pesar de ello, contrasta el hecho de la predisposición a guardar en secreto la información obtenida o elaborada por uno mismo (la información es poder, y si es propia, hay que preservar ante todo los derechos de autor).

Figura 4: El inmigrante digital estará constantemente enfrentándose a nuevos retos que deberá resolver si quiere avanzar.

En definitiva, podríamos indicar, que el inmigrante digital estará a lo largo de su vida inmerso en un período de transición/adaptación a la nueva tecnología que va evolucionando asiduamente y que provocará por parte del inmigrante, un esfuerzo perseverante que conlleva en ocasiones a un cambio de hábitos y de forma de pensar, provocados por el impulso de las TICs.

Nativo digital

El concepto de **nativos digitales** ("digital natives") fue mencionado por primera vez en el año 2001 por Marc Prensky en un trabajo titulado "Digital natives. Digital Immigrants".

Esta generación será formada por aquellas personas que han nacido en una era donde todo a su alrededor está influenciado por el cambio tecnológico. Serán adolescentes nacidos a partir de 1995, adolescentes que crecieron cerca de una computadora o consola, y que incluso han aprendido antes el lenguaje y gestos digitales, que conseguir pronunciar sus primeras palabras.

En la actualidad, no nos sorprende como un bebé le llama la atención un Smartphone que lleva el adulto próximo a él, este se lo acerca y le permite interactuar con dicho dispositivo. Enseguida demostramos nuestro asombro puesto que un breve espacio de tiempo, un individuo

que apenas sabe hablar, consigue realizar una acción de dicho dispositivo, y que puede ser que en su día, el inmigrante digital necesitara incluso de la lectura del manual de instrucciones para poder realizarla.

Las computadoras, Internet, móviles, consolas tablets o redes sociales son parte de su vida cotidiana. No entienden que es lo que los inmigrantes digitales hemos estado haciendo estos años sin un portátil, una Tablet o una conexión a internet. Ya que para ellos, las computadoras, y demás accesorios para la conexión a internet, son tan cotidianos como la televisión o la radio lo fueron para generaciones más antiguas.

Figura 5: Los adolescentes y su forma de ver el mundo y relacionarse con él, marcará el rumbo que tomará su educación.

Las diferencias entre nativos digitales y los inmigrantes se manifiestan diariamente en el hogar, en la escuela, el trabajo, etcétera.

En función del uso de la tecnología, los nativos digitales hay desarrollado gestos o hábitos potenciados por el uso de las tecnologías tanto en situaciones cotidianas, de ocio y/o trabajo. Por ejemplo, los jóvenes tocan el timbre con el dedo pulgar en lugar de con el dedo índice, tal y como los inmigrantes y analfabetos estamos acostumbrados a hacerlo. Ellos, sin darse cuenta, han adquirido mayor movilidad para ese dedo, el mismo que usan para jugar con las consolas de videojuegos y con el que se comunican los adolescentes de hoy vía SMS por el móvil. Estos hábitos han desarrollado una destreza única en esta generación, dando lugar a otra denominación

Ante la necesidad de obtener una información, los nativos quieren obtenerla de forma ágil e inmediata, por lo que basan su búsqueda de información en internet, a diferencia de los inmigrantes digitales, que aunque también utilizamos esa opción, muchas veces preferimos buscarla en otros formatos tales como libros especializados en dicho tema en cuestión.

Los jóvenes nativos, se sienten influenciados por la tecnología y se sienten atraídos por multitareas y procesos paralelos. Esta actitud choca con la de los inmigrantes que prefieren realizar las cosas paso a paso y sobre una actividad a la vez, se embarcan en la lectura de manuales impresos para obtener más información y aprender a su ritmo, sin descanso, pero detrás de una actividad, la siguiente. Sus actividades

son secuenciales, aunque en escasas ocasiones pudiera permitirse realizar un baja número de procesos paralelos.

Otra diferencia entre los nativos e inmigrantes será el formato elegido para la obtención de la información, mientras que el nativo muestra su preferencia a archivos gráficos, visuales e interactivos, la elección del inmigrante se decanta más hacia el texto, aunque siempre acepta los archivos gráficos como apoyo o complementación a su ansiada búsqueda de información.

Según Marc Prensky, en su artículo "Nativos e Inmigrantes digitales", los nativos digitales se inclinan por los accesos al azar (desde hipertextos), es decir, en la red hacen consultas generales y a medida que van adquiriendo información, van profundizando y eligiendo su propio camino para la obtención de la información definitiva deseada.

Los nativos, están acostumbrados a estudiar con la ayuda de internet, lo consultan todo y ante alguna duda, buscan en la red, siendo más efectivos y rinden más cuando trabajan en red, pues tienen la conciencia de que van progresando, lo cual les reporta satisfacción y recompensa inmediatas.

Los nativos prefieren instruirse de forma lúdica a embarcarse en el rigor del trabajo tradicional, este diferencia, se sufre casi a diariamente en el seno de cualquier familia, puesto que los padres no comprenden como sus hijos pueden estar estudiando con la televisión y/o el ordenador encendidos, piensan que los nativos digitales solo las emplean para

divertirse, y no necesariamente como instrumentos para favorecer el aprendizaje o mejorar la productividad, es decir, no entienden que mientras sus hijos están jugando o explorando en internet, estos puedan estar aprendiendo.

Los padres no lo entienden, y quieren que el hijo deje de "jugar", se siente a la mesa, abra un libro, lo lea y comience a estudiar, como los inmigrantes lo hemos hecho toda la vida, porque leer conlleva que haya una historia, una lógica, mientras que internet y los videojuegos se refieren más a la interacción, respuestas rápidas, resolución de problemas,…. No nos damos cuenta, pero cuando nuestros hijos están jugando, también están aprendiendo esos valores, y es importante que los padres entiendan esto.

Cuanto más comprendamos a nuestros hijos, menor distancia digital tendremos con ellos.

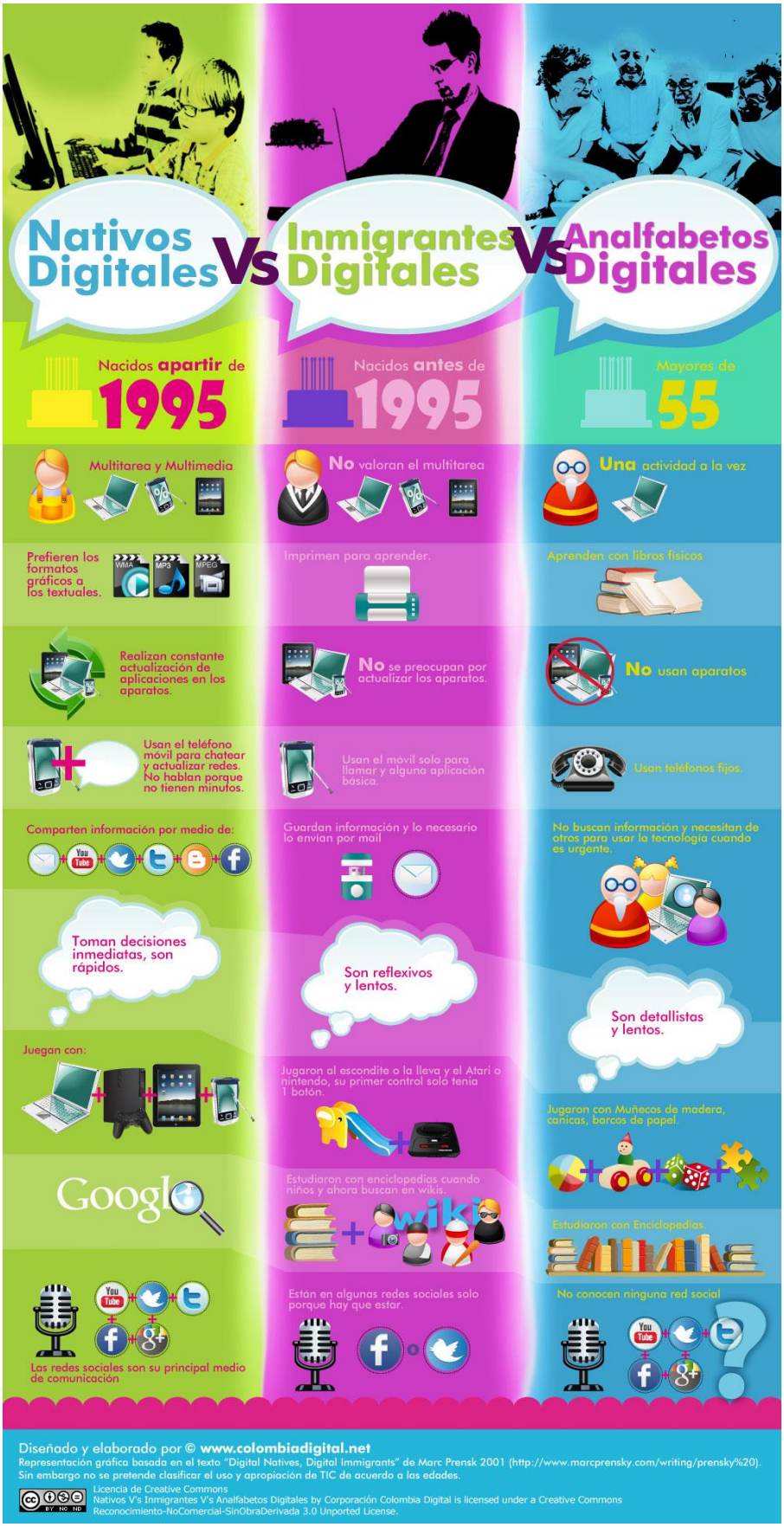
Los nativos digitales sienten atracción por todo lo novedoso en tecnología, logrando tener inmediatamente una habilidad extraordinaria en su uso, sin necesidad de leer ningún manual de instrucciones previamente,

Su forma de estudiar, por lo tanto pasa por absorber rápidamente la información multimedia de imágenes y videos, igual o mejor que si fuera texto, consumiendo datos simultáneamente de múltiples fuentes, interactuando con ellas cuando es preciso e incluso, recibiendo

respuestas instantáneas, permaneciendo comunicados permanentemente

Navegan con fluidez, e incluso crean también sus propios contenidos, utilizando reproductores a diario y comparten sus creaciones.

En la siguiente figura mostramos una representación gráfica basada en el texto "Digital Natives, Digital Immigrants" de Marc Prensky 2001 Fuente: http://marcprensky.com (Figura 6).


Nativos Digitales
Vs
Inmigrantes Digitales
Vs
Analfabetos Digitales
Nacidos apartir de 1995
Nacidos antes de 1995
Mayores de 55
Multitarea y Multimedia
No valoran el multitarea
Una actividad a la vez
Prefieren los formatos gráficos a los textuales.
Imprimen para aprender.
Aprenden con libros físicos
Realizan constante actualización de aplicaciones en los aparatos.
No se preocupan por actualizar los aparatos.
No usan aparatos
Usan el teléfono móvil para chatear y actualizar redes. No hablan porque no tienen minutos.
Usan el móvil solo para llamar y alguna aplicación básica.
Usan teléfonos fijos.
Comparten información por medio de:
Guardan información y lo necesario lo envían por mail
No buscan información y necesitan de otros para usar la tecnología cuando es urgente.
Toman decisiones inmediatas, son rápidos.
Son reflexivos y lentos.
Son detallistas y lentos.
Juegan con:
Jugaron al escondite o la lleva y el Atari o nintendo, su primer control solo tenia 1 botón.
Jugaron con Muñecos de madera, canicas, barcos de papel.
Estudiaron con enciclopedias cuando niños y ahora buscan en wikis.
Estudiaron con Enciclopedias.
Las redes sociales son su principal medio de comunicación
Están en algunas redes sociales solo porque hay que estar.
No conocen ninguna red social
Diseñado y elaborado por © www.colombiadigital.net
Representación gráfica basada en el texto "Digital Natives, Digital Immigrants" de Marc Prensk 2001 (http://www.marcprensky.com/writing/prensky%20).
Sin embargo no se pretende clasificar el uso y apropiación de TIC de acuerdo a las edades.
Licencia de Creative Commons
Nativos V's Inmigrantes V's Analfabetos Digitales by Corporación Colombia Digital is licensed under a Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported License.

Alfabetización digital

El concepto de **alfabetización** ha evolucionado con el paso de los años. La idea tradicional que lo limitaba al aprendizaje de la lectura, la escritura y las nociones básicas de cálculo todavía se utiliza ampliamente, así como el concepto de **alfabetización funcional**, que lo vincula con el desarrollo socioeconómico. Pero han surgido otras modalidades de alfabetización con el fin de abordar las distintas necesidades de aprendizaje de las personas en las sociedades del conocimiento.

> *"La alfabetización es mucho más que una prioridad educativa. Es la inversión de futuro por antonomasia y la primera etapa de cuanta nueva alfabetización se emprenda en el siglo XXI. Queremos un siglo en el que todos los niños sepan leer y explotar esta ventaja para ganar en autonomía."*
>
> *Irina Bokova, Directora General de la UNESCO*

Desde hace más de 40 años, la UNESCO viene celebrando el Día Internacional de la Alfabetización, en el que recuerda a la comunidad mundial que la alfabetización es un derecho humano y constituye la base de todo aprendizaje. Se han logrado muchos progresos realizados en gran cantidad de países para que la población aprenda a leer y escribir.

Sin embargo, todavía hoy, existen en el mundo 880 millones de adultos que no saben leer ni escribir, de los cuales dos terceras partes son mujeres. De los más de 120 millones de niños que se ven privados de educación básica, las dos terceras partes son niñas.

Uno de los grandes desafíos que permanecen es la **alfabetización de las mujeres**, marginadas históricamente del acceso a estos conocimientos. Sin embargo, la experiencia ha demostrado que la inversión en la educación de las niñas y la consiguiente capacitación de las mujeres se traducen directamente en una mejor nutrición, salud y rendimiento económico para sus familias, sus comunidades y, por último, para sus países. De hecho, resulta más eficaz incluso que la inversión en educación masculina.

Figura 7: Cartel anunciador del día Internacional de la alfabetización 2013. Fuente: UNESCO.

El día indicado por la UNESCO para celebrar esta conferencia de dos días de duración y que lo forman parte más de 45 países, será el 8 de septiembre y estará dedicado según explica en su página web, a "las

modalidades de alfabetización del siglo XXI", con miras a poner de relieve la necesidad de alcanzar "las competencias básicas de alfabetización para todos" y dotar a cada persona de las más avanzadas aptitudes de lectoescritura y cálculo, como parte del aprendizaje a lo largo de toda la vida. A continuación indicamos el enlace a la web:

http://www.unesco.org/new/es/unesco/events/prizes-and-celebrations/celebrations/international-days/literacy-day/

La alfabetización es a la vez un derecho humano, un instrumento de autonomía personal y un medio de alcanzar el desarrollo individual y social. Las oportunidades educativas dependen de la alfabetización. Además, la alfabetización es el eje mismo de la Educación para Todos y resulta esencial para erradicar la pobreza, reducir la mortalidad infantil, frenar el crecimiento demográfico, lograr la igualdad de género y garantizar el desarrollo sostenible, la paz y la democracia.

Una educación básica de calidad dota a los alumnos de competencias en lectura, escritura y cálculo que les acompañan durante toda la vida y propician el aprendizaje posterior; es más probable que los padres alfabetizados escolaricen a sus hijos; las personas alfabetizadas tienen más capacidad para acceder a las oportunidades de la educación permanente y las sociedades alfabetizadas están mejor equipadas para afrontar las urgencias del desarrollo.

El uso de la alfabetización para intercambiar conocimientos evoluciona constantemente, a medida que progresa la tecnología. Desde la Internet hasta el envío de mensajes de texto por los teléfonos móviles, la

disponibilidad cada vez mayor de medios de comunicación propicia el aumento de la participación social y política. Una comunidad alfabetizada es un colectivo dinámico, en el que se intercambian ideas y se suscitan debates. En cambio, el analfabetismo es un obstáculo en la consecución de una calidad de vida superior e incluso puede ser el caldo de cultivo de la exclusión y la violencia.

Las imágenes presentadas en la página siguiente, representan el gráfico informativo, publicado por la UNESCO, para la celebración del 8 de septiembre de 2013 como Día Internacional de la Alfabetización 2013.

Fuente: http://www.unesco.org/new/es/unesco/events/prizes-and-celebrations/celebrations/international-days/literacy-day/


DÍA INTERNACIONAL DE LA ALFABETIZACIÓN 2013
MILLONES DE NIÑOS ESTÁN DESTINADOS A TRANSITAR POR LA VIDA SIN SABER LEER NI ESCRIBIR
Todos los años, se observa una reducción del número de adultos que no saben leer ni escribir. Gracias a un mayor acceso a la educación, los adultos jóvenes de hoy tienen una posibilidad bastante mayor que sus padres de estar alfabetizados. Sin embargo, millones de niños aún se encuentran fuera de la escuela y millones más abandonan la escuela primaria sin haber adquirido las competencias básicas de alfabetismo. En otras palabras, estos menores del siglo XXI, la mayoría de los cuales son niñas, están destinados a vivir marginados de la vida social y económica de nuestro mundo. Debemos cumplir nuestra promesa: Educación para Todos.
DÉMOSLE UN VISTAZO MÁS DE CERCA
HAY
774 MILLONES
de ADULTOS analfabetos
(mayores de 15 años de edad)
HAY
123 MILLONES
de JÓVENES analfabetos
(15 a 24 años de edad)
2/3
493 MILLONES
son mujeres
Para ellas, leer la etiqueta de un envase de remedios, completar un formulario o enviar un mensaje de texto requiere mucho esfuerzo.
2/3
76 MILLONES
son mujeres
En el caso de las mujeres en condición de pobreza, aprender a leer es una actividad que conlleva sacrificios y requiere tiempo del que no disponen.
UN HECHO SORPRENDENTE
EL GRUPO DE JÓVENES QUE NO SABE LEER NI ESCRIBIR SE HACE CADA VEZ MÁS PEQUEÑO, PERO NO ASÍ LA PROPORCIÓN DE MUJERES JÓVENES ANALFABETAS.
¿DÓNDE VIVEN?
De las 76 millones de mujeres jóvenes analfabetas, 54 millones se concentran en solo 9 países.
0
5 MILLONES
10 MILLONES
15 MILLONES
20 MILLONES
25 MILLONES
30 MILLONES
INDIA
PAKISTÁN
NIGERIA **
ETIOPÍA
BANGLADESH *
REPÚBLICA DEMOCRÁTICA DEL CONGO **
REPÚBLICA UNIDA DE TANZANIA **
EGIPTO
BURKINA FASO
Población analfabeta jóvenes, mujeres
Población analfabeta jóvenes, hombres
Datos para 2011 o el año más reciente disponible
* Estimación del UIS
** Datos basados en una prueba de lectura de una encuesta nacional de hogares


En algunas partes del mundo se ha observado un aumento constante de las tasas de alfabetización. En otras, éstas se han estancado y permanecen lejos de la meta del 2015 de reducir el analfabetismo a la mitad.
ASIA ORIENTAL Y EL PACÍFICO
ASIA MERIDIONAL Y OCCIDENTAL
AMÉRICA LATINA Y EL CARIBE
ÁFRICA SUBSAHARIANA
1990 2000 2011 2015
Tasa de alfabetización de adultos
Tasa de alfabetización de jóvenes
De no mediar cambios, algunos países continuarán soportando altas tasas de analfabetismo. Este hecho dificultará los esfuerzos de desarrollo de las próximas décadas.
EGIPTO
MALI
INDIA
Datos para jóvenes (15-24 años de edad)
Población analfabeta jóvenes, mujeres
Población analfabeta jóvenes, hombres
¿QUIÉNES SERÁN ANALFABETOS EN EL FUTURO?
57 MILLONES
de niños fuera de la escuela
1 de cada 2
vive en África Subsahariana
1/2 nunca asistirá a clases
1/2 abandonó la escuela o ingresará con rezago
A NIVEL MUNDIAL
250 MILLONES de niños en edad de cursar educación primaria, asistan o no a la escuela, carecen de las competencias básicas de lectura y escritura.*
*Fuente: Informe de Seguimiento de la EPT en el Mundo - 2012

Figura 8: Infografico 2013 publicado por la UNESCO, para la celebración del 8 de septiembre como Día Internacional de la Alfabetización 2013

Definición del Ciberacoso

DEFINICION DEL CIBERACOSO

El Diccionario de la Real Academia de la Lengua, define **acosar** como:

«1. Perseguir, sin darle tregua ni reposo, a un animal o a una persona. 2. (…) 3. Perseguir, apremiar, importunar a alguien con molestias o requerimientos».

Y el Diccionario también tiene registrada otra palabra clave como lo es **acoso** y la define de la siguiente manera:

«1. Acción y efecto de acosar. 2. (…) 3. ~ *Sexual*. El que tiene por objeto obtener los favores sexuales de una persona, cuando quien lo realiza se halla en posición de superioridad respecto de quien lo sufre».

Sin embargo la palabra ciberacoso por el momento no se encuentra registrada en el diccionario. Como consecuencia la definición todavía no tiene versión oficial pero podríamos intentar definir el **ciberacoso**, como la acción de llevar a cabo "amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, correo electrónico, mensajería instantánea, videoconsolas online, etc.".

El ciberacoso, por lo tanto, se convierte en una situación aún más grave cuando hablamos de la implicación de menores o de adultos y menores. La línea que separa el acoso del ciberacoso es ya inexistente; todos los conflictos que se inician en el ciberespacio afectan de forma inexorable a la comunidad social y educativa donde el menor se

integra. Y las consecuencias sociales, morales, psicológicas,... son imprevisibles.

Con esta definición, dentro del contexto del mal uso de las nuevas tecnologías, nos encontramos, como ya hemos introducido, con dos fenómenos que suponen una clara situación de riesgo para los menores y que los tienen como actores: el *Cyberbulling* y el *grooming*.

Ciberbullying

El ciberbullying es un tipo concreto de ciberacoso aplicado en un contexto en el que únicamente están implicados menores que supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de los medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de dispositivos móviles o la publicación de vídeos o fotografías en plataformas electrónicas de difusión de contenidos.

¿Cuáles pueden ser las causas de la aparición de este fenómeno? Algunos especialistas lo achacan a la temprana inmersión en las nuevas tecnologías de los menores de esta generación, sin contar con un apoyo educativo en los conceptos relacionados con la seguridad de la información o de utilidad de los datos, además de tener una falta de conceptualización de la privacidad tanto propia como de los demás. A

esto se añade el que los menores no se dan cuenta de la viralización de los contenidos que se produce al utilizar las redes sociales.

Según indica el gerente del Observatorio de la Seguridad de la Información de INTECO, Pablo Pérez, "en general, se trata de conductas que no tienen su origen en las TIC en un sentido estricto, sino en situaciones y actitudes humanas preexistentes, que han encontrado en Internet un canal rápido de difusión."

La **Guía legal sobre el ciberbullying y grooming**, editada por el Observatorio de la Seguridad de la Información de INTECO http://www.inteco.es/tagObservatory/Seguridad/Observatorio/Actualidad_Observatorio/guia_ciberbullyin_es , indica cuáles son las **características** del *ciberbullying*:

- "Que la situación de acoso se dilate en el tiempo: excluyendo las acciones puntuales.

- Que la situación de acoso no cuente con elementos de índole sexual. En este caso ya se consideraría *grooming*.

- Que víctimas y acosadores sean de edades similares.

- Que el medio utilizado para llevar a cabo el acoso sea tecnológico: Internet y cualquiera de los servicios asociados a ésta: telefonía móvil, redes sociales, plataformas de difusión de contenidos".

Como avance, desde el punto de vista legal, el **tipo penal** más próximo al *ciberbullying* es el que recoge el artículo 197 del Código Penal, en el que se detalla la revelación de información a terceros sin

consentimiento del titular y en el que se recoge la posibilidad de que la víctima sea un menor o un incapaz.

En octubre del 2012, se hace pública mundialmente un video de una adolescente llamada Amanda Todd víctima del bullying que subió a You Tube el video de su desesperación antes de terminar con su vida. Por desgracia fue el primero que se hizo público es te tipo de denuncia por internet, pero sin embargo no es el único, otros adolescentes se han visto en la misma situación. Y nosotros como padres y/o educadores debemos tener en cuenta para evitar que ocurran más situaciones como las vividas por Amanda, cuyo enlace es el que sigue:

http://www.youtube.com/watch?v=NaVoR51D1sU

Grooming

El **child grooming** es un término anglosajón que se refiere al acoso de carácter sexual por parte de un adulto hacia un menor, y se refiere a acciones llevadas a cabo deliberadamente, con el objetivo de establecer una relación y control emocional sobre un niño/a para luego abusar sexualmente del mismo. A diferencia del Cyberbulling, este tipo de acoso tiene un objetivo explícitamente sexual.

El grooming se da cuando un adulto engaña a un menor a través de programas de comunicación como los chat, redes sociales o servicios de mensajería, intentando obtener imágenes de contenido erótico,

para luego extorsionar al menor, dificultando que la víctima pueda salirse o protegerse de esta situación e impidiendo que la relación se corte.

Los sujetos que realizan estas acciones ingresan a estos sitios virtuales cambiando su identidad, sexo y edad, aparentando ser menores de edad (o simplemente como adultos bien intencionados) y, tratan de establecer una amistad con su víctima. Las víctimas, generalmente son convencidas para que realicen actos de tipo sexual ante la cámara web. Los acosadores comienzan a chantajear a los niños o niñas o les prometen regalos, con el fin de ir estableciendo mayores grados de compromiso en la relación. Algunos incluso suelen concertar citas directas con las potenciales víctimas, para luego abusar sexualmente de ellos.

El primer contacto se genera, en la mayoría de casos, sin haberlo pedido ni buscado, o por un error cometido por el menor, al facilitar su correo en cualquier sitio web que ofrece juegos o actividades para niños.

Figura 9: Hay que controlar las relaciones que establecen sus hijos por internet.

Desde el punto de vista legal, el tipo penal más próximo al *grooming* se encuentra en el artículo 183 bis del Código Penal, en el que, como se verá en el apartado correspondiente, se determinan los actos encaminados al contacto por cualquier medio con menores, acompañados de actos materiales de acercamiento y con el fin de cometer delitos de agresiones y abusos sexuales o relativos a la corrupción y prostitución de menores.

Según explica el juez de lo Penal Lorenzo Álvarez de Toledo, "constituye una figura en la que se combinan la protección de un determinado bien jurídico, la indemnidad sexual de menores de trece años, y la utilización de procedimientos tecnológicos. No existe una única figura penal que se corresponda con el ciberacoso, sino que el ciberacoso constituiría un medio utilizable para atentar contra la vida, la seguridad personal, la indemnidad sexual y por lo tanto, con independencia del art. 183 bis recientemente introducido en el Código Penal, tendría que reprimirse a través de las figuras delictivas generales: el delito de homicidio, el de amenazas, el de coacciones, el de revelación de secretos….".

Además, si no se llegase a producir el contacto entre el menor y el adulto, según indica la abogada Paloma Llaneza, "habría que desglosar los actos realizados por parte del adulto", entre los que se pueden encontrar casos de coacciones o allanamiento informático, entre otros.

Sexting

Según Wikipedia, **Sexting** (contracción de *sex* y *texting*) es un anglicismo para referirse al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles.

Figura 10 y 11: Representan la obtención de fotos comprometidas a través de un móvil y posteriormente remitida a otros usuarios, difícilmente podremos controlar a que usuarios se han recibido.

Comenzó haciendo referencia al envío de mensajes de texto (SMS) de naturaleza sexual. No sostiene ninguna relación y no se debe confundir el envío de vídeos de índole pornográfico con el término "Sexting". Es una práctica común entre jóvenes, y cada vez más entre adolescentes.

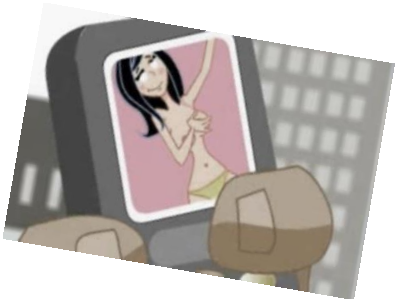
El desconocimiento de las implicaciones que puede tener el hecho de mandar fotos de desnudos o semidesnudos a través del celular o internet, así como la carencia de una educación desde la escuela y el hogar, hacen que los menores sean blancos para redes de trata de personas, turismo sexual y pedofilia.

Por el momento, no hay legislación que recoja explícitamente el sexting, tan sólo puede ser "recogida" dentro de las aseveraciones que la Unión europea recoge en el convenio del Consejo de Europa para la protección de los niños contra la explotación y abuso sexual.

También encontramos que en Estados Unidos, hay diversos proyectos en marcha para prohibir el sexting, donde se plantean prohibir que los menores de 12 a 17 años manden fotografías donde se muestren ellos mismos u otros adolescentes en una actividad sexual o en estado de desnudez sexual explícita. *Según la página web* http://www.ncsl.org/issues-research/telecom/sexting-legislation-2012.aspx

En 2007, 32 adolescentes de Victoria (Australia) fueron denunciados a causa de actividades de sexting. En enero de 2009 se imputaron cargos de pornografía infantil a seis adolescentes en Pennsylvania después de que tres chicas hubieran pasado fotos sexuales a tres compañeros masculinos de clase. En Florida, un chico de 19 años permanecerá inscrito en el registro de delincuentes sexuales del Estado hasta que tenga 43, por haber reenviado una foto de su ex-novia desnuda a varias decenas de personas.

Las razones más comunes por las que realizan el sexting son: romance, coqueteo, popularidad, presión por amistades venganza, intimidación,… chantaje.



El peligro del sexting es que ese material puede ser difundido de manera muy fácil y amplia, de manera que el remitente inicial pierde totalmente el control sobre la difusión de dichos contenidos.

Se ha señalado al sexting como causante de ciertas consecuencias imprevistas y graves. Se ha relacionado con situaciones tan embarazosas, tras haberse pasado fotos a terceros, que han conducido al suicidio del remitente original.

Happy Slapping

Entre los distintos tipos de ciberbullying, uno de los que mayor repercusión social ha alcanzado, si no el que más, es el conocido como happy slapping. Su importancia y sus características, de algún modo diferentes al resto de agresiones online, hacen que consideremos este fenómeno como otra forma de acoso.

Según Wikipedia, se describe el **Happy Slapping** como el ataque inesperado sobre una víctima mientras un cómplice del agresor graba lo que está sucediendo, normalmente por medio de la cámara de un teléfono móvil, con el objetivo de difundirlo a redes sociales o plataformas de compartición de contenidos.

Los agresores graban de forma premeditada una acción de violencia, poniendo el énfasis en la imagen indefensa de la víctima, su cara de miedo, indefensión, impotencia,…. Que posteriormente al ser subidas a la red, estarán expuestas al dominio público.

La expresión happy slapping aparece por primera vez en enero de 2005 dentro del suplemento de educación del periódico The Times. En el artículo *"Bullies film fights by phone"* de Michael Shaw (21 de enero de 2005) se describe la preocupación creciente de los profesores de las escuelas londinenses por la nueva moda de grabar con las cámaras de los teléfonos móviles los episodios de bullying que se producen en las escuelas. Tanto en este artículo, como en otros del mismo periodo, se señala como de incidentes aislados producidos a finales de 2004 en el sur de Londres, aunque no por ello menos graves, se había pasado a un fenómeno generalizado en todo el país en un breve intervalo de tiempo. Desde entonces el fenómeno del happy slapping sigue extendiéndose, siendo cada vez más frecuente en distintos países.

Pese al nombre, las agresiones que se desarrollan bajo esta modalidad no son sólo bofetones o tortazos. Incluso se han llegado a grabar violaciones, agresiones sexuales de todo tipo o palizas, que en algún desgraciado caso han llegado a terminar con la muerte de la víctima. La característica que parecería dar coherencia interna a la gran variedad de formas de agresión que se incluyen dentro del ***happy slapping*** es la intención, por parte de los agresores, de mostrar los ataques como un juego, aunque como ya hemos mencionado en algunos casos se alcancen cotas de gran violencia.

Figura 12: Escena en figuras de porcelana simulando "happy slapping" obtenida en la página: http://www.infoniac.com/offbeat-news/artist-uses-porcelain-figures-to-illustrate-modern-youth.html

Entre las características que posee este fenómeno, podemos destacar su carácter grupal. Dentro de los diferentes tipos de ciberbullying la mayoría poseen una naturaleza donde destacan, aunque no sean las únicas formas posibles, las agresiones uno contra uno, es decir, un agresor que ataca a una víctima cada vez.

En los episodios de happy slapping, por el contrario, son necesarios al menos dos agresores, ya que uno de ellos debe grabar la agresión que protagoniza el otro. Esta colaboración daña, si cabe, aún más a la víctima, que percibe un mayor número potencial de agresores y, como consecuencia, menos opciones para poder resolver la situación por sí misma. *(Extraído de: Acting against school bullying and violence. The role of media, local).*

Debido al incremento de número de adolescentes que disponen de un terminal móvil ha facilitado que este fenómeno del happy slapping siga extendiéndose como la pólvora, desde patios de las escuelas a ciudades de distintos países. Los adultos nos debemos plantear seriamente la forma en que los niños acceden a estas situaciones, y controlar el tráfico de datos que realizan, para evitar llegar a esta situación en la que el menor pueda ser víctima o agresor.

Hay que plantearse como evitar que la difusión de tal violencia se convierta en entretenimiento. La mejor opción pasará por una educación y una comunicación permanente con ellos.

Phishing.

El **phishing** es el intento de fraude a través de Internet que busca la adquisición de información personal y/o financiera del usuario.

La amenaza consiste en que el atacante, simula la identidad de alguna entidad bancaria conocida y de confianza por el usuario. Las vías de este ataque pueden ser un correo electrónico, un mensaje de texto o una llamada telefónica, entre otros.

El atacante intenta duplicar la identidad simulada de la forma más realista posible, y cercana a la realidad para hacer más creíble el engaño y lograr que mayor cantidad de usuarios caigan en la trampa.

Una vez que hemos "mordido el anzuelo" y creyendo estar otorgando la información a alguien de confianza, entregaremos información confidencial al delincuente, el cual podrá utilizarla para realizar un robo, una estafa o un fraude.

En el caso de adolescentes, el atacante se suele ganarse la confianza del menor, mediante llamada telefonica o tambien es muy común, que duplique la entrada del juego favorito del menor y le indique mendiante ventanas que para continuar jugando o para adquirir la "super-arma" que va a matar a todos los malos del juego para quien la posea, es necesario que rellene ciertos datos y esos la mayoria de las veces sulen ser los datos de la tarjeta bancaria de los padres.

Si es fácil que un adulto sea engañado de esta forma, imaginar la facilidad que tendrán con los menores. Por lo tanto, hay que adquirir unos hábitos para asegurarnos una navegación lo más segura posible.

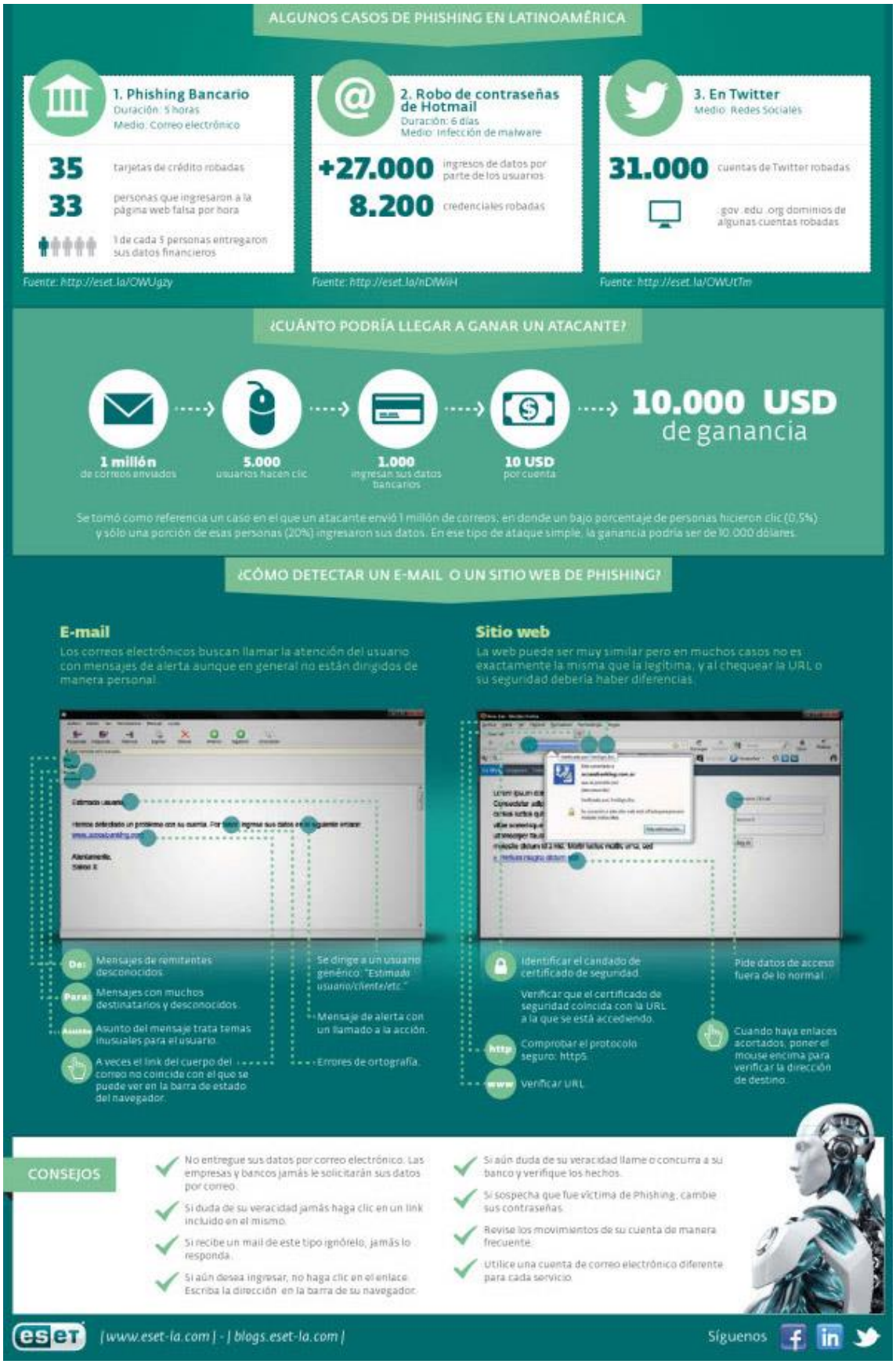
Para ello, debemos tener en cuenta que no debemos entregar información personal y/o financiera en ningún sitio sin previamente verificar con quien nos comunicamos, y si anteriormente ya la hemos facilitado o no la misma información, pues las entidades bancarias nunca solicitan este tipo de documentación por correo, teléfono o fax,

sino que suelen remitir a la entidad bancaria y allí comprobar personalmente los datos a completar.

A continuación, asociamos una infografía que realiza la empresa ESET, especialista en creación de sistemas de seguridad informática, que explica cómo funciona el phising y el robo de identidad. (Figura 13).

Fuente: http://noticias.eset.es/node/42


¿Cómo funciona el Phishing?
El Phishing consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante. Para lograr su cometido, este tipo de ataque se vale de técnicas de Ingeniería Social para engañar a los usuarios y que estos confíen sus datos al atacante.
¿QUÉ TIPO DE INFORMACIÓN ROBA?
Datos personales
Información financiera
Credenciales de acceso
PRINCIPALES MEDIOS DE PROPAGACIÓN
Correo electrónico
Redes Sociales
SMS/MMS
Llamados telefónicos
Infección de malware
CIRCUITO DE UN ATAQUE
1
2
3
4
Consecuencias:
• Robo del dinero en la cuenta bancaria
• Uso indebido de la tarjeta de crédito
• Estafa
• Venta de los datos personales
• Suplantación de identidad
• Envío de publicidad
5
PHISHING CON GEOLOCALIZACIÓN


ALGUNOS CASOS DE PHISHING EN LATINOAMÉRICA
1. Phishing Bancario
Duración: 5 horas
Medio: Correo electrónico
35 tarjetas de crédito robadas
33 personas que ingresaron a la página web falsa por hora
1 de cada 5 personas entregaron sus datos financieros
Fuente: http://eset.la/OWUgzy
2. Robo de contraseñas de Hotmail
Duración: 6 días
Medio: Infección de malware
+27.000 ingresos de datos por parte de los usuarios
8.200 credenciales robadas
Fuente: http://eset.la/nDWiH
3. En Twitter
Medio: Redes Sociales
31.000 cuentas de Twitter robadas
.gov .edu .org dominios de algunas cuentas robadas
Fuente: http://eset.la/OWUtTm
¿CUÁNTO PODRÍA LLEGAR A GANAR UN ATACANTE?
1 millón de correos enviados
5.000 usuarios hacen clic
1.000 ingresan sus datos bancarios
10 USD por cuenta
10.000 USD de ganancia
Se tomó como referencia un caso en el que un atacante envió 1 millón de correos, en donde un bajo porcentaje de personas hicieron clic (0,5%) y sólo una porción de esas personas (20%) ingresaron sus datos. En ese tipo de ataque simple, la ganancia podría ser de 10.000 dólares.
¿CÓMO DETECTAR UN E-MAIL O UN SITIO WEB DE PHISHING?
E-mail
Los correos electrónicos buscan llamar la atención del usuario con mensajes de alerta aunque en general no están dirigidos de manera personal.
De: Mensajes de remitentes desconocidos
Para: Mensajes con muchos destinatarios y desconocidos
Asunto: Asunto del mensaje trata temas inusuales para el usuario.
A veces el link del cuerpo del correo no coincide con el que se puede ver en la barra de estado del navegador.
Se dirige a un usuario genérico: "Estimado usuario/cliente/etc."
Mensaje de alerta con un llamado a la acción.
Errores de ortografía.
Sitio web
La web puede ser muy similar pero en muchos casos no es exactamente la misma que la legítima, y al chequear la URL o su seguridad debería haber diferencias.
Identificar el candado de certificado de seguridad.
Verificar que el certificado de seguridad coincida con la URL a la que se está accediendo.
http: Comprobar el protocolo seguro: https
www: Verificar URL
Pide datos de acceso fuera de lo normal.
Cuando haya enlaces acortados, poner el mouse encima para verificar la dirección de destino.
CONSEJOS
No entregue sus datos por correo electrónico. Las empresas y bancos jamás le solicitarán sus datos por correo.
Si duda de su veracidad jamás haga clic en un link incluido en el mismo.
Si recibe un mail de este tipo ignórelo, jamás lo responda.
Si aún desea ingresar, no haga clic en el enlace. Escriba la dirección en la barra de su navegador.
Si aún duda de su veracidad llame o concurra a su banco y verifique los hechos.
Si sospecha que fue víctima de Phishing, cambie sus contraseñas.
Revise los movimientos de su cuenta de manera frecuente.
Utilice una cuenta de correo electrónico diferente para cada servicio.
eset [www.eset-la.com] - [blogs.eset-la.com]
Síguenos

Pedofilia y pornografía infantil.

Según la Wikipedia, etimológicamente, **paidofilia o pedofilia** es derivada del griego *παιδοφιλια* y éste de *παις-παιδος páis-paidós*, "muchacho" o "niño", y *φιλία* filía, "amistad". Es la inclinación sexual por parte de adultos a sentir una atracción sexual primaria hacia niños o adolescentes.

Se considera que *paidofilia* es un término etimológicamente más correcto que *pedofilia*, si bien esta segunda forma es más usada. En relación con la atracción hacia los adolescentes, también suele usarse el término «hebefilia» o «efebofilia».

Por lo tanto, un pedófilo, será un sujeto con una orientación sexual dirigida primariamente a niños, sin apenas interés por los adultos, y con conductas compulsivas no mediatizadas por situaciones de estrés.

El pedófilo suele ser hombre, aunque también hay mujeres pedófilas, estas suelen ser o bien personas con trastornos mentales o bien personas muy solitarias y que viven al margen de la sociedad.

El término **pedofilia** se ha visto confundido con el término **pederastia**. A pesar de que etimológicamente significan lo mismo (ya que ambas se basan en paidós: "niño" o "adolescente"), la pedofilia no se refiere al abuso sexual, sino a la mera tendencia sexual o atracción por un adulto hacia un menor.

La **pederastia** (del griego *παιδεραστία*) es la práctica sexual entre un varón adulto y un menor de edad.

La **Pornografía Infantil** es la reproducción sexualmente explícita de la imagen de un menor. La distribución de este tipo de pornografía, se relaciona estrechamente con la pedofilia.

Cuando el adulto consigue ganarse la confianza y el cariño del menor, pasa a la acción maléfica de engañar, forzando en algún momento a los niños a posar en fotografías, o participar en videos pornográficos, hechos que están penados por ley y atentan contra la dignidad de los niños.

La tecnología juega un rol fundamental en esta amenaza. Por un lado, facilita la tarea para el agresor, de "ganarse la confianza" del niño, utilizando las nuevas herramientas web (chat, foto blogs, foros, etc.) y; por el otro, facilita la distribución de pornografía infantil a través de Internet.

Los padres y educadores como usuarios

LOS PADRES Y EDUCADORES COMO USUARIOS

Señales de alerta de que su hijo pueda ser una víctima.

Debemos educar a nuestros hijos en los valores del respeto, la amistad, la no agresión y la confianza, para poder hablar siempre de todos los temas, expresar sus sentimientos, sus dudas, sus miedos, o cualquier cosa que les pueda suceder. Si acuden al seno familiar los padres podrán actuar, si no recurren a nosotros, difícilmente podremos detectar que están siendo acosados o víctimas de bullying. Los menores que son objeto de acoso casi nunca lo manifiestan voluntariamente. La humillación a la que suelen ser sometidos provoca que guarden silencio sobre su situación, y es ahí donde los padres o tutores comenzaran su función de tanteo y detección del problema que está causando un cambio en la actitud del adolescente.

La mejor forma de prevenir el ciber-acoso es fomentar la comunicación del menor con sus padres y profesores y darle al menor la confianza suficiente para que pueda hablar de sus problemas abiertamente. Además, con una adecuada educación sobre las nuevas tecnologías y su uso pueden hacer que el menor sea menos propenso a caer en este tipo de acoso (no dando datos personales en la red, desconfiando de los desconocidos…).

Pese al silencio por parte de las víctimas de acoso, podemos observar ciertas conductas que pueden ser las señales de que algo no marcha bien en el colegio, y aunque cada adolescente puede verse afectado de distinta manera, las siguientes conductas son las más comunes.

Conductas que nos indican que nuestro hijo sufre bullying escolar

- No quiere ir al colegio y falta a clase, hecho que anteriormente no había sucedido, en ocasiones, va relacionado con malos resultados académicos.

- Siempre sale el último del colegio, pues se espera para salir solo.

- Cambia sus rutas de casa a la escuela, y de la escuela a casa, cuando antes siempre tomaba el mismo camino (tal vez, para que no le siga el compañero que le está haciendo la vida imposible).

- En casa oculta el problema, casi no habla del colegio.

- Muestra dolor físico, llora.

- Se le ve triste, y detectamos cambios de humor.

- Muestra ira o rabia, (se produce un incremento en las conductas que implican agresividad).

- Parece que se muestre más infantil.

- Pesadillas, pérdida de apetito, enuresis, vómitos.

- Puede fingir enfermedades o malestar para evitar ir a clase.

- Estado de ansiedad, nerviosismo, podrían desencadenar ataques de pánico.

- Baja autoestima.

- Pasa más tiempo en casa que antes, ya no sale a jugar con sus amigos.

- Busca amigos de menor edad, pues con ellos se siente seguro.

- Empieza gradualmente a bajar su rendimiento escolar, perdiendo el interés por estudiar, trabajos o deberes escolares,...

- Nos pide dinero sin decir para qué lo necesita, cuando nunca antes lo hacía.

- Hace los trabajos o deberes de otros.

- Presenta señales de agresión física y al preguntarle qué ha ocurrido se pone agresivo, nervioso, no responde con naturalidad y miente.

- Le suelen faltar objetos personales escolares, lápices, carpeta, libros, siempre dice que los ha perdido o descuidado.

- En definitiva, cualquier situación que nos pueda parecer distinta a la habitual.

Señales de alerta de que su hijo pueda ser el acosador.

¿Y si nuestro hijo es el responsable del bullying?

Cuando hablamos de bullying siempre se hablan de víctimas, de los padres o familiares de las víctimas, y de las secuelas de éstos. Pero ¿qué ocurre si nuestro hijo es el agresor?, ¿cómo puedo saber que nuestro hijo maltrata o agrede?

Primeramente, debemos tener en cuenta el entorno familiar, por si ese es la raíz en la que provoca una actitud desfavorable para nuestro hijo,

que se comporta como un espejo de lo que vive y experiencia en su propia casa y lo traslada a la escuela. Si fuera este caso, los padres o tutores no se percatarían del problema, sino que lo verían como una actitud normal según la vivencia de su hogar.

Pero, si por el contrario, el seno del hogar no es motivo para que se expresen de esa forma, tendremos que estar alerta igualmente, pero detectaremos con mayor facilidad dichas conductas que nos puedan hacer sospechar que le pasa algo a nuestro hijo.

Conductas que nos indican que nuestro hijo es el agresor:

- Tiene comportamientos agresivos o impulsivos con miembros de la familia.

- En los juegos vemos que se enfada con mucha facilidad si pierde.

- Encontramos entre sus cosas objetos que no son suyos.

- Vemos como se muestra enfadado, cambios de humor con agresividad, tono alto al hablar.

- Se muestra muy intolerante en casa.

- Insulta o se burla de la familia, o de personajes de la tele.

- Gasta bromas muy desagradables.

- Se muestra insatisfecho, siempre quiere más.

- Su rendimiento escolar suele ser bajo.

- Frecuentemente nos llaman del colegio pues se ve involucrado en conflictos.

- No controla sus reacciones si se le niega una cosa, o se le impone un determinado horario.

- Desde el colegio nos advierten de un cambio de actitud.

- …

Como proteger a nuestros hijos en internet

¿Dónde debemos acudir si nuestro hijo es víctima o culpable de bullying?

Si evidenciamos estos o algunos de estos cambios en nuestros hijos, debemos acudir al colegio, hablar con la tutor/a, psicólogo/a o director/a. Ellos/as nos podrán ayudar a buscar un profesional que nos de unas pautas para solucionar el conflicto.

En muchos casos de bullying las profesoras son las que lo solucionan desde el colegio, pues no son por fortuna casos muy graves. Debemos siempre mantener una relación de confianza con la escuela, y en cualquier caso poder contar con su apoyo, para poder ayudar a nuestros hijos, y educarlos en la no agresión, en la amistad, en la tolerancia, el respeto, para que sean adultos responsables y libres.

Consejos para padres

Las principales armas con que cuentan los padres son la confianza y la educación de sus hijos, para que los menores, confíen y se sientan impulsados a contar cualquier acción sospechosa en la que se vean

envueltos. Además es recomendable tomar una serie de precauciones, tales como:

- Limita la conexión de los menores a solamente cuando los mismos se encuentren acompañados por tí o por otro adulto.
- Limita el tiempo de acceso a internet.
- Crea una cuenta de usuario limitado para el acceso del menor al sistema.
- Intenta controlar el uso inadecuado de la cámara web.
- Habla con tus hijos. Debes saber qué páginas visitan, con quién conversan, qué les gusta ver, etc.
- Infórmate sobre las herramientas que ofrece la web a los menores, los peligros de las mismas y la forma de evitarlos. Así podrás aconsejar a tus hijos sobre la forma más segura de disfrutar de aquello que les gusta.
- Prohíbe a los menores dar información confidencial. Debes enseñar a tus hijos a no facilitar datos como su nombre, su dirección,… a través de la Red.
- Controla las fotos publicadas por tí y por el menor en la red. No se debe llegar al extremo de prohibir pero se debe conocer las fotos publicadas.
- Controla las relaciones que establecen tus hijos por internet. Educa a los menores sobre los riesgos de la red y las formas de evitar caer en trampas de personas inescrupulosas.
- Educa a los menores para que ante la menor duda o problema, confíe en tí y te cuente el inconveniente.
- Permanece atento al comportamiento del menor en su vida real, para detectar cualquier cambio de conducta que podría delatar un abuso por parte de un tercero.

- Decide qué programas se instalan en el ordenador e impedir que se instalen nuevos programas sin autorización.
- Enseña a tus hijos a desconfiar de las apariencias. Muchas veces en la Red nada es lo que parece. Por eso, debes enseñar a los menores a ser desconfiados y a no realizar acciones que pongan en riesgo su seguridad y su intimidad.
- Supervisa las páginas web que visitan tus hijos.
- Vigila (con el único objetivo de protegerles), lo que escriben en el Messenger y otros chats, correos electrónicos, foros,….
- Intenta controlar mediante acceso remoto lo que están haciendo tus hijos en el ordenador.
- Instala un programa de Control Parental que te permitirá asegurarte que tus hijos navegan de manera segura.

Figura 14: Los adolescentes navegan accediendo a foros, chats, juegos, artículos, videos, redes sociales y sería interesante limitar los contenidos a los que acceden

Consejos para educadores

El educador es una figura fundamental para garantizar la seguridad del menor en la ausencia de los padres. Debe, por lo tanto, conservar esa confianza que tiene en el menor y potenciar la educación de sus alumnos.

Además de las recomendaciones propias de los padres, un educador debe adoptar una serie de precauciones, tales como:

- Instala un programa "congelador" en cada ordenador del aula, que evitará que se pueda instalar en el ordenador, nada que no hubiera en el mismo momento en que fue congelado.
- Estudia previamente los conceptos relacionados con los peligros de la red. Descubre cuáles son y qué consecuencias tienen y cómo puedes hacerle llegar esa información a tus alumnos.
- Establece un plan de educación en seguridad informática. Al tiempo que aprenden a manejar y a relacionarse con la informática, los más pequeños deben tomar conciencia de los peligros que encierra.
- Enséñales a protegerse. Entre las clases prácticas, incluye algunas sobre la configuración del antivirus, la creación de contraseñas seguras, etc.

Programas (controles parentales)

Ya hemos visto los posibles riesgos a los que puede darse el caso que nuestros hijos estén sometidos en internet. La obligación de los padres es hacer frente a esta situación y dejar de mirar atrás para no ver lo que ocurre, puesto que nuestros hijos necesitan toda la ayuda y seguridad que les podamos aportar, y eso es un derecho y un deber como padres y educadores que somos.

Los adolescentes navegan accediendo a foros, chats, juegos, artículos, videos, redes sociales y sería interesante limitar los contenidos a los que acceden, las búsquedas que realizan, las personas con las que se relacionan y la información que dan sobre ellos mismos o sobre las personas cercanas. Ya que está en peligro la privacidad y seguridad de nuestros hijos y el resto de familia, amigos, conocidos si dicen lo que no deben, o emiten algún tipo de documento que no deberían.

Es necesario, aplicar algunos programas que nos permitan darnos esa confianza o seguridad requerida, estos programas serán los llamados de "control parental", que serán herramientas o aplicaciones que nos permiten bloquear o limitar el acceso a determinados contenidos en internet y vigilar las actividades que realizan en los ordenadores que emplean nuestros hijos/alumnos y no son aptas para ellos.

Este software de control parental, nos permitirá restringir distintas opciones sobre el ordenador al que se lo apliquemos, tales como: establecer un límite de tiempo para el uso del equipo, evitar el uso de

determinados juegos, bloquear determinadas páginas web, control de informes…

La mayoría de las soluciones disponibles en Internet son de pago, aunque existen algunas que son gratuitas o que al menos permiten probar primero la aplicación para ver si cumple con nuestras expectativas y posteriormente previo pago actualización de versiones más completas que ofrecen mayores garantías de protección que las gratuitas.

Otras aplicaciones, funcionan sobre la base de un pago reducido mensual, mientras que otras permiten la compra del programa y su uso de por vida mediante un único pago. También existen herramientas de las propias operadoras como ONO, Vodafone, Orange,… o Movistar que pueden ayudarnos a controlar lo que nuestros hijos ven.

Existen herramientas especializadas dedicadas solamente a esto y también suites o paquetes de protección que engloban el control parental, el antivirus, firewall y demás herramientas para proteger el ordenador de programas malintencionados y de los hackers.

Hay que tener en cuenta que no todas las aplicaciones proporcionan las mismas herramientas de control ni disponen de todas las características recomendables. Esto hace que a los padres se nos plantee enseguida la duda ¿si no todas me aseguran al completo, entonces cuales o cantas tengo que instalar en mi ordenador?

La respuesta está en los padres, que deben observar a los hijos y en función de lo que ellos utilicen, necesitaran una u otra herramienta.

Evidentemente estos programas no cubren el ámbito de los teléfonos móviles o de las consolas de videojuegos que también proporcionan acceso a Internet. Existen aplicaciones para móviles en exclusiva, diferenciadas de las aplicaciones para PC

Las aplicaciones más sencillas permiten filtrar los contenidos prohibiendo que en los mismos aparezcan ciertas palabras, como puedan ser sexo, pene, bomba, vulva, etc. También permiten prohibir el acceso a páginas web concretas, incluso algunas herramientas disponen de una lista de páginas web a las que prohíben el acceso por defecto, y la lista va creciendo poco a poco.

Este tipo de filtros pueden disponer de listas negras, donde se indican las páginas web prohibidas, con lo que nuestro hijo/alumno gozará de acceso a todas las páginas que no estén en la citada lista; o de listas blancas, que indican las páginas permitidas, quedando prohibidas todas las webs que no estén expresamente indicadas. En ocasiones se trata de una combinación de ambas protecciones y se añaden mecanismos para descartar o marcar como peligrosas páginas con palabras no aconsejables para los menores y que identifican contenidos prohibidos, creando una base de datos cada vez más completa.

Hay determinados programas que impiden la ejecución o puesta en marcha de determinados programas, como los de mensajería

instantánea o redes sociales, por ejemplo, donde podemos indicar o elegir entre una larga lista de programas que no queremos que nuestros hijos puedan utilizar nunca o fuera de determinados horarios y así poder controlar si nuestros hijos pasan demasiado tiempo al ordenador, o que se conecten cuando no estamos.

También hay herramientas que permiten capturar las pantallas que nuestros hijos ven al navegar por Internet, o lo que escriben en sus emails, chats, foros o redes sociales. Son funciones principalmente de programas espía (los llamados "sniffers"). Los hay que toman nota de los programas usados, del tiempo que han sido empleados y de las páginas o servidores accedidos en Internet.

En cualquier caso, si decidimos instalar alguna de estas herramientas, debemos conocer las necesidades y usos habituales que nuestros hijos hacen del PC para no dificultarles su uso más de lo necesario. Y también deberíamos explicarles las razones por las que lo hacemos y qué datos o información de lo que hacen quedan registrados. Siempre debe haber una comunicación de los padres con los hijos al respecto, ya que de lo contrario generaría un malestar de niño puesto que se estaría viendo "observado" y sentirá que su intimidad se está viendo comprometida, potenciando entonces sentimientos y hechos de rebeldía y eso es justamente lo contrario de lo que los padres y educadores deseamos.

En el siguiente apartado hablaremos de algunos programas que nos pueden ayudar a garantizar la seguridad de nuestros hijos en internet, pero me gustaría aclarar que no tengo relación alguna con los creadores de los programas propuestos y que tan siquiera me he puesto

en contacto con ellos. Simplemente me he ido descargando sus aplicaciones –como lo podría hacer cualquier padre– y bajo mi criterio he ido realizando una selección, por lo tanto, dicha selección no será ni mucho menos completa, pero hay que entender que internet cada día va evolucionando y los programas se van actualizando e incluso saliendo nuevos, pero el caso es que los que nombraré les pueden orientar acerca de lo que necesiten para que la navegación de sus hijos sea lo más segura posible.

No incluimos los enlaces, puesto que en el caso de incluirse podrían ser susceptibles de que cambiaran con el tiempo, por lo tanto, si es de su interés, simplemente con buscar el nombre del programa en cualquier buscador, pueden encontrar la versión actualizada de dicho programa en su página oficial correspondiente.

Software bloqueador.

Herramientas de control parental para móviles.

Los teléfonos inteligentes o smartphone, son uno de los dispositivos más usados por los adolescentes para acceder a Internet, su uso se suele referir para ver la transmisión de video y para comunicarse con otras personas mediante el uso de aplicaciones específicas (WhatsApp, u otros similares de mensajería instantánea.

APLICACIÓN	ESPECIFICACIONES	CARACTERISTICAS
Safe Eyes	Para iPhone, iPad o IPod Touch.	Filtra contenido web.
Kaspersky Mobile Security	Para: BlackBerry, Windows Mobile, Android.	Protege contra virus, amenazas de Internet, phishing, spyware y spam. Protege de forma remota los datos y encuentra la ubicación del teléfono en caso de robo.
Kaspersky Tablet Security	Para: BlackBerry, Windows Mobile, Android	☺Protege contra amenazas de Internet, virus y robo del dispositivo. .
SMobile Security Shield		Incluye antirrobo, protección de identidad, escudos ante todo tipo de malware, control parental y fácil de configurar.
Vodafone Protect	Para: BlackBerry Android.	http://www.vodafone.es/apps-y-descargas/es/apps/catalogo/protect/?uuid=

Herramientas de control parental para consolas.

Las consolas de juegos están diseñadas para juegos y no se utilizan masivamente para acceder a Internet. Su uso se basa principalmente para juegos online, chatear con otros jugadores o descarga de contenidos.

Al haber poco uso de internet a través de las consolas, ha ocasionado que sean pocas y no muy conocidas las herramientas para consolas que ofrecen funcionalidades de filtrado y para algunos de ellos todavía parecen en una fase de desarrollo.

Las principales consolas en la actualidad (WII, PS3, Xbox), tienen su propia herramienta de control parental integrada, pero ninguno es capaz de filtrar las páginas web de acuerdo con el contenido.

Estas herramientas se centran en el control de las siguientes actividades en línea: chatear con otros jugadores, juegos en línea y el contenido de la descarga / compra.

APLICACIÓN	ESPECIFICACIONES	CARACTERISTICAS
Trend Micro Kids Safety	Para PS3.	Examina los sitios Web en busca de fraudes, según su registro e historial de cambios, y bloquea los sitios que considera maliciosos.
Astaro Parental Control.	Para WII y Nintendo DS	Ofrece a todos los usuarios de la Nintendo DS Browser y WII, un contenido libre de cargo servicio de filtrado para evitar que los usuarios accedan a contenidos potencialmente inapropiados web.

Herramientas de control parental para PC.

Las herramientas de control parental para PC son las más conocidas por los usuarios de internet, puesto que el PC (ya sea en su versión de sobremesa o portátil) ha sido hasta el momento la forma más común de conectarse a la red, pero va perdiendo terreno en detrimento de los smartphones y las tablets.

Hay resaltar que aunque estas soluciones informáticas son fundamentales, los usuarios deberían conocer sus limitaciones. Para

aumentar la seguridad, sería recomendable, acompañarlas con unos buenos hábitos, que garanticen un uso responsable y seguro de las nuevas tecnologías.

APLICACIÓN	ESPECIFICACIONES	CARACTERISTICAS
Canguro Net Plus (Movistar)	Válido para cualquier navegador (Internet Explorer, Mozilla, Firefox, Safari, Opera, ...)	http://www.movistar.es/particulares/internet/seguridad/listado-completo/ficha/canguro-net-plus Limita acceso a páginas web con contenidos no apropiados, elimina publicidad no deseada, controla descarga de archivos,…
Pack de Seguridad Total (Centinela de ONO)	Válido para cualquier navegador (Internet Explorer, Mozilla, Firefox, Safari, Opera, ...)	http://www.ono.es/productos/internet/pack-seguridad-total/ Incluye: Antivirus + Firewall + AntiSpyware + AntiFraude + AntiPop-ups + Control Parental + Gestor de privacidad.
Control Parental Windows Vista	Inicio>Panel de control.	Establece bloqueos para determinadas páginas webs o aplicaciones, también puede enviar registros de actividad a un email que introduzcamos, establecer distintos filtros web, etc.
Norton On line Family	Valido para Windows y Mac. ,	https://onlinefamily.norton.com/familysafety/loginStart.fs Puede bloquear el acceso a contenido específico, activar funcionalidad “monitor” que proporcionará informes a los padres, bloquear el Messenger, Skype, …
Kaspersky Internet Security	Válido para Windows.	http://www.kaspersky.es/ Es posible bloquear / permitir aplicaciones, también puede fijar un calendario específico para cada aplicación, el padre puede reportado (pero no puede bloquear), el uso de determinadas palabras clave de una lista definida por el padre.
AVG Family Safety	Válido para laptop, iPhone, iPad, iPod Touch, Windows Phone y Windows PC.	http://www.avg.com/us-en/avg-family-safety El control parental de Internet es capaz tanto de personalizar la página web y filtrado para gestionar el uso de algunas aplicaciones. NO proporciona filtrado de palabras clave. Es posible bloquear las redes sociales y el MSN, pero no el Skype.
Cybersieve	Válido para Windows.	http://www.cybersieve.com/ Puede bloquear aplicaciones MSN, P2P, correo electrónico y redes sociales, pero no puede bloquear Skype. Ofrece informe detallado de la actividad en internet y también registro acceso remoto.

F-secure INTERNET SECURITY.		http://www.f-secure.com/en/web/home_global/internet-security Protección contra virus, spyware y otras amenazas de Internet.
Mac OS X Parental Controls.	Para Mac OS X.	http://support.apple.com/kb/VI28 Cada cuenta de usuario en el Mac OS X puede ser controlado por el administrador del sistema (el padre) que puede seleccionar para cada una de las restricciones adecuadas. Hay tres niveles de filtrado de sitios web: (1) sin restricciones, (2) limitan automáticamente la navegación de algunos sitios web, opcionalmente, añadir sitios web personalizados a una lista blanca y una lista negra, (3) Fuerza de navegación sólo en un subconjunto de sitios web que aparecen en una lista blanca precargada con algunos sitios web de cómics relacionados.
Safe Eyes (McAfee) y McAfee Family Protection.	Para Windows y Mac OS.	http://www.internetsafety.com/ Es posible crear varios usuarios y para personalizar el filtrado de acuerdo con las clases de edad. El padre puede crear una lista negra para bloquear el acceso a determinadas páginas, también puede bloquear el acceso a las redes sociales.
File Sharing Sentinel.		http://file-sharing-sentinel.software.informer.com/ Bloquea el uso compartido de archivos P2P, también dispone de función anti-spyware, y evita la descarga de ficheros con contenido inadecuado (pornográfico) o malicioso (virus).
K9 Web Protection.	Valido para IPhone, iPad, Android, PC Windows, IOS,…	http://www1.k9webprotection.com/ Es un filtro de contenidos por categorías altamente configurable que funciona como servicio Web. Permite restricciones por tiempo, listas blancas y negras, además de control sobre aplicaciones P2P, salas de Chat y mensajería instantánea, monitorización de actividad en Internet.

Conclusiones

CONCLUSIONES

El desarrollo de las tecnologías ha estado siempre motivado por el deseo del hombre de controlarlo todo y superar las limitaciones que el ser humano va encontrando a lo largo de su existencia, con la idea de conseguir un mundo mejor, más rápido y cómodo.

> *"Las tecnologías son el conjunto de posibilidades y procedimientos técnicos para transformar la materia que la naturaleza suministra en forma de materiales, bienes, aparatos, conjuntos… requerido para las necesidades humanas y sociales. cómo utilizarlas."*
>
> *(Hillmann, 2001)*

Así, parece que la existencia humana ha evolucionado a medida que ha evolucionado la tecnología.

El uso de internet se ha popularizado y ha conseguido que la inmensa mayoría de los hogares españoles cuenten con al menos un equipo conectado a internet.

Como hemos podido comprobar, toda persona en internet es susceptible alguna vez de experimentar alguna clase de acoso debido a que el uso de internet se ha convertido en parte de nuestra vida cotidiana.

Si un individuo quiere sentirse dentro de la sociedad actual, debe ser usuario de las nuevas Tecnologías de información y Comunicación (TIC), e introducirlo como una parte de su rutina diaria.

El adolescente es una persona muy vulnerable y necesita sentirse incluido en esta sociedad, e incluso ellos, reciben o realizan parte de sus tareas escolares mediante el uso de esta tecnología, por lo tanto, ya sea educadores o familiares del adolescente, deben de asegurar dentro de la medida de lo posible la máxima seguridad en el uso de internet por el adolescente, aplicando las herramientas indispensables de protección en la red contra los fenómenos como el grooming o Ciberbullying.

Toda persona debe aprender a aprovechar las ventajas de la red, siendo conscientes también de los peligros que entraña su uso.

Los padres deben vigilar y supervisar lo que buscan, ven y escuchan sus hijos en internet, a quien conocen y qué datos personales comparten con otros usuarios y principalmente a que edades pertenecen.

La educación y comunicación por parte de niños, padres y educadores, serán por lo tanto pilares fundamentales para el establecimiento del uso seguro, consciente y responsable de internet.

Otro elemento fundamental será la utilización de un conjunto de herramientas de control y seguridad, que aplicadas correctamente

permitirán al adolescente saciar su sed de conocimiento, ocio y entretenimiento sin que sus seguridad se vea comprometida.

Al igual que en la última reforma del Código Penal se ha introducido el delito de "*child grooming*", se hace imprescindible llevar a cabo las reformas necesarias para dar cabida a todos aquellos actos ilícitos que se están generando por el uso intensivo de Internet por los menores: *ciberbullying*, *sexting* , *happy slapping, phishing* , fraudes a menores en SMS Premium , etc.".

En la actualidad, se plantea la necesidad de definir otro nuevo conjunto de derechos a incluir en los textos constitucionales, vinculados a lo que empieza a conocerse como la Sociedad del Conocimiento y que vayan más allá de la mera protección de los datos personales o de una adaptación más o menos forzada de los derechos tradicionales.

Además, cada día aparecen nuevos problemas derivados del uso generalizado de las nuevas redes sociales, tipo MySpace, Facebook, Tuenti o Twitter, por citar solo algunas, que implican a miles de ciudadanos, entre ellos a muchos menores de edad.

Pero todo ello solo puede ser un incentivo para que desde el ámbito jurídico constitucional nos ocupemos continuamente de esta 'nueva frontera' de los derechos fundamentales, donde se están construyendo las bases de la sociedad futura y en la que hay que tener en cuenta estas nuevas necesidades, manteniendo las garantías y los derechos de los ciudadanos. A todos nos compete, bien como ciudadanos o bien

como juristas, no abandonar nuestras responsabilidades y, en el ámbito que a cada uno nos corresponda, ejercer responsablemente nuestros derechos y defender su ejercicio. Del éxito que tengamos va a depender nuestra libertad y la naturaleza del modelo de sociedad que se avecina.

Glosario

GLOSARIO

AC (Tecnologías del Aprendizaje y la Comunicación): tratan de orientar las Tecnologías de Información y Comunicación (TIC) hacia usos más formativos, tanto para el estudiante como para el docente. Estas tratan de explorar los usos didácticos que las TIC tienen para el aprendizaje y adquisición de conocimiento.

Adsense: sistema de publicidad en línea que tiene como objetivo insertar en páginas web anuncios de texto relacionados con el contenido de las páginas, y sacar dinero si sus visitas pinchan en los enlaces.

Android: Sistema Operativo orientado a dispositivos móviles, basado en Linux. Entre sus características se destacan que es libre, gratuito y multiplataforma.

Apropiación TIC: las nuevas tecnologías han despertado el interés de los usuarios frente a la usabilidad de herramientas digitales modernas. Apropiación TIC hace referencia a los conocimientos y prácticas implementadas por los ciudadanos ante los desarrollos y recursos informáticos que hacen presencia en el siglo XXI, contribuyendo al cierre de la brecha digital desde el acceso a Internet.

Autopista de la información: el término se asocia a Internet, entendido como en canal donde se transmiten contenidos y conocimientos. Los

usuarios navegan a través de ella para la obtención de información de interés y/o acercamiento a comunidades online.

Avatar: Representación digital (foto o imagen) que identifica a un usuario en el perfil de una cuenta en redes sociales, chats, videojuegos; entre otros.

Banda ancha: Transmisión de datos que permite incrementar la velocidad de acceso a Internet, facilitando el intercambio y envío de correos electrónicos, navegación web, descarga de documentos y archivos multimedia, ver videos online, realizar videoconferencias, entre otras funciones.

Blended Learning: También conocido como B-Learning, se apoya en las metodologías y procesos de enseñanza que mezcla la comunicación en ambientes de aprendizaje, virtuales y físicos. Los estudiantes tienen la posibilidad de tomar las clases a través de conexión a Internet y asistir a sesiones cara a cara con el docente y demás compañeros.

Blog: Sitio web que almacena archivos multimedia, textos y artículos de cualquier tema, los cuales son actualizados periódicamente por el bloguero o administrador de este. Este término hace referencia a una bitácora personal que recopila informaciones de interés de acuerdo al perfil del blogger. En él pueden participar uno o varios autores, y existe una interactividad entre los lectores que visiten el sitio web, quienes podrán dejar sus comentarios así como calificar el contenido y compartirlo en redes sociales. Las aplicaciones de los blogs permiten

personalizar sus diseños, plantillas y configurar sus gadgets de acuerdo al gusto del bloguero. Estos blogs pueden ser corporativos, tecnológicos, periodísticos, educativos, políticos, personales, culturales, deportivos, etc.

Brecha digital: diferencias socio-económicas entre las comunidades (ya sean ciudades o países) frente a las dificultades de acceso a Internet. Estas limitaciones se relacionan con los usos, apropiación, alfabetización digital, condiciones y calidad de vida de los ciudadanos.

Chat: Conversaciones que desarrollan los internautas a través de plataformas online de manera instantánea y rápida. El software que se utiliza para estos servicios debe contar con conexión a Internet. Los chats pueden ser públicos o privados.

Ciber-café: Es un lugar público que ofrece a los usuarios servicio de Internet y el uso de aplicaciones como procesadores de texto, hojas de cálculo, editores gráficos, videojuegos, impresores, entre otros); habitualmente a un coste determinado por los servicios prestados.

Ciberataques: También se habla de guerra informático o guerra digital, donde el campo de batalla no se traduce a un escenario bélico como tal, sino al uso del ciberespacio y la autopista de la información para provocar ataques informático de alto impacto, que pueden desestabilizar la economía y relaciones políticas de las naciones.

CGU (Contenido Generado por el Usuario): Se refiere a todos los formatos de contenido (videos, audio, fotografías, texto) que una persona crea por sí misma y comparte a través de diferentes sitios Web.

Competencias digitales: Capacidades, habilidades y destrezas que desarrollan los individuos a través de la generación de conocimientos en diversos escenarios (académico, profesional y/o laboral), poniendo en práctica tales destrezas y apoyándose en el uso de recursos tecnológicos.

Computación en la nube: llamado también **Cloud computing**, este término ha roto los paradigmas tradicionales de la tecnología, ofreciendo todo tipo de informaciones y contenidos en Internet, de modo que los cibernautas podrán acceder a todos los servicios ofrecidos en la red. La introducción de este concepto elimina las fronteras de la información, permitiendo el flujo continuo de datos y mensajes. Sin embargo, los usuarios en su mayoría navegan a través de la red sin un conocimiento profundo y experto, solo buscando contenidos de su interés y afinidad.

Copyright: Hace referencia al derecho de autor y a las normas jurídicas y principios que regulan los derechos morales y patrimoniales. No permite compartir ni divulgar cualquier contenido sin autorización expresa del titular de los derechos.

Comunidades online genéricas: Se refieren a los grupos en línea que apuntan a un amplio grupo objetivo, el cual incluye diferentes gustos,

edades, regiones, culturas, etc. Estas comunidades suelen estar en renovación constante de usuarios, lo que difícilmente las puede convertir en líderes de marca u opinión.

Ciberbullying /Ciberacoso: Acoso presentado entre niños y jóvenes usando información electrónica y medios de comunicación: correo electrónico, redes sociales, blogs, mensajería instantánea, mensajes de texto, teléfonos móviles y sitios web con el objetivo de chantajear, insultar, humillar, crear burlas y desprecio a una persona o grupo determinados.

Edublog: Blog con fines educativos. Su objetivo principal es apoyar de forma dinámica el proceso enseñanza-aprendizaje en los estudiantes y lograr aprendizajes significativos a través de la retroalimentación.

E-Books (libro digital): corresponde a la versión electrónica de un libro en físico, publicado en Internet. También se le atribuye este nombre al dispositivo que se emplea para leer los libros en formato electrónico.

E-learning: Modalidad de enseñanza que ha sido posible gracias a la revolución digital y puede desarrollarse de dos formas:

> ***Virtual:*** a través de un computador con acceso a Internet, el docente presenta a sus estudiantes una tutoría con un orden claro y específico de su clase, asignándoles tareas y actividades las cuales deberán ser cumplidas en los plazos establecidos por el tutor.

Semi-presencial: al igual que en la anterior, los estudiantes hacen uso de un PC para comunicarse con el docente, pero al mismo tiempo pueden asistir a sesiones presenciales a fin de aclarar dudas o interrogantes sobre algún tema en específico.

Emoticones: Proviene de las palabras "emoción" e "ícono". Son símbolos gráficos que representan gestos y emociones de una persona: felicidad, tristeza, enojo, llanto, sorpresa, etc. Son utilizadas en servicios de mensajería instantánea como: chat, foros, SMS y correo electrónico.

Fibra óptica: medio a través del cual se transmiten datos de las redes interconectadas a distancia. Estas señales no son afectadas ni por el clima o radiaciones electromagnéticas y la velocidad de transmisión de la información en Internet es mayor a la de un módem.

Flame (Llama de fuego): Se define como aquellos mensajes de tipo groseros, insultantes enviados por correo electrónico y publicado en foros, redes sociales, sitios web entre otros; con el fin de atacar o amenazar a los usuarios.

Foro virtual: Herramienta web que se utiliza como escenario para el intercambio de opiniones y medio de discusión a través de mensajes, de aquellas personas que desean discutir sobre problemáticas específicas.

3G: Es la abreviación que corresponde a la telefonía móvil de tercera generación (servicio universal de telecomunicaciones móviles). Gracias a las características y funcionalidades de este servicio es posible realizar

transferencias de audio, datos, descarga de programas, aplicaciones, envío de correos electrónicos y mensajería instantánea. Actualmente, las operadoras móviles ofrecen este tipo de tecnología a través de un módem USB que proporciona acceso a internet desde un computador o equipo portátil, sin necesidad de tener un teléfono celular. Entre las ventajas del 3G se destaca una mayor velocidad de conexión, aunque la cobertura es limitada ya que depende de la localización del usuario móvil.

4G: Corresponde a la cuarta generación de tecnologías de telefonía móvil. La diferencia de las 2G y 3G es su capacidad de velocidades de acceso a conexión, e igualmente incluye técnicas de avanzado rendimiento. Este servicio está basado en el protocolo IP.

Gadgets o widget: Son objetos en miniaturas que pueden ser colgados en cualquier sitio web, a fin de ofrecer un contenido más dinámico, fresco y creativo. Lista de tareas, horóscopos, reloj, contador de visitas, conversor de monedas, calculadora, herramienta de traducción son algunos de los gadgets utilizados por los cibernautas en las páginas virtuales o blogs.

Gamer: Personas amantes a los videojuegos, quienes concentran gran parte de su tiempo y actividades diarias en estar frente a una videoconsola. Además de ser apasionados y fanáticos por cualquiera de ellos, se interesan por aprender todo lo relacionado con este mundo y ampliar sus conocimientos. Entre sus características, buscan romper y alcanzar sorprendentes récords de juego.

Geek: (del inglés geek, pronunciado "guik": IPA /gi:k/) es un término que se utiliza para referirse a personas amantes de la tecnología y la informática. Poseen amplios conocimientos en esta última área y sus relaciones están atadas a las redes sociales, donde sus lazos más fuertes se sostienen gracias a Internet. Son grandes apasionados a las novedades y suelen dominar con gran facilidad cualquier tipo de gadgets.

Google Plus: o Google+ es la red social de Google, siendo la segunda plataforma más popular del mundo. A diferencia de Facebook y Twitter, esta permite la creación de círculos a los cuales se les añaden los contactos de acuerdo a los intereses del administrador. Pueden ser laborales, académicos, personales, familiares, etc. Ofrece hangouts, servicio de mensajería instantánea, creación de grupos o páginas de intereses y permite la integración con Gmail, Calendar, Docs., entre otros.

Hackers: Personas con grandes conocimientos y habilidades en informática y telecomunicaciones, aplican su talento con un objetivo determinado.

Hangout: Servicio de videoconferencias que ofrece Google, a través de su red social Google+. Permite que los usuarios conversen a través de la cámara web de su ordenador en tiempo real; el tope máximo de participantes es 10. El hangout puede orientarse a cualquier temática y promover la participación de otros usuarios a través del chat.

Hashtag: Etiqueta formada por una o varias frases unidas, antecedidas de símbolo #. Por ejemplo: Días de lluvia, tráfico y calles llenas de gente #Esoctubre. En Twitter, los hashtags más utilizados por los usuarios se convierten en Trending Topic o temas del momento (TT).

Herramientas asincrónicas: Permiten una comunicación que se establece en tiempo no real, es decir los participantes no están conectados en el mismo espacio de tiempo. Ejemplo: correo electrónico, foros, wikis, blogs, FAQ: (Frequentry Asked Question).

Herramientas sincrónicas: Permiten una comunicación en tiempo real. Los participantes deben estar conectados en el mismo momento: ejemplo: chat, videoconferencias, mensajería instantánea.

Hipervínculos: Una o más palabras que hacen parte de un texto web o cualquier otro documento, las cuales se diferencian del resto porque permiten la navegación a otros sitios, para contextualizar la información. Se da clic sobre ellas y automáticamente se abrirá otra ventana.

Identidad digital: Conjunto de información como nombres, imágenes, registros, noticias, vídeos, comentarios, mensajes, etc., que una persona u organización expone en Internet sobre sí misma. Estos datos conforman una descripción sobre sus intereses y gustos.

Inclusión digital: Se define como la democratización y acceso de toda la población en relación al uso de las tecnologías de la información, a fin de reducir las brechas digitales. Este tipo de inclusión también busca

que los ciudadanos puedan aprovecharse de las TIC para mejorar su calidad de vida.

Infografía: Representación gráfica y visual de un texto, el cual generalmente destaca cifras, datos estadísticos, descripciones, narraciones cortas e interpretaciones específicas sobre un tema determinado.

Inmigrantes digitales: Personas nacidas antes de los años 80 (inicio de la era digital). Tuvieron una infancia analógica, sin pantallas, teclados, móviles. Sus equipos culturales y de apoyo para el aprendizaje fueron y siguen siendo: libros, bibliotecas, papeles, pizarras con tiza, etc. Se caracterizan por ser individuos que siguen una estructura mental mediada por procesos paso a paso, actúan bajo el análisis deductivo y aplican un aprendizaje basado en el enlace con conocimientos pre-adquiridos.

Internauta: Palabra compuesta por Inter: internet y Nauta: navegante, que se traduce a persona que navega por la red de Internet.

Keylogger (derivado del inglés: *key* (tecla) y *logger* (registrador); registrador de teclas). Nombre genérico por el cual se conoce a un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet, permitiendo que otros usuarios tengan acceso a contraseñas

importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

Linkedin: Red social para profesionales de todas las áreas y campos, que sirve como plataforma para que personas, organizaciones y comunidades de todo el mundo pueda conectarse a través de grupos o foros. Los usuarios pueden publicar y actualizar su hoja de vida, agregando experiencia laboral, académica, reconocimientos, premios, conocimientos, etc.

Meme: Representaciones gráficas de las emociones y estados de ánimo, que han cobrado fuerza en internet gracias a su versatilidad, ingenio, creatividad, humor y popularidad. El diseño de estas figuras se traduce a un conjunto de caras que expresan diversos rasgos faciales como: rabia, alegría, sorpresa, impresión, desconcierto y demás emociones.

Moodle (Modular Object-Oriented Dynamic Learning Environment): Ambiente de Aprendizaje Dinámico Modularmente Orientado a Objetos. Moodle es una aplicación Web libre que permite la creación de contenidos educativos en ambientes virtuales de aprendizaje. A través de este recurso es posible enseñar a distancia.

Nativos digitales: Personas a partir de 1980, a dicha época se le acuña el nacimiento de la tecnología. Los nativos digitales han crecido, se han desarrollado y han adquirido sus conocimientos y experiencia socioculturales de la mano con Internet y los dispositivos electrónicos.

Nickname: Apodo o nombre de un usuario. Los niños y adolescentes suelen ponerse a veces unos "*nicks*" con información personal que puede ocasionarles problemas.

Nomofobia: Angustia, estrés o miedo a perder cualquier dispositivo móvil, o dejarlo olvidado en casa u oficina. Las personas que sufren de esta fobia llegan a sentirse aisladas al no tener contacto o ningún tipo de información sobre sus llamadas, mensajes o chats.

Notebook o computadora portátil: ordenadores personales que pueden ser llevados a cualquier lugar, a diferencia de un ordenador de mesa. En su mayoría cumplen las mismas funciones que un computador tradicional, aunque suelen ser más livianos y de tamaños más pequeños.

Omnívoros digitales: Según comScore (compañía de investigación de marketing en Internet), son todos aquellos usuarios móviles que a través de sus muchos dispositivos (computadores, ordenadores, tabletas, smartphones, etc.) consumen a lo largo del día y de manera simultánea grandes cantidades de información.

Outing: Acción de hacer públicos los secretos o imágenes privadas de otras personas con intención de desprestigiarlas.

Phishing: tipo de abuso informático que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una

contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como ***phisher***, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. (Respecto a los menores), se requieren métodos adicionales de protección.

Plataforma LMS (Learning Management System): Sistema de gestión de aprendizaje que se aplica a través de una plataforma en línea, a fin de gestionar, distribuir, controlar y hacer seguimiento a contenidos y recursos educativos en un entorno compartido de colaboración y aprendizaje. Los administradores, tutores y alumnos se conectan a través de Internet y acceden a los contenidos, comunicándose por medio de herramientas asíncronas y síncronas como chats, foros, correos entre otras.

Plug-in (Componente enchufable): Aplicación informática que se agrega a otra para aumentar funcionalidades y características.

Podcasting consiste en la distribución de archivos multimedia (normalmente audio o vídeo, que puede incluir texto como subtítulos y notas) mediante un sistema de *redifusión* (RSS) que permita suscribirse y usar un programa que lo descarga para que el usuario lo escuche en el momento que quiera, generalmente en su tiempo libre. No es necesario estar suscrito para descargarlos. Actualmente hay podcasts de cualquier temática. Hay que tenerlos en cuenta (respecto a los menores) porque en ocasiones se usan como vehículos de

adoctrinamiento de los nuevos adeptos que caen en manos de grupos indeseables.

Portales educativos: espacios web que ofrecen una variedad de servicios a la comunidad educativa (directivos, docentes, estudiantes, padres de familia): información, instrumentos para la búsqueda de datos, recursos didácticos, herramientas para la comunicación interpersonal, formación, asesoramiento y entretenimiento.

PRISM: Programa de vigilancia electrónica de la Agencia de Seguridad Nacional (NSA) de Estados unidos, el cual le permite el organismo acceder a información privada de millones de usuarios a nivel mundial como correos electrónicos, chats, historial de navegación, direcciones IP, transferencia de archivos, perfiles en redes sociales, videos y notificaciones de inicio de sesión.

Realidad Aumentada: hace referencia a una visión directa o indirecta de cualquier entorno físico de la realidad, donde los elementos existentes se mezclan con los virtuales, creando al mismo tiempo una realidad mixta en tiempo real, la cual se registra en 3D. Un conjunto de dispositivos móviles añaden información virtual a la física, es decir que se complementa una parte sintética virtual a lo real, donde no se sustituye la realidad física, sino que adiciona los datos informáticos al mundo actual.

Red social: estructura virtual que proporciona interactividad constante entre los usuarios, quienes comparten distintos intereses y relaciones en

común. A través de este espacio se promueve la comunicación y participación de los cibernautas desde la publicación de imágenes, videos, links de referencias o contenidos de su interés.

RSS son las siglas de ***Really Simple Syndication***, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS. A pesar de eso, es posible utilizar el mismo navegador para ver los contenidos RSS. Cuando hablamos de RSS nos referimos usualmente a la tecnología completa para distribución de contenidos de los sitios web. Pero un RSS es realmente un formato de archivo, basado en XML, que sirve para recoger contenidos publicados en páginas web. Los RSS tienen extensión .rss o bien .xml, pero en realidad son un simple archivo de texto donde aparecen referencias a contenidos publicados, en un formato específico, creado a partir de XML.

Screencast es una grabación digital de la salida por pantalla de la computadora, conteniendo narración de audio y/o video, es decir, es esencialmente una película de lo que el usuario observa en su monitor.

Screenshot (también llamada *pantallazo*, o *captura de pantalla*) es una imagen tomada por una computadora para capturar los elementos vistos en el monitor u otro dispositivo de salida visual. Se suelen usar para ilustrar y explicar un programa, un problema particular que un usuario

pueda tener o, de manera más general, cuando la salida de la pantalla se debe mostrar a otros o ser archivada.

Sexting: práctica realizada comúnmente entre los adolescentes y jóvenes, quienes envían imágenes, mensajes y vídeos obscenos o pornográficos (de ellos mismos) a través de los dispositivos móviles. Este movimiento sin límites, además de desencadenar la sobre-exposición de material sensible en la web, propicia el cyberbullying.

Smartbook: Estos dispositivos son mundialmente famosos gracias a su fácil portabilidad y uso. Entre sus características se destacan la duración de la batería (de 2 a 4 horas), conexión a Wi-Fi, GPS, algunos carecen de unidad de CD, mouse táctil, etc. Estos aparatos electrónicos no tienen un estándar de fabricación ya que cada uno tiene su propio estilo y diseño.

Smartphones (teléfonos inteligentes): estos aparatos permiten la descarga e instalación de programas o software con diferentes aplicaciones móviles. Entre sus características se hallan, conectividad a internet, WIFI, reconocimiento de voz, pantalla táctil, cámaras fotográficas y de vídeos con alta resolución y calidad, alta capacidad de memoria de almacenamiento, lectura de documentos en PDF y Microsoft Office.

Smart TV o televisión inteligente: Una nueva tecnología incorporada en la televisión digital que fusiona características de la Web 2.0 con la televisión digital, a través de la conexión a Internet.

SMS(Short Message Service): Servicio de mensajes cortos que permite el intercambio de mensajes de texto entre teléfonos fijos, móviles y otros dispositivos.

Sociedad del conocimiento: Transformaciones alcanzadas por los desarrollos y descubrimientos tecnológicos, que al tiempo generan nuevos conocimientos y modelos sostenibles económicos para la apropiación y bienestar social de los individuos.

Software libre: La Free Software Foundation lo define como la libertad que tienen los usuarios para ejecutar, copiar, distribuir, estudiar el software e incluso modificarlo y distribuirlo modificado.

Spam: Conocido como correo no deseado. Son aquellos correos recibidos con contenidos publicitarios e información engañosa, que no han sido solicitados por los propietarios de las cuentas.

Stalking o acecho: Se refiere al acoso ininterrumpido de parte de un sujeto hacia alguna persona conocida o desconocida. Con las nuevas tecnologías, el "**stalker**" o acosador utiliza las redes sociales para asechar virtualmente a sus víctimas, escudriñando en cada una de sus cuentas personales, y siguiendo los movimientos de la persona en el mundo digital. En psicología se califica como un trastorno o patología que lleva al sujeto a obsesionarse con una persona desde perseguirla hasta cometer actos violentos contra ella.

Streaming: formato de distribución de multimedia (audio y video) a través de una red de computadores conectados a Internet, permitiendo la descarga y visualización de los datos en audio y video. Este se utiliza para transmisiones de videos online.

Tableta: Tipo de computadora móvil pequeña, en la que se puede escribir a través de una pantalla táctil usando un lápiz (Stylus), el texto manuscrito es digitalizado mediante reconocimiento de escritura.

Tags: También llamada etiqueta o metadato, hacen referencia a las palabras claves de un texto las cuales sirven como elementos diferenciadores en los motores de búsqueda. Entre sus ventajas, es que estos permiten la clasificación de las distintas publicaciones de cualquier sitio virtual, ya que filtra las palabras comunes y reclasifica los datos de los artículos. De esta manera, el sistema de etiquetado proporciona una ayuda eficaz al momento de acceder a informaciones de interés y temas específicos.

TIC: Nuevas tecnologías de la información y comunicación empleadas para la transmisión de contenidos a través de internet, las cuales funcionan como medios y aplicaciones en el desarrollo de las actividades de los individuos. Gracias a estas, los campos de la educación, cultura, política, opinión y demás han logrado avanzar en la distribución y masificación de sus contenidos, planes de acción y trabajo y las diversas funcionalidades en sus áreas.

Troll: Individuo que utiliza la Web para publicar mensajes y comentarios incitantes, provocativos, despectivos e irrelevantes en comunidades o plataformas online, con el propósito de atacar, provocar y molestar a los usuarios y lectores.

Tutor virtual: Guía o formador en los distintos procesos pedagógicos y académicos implementados a través del desarrollo de conocimientos actualizados aprehendidos mediante herramientas tecnológicas. La conexión con el aprendiz o alumno es realizada en la plataforma del Internet, donde la comunicación puede ser constante o frecuente de acuerdo a las necesidades de aprendizaje y contenidos a desarrollar.

Twitter: una de las redes sociales más utilizadas en la web, basada en el microblogging. Su plataforma está desarrollada en el envío de mensajes de 140 caracteres, llamados tweets. Entre sus distintos aplicativos se destacan los seguidores (followers), quienes son los usuarios que siguen los tweets del internauta, que a su vez también sigue (follow) a otros tuiteros.

Su interfaz se caracteriza por un TL o Timeline (cronología), donde se visualizan los tweets publicados por las personas a quienes sigue y los propios. Asimismo, integra las menciones realizadas por otros usuarios, los mensajes directos, los retweets (sus tweets replicados por otros internautas) las listas, que funcionan para crear grupos y temáticas; y búsqueda. Una de las características más populares de Twitter es el uso del **hashtags**, el cual funciona como una etiqueta, que se puede convertir en **Trending Topic** (tema del momento).

URL (Localizador de Recurso Uniforme): Sistema unificado que identifica recursos en la red y organiza la información que se encuentra alojada en esta, o recursos como páginas html, php, asp, o archivos gif, jpg, entre otros, a través de una secuencias de caracteres que identifica cada recurso disponible en la WWW. Es la dirección en internet de un sitio web.

Virus informático: se define como un programa informático malicioso (malware) diseñado para alterar o destruir el normal funcionamiento de un computador. Los archivos directamente afectados son: ejecutables del sistema operativo y archivos de los disco locales. El virus puede llegar a través de un software o programa descargado de Internet, un juego en flash, un archivo recibido por correo electrónico, entre otros.

Web 2.0: el término está relacionado a aplicaciones web que permiten compartir informaciones. Ejemplos de este son las redes sociales, canales de vídeos, blogs, las wikis, etc., los cuales de acuerdo a expertos y teóricos de red sostienen que la Web 2.0 sirve como punto de encuentro para internautas de acuerdo a sus sitios de interés.

Web 3.0- Web semántica: Tercera fase de la World Wide Web, según Tim Berners-Lee creador de la World Wide Web y director del World Wide Web Consortium (W3C). Berners-Lee define la Web semántica como una red de datos que pueden ser procesados directa e indirectamente por máquinas. A través de esta es posible expresarse no solo en lenguaje natural, sino también emplear un lenguaje que se puede entender e interpretar por agentes de software.

Webgrafía: conjunto de enlaces/link de un tema determinado, donde los usuarios se remiten a Internet a realizar una búsqueda. Su diferencia con la bibliografía, es que la fuente procede de la Web.

Webmaster: término que se usa para referirse a la persona responsable de un sitio web. Es quien crea, diseña, administra, gestiona y mantiene en funcionamiento la página.

WhatsApp Messenger: aplicación disponible para smartphone, de mensajería instantánea que tiene la característica de ser multiplataforma. Entre sus herramientas se destaca el envío y recepción de mensajes de texto incluyendo imágenes, videos, audio, participación de conversaciones grupales, entre otras.

Wi-fi: mecanismo de conexión a internet de forma inalámbrica. Los niños y adolescentes suelen hacer lo posible para encontrar redes WIFI a las que conectar sus dispositivos móviles inteligentes, consola de videojuegos o reproductor de audio digital y así poder acceder gratis a internet.

Anexo 1: Textos legales

ANEXO 1: TEXTOS LEGALES

Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual

En Lanzarote, en octubre de 2007 se da lugar a la reunión del consejo de Europa, donde se reúnen 47 estados y tiene por objetivo crear un espacio democrático y jurídico común basado en la Convención Europea de Derechos Humanos y otros textos de referencia relativos a la protección del individuo, incluidos los niños.

En él se presenta el programa "Construir una Europa para y con los niños", creado para garantizar y promover los derechos de los niños, así como para prevenir y erradicar todas las formas de violencia que les afectan.

Este convenio obliga a los Estados que lo han suscrito a penalizar un listado de conductas (abuso sexual, prostitución, pornografía infantil, corrupción, proposiciones con fines sexuales a través de las nuevas tecnologías de la información...) y establece medidas de protección y asistencia a las víctimas durante todas las fases del procedimiento penal (denuncia, investigación,

enjuiciamiento), procurando dar intervención en todos los ámbitos a ONG y sociedad civil.

También incide en la necesidad de llevar a cabo medidas preventivas de naturaleza educativa y formativa dirigidas tanto a los propios menores como a los profesionales que trabajan o están habitualmente en contacto con ellos".

Este convenio entra en vigor el 1 de diciembre de 2010 en España.

¿Qué delitos incluye este convenio?

El convenio tipifica la conducta constitutiva de explotación y abuso sexual en los artículos 18 a 23 recogidos en el capítulo VI que vemos a continuación:

CAPÍTULO VI. DERECHO PENAL SUSTANTIVO.

Artículo 18. Abuso sexual.

1. Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito las siguientes conductas intencionales:

a. Realizar actividades sexuales con un niño que, de conformidad con las disposiciones aplicables del derecho nacional, no haya alcanzado la edad legal para realizar dichas actividades;

b. realizar actividades sexuales con un niño:

** Recurriendo a la coacción, la fuerza o la amenaza; o*

** abusando de una posición reconocida de confianza, autoridad o influencia sobre el niño, incluso en el seno de la familia; o*

** abusando de una situación de especial vulnerabilidad del niño, en particular debido a una discapacidad psíquica o mental o una situación de dependencia.*

2. A efectos de la aplicación del apartado 1, cada Parte determinará la edad por debajo de la cual no está permitido realizar actividades sexuales con un niño.

3. Las disposiciones del apartado 1.a no tienen por objeto regular las actividades consentidas entre menores.

Artículo 19. Delitos relativos a la prostitución infantil.

1. Cada parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito las siguientes conductas intencionales:

a. Reclutar a un niño para que se dedique a la prostitución o favorecer la participación de un niño en la prostitución;

b. obligar a un niño a dedicarse a la prostitución o beneficiarse de un niño o explotarlo de otro modo para tales fines;

c. recurrir a la prostitución infantil.

---

2. A efectos del presente artículo, por prostitución infantil se entenderá el hecho de utilizar a un niño para actividades sexuales a cambio de dinero o de la promesa de dinero, o de cualquier otra forma de remuneración, pago o ventaja, con independencia de que dicha remuneración, pago, promesa o ventaja se ofrezcan al niño o a una tercera persona.

Artículo 20. Delitos relativos a la pornografía infantil.

1. Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito las siguientes conductas intencionales, cuando se cometan de forma ilícita:

a. La producción de pornografía infantil;

b. la oferta o puesta a disposición de pornografía infantil;

c. la difusión o transmisión de pornografía infantil;

d. la adquisición para sí o para otro de pornografía infantil;

e. la posesión de pornografía infantil;

f. el acceso a pornografía infantil, con conocimiento de causa y por medio de las tecnologías de la información y la comunicación.

2. A efectos del presente artículo, por pornografía infantil se entenderá todo material que represente de forma visual a un niño manteniendo una conducta sexualmente explícita, real o simulada, o toda representación de los órganos sexuales de un niño con fines principalmente sexuales.

---

3. Cada Parte se reserva el derecho de no aplicar, en todo o en parte, el apartado 1.a a la producción y a la posesión de material pornográfico:

** Que consista exclusivamente en representaciones simuladas o imágenes realistas de un niño no existente;*

** en el que participen niños que hayan alcanzado la edad fijada en aplicación del apartado 2 del artículo 18, cuando dichas imágenes hayan sido producidas por ellos y estén en su poder, con su consentimiento y únicamente para su uso particular.*

4. Cada Parte podrá reservarse el derecho de no aplicar, en todo o en parte, el apartado 1.f.

Artículo 21. Delitos relativos a la participación de niños en espectáculos pornográficos.

1. Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito las siguientes conductas intencionales:

a. Reclutar a un niño para que participe en espectáculos pornográficos o favorecer la participación de un niño en dichos espectáculos;

b. obligar a un niño a participar en espectáculos pornográficos o beneficiarse de un niño o explotarlo de otro modo para tales fines;

---

c. asistir, con conocimiento de causa, a espectáculos pornográficos en los que participen niños.

2. Cada Parte podrá reservarse el derecho de limitar la aplicación del apartado 1.c a los casos en que los niños hayan sido reclutados u obligados según lo dispuesto en el apartado 1.a o b.

Artículo 22. Corrupción de niños.

Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de hacer presenciar, con fines sexuales, a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del artículo 18, aun sin que él participe, abusos sexuales o actividades sexuales.

Artículo 23. Proposiciones a niños con fines sexuales. ("grooming")

Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a del artículo 20, cuando a dicha

proposición le hayan seguido actos materiales conducentes a dicho encuentro.

¿Quién puede ser castigado?

Toda persona que cometa cualquiera de los delitos establecidos en el convenio puede ser llevado ante los tribunales. En el caso de los delitos más graves, el autor podrá ser perseguido penalmente tras su retorno al país del cual es nacional incluso cuando el hecho no sea constitutivo de delito en el país en el que ha sido perpetrado. Se pretende combatir así el turismo sexual infantil.

¿Qué pide el Convenio a los Estados?

Medidas preventivas

- Seleccionar, reclutar y formar a las personas que trabajan en contacto con niños.
- Garantizar que los menores son conscientes de los riesgos de explotación y abuso sexual así como de los medios para protegerse.
- Garantizar medidas de intervención controladas regularmente, dirigidas tanto a delincuentes sexuales como a potenciales delincuentes y encaminadas a prevenir los delitos sexuales contra menores.

Medidas de protección

- Establecer programas de apoyo a las víctimas y a sus familias. Poner en marcha una asistencia terapéutica y atención psicológica de urgencia.
- Fomentar la denuncia cuando se tengan sospechas de la existencia de un caso de explotación o abuso sexual.
- Crear líneas de asistencia telefónica y por Internet para prestar asesoramiento.

Medidas de derecho penal

- Garantizar que determinadas conductas sean tipificadas como delitos, tales como realizar actividades sexuales con niños por debajo de la edad legal para realizarlas.
- Tipificar como delito conductas que se sirven de las nuevas tecnologías, en particular Internet, para agredir sexualmente a los menores, por ejemplo, el 'grooming' o ciber-acoso infantil (proposiciones a menores con fines sexuales).
- Establecer criterios comunes claros para garantizar la creación de un sistema punitivo que sea efectivo, proporcionado y disuasorio.
- Reunir y almacenar los datos sobre delincuentes condenados por delitos sexuales contra niños.

Procedimientos de investigación y judiciales adecuados a los menores

- Garantizar la adecuada protección de los niños y niñas víctimas durante los procedimientos, y procurar que no se agrave la experiencia traumática.

- Proteger la intimidad, identidad e imagen de las víctimas.
- Establecer medidas adaptadas a las necesidades de las víctimas, respetando los derechos de los niños y de sus familias.
- Limitar al máximo el número de entrevistas con los menores, asegurando que éstas se realicen en entornos tranquilizadores, con profesionales formados a tal fin.

Seguimiento

- Crear un mecanismo de seguimiento específico para garantizar la aplicación del convenio. Con ello se pretende asegurar el cumplimiento del convenio por parte de los Estados, y su eficacia a largo plazo.

Código Penal (artículo 183 bis)

Uno de los fenómenos criminales más reprobables es el denominado "***child grooming***" introducido por primera vez en nuestra legislación penal por la reforma del código penal llevado a cabo tras la aprobación de la Ley Orgánica 5/2010. Y que entra en vigor desde finales de 2010.

Artículo 183 bis.

El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, 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.

En los casos de delitos sexuales cometidos sobre menores, el bien jurídico a proteger adquiere una dimensión especial por el mayor contenido de injusto que presentan estas conductas, ya que mediante las mismas se lesiona no solo la indemnidad sexual sin un consentimiento

válidamente prestado, sino también la formación y desarrollo de la personalidad y sexualidad del menor. De otra, la extensión de la utilización de internet y de las tecnologías de las información y la comunicación con fines sexuales contra menores ha evidenciado la oportunidad de castigar penalmente las conductas que una persona desarrolla a través de tales medios para ganarse la confianza de menores (en nuestro caso, menores de trece años) con el fin de concertar encuentros para obtener concesiones de índole sexual

Código Penal (artículo 197)

CÓDIGO PENAL

LIBRO II. DELITOS Y SUS PENAS

TÍTULO X. DELITOS CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y LA INVIOLABILIDAD DEL DOMICILIO

CAPÍTULO I. DEL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

ARTÍCULO 197. SUPUESTOS

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda

sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrá las penas previstas en su mitad superior.

7. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

8. Si los hechos se descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.

La gente se cree con derecho de "pasar a sus colegas" videos que nos envían porque nos hacen gracia, pero la verdad es que no debemos hacerlo. Por varios motivos, el principal es que debemos tener permiso del dueño, es más, para poder grabarlo también se necesita dicha autorización. Se está violando el derecho a la intimidad, un derecho que está recogido en la Constitución Española, más concretamente en el artículo 18, en el que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Además, también garantiza el secreto de las comunicaciones.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo.

http://www.cmt.es/reglamentos_ue

Enlace donde podemos encontrar todos los reglamentos por los que se rige la Unión Europea.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:ES:PDF

Enlace donde podemos encontrar el archivo pdf de la directiva.

DIRECTIVA 2009/136/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 25 DE NOVIEMBRE DE 2009

POR LA QUE SE MODIFICAN LA DIRECTIVA 2002/22/CE RELATIVA AL SERVICIO UNIVERSAL Y LOS DERECHOS DE LOS USUARIOS EN RELACIÓN CON LAS REDES Y LOS SERVICIOS DE COMUNICACIONES ELECTRÓNICAS, LA DIRECTIVA 2002/58/CE RELATIVA AL TRATAMIENTO DE LOS DATOS PERSONALES Y A LA PROTECCIÓN DE LA INTIMIDAD EN EL SECTOR DE LAS COMUNICACIONES ELECTRÓNICAS Y EL REGLAMENTO (CE) N 2006/2004 SOBRE LA COOPERACIÓN EN MATERIA DE PROTECCIÓN DE LOS CONSUMIDORES

La eclosión de las Tecnologías de la Información y la Comunicación (TIC) y todas las derivaciones que existen a su alrededor (correo electrónico, mensajería instantánea, foros, videoconferencias, etc.)

están obligando a reelaborar muchos derechos y libertades tradicionales, pero desde nuevas perspectivas ya que continuamente se va evolucionando en las comunicaciones, este hecho va a estar sujeto a revisiones periódicas por parte de la Comisión del Mercado de las Telecomunicaciones (CMT) , con objeto, en particular, de determinar si es necesario introducir alguna modificación, habida cuenta de la evolución de la tecnología y del mercado.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo.

DIRECTIVA 2011/92/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO

DE 13 DE DICIEMBRE DE 2011

RELATIVA A LA LUCHA CONTRA LOS ABUSOS SEXUALES Y LA EXPLOTACIÓN SEXUAL DE LOS MENORES Y LA PORNOGRAFÍA INFANTIL

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:ES:PDF

Directiva del parlamento europeo, cuyo enlace arriba indicado lleva al archivo pdf de la DIRECTIVA 2011/92/UE, pero es un error contemplado por el parlamento corrigiendo el nombre de la directiva al 2011/93/UE tal y como se puede observar en el siguiente enlace destinado a la corrección de errores:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:018:0007:0007:ES:PDF

A partir del 18 de diciembre de 2013, los estados miembros de la Unión Europea ponen en vigor las disposiciones legales reglamentarias y administrativas para dar cumplimiento a lo establecido en dicha directiva, pero sigue habiendo una comisión que lo va a tener sujeto a revisiones periódicas con el objeto de ajustarse a la evolución de la tecnología con los derechos del menor.

El Parlamento Europeo y el Consejo piden a los Estados miembros que comprueben cuidadosamente las definiciones recogidas en su Derecho penal en lo que respecta al embaucamiento de menores "en la vida real" con fines sexuales, y que, en su caso, mejoren y corrijan su Derecho penal en lo que respecta a las posibles lagunas jurídicas que pudieran subsistir en este sentido.

El 5 de abril de 2013, España presenta un anteproyecto de Ley al consejo de Estado, recogido en el siguiente apartado.

Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de Noviembre, del Código Penal.

El anteproyecto de reforma de la Ley del Código Penal, propuesto por el Ministerio de Justicia de España ha sido remitido al Consejo de Estado para su revisión previa a la aprobación en el Consejo de Ministros.

http://www.rtve.es/contenidos/tec/Texto_enviado_al_Consejo_de_Estado_(5_abril_2013).PDF

En esta reforma, pretende entre otras cosas, introducir .modificaciones en los delitos contra la libertad sexual para llevar a cabo la transposición de la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo. La citada Directiva obliga a los Estados miembros a endurecer las sanciones penales en materia de lucha contra los abusos sexuales, la explotación sexual de menores y la pornografía infantil, que sin duda constituyen graves violaciones de los derechos fundamentales y, en particular, de los derechos del niño a la protección y a los cuidados necesarios para su bienestar, tal como establecen la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y la Carta de los Derechos Fundamentales de la Unión Europea.

Ley Orgánica 1/1996, de 15 de Enero CAPÍTULO II Derechos del menor.

LEY ORGÁNICA 1/1996, DE 15 DE ENERO, DE PROTECCIÓN JURÍDICA DEL MENOR, DE MODIFICACIÓN PARCIAL DEL CÓDIGO CIVIL Y DE LA LEY DE ENJUICIAMIENTO CIVIL.

Artículo 4. Derecho al honor, a la intimidad y a la propia imagen.

1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

2. La difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

3. Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

4. Sin perjuicio de las acciones de las que sean titulares los representantes legales del menor, corresponde en todo caso al Ministerio Fiscal su ejercicio, que podrá actuar de oficio o a instancia del propio menor o de cualquier persona interesada, física, jurídica o entidad pública.

5. Los padres o tutores y los poderes públicos respetarán estos derechos y los protegerán frente a posibles ataques de terceros.

Artículo 5. Derecho a la información.

1. Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo.

2. Los padres o tutores y los poderes públicos velarán porque la información que reciban los menores sea veraz, plural y respetuosa con los principios constitucionales.

3. Las Administraciones públicas incentivarán la producción y difusión de materiales informativos y otros destinados a los menores, que respeten los criterios enunciados, al mismo tiempo que facilitarán el acceso de los menores a los servicios de información, documentación, bibliotecas y demás servicios culturales.

En particular, velarán porque los medios de comunicación en sus mensajes dirigidos a menores promuevan los valores de igualdad, solidaridad y respeto a los demás, eviten imágenes de violencia, explotación en las relaciones interpersonales o que reflejen un trato degradante o sexista.

4. Para garantizar que la publicidad o mensajes dirigidos a menores o emitidos en la programación dirigida a éstos, no les perjudique moral o físicamente, podrá ser regulada por normas especiales.

5. Sin perjuicio de otros sujetos legitimados, corresponde en todo caso al Ministerio Fiscal y a las Administraciones públicas competentes en materia de protección de menores el ejercicio de las acciones de cese y rectificación de publicidad ilícita.

Con esta ley, los padres pueden ejercer su derecho a supervisar las actividades on line que puedan realizar sus hijos.

Podría darse el caso en el cual, los menores tuvieran en su consola algunas fotos no recomendables para su edad, y sin ni tan siquiera saberlo sus padres, por lo que estarían incumpliendo la ley del menor, porque no estarían defendiendo la imagen, el honor y la reputación de sus hijos debidamente.

Además, los padres tienen el derecho y la obligación de denunciar a quien haya difundido por internet una foto de su hijo, incluso con el consentimiento del mismo.

ANEXO 2: Consejos para Adolescentes

ANEXO 2: CONSEJOS PARA ADOLESCENTES

Como nos podemos proteger en internet

Es posible que hayas escuchado historias sobre abusos a niños en Internet, ya sea mediante propuestas no deseadas provenientes de adultos o mediante el acceso a contenidos sexuales o violentos. Personas como tú, que un día descubren que la persona con la que llevaban tiempo chateando y que era su mejor amigo en internet, les ha engañado y resulta que no es lo que decía ser, además, se sienten acosados y comienzan a tener miedo.

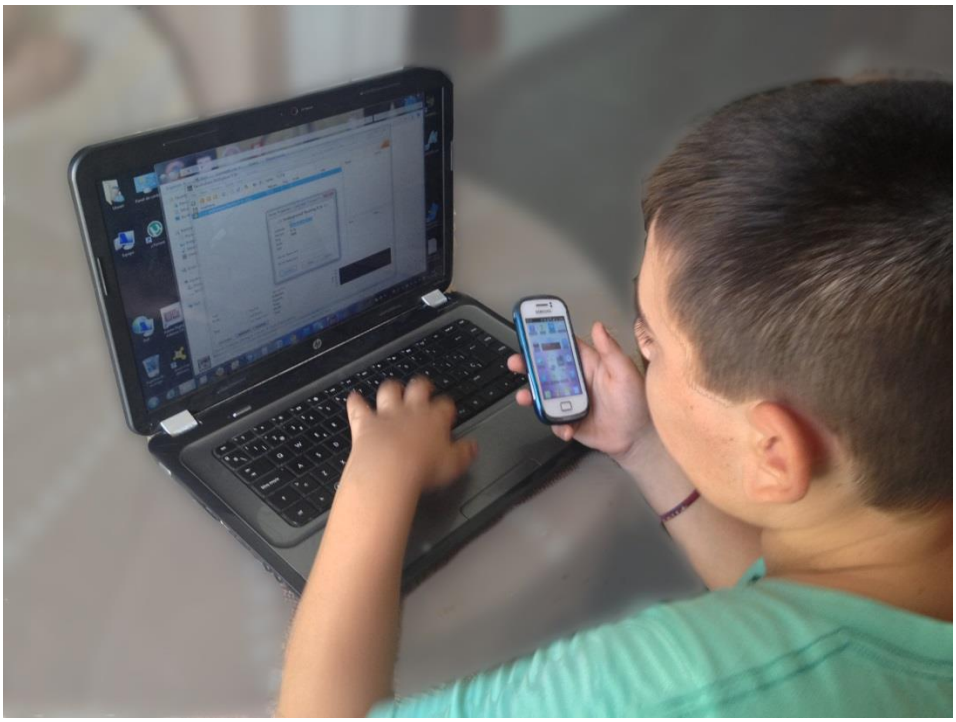


Figura 19: Los niños aprenden con facilidad a descargarse e instalarse programas sin preguntarse si la procedencia es segura.

En cualquier caso, en Internet debes cuidarte al igual que en el mundo real de cualquier tipo de persona o extraño. Esta es una serie de consejos que deberías llevar adelante para establecer buenas prácticas de uso y comportamiento en el uso de Internet junto con tus padres y docentes:

Consejos para los menores

1. **No pulses sobre links.** Cuando estés hablando por un sistema de mensajería instantánea o recibas un correo no pulses nunca directamente sobre ningún vínculo, especialmente si procede de gente desconocida.

2. **No descargues ni ejecutes archivos de procedencia desconocida.**

3. **No hables con desconocidos sin el conocimiento o autorización de tus padres.** En los chats o en los sistemas de mensajería instantánea, nunca podemos tener una completa seguridad de quién está al otro lado. Hay personas que mienten sobre la edad e intenciones que tienen y podrían hacerte daño.

4. **No contestes mensajes que te hagan sentir incómodo o avergonzado**, corta el dialogo cuanto antes y comunícaselo a tus padres si esto ocurre. **Ni respondas a mensajes obscenos, agresivos, o de acoso sexual.**

5. **Graba las conversaciones que mantienes por chat con otras personas**, de este modo podrás mostrárselo a alguien si lo necesitas hacer.

6. **Intenta no utilizar cámara web para chatear** ya que alguien podría tomarte fotos para luego aprovecharlas contra ti o tu familia.

7. **Utiliza contraseñas seguras** y no se las entregues a nadie ya que, quien tenga tu contraseña, podría hacerse pasar por tí.

8. **No te identifiques con un Nick que delate año de nacimiento o edad u otro dato privado**. Por ejemplo: marc_93 podría delatar que naciste en 1993 o juan_13 podría indicar que tienes 13 años de edad y eres varón.

9. La diferencia entre lo que está bien y lo que está mal es la misma en Internet que en la vida real.

10. **No proporciones información confidencial a través de la red.** Nunca envíes información sensible (datos privados, fotos, tu dirección, claves personales, etc.) a través de e-mail o mensajería instantánea y mucho menos aún la publiques en un blog o en un foro, para que tus datos personales o los de tu familia no puedan ser obtenidos por personas con malas intenciones.

11. Entrega tus datos **sólo** a personas que conozcas personalmente.

12. **Sospecha al menor indicio**. Si algún programa que no recuerdas haber instalado comienza a mostrarte ventanas emergentes o pop-ups en los que se te invita a comprar algún tipo de producto, desconfía.

13. **No ejecutes archivos sospechosos.** Si tu solución de seguridad te señala que un archivo es sospechoso de tener un malware o que, efectivamente, lo tiene, no lo abras. Simplemente, elimínalo de tu ordenador.

14. **Ignora el spam** y no abras archivos de desconocidos ya que pueden contener algo dañino. Es posible que a través de estos medios alguien descifre tus claves de chat o de correo electrónico para luego robarte tus datos o infecte tu computadora con virus.

15. **Habla con los mayores.** Cuando tengas dudas sobre algún tema, veas algo sospechoso o recibas correos o mensajes ofensivos o peligrosos, habla con un adulto. Él podrá aconsejarte.

16. **Respeta la propiedad de los demás**. Descargar o realizar copias ilegales del trabajo de otras personas (música, videojuegos y otros programas) puede ser considerado, según las leyes de cada país, **plagio, robo o piratería** y puede representar un problema legal para familia.

17. **Intenta utilizar alguna aplicación de Control Parental** para que la misma controle los sitios a los que ingresas y su contenido. De esta forma te estarás protegiendo a tí mismo.

18. **Recuerda que lo que se dice en Internet puede ser falso.**

19. En el caso de las Redes Sociales, también deberías tener en cuenta estos aspectos al utilizarlas:

- no aceptes como contactos o amigos a personas que no conoces.
- Organiza tus contactos por grupos. Establece la privacidad de tu perfil sólo a tus amigos conocidos.
- Delimitar quien puede visualizar los datos publicados.
- No colocar fotos de terceros, imágenes o caricaturas en el perfil personal.
- No contactar o ser contactado con el fin exclusivo de encuentro personal ya que puede atraer a personas con malas intenciones.
- A la hora de emitir una opinión en Internet, es necesario tener en cuenta de que lo publicado podrá ser visto por muchas personas.
- Las redes sociales han hecho muy fácil el proceso de aceptar una invitación a un grupo o aplicaciones. Lo mejor es medir la necesidad de suscribirnos o no.
- No tolerar comportamientos criminales o incorrectos y no abusar verbalmente de otros usuarios.
- No añadir contenidos pornográficos, de mal gusto, con publicidad o con spam a las redes.

Webs de interés

WEBS DE INTERÉS

- www.inteco.es

El instituto Nacional de las Tecnologías de la Comunicación dispone de una sección de guías y manuales dentro del observatorio de la Seguridad de la Información.

- http://www.inteco.es/tagObservatory/Seguridad/Observatorio/Actualidad_Observatorio/guia_ciberbullyin_es

Guía sobre Cyberbulling y grooming, sobre configuración del control parental, redes sociales, menores de edad y privacidad

- www.osi.es

La oficina de seguridad del internauta (OSI) es un servicio para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por internet.

- http://menores.osi.es/

Pone a disposición de todos los usuarios una serie de consejos para mantener la seguridad del menor en internet.

- https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

El grupo de delitos Telemáticos de la guardia civil investiga y persigue delitos en internet, además de proporcionar un lugar donde denunciar dichas conductas, además de dar consejos y recomendaciones.

- http://www.alia2.org/

Página web de la fundación alia2 que lucha contra la pornografía infantil.

www.protegeles.com

Página web del centro de internet seguro para el menor en casa, donde se puede denunciar webs con contenidos inadecuados y apartados de asesoramiento sobre seguridad en la telefonía móvil, ciberbullying, acoso escolar (buylling), drogas, videojuegos, ciberfamilias…

- www.agpd.es

Página web de la Agencia Española de protección de datos.

- www.kiddia.es

Página web donde niños, padres y educadores aprendan un uso adecuado de las TIC.

- www.kidbox.net

Página web donde niños pueden navegar seguros en internet, con contenidos especiales para niños de 2 a 8 años, con interfaz muy fácil para que puedan navegar incluso niños que no sepan leer.

- www.secukid.es

Secukid es un juego para móviles dirigido a todos los públicos, especialmente niños y adolescentes a partir de los 11 años. Está

concebido para conocer mejor algunos riesgos de Internet, sus efectos y como prevenirlos.

- www.pantallasamigas.net

Es una iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia

- www.chaval.es

Portal infantil creado por la entidad Red.es que ofrece enlaces a páginas web de contenidos adecuados para la infancia.

- www.sexting.es

Página web que informa y aconseja acerca del sexting

www.seguridadenlared.org/menores
Página web de la Asociación de internautas

- http://www.ciberfamilias.com

Portal para padres y educadores interesados en conocer mejor internet e informarse sobre las cuestiones relativas a la seguridad de los menores.

- www.pandasecurity.com/spain/about/social-responsibility/children-internet/

Página con consejos para niños y consejos para padres

- www.internetyfamilia.es

Página dedicada al mundo de internet y los menores donde los menores encontrarán videos, juegos para aprender de internet y seguridad.

- http://www.juventud.jcyl.es/web/jcyl/Juventud/es/Plantilla100/1284233163355/_/_/_

Página web de la junta de Castilla y León para información juvenil

- http://www.portaldelmenor.es/

Portal donde encontrar información, juegos y consejos sobre internet para menores y padres.

- http://www.jovenyenred.com/

Página para que el joven pueda compartir sus ideas, inquietudes e intereses. Sus aportaciones ayudarán a mejorar el uso que hacemos de los móviles e internet.

- http://www.policia.es/org_central/judicial/udef/bit_alertas.html

Página web de la brigada de Investigación Tecnológica de la Policía Nacional

- http://www.protegits.gva.es/lang/va/index.php

Página web de la Generalitat Valenciana

- http://www.cmt.es/directivas_ue

Página web de la Comisión del Mercado de la Telecomunicaciones.

- http://europa.eu/eu-law/legislation/index_es.htm

Página web del buscador de legislación de le Unión Europea.

Paginas en inglés:

- www.inhope.org

Página de denuncia a nivel europeo para que los usuarios denuncien cualquier comportamiento o hecho que consideren ilegal.

- www.saferinternet.org

Es una red internacional para coordinar la seguridad en internet.

- http://ec.europa.eu/information_society/activities/sip/index_en.htm

Programa de la Unión europea para la seguridad de los menores en internet. (Ingles)

- https://www.wiredsafety.org/

Portal en inglés con noticias de actualidad, agenda, consejos, recomendaciones y preguntas frecuentes para padres y menores.

- http://www.wisekids.org.uk/

Portal en inglés para la promoción de un internet más seguro, con noticias, consejos y recomendaciones y juegos dirigido a menores, padres y educadores.

- http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Página de la Unión europea donde se presentan proyectos de desarrollo sobre la seguridad en internet para menores.

- http://www.yprt.eu/yprt/content/sections/

La Youth Protection Roundtable (Mesa redonda para la protección de la juventud) de la comisión europea.

- http://www.childhelplineinternational.org/

Portal en inglés para la protección de los derechos de los niños.

- http://kidoz.net/

Portal en inglés destinado a aplicaciones que los niños pueden utilizar para jugar en sus móviles o tablets de manera segura.

Bibliografía

BIBLIOGRAFIA

📖 Carrington Victoria, Robinson, Muriel (2009). "Digital Literacies: Social Learning and Classroom Practices" ("Alfabetización digital: Aprendizaje Social y Prácticas en el aula". SAGE Publications Ltd. Paperback. Londres. (Reino Unido). ISBN- 9781847870384

💻 Casanovas, Joseph ; Carretero, Merche;(2007) "Ordenadores, hijos e Internet: guía de supervivencia" en Desarrollo web. 2007 (http://www.desarrolloweb.com/articulos/ordenadores-hijos-e-internet.html) consulta, Septiembre 2013.

💻 El País (2009) "Los menores ignoran su grado de desprotección en Internet" http://sociedad.elpais.com/sociedad/2009/02/13/actualidad/1234479605_850215.html Madrid, 13/02/09.

💻 Less Andrade, P. (2009). "Google, protegiendo la privacidad en Internet. *VI Encuentro Iberoamericano de Protección de Datos*" *https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/pla_privacidad_internet_vi_encuentro_iberoamerica.pdf* Cartagena de Indias, 2009.

📖 Hillmann, Karl-Heinz (2001). *Diccionario enciclopédico de sociología*. Herder. Barcelona

📖 Monsoriu, Mar (2008). "Técnicas de Hacker para padres". Creaciones Copyright. *ISBN: 978-84-96300-45-3*

Prensky, Marc (2001). "Digital Natives, Digital Immigrants". From *On* the Horizon (MCB University Press, Vol. 9 No. 5, October 2001)

📖 Prensky, Marc (2005). "Don´t Bother Me Mom – I´m Learning". Corwin. ISBN- 9781452230092.

📖 Prensky, Marc (2012). "From Digital Natives to Digital Wisdom: Hopeful Essays on Education". Corwin. ISBN- 9781452230092.

📖 Prensky, Marc (2012). "Brain Gain: Technology and the Quest for Digital Wisdom" ("Brain Gain: Tecnología y la búsqueda de la Sabiduría Digital"). Macmillan. ISBN: 978-0230338098.

💻 Stanley, Janet. "*Child abuse and the Internet*". Melbourne, Australia, National Child Protection Clearinghouse, 2001 (http://www.aifs.gov.au/nch/pubs/issues/issues15/issues15.html , Consulta Septiembre 2013).

📖 Turkle, Sherry. (1997) 4º ed., "*Life on the screen: Identity in the age of the Internet*", Simon and Schuster, New York. ISBN 0684833484

UNESCO (2001) y A. Arnaldo (ed.), "*Child abuse on the Internet: Ending the silence*", Berghahn Books and UNESCO, ISBN (UNESCO) 92-3-103728-5 Paris, pp.169—72.

Willard, Nancy (2007) "Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social aggression, threats, and distress". Research Press. United States of America. ISBN: 978-0-87822-537-8.

Willard, Nancy (2007) "Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly". Jossey-Bass. United States of America. ISBN: 9780787994174.

Willard, Nancy E. (2011) "Cyber Savvy: Embracing Digital Safety and Civility". (Paperback) Corwin Publishers. United States of America. ISBN: 9781412996211.