Educar a los menores en el uso sin riesgos de Internet

Guía para Madres y Padres

Vitoria-Gasteiz

Vitoria-Gasteiz
Hiri Hezitzailea
Ciudad Educadora

Ayuntamiento
de Vitoria-Gasteiz
Vitoria-Gasteizko
Udala

Educar a los menores en el uso sin riesgos de Internet

Guía para Madres y Padres

Ayuntamiento
de Vitoria-Gasteiz
Vitoria-Gasteizko
Udala

Edita: Ayuntamiento de Vitoria-Gasteiz
Realiza: Departamento Municipal de Educación
Colección: Educación
Textos: Mintza
Traducción: Servicio de Euskera del Ayuntamiento de Vitoria-Gasteiz
Maquetación: La Debacle S.L.
Imprime:
D.L.: VI-
www.vitoria-gasteiz.org

Indice

Introducción

Tras la sociedad industrial, vivimos actualmente en la sociedad de la información, que se caracteriza por la extraordinaria expansión de las tecnologías de la información y la comunicación y, en especial, de Internet. En este modelo de sociedad, todo lo relacionado con las Tecnologías de la Información y la Comunicación (TIC) desempeña un papel substancial. La extraordinaria expansión de estas tecnologías se ha constituido en una herramienta imprescindible para el desarrollo individual y colectivo de los pueblos.

Las administraciones públicas, como no podía ser de otra manera, apoyan este cambio cultural. **El Plan Avanza**, por ejemplo, prevé entre sus medidas la adopción de una serie de normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de la comunicación y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

Dirección general de la sociedad de la información
www.mityc.es/dgdsi/es-ES/Paginas/index.aspx

En Euskadi, el **Plan Euskadi en la Sociedad de la Información 2010: la Agenda Digital de Euskadi** busca consolidar una Sociedad de la Información y del Conocimiento plena para avanzar hasta convertir a Euskadi en el referente europeo en innovación.

Euskadi en la sociedad de la información
www.euskadi.net/eeuskadi/new/eu/index.html

De acuerdo con la declaración de principios de la Cumbre de la Sociedad de la Información [12-05-2004], "la educación, el conocimiento, la información y la comunicación son esenciales para el progreso, la iniciativa y el bienestar de los seres humanos. La capacidad de las TIC para reducir muchos obstáculos tradicionales, especialmente el tiempo y la distancia, posibilitan, por primera vez en la historia, el uso del potencial de estas tecnologías en beneficio de millones de personas en todo el mundo".

www.itu.int/wsis/index-es.html

Por su parte, el **Ayuntamiento de Vitoria-Gasteiz**, al asumir la consolidación de nuestra ciudad como Ciudad Educadora, comparte la preocupación de los padres y madres porque sus hijas e hijos hagan un uso adecuado de las tecnologías de la información y la comunicación, evitando así los riesgos que pueden derivarse de su incorrecta utilización.

Esta guía se edita con la intención de lograr los siguientes objetivos:

- Informar a padres y madres de menores sobre las posibilidades que ofrecen las nuevas tecnologías de la información y comunicación, así como ofrecerles contenidos y plantearles retos que les sean de utilidad en su relación con los menores.
- Alertar sobre los peligros de las tecnologías de la información y la comunicación sin infundir fobias tecnológicas. Conseguir confianza mediante la adquisición de conocimientos.
- Concienciar a la población sobre la utilidad de conocer, practicar y fomentar el uso seguro de las estas tecnologías. Promover prácticas seguras y hábitos saludables en Internet.
- Aprender estrategias para afrontar los principales riesgos que conlleva el acceso a las tecnologías de la información y la comunicación.

Las Tecnologías de la Información y la Comunicación (TIC)

Asentando conceptos

Las tecnologías de la información y la comunicación tienen una importante repercusión en prácticamente todos los aspectos de nuestra vida. El rápido progreso de estas tecnologías brinda oportunidades sin precedentes para alcanzar niveles más elevados de desarrollo.

La situación, permanentemente actualizada, de Euskadi en relación con las TIC se puede conocer en profundidad a través de la información que ofrece la página web del Portal de las Administraciones Vascas.

➘ www.euskadi.net/eeuskadi/new/es/esi_tic.html

Las redes de acceso a las TIC que emplean los menores, con más relevancia para el tema que nos ocupa, son las redes de telefonía (fija y móvil) y las redes de banda ancha que permiten una conexión de gran calidad a Internet a través de los ordenadores personales.

Los servicios más demandados por los menores, a través de estas vías, son las comunidades virtuales (redes sociales, foros, blogs, etc.), los servicios Peer To Peer (P2P) para compartir contenidos y la navegación por Internet.

La mayor parte de los menores que utilizan Internet lo concibe como una herramienta de ocio (para chatear, para jugar, para buscar música), pero se observan diferencias significativas atendiendo a los distintos niveles escolares. Por ejemplo, los alumnos de Primaria son el grupo que más utiliza Internet para buscar información; los alumnos de la ESO utilizan Internet fundamentalmente para chatear; y los alumnos de Bachillerato buscan en la red, básicamente, un lugar en el que relacionarse y conocer a otras personas.

➘ Seguridad infantil y costumbres de los menores en Internet
www.asociacion-acpi.org/seguridad%20y%20costumbres.htm

Hábitos de los menores ante las actuales tecnologías

Los hábitos de los menores, en lo que respecta al acceso a estas tecnologías, han sido profusamente estudiados por iniciativas como:

El *"Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres"* del Observatorio de la Seguridad de la Información del INTECO (Instituto Nacional de Tecnologías de la Comunicación).

www.inteco.es

El *"Estudio sobre seguridad infantil y costumbres de los menores en Internet"* realizado por las organizaciones independientes ACPI (Acción Contra la Pornografía Infantil) y PROTÉGELES para el Defensor del Menor en la Comunidad de Madrid.

www.protegeles.com/es_estudios5.asp

Entre los resultados más llamativos, relativos a los menores que utilizan Internet de forma habitual (una cuarta parte, aproximadamente), figuran:

— Los menores acceden a la Red principalmente desde sus propias casas, mayoritariamente desde ordenadores que no disponen de sistemas de filtrado. Un tercio de ellos reconoce sentir la necesidad de conectarse a Internet con frecuencia.

— Los niños y niñas utilizan Internet para enviar y recibir correos electrónicos, para descargarse archivos y para buscar información. Por detrás de estos usos, la mensajería instantánea y el chat también presentan tasas de utilización muy altas. Una cuarta parte de los menores que se conectan con regularidad lo hacen para jugar.

— La edad media del primer acceso a Internet de los menores se sitúa en torno a los 10 u 11 años. Los menores acceden a Internet con mucha frecuencia: la mitad se conecta diariamente a Internet y más de la tercera parte lo hace con una frecuencia de 2 ó 3 días por semana.

— Casi un 80% de los padres considera que el tiempo dedicado por sus hijos a Internet es normal, considerando normal como "equivalente al que dedican otros menores de su entorno".

— La **mitad** de los menores **no ha recibido información** alguna sobre las normas básicas de seguridad a la hora de utilizar Internet.

— Una **cuarta parte** de los menores entra en páginas **pornográficas**, en páginas de **violencia** (aquí el porcentaje probablemente es mayor), o en páginas de contenido **racista y/o xenófobo**.

— Después del ordenador de sobremesa (88 %), los equipos tecnológicos más utilizados por los menores son el reproductor de DVD (72 %), el teléfono móvil (64 %) y el MP3 ó MP4 (53 %).

— La penetración del **teléfono móvil** entre los menores españoles de 10 a 16 años es alta: alrededor de dos tercios posee un terminal de telefonía móvil propio. La posesión de teléfono móvil aumenta con la edad y se generaliza entre las chicas y chicos de 15 a 16 años, con un 89 % que lo poseen.

— El tipo de contrato del teléfono que los menores utilizan se reparte casi al 50 % entre teléfonos de prepago y de contrato, siendo el prepago el sistema más generalizado para las chicas y chicos de menor edad.

— Un 41 % de los hogares dispone de **videoconsolas** y un 19 %, de videoconsolas portátiles. El uso de videojuegos online, ya sea a través de videoconsola o de ordenador, se acerca al 30 % de los menores españoles.

— El **30 %** de los menores que habitualmente utiliza Internet ha facilitado su **número de teléfono** en alguna ocasión durante sus conexiones y el **16 %** de los menores encuestados ha facilitado **su dirección** y/o ha **concertado una cita** con un desconocido a través de Internet.

— Casi la **mitad** de los menores que se conectan a Internet con regularidad, reconoce buscar **materiales protegidos** por derechos de autor a través de la Red, tendencia que va aumentando con la edad.

— Lo que más preocupa a los padres y madres es el riesgo de **dependencia** o **uso abusivo**, muy por delante del resto de situaciones: las amenazas al sistema informático del tipo malware, el acoso sexual, la interacción con desconocidos, los timos y fraudes o el acceso a contenidos inadecuados.

> Las tecnologías de la información y la comunicación no son ninguna panacea ni fórmula mágica, pero pueden mejorar la vida de todos los habitantes del planeta

(Kofi Annan, Secretario general de la ONU, Ginebra 2003).

Comprendiendo las ventajas

Las posibilidades que actualmente brinda el acceso a las redes han modificado los hábitos de las personas. El acceso a información, permanentemente actualizada, de que disponemos, enriquece la sociedad y ofrece alternativas de relación entre las personas, inimaginables hace pocos lustros.

Parece importante llegar a comprender que el problema no radica en la tecnología en sí misma (éticamente neutra), sino en el uso que se haga de ella. En el caso de los colectivos más desprotegidos (los menores, principalmente), **la responsabilidad sobre las buenas prácticas en el uso de estas herramientas recae en padres, madres y educadores**, que deben optar por apoyar el buen empleo de las TIC con sus conocimientos y su buen sentido.

Desde las instituciones públicas se puede, y debe, colaborar en transmitir a todos los responsables de la educación de nuestros menores pautas de actuación fiables y seguras que ayuden a formar a nuestros jóvenes en aspectos tan relevantes como la discriminación de la calidad de la información, los peligros del contacto indiscriminado con personas desconocidas o la necesidad de mantener controlado el acceso a nuestra privacidad.

Entre las indudables ventajas que ofrecen las tecnologías de la información y la comunicación cabría señalar, a modo de ejemplos, que:

— **A través de las páginas web**, permiten encontrar recursos educativos y culturales (enciclopedias en línea, obras de referencia, imágenes, podcast, vídeos, etc.), tener acceso a la actualidad informativa, obtener documentación que permita profundizar en los temas que más nos interesen, jugar en solitario o con otras personas, etc.

— **A través de correo, chat y mensajería electrónica**, facilitan el poder comunicarse con un ilimitado número de personas, intercambiar ideas y opiniones con ellas y formar parte de comunidades de intereses, compartir información o contactar con expertos.

— **A través de blogs y redes sociales**, ayudan a trabajar en colaboración en red, aprender a utilizar mejor estas tecnologías, responsabilizarse de los contenidos publicados y, en definitiva, adquirir aquellas habilidades que cada vez son más solicitadas en el mercado laboral.

Los riesgos en la red más relevantes para los menores se pueden clasificar en:

- Riesgos de **uso abusivo** y **adicción**.
- Riesgos relacionados con la **vulneración de derechos de propiedad intelectual**.
- Riesgo de acceso a **contenidos inapropiados**.
- Riesgo de **interacción y acecho por otras personas**.
- Riesgo de **acoso sexual**.
- Riesgo de **amenazas a la privacidad**.

Entendiendo los riesgos

Las tecnologías actuales tienen un desarrollo imparable y son fuente de grandes beneficios sociales y personales: acceso a la información, mejora de la comunicación, intercambio de conocimientos, facilitación de las relaciones, etc. Sin embargo, cada vez son más las voces que alertan sobre el uso desmesurado que los adolescentes hacen de estas herramientas en detrimento de otras actividades, como las escolares o las lúdicas tradicionales.

El uso compulsivo de Internet, la exposición del ámbito privado o el acceso ilimitado e indiscriminado a las prestaciones que ofrecen los nuevos teléfonos móviles han generado inquietud en padres, educadores y psicólogos. Enrique Echeburúa, catedrático de Psicología Clínica de la Universidad del País Vasco, aporta interesantes publicaciones al respecto, como *"¿Adicciones… sin drogas? Las nuevas adicciones"*.

➘ www.ehu.es/echeburua/index.asp

La utilización de las redes de información y comunicación por los menores es muy útil y gratificante para ellos, pero no está exenta de situaciones conflictivas, como pueden ser la recepción de correos no solicitados con un contenido desagradable, el intercambio de insultos por parte de varios interlocutores o, incluso, la posibilidad de sufrir una amenaza, de manera más o menos velada, por parte de personas conocidas (generalmente otros jóvenes) o desconocidas.

La capacidad de acceder a niveles de información nunca vistos, si se realiza de manera masiva e indiscriminada es susceptible de generar problemas de gran calado social. Todas las hemerotecas aportan evidencias sobre ello:

"La Ertzaintza alerta de varias agresiones sexuales a menores tras contactar por Internet"

(Deia.com) 24-03-2009

"Tres hermanos que utilizaban Internet para hostigar a menores y descargaban pornografía infantil en sus ordenadores personales han sido detenidos hoy por los agentes del Cuerpo Nacional de Policía"

(El Pais.com) 19-12-2009

"El 62 por ciento de los adolescentes del País Vasco se conectan todos los días a la semana a Internet y el 40 por ciento reconoce que ha contactado con desconocidos a través de la red, según los datos del segundo Estudio de Seguridad de Menores en el País Vasco"

(El Mundo.es) 17-12-2009

Conceptos básicos de seguridad

¿Qué es un firewall (cortafuegos)?

Software cuya función es proteger el equipo informático de intrusiones externas no deseadas. Es un componente fundamental del sistema de seguridad de los ordenadores. Permite o limita el tráfico de información entre el ordenador y la Red sobre la base de un conjunto de normas y otros criterios.

¿Qué son las actualizaciones del Sistema Operativo?

Modificaciones sugeridas por el fabricante en el sistema operativo del ordenador con intención de enmendar problemas aparecidos o prevenir inconvenientes en el futuro. Todos los sistemas operativos (Windows, Linux, Mac OS, etc.) las ofrecen. Un sistema operativo permanentemente actualizado es fundamental para la seguridad y la confiabilidad del equipo.

¿Qué significa malware?

➘ http://es.wikipedia.org/wiki/Malware#Clasificaci.C3.B3n

Es todo software que tiene como objetivo infiltrarse en el sistema operativo de un ordenador sin el conocimiento de su dueño. El programa aprovecha errores (bugs o agujeros) en el código de los sistemas operativos para introducirse. Las actualizaciones de los sistemas operativos intentan prever o evitar estos errores. También se emplea con frecuencia la palabra vulnerabilidad para referirse a cualquier fallo en el diseño, configuración o funcionamiento de un software que, cuando es descubierto por un atacante, puede conducir a una intromisión no autorizada que comprometa la seguridad del sistema.

Incluye, fundamentalmente, los virus informáticos (la variante popularmente más conocida), los gusanos, los troyanos y el spyware.

¿Qué es un antivirus?

Es una aplicación informática diseñada para detectar, bloquear, eliminar y, si es posible, prevenir las operaciones malintencionadas en un ordenador. Es el complemento obligado a un firewall en los sistemas de seguridad. Aunque hay diferentes tipos de malware actualmente los usuarios pueden disponer de programas informáticos muy completos que se enfrentan a todos los tipos de software malintencionado con una sola aplicación.

Puede acceder a una comparativa actualizada al año 2010 de los mejores productos antivirus, con sus precios y características, en www.pcasalvo.com

¿Qué es el hacking?

Es la entrada directa de una persona en un sistema informático sin el conocimiento de su dueño, ayudándose de alguna vulnerabilidad que lo permita.

Las intenciones de los hackers varían desde demostrar los errores de diseño de una aplicación informática, con objeto de permitir generar un parche que la elimine, hasta explotar ese error del software para fines perjudiciales para las víctimas o beneficiosos para los atacantes.

¿Qué es el spam?

El spam o 'correo electrónico no deseado' o 'correo basura' es el conjunto de mensajes no solicitados, que, enviados masivamente, están en condiciones de perjudicar de alguna manera al receptor de los mismos. El sistema más frecuentemente empleado es el correo electrónico, pero también han sido objeto del 'correo basura' los grupos de noticias, los blogs, los foros e incluso los teléfonos móviles, a través de mensajes de texto.

En el mes de abril del año 2009, Sophos http://esp.sophos.com, una compañía especializada en soluciones de seguridad y autora de la célebre lista "Dirty Dozen" (en ocurrente alusión a la célebre película "Los doce del patíbulo"), informaba de que España ocupa la octava plaza entre los países afectados por el spam (el número 1 corresponde a Estados Unidos).

¿Qué es un elemento emergente (pop-up)?

Son las pequeñas ventanas que se abren en el navegador, encima de la página web que se está viendo, para ampliar la información o, como es más frecuente, introducir publicidad durante la navegación o mostrar material de contenido sexual explícito.

Aunque no suele provocar problemas de seguridad, puede ser muy molesto o inconveniente, por lo que los navegadores incorporan "bloqueadores de elementos emergentes" que pueden ser configurados con facilidad por los propios usuarios.

¿Qué es una cookie?

Es un fragmento de información que se almacena en nuestro disco duro cuando visitamos determinadas páginas web, a petición del autor de la página. Se emplea para llevar un control de los visitantes u obtener información sobre los hábitos de navegación del usuario.

No suelen generar problemas de seguridad, pero significan intrusiones en el ámbito de la privacidad, por lo que los navegadores incorporan la opción de permitirlas o no.

¿Qué es un certificado digital?

Es un documento digital que contiene, entre otros, los datos que identifican a su poseedor. Permite identificarse inequívocamente en Internet e intercambiar información con otras personas con la garantía de que sólo usted y su interlocutor pueden acceder a ella.

¿Qué es una conexión wi-fi?

Es un sistema que permite la conexión de los ordenadores a Internet 'sin cables' (inalámbrica). Esto tiene múltiples ventajas, pero también puede conllevar ciertos riesgos. En el capítulo Medidas y herramientas de seguridad de esta guía encontrará consejos al respecto.

¿Qué es una conexión segura?

Es la que se realiza mediante métodos de encriptación (habitualmente mediante el 'protocolo SSL' -Secure Sockets Layer o Protocolo de Capa de Conexión Segura-), que impiden que se pueda acceder a la información intercambiada entre un ordenador personal y el servidor al que se conecta (garantía de confidencialidad) o pueda ser manipulada (garantía de integridad) en caso de ser interceptada.

Problemas de seguridad relacionados con menores

El entorno de Internet tiene innegables ventajas, no cabe duda, pero con el tiempo también ha sido objeto de la actuación de una nueva "delincuencia tecnológica", muy favorecida por la buena fe de muchos usuarios que no concebían encontrar en la Red nada desfavorable.

El malware, en general, las vulnerabilidades de los programas informáticos y el correo basura (spam) son problemas de seguridad que amenazan a todos los usuarios de ordenadores, particularmente si interactúan con otros usuarios a través de una red.

Existen, no obstante, otras amenazas que significan un problema aún mayor para los usuarios de las modernas TIC. Hablaremos de las más peligrosas en lo que se refiere a los menores.

Observatorio de la infancia
www.observatoriodelainfancia.msps.es

Los riesgos del correo electrónico y la mensajería instantánea

Los programas de mensajería instantánea (y chat) y el correo electrónico (e-mail) son servicios de comunicación que han alcanzado un gran nivel de desarrollo en Internet. El mismo hecho de su éxito y nivel de utilización los convierte en uno de los medios más utilizados para la difusión de software malicioso y contenidos no solicitados, con la ventaja para sus autores de una difusión masiva y un coste reducido.

Los riesgos relacionados con la deficiente utilización de estas tecnologías son, principalmente, de tres tipos:

— **La recopilación de direcciones de correo electrónico** mediante, por ejemplo, la utilización de 'programas de cosecha' de direcciones (harvesting), que son posteriormente utilizadas para el envío masivo de comunicaciones no solicitadas (spam) o la difusión de falsas noticias en un intento de hacer creer a un grupo de personas que algo falso o innecesario es real o necesario (hoax).

— **La suplantación de identidad**, porque, en general, no se emplean sistemas de establecimiento fiable de la identidad de emisor y receptor ni mecanismos que garanticen la confidencialidad en el intercambio de la información. ¿Tiene usted siempre la seguridad de que intercambia correos con la persona que el destinatario dice ser?

— **La instalación de software malicioso**, que se realiza, frecuentemente, mediante la inclusión de malware en documentos adjuntos a los mensajes de correo. Buscar "Recomendaciones dirigidas a usuarios de Internet" en la Agencia de Protección de Datos www.agpd.es.

Las amenazas personales: Grooming, Ciberacoso y Sexting

Las amenazas a través de la Red (las injurias, los insultos y los comentarios vejatorios contra otra persona) adquieren una especial relevancia porque se realizan por escrito y producen en el receptor una fuerte sensación de indefensión. Este efecto es aún más dañino cuando el destinatario es un menor.

Línea de ayuda ante el acoso escolar
www.acosoescolar.info/index.htm

En palabras de Parry Aftab, directora ejecutiva de Wiredsafety www.wiredsafety.org, una iniciativa mundial en red sobre seguridad y educación, "el ciberacoso es el riesgo más frecuente para los niños".

También tienen cabida en este apartado los delitos de opinión, la apología del terrorismo o la incitación a la comisión de delitos, conductas agravadas legalmente si se cometen a través de Internet.

Entre los problemas de seguridad más graves se encuentran los delitos contra la libertad sexual, que van desde el mero acoso hasta el exhibicionismo o la provocación explícita:

1. **Grooming** [*engatusar*]. www.internautas.org/html/5349.html
   Es un término anglosajón que se refiere a los procedimientos (establecer lazos emocionales, obtener datos personales, enviar o solicitar imágenes de contenido erótico o pornográfico y chantaje posterior) que utilizan **pederastas y pedófilos** a la hora de ganarse la confianza del internauta menor de edad.

2. **Ciberbullying** [*ciberacoso*]. www.ciberbullying.net
   Se entiende por ciberacoso la persecución y hostigamiento, entre menores, en el entorno de una red de comunicaciones (Internet, teléfonos móviles u otras tecnologías telemáticas). Suele consistir en **amenazas**, **humillaciones**, **chantaje**, **vejaciones** o **insultos** de jóvenes a otros jóvenes. El anonimato, la falta de percepción del daño real causado y la frecuente adopción de roles imaginarios en la red convierten al ciberacoso en un grave problema.

↘ ¿Cómo actuar ante amenazas?
www.ciberfamilias.com/conflictos1.htm

↘ En la página web de INTECO se puede descargar una 'Guía sobre ciberbullying y grooming'
www.inteco.es

3. **Sexting** [*juego de palabras traducible por 'enviando sexo'*]. www.sexting.es
   El sexting consiste en el **envío de contenidos de tipo sexual** (principalmente fotografías y/o vídeos), producidos generalmente por el propio remitente, a otros menores **por medio de teléfonos móviles**. La presión de sus 'colegas', el deseo de ser reconocidos, la necesidad de que les presten atención, la inmadurez y otros motivos típicos de determinadas edades conforman las razones que descansan detrás de esta práctica.

Tristemente célebre fue el caso (julio de 2008) de una adolescente norteamericana (Jessie Logan) de 18 años, que se suicidó tras el escándalo generado por el paso al ámbito público de unas fotos privadas que la joven había enviado a su novio en el instituto y éste, maliciosamente, reenvió a cientos de estudiantes de su entorno.

La exposición al fraude

El fraude tiene cabida, cómo no, en las TIC. En el fondo, se trata de herramientas de comunicación que suponen una nueva 'oportunidad' para los timadores.

Las amenazas más importantes relacionadas con fraudes no afectan, afortunadamente, a los menores, pues se refieren a servicios que requieren una especial confidencialidad: banca electrónica, comercio electrónico, trámites con la administración, etc.

El principal componente fraudulento en la interacción de los menores con las redes es la suplantación de la personalidad (ver el apartado Privacidad y seguridad en esta guía). En este grupo de edad es frecuente un exceso de confianza, lo que convierte en más vulnerable a este colectivo.

➘ www.osi.es/ABC_Seguridad/Fraude_ingenieria_social

Privacidad y seguridad

El riesgo de exponer públicamente información privada o confidencial, que ya es a veces difícil de comprender para los adultos, se ve incrementado, en el caso de los menores, ante su mayor ingenuidad al facilitar datos personales, tanto suyos como de familiares o de compañeros.

Los delitos contra la intimidad se circunscriben generalmente a la utilización de datos personales de terceros sin su consentimiento, con ánimo de perjudicarles. Puede tratarse de difundir su teléfono o domicilio, o de exponer su fotografía o conversaciones privadas.

Se denomina ingeniería social (Social Engineering en inglés) a todas las acciones o conductas enfocadas a obtener información confidencial sobre personas a través de una estrategia de manipulación. Se trata de obtener información sobre una persona a través de ella misma sin que se dé cuenta de que está revelando 'información sensible'. En el fondo, se aprovecha el eslabón más débil de los sistemas de seguridad: el ser humano.

Se pretende obtener información, acceso o privilegios en sistemas de información que permitan realizar algún acto que perjudique o exponga a la persona a riesgos o abusos.

Se trata de conductas expresamente contempladas en la legislación como "descubrimiento y revelación de secretos", que pueden conllevar varios años de cárcel.

> "Buenos días, señor:
>
> Le llamamos del servicio de marketing de una empresa de gran implantación. Estamos ofreciendo una promoción especial a nuestros mejores clientes. Consiste en que las llamadas a un número fijo nacional de su elección serán gratis durante un año.
>
> Por favor, para poder acceder a esta promoción necesitamos que nos confirme una serie de datos…."

www.privacidad-online.net

Los timos en la Red

Las páginas web falsas son un buen ejemplo. Suelen ser utilizadas para ofrecer servicios inexistentes (un servicio de pago sin entrega posterior, por ejemplo), o para suplantar sitios web oficiales (imitando el aspecto de la página web de entidades bancarias, comercios o administraciones públicas), con el objetivo de robar la información que se intercambia habitualmente con dichas entidades.

El caso más común se conoce como phishing y consiste en utilizar un correo electrónico que, aunque a primera vista puede parecer que lo remite una entidad legítima, contiene un enlace a una página falsa en la que, si introducimos nuestros datos, éstos pasarán directamente a manos del estafador. Otro caso, más complejo y mucho más peligroso, es el pharming, en el que se redirige a un usuario a una página falsa a pesar de que tecleó sin error la verdadera dirección web. Mediante este sistema la página web de la Guardia Civil fue atacada en 1999, de manera que, a pesar de teclear la dirección correctamente, www.guardiacivil.org, el usuario era redirigido a una página web de contenido sexual.

La mejor manera de evitar este tipo de fraude consiste en aprender a reconocer mensajes fraudulentos y conocer las recomendaciones para realizar trámites en línea.

➘ www.osi.es/econf/Protegete/Tramites_en_linea/Reconocer_mensajes_fraudulentos

El acceso a contenidos inapropiados

Nada puede sustituir la labor de vigilancia y educación de los padres en la protección de sus hijos frente al contenido inapropiado de Internet

Internet, en su concepción actual, es un sistema abierto a los usuarios en las dos direcciones. Por una parte, se benefician de los contenidos que encuentran durante su navegación y, por otra, pueden contribuir al enriquecimiento de la propia oferta de contenidos. La oferta de información y archivos compartidos en la Red es de tal magnitud que no es posible un control general sobre todos ellos, por lo que la vigilancia sobre el acceso a los mismos depende, en última instancia, de los deseos y la implicación de los propios usuarios.

Al navegar por Internet, el menor puede encontrarse, incluso sin buscarlo, con contenidos no adecuados para su edad, como páginas que ofrecen **sexo explícito** o páginas con **contenidos violentos**, **lenguajes inadecuados** o **informaciones malintencionadas**.

Existen herramientas que facilitan la tarea de controlar los contenidos inapropiados para los menores, como WOT (una extensión para los navegadores Mozilla Firefox e Internet Explorer que advierte sobre la confianza de un sitio web antes de acceder a él, mediante el uso de un código de colores asociado a los enlaces que llevan a dicho sitio web), pero **nada puede sustituir la labor de vigilancia y educación de los padres** en la protección de sus hijos frente al contenido inapropiado de Internet.

↘ www.mywot.com/es

Los riesgos de compartir archivos

El intercambio de archivos (música, vídeo, software, etc.) a través de programas específicos para esa función (P2P), es practicado en la Red todos los días por millones de usuarios. Se trata de un procedimiento tan sencillo como instalar un programa informático, generalmente gratuito y de fácil acceso, y pedirle que busque el objeto de nuestro interés.

El sistema permite que la información viaje a gran velocidad y que se pueda compartir una enorme cantidad de ficheros sin tener que disponer de un único ordenador que almacene toda la información, pues la carga, tanto de ancho de banda como de espacio en disco, se reparte entre todos los participantes.

Los riesgos de esta práctica son elevados, y no solamente por la posibilidad de infringir los derechos de autor del material descargado, sino también por la frecuencia con la que este material está infectado por malware y la facilidad con la que un usuario poco cuidadoso puede exponer todo el contenido de su propio ordenador a cualquier persona malintencionada.

En septiembre de 2009, la empresa G Data www.gdata.es advertía que más de un 90 % de los archivos ejecutables procedentes de una determinada página web, muy visitada con estos fines, estaba infectado por algún tipo de malware.

➘ www.ftc.gov/bcp/edu/pubs/consumer/alerts/salt128.shtm

Los peligros de las Redes Sociales

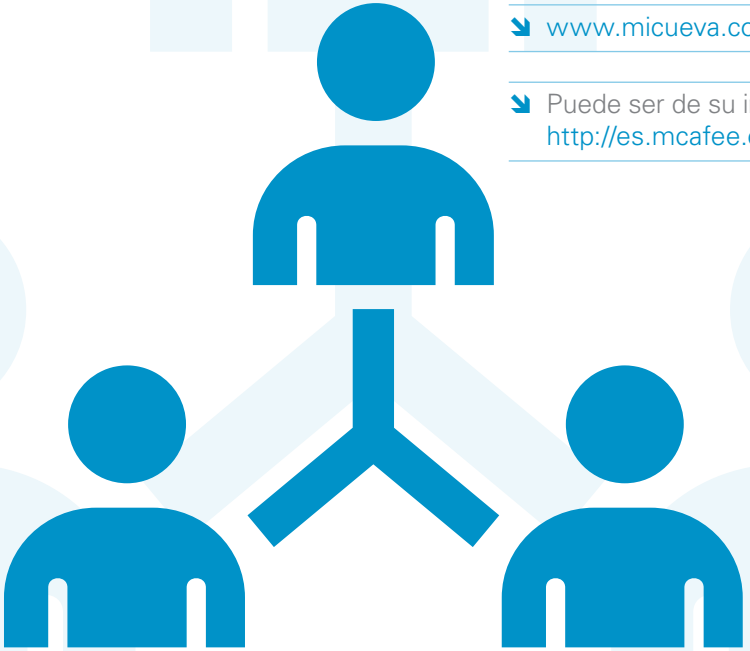
Las Redes Sociales son sistemas de interacción social consistentes en la facilitación, a través de un sistema informático, de un intercambio entre personas. Por su propia naturaleza son sistemas abiertos y muy dinámicos que invitan a la participación activa, a compartir contenidos y, en general, a la comunicación y el encuentro. Estas redes son muy populares entre los menores porque les permiten crear una página personal, expresarse libremente y establecer vínculos con amigos.

Las redes sociales pueden afectar a la seguridad de los menores porque ofrecen tantas opciones que dificultan el empleo de criterios de selección, porque disponen de muchos automatismos (falsa sensación de seguridad) y porque ofrecen opciones tan avanzadas que pueden comprometer la seguridad de los usuarios menos avezados ("¡... pero si no sabía que hacía eso...!").

No se trata de satanizar las redes sociales, que son una herramienta de gran utilidad, sino de conocer en profundidad sus aportaciones, sus riesgos y la manera correcta de interactuar con ellas. En Internet existen excelentes iniciativas, como la red social para menores Mi cueva, creada y promovida por PROTÉGELES, en la que la seguridad juega un papel principal.

- www.micueva.com

- Puede ser de su interés revisar la *"Guía para padres sobre las redes sociales"* http://es.mcafee.com/es/local/docs/SocialNetworkinge-guide.pdf



Seguridad en el teléfono móvil

Los avances tecnológicos permiten utilizar estos terminales para usos diferentes a los tradicionales: enviar mensajes cortos (SMS), jugar, hacer y enviar fotografías, descargar archivos, etc. Los teléfonos móviles modernos poseen tecnología para conectarse a Internet. Para poder hacer un uso seguro de los teléfonos móviles (básicos o avanzados -Smartphone y PDA-), es necesario conocer sus funcionalidades y leer cuidadosamente los consejos de utilización que ofrecen en la documentación del aparato todas las compañías.

En el estudio que sobre *"Seguridad infantil y costumbres de los menores en el empleo de la telefonía móvil"* realizó PROTÉGELES para el Defensor del Menor de la Comunidad de Madrid se demuestra que las situaciones de riesgo a las que se enfrentan los menores con esta tecnología son ya casi las mismas que pueden encontrarse en Internet.

Resulta llamativo el hecho de que los menores no usan el teléfono móvil para hablar con otras personas utilizando la voz en tiempo real. Lo usan con mucha mayor frecuencia para enviar SMS que para mantener conversaciones orales. Sólo el 24% de los menores realiza llamadas telefónicas con su móvil diariamente.

➘ www.protegeles.com/es_estudios2.asp

Medidas y herramientas de seguridad

La seguridad de un sistema se basa en conocer dónde se encuentran sus principales vulnerabilidades y corregirlas. No hace falta ser un experto para ello, simplemente es necesario conocer la información precisa, emplear los medios disponibles y utilizar el sentido común.

No obstante, nunca debemos perder de vista que la **principal herramienta** de seguridad en un sistema informático no es el último descubrimiento de un experto, un caro software o la utilización de complejas herramientas, sino el mantenimiento de unos **buenos hábitos de interconexión con la Red** (ver el capítulo Recomendaciones para una conexión segura) y evitar la exposición a riesgos innecesarios.

En el ordenador

OCHO consejos básicos de SEGURIDAD:

1. Comience a cuidar su equipo informático desde el primer día. Cuando instale un nuevo sistema operativo o estrene un ordenador, empiece a interactuar con él descargando todas sus **actualizaciones**, instalando un software **antivirus** y conectando el **firewall**. Después, haga una **copia de seguridad** de todo el sistema. Los sistemas operativos modernos tienen excelentes herramientas para realizar estas labores, excepto el software antivirus, que debe ser instalado individualmente.

   Por ejemplo: avast! (gratuito) en www.avast.com/es-es/index

2. Haga, con frecuencia semanal, **copias de seguridad** (backups) de toda la información que va generando con su trabajo para evitar la pérdida irrecuperable de datos importantes. Las aplicaciones informáticas se pueden reinstalar, pero los archivos personales que se han creado con ellas no. Si le parece complejo o le da pereza utilizar las opciones que ofrecen los propios sistemas operativos, utilice programas gratuitos que lo hacen por usted.

   Por ejemplo: Cobian Backup en www.educ.umu.se/~cobian/cobianbackup.htm

3. Mantenga **actualizado** el equipo informático (sistema operativo y software antivirus sobre todo), empleando para ello las opciones de actualización que ofrecen los propios programas. Utilice software legal, que suele ofrecer garantía, soporte y actualizaciones.
   En el caso de los navegadores, Internet Explorer (el navegador de Microsoft) se actualiza a través del mismo mecanismo que el sistema operativo, activando las actualizaciones automáticas. Mozilla Firefox www.mozilla-europe.org/es y Safari www.apple.com/es/safari se actualizan de forma automática por defecto.

4. Cuando se conecte a Internet a través de una conexión inalámbrica (Wi-Fi) hágalo de **modo seguro**. Utilice los sistemas de protección que ofrecen los navegadores y aproveche las opciones que ofrece el **control parental**. Utilice encriptación WPA (o mejor WPA2 si su sistema lo permite) para evitar la captura de los datos que envíe.
   La página web de INTECO ofrece la descarga de una *"Guía para proteger la conexión inalámbrica de su hogar"*. www.inteco.es.

5. Sea **confiado, pero no ingenuo**. No todo lo que se lee en Internet tiene porqué ser cierto. Utilice fuentes contrastadas que le inspiren confianza y corrobore la información en otras fuentes para evitar los contenidos faltos de rigor y los bulos. No dé información personal a través de la línea telefónica. Sospeche de las páginas con mensajes llamativos o muy alarmantes. En ocasiones, podrían intentar captar su atención para redirigirle a páginas maliciosas que propagan virus. Hay herramientas gratuitas para analizar la peligrosidad de los contenidos de las páginas web, como Mc Afee SiteAdvisor (asesor de navegación) http://es.mcafee.com/root/product.asp?productid=sa
6. Acostúmbrese a utilizar **buenas contraseñas**. Más de 8 caracteres y que incluyan una combinación aleatoria de letras mayúsculas y minúsculas, números y símbolos, es una buena elección. Cambie sus contraseñas de forma periódica.
   Puede ver consejos al respecto en el centro de seguridad de Microsoft www.microsoft.com/latam/athome/security/default.mspx o en la página web de McAfee http://es.mcafee.com/es/local/docs/FamilySafetyPlan.pdf.
   También puede ser una buena idea emplear contraseñas muy seguras, imposibles de recordar, e instalar un software encriptado gratuito para almacenarlas.

> Por ejemplo:
> LoginControl en www.pandreonline.com/productos/logincontrol

7. Protéjase contra las descargas que incluyen software malintencionado. Cuando necesite descargar algún programa, hágalo siempre desde las páginas oficiales, o al menos desde **páginas de confianza**. Todo lo que descargue, analícelo con un antivirus antes de ejecutarlo.
8. Utilice **programas de filtrado** de contenidos web. Se trata de herramientas de control y monitorización capaces de bloquear el acceso a contenidos no apropiados para menores. El sistema empleado para impedir el acceso a dichos contenidos es muy variado: bloqueo de determinadas direcciones, control de las horas de acceso, inhabilitación de acceso a páginas con determinados contenidos, etc. Es el caso de Canguro Net, que en España comercializa Telefónica www.telefonica.es en hogar/internet/seguridad/servicios o los programas gratuitos de filtrado que ofrece el portal Archivos PC www.archivospc.com en el apartado Protección PC.

En los teléfonos móviles

Le ofrecemos algunas recomendaciones de seguridad para los teléfonos móviles. Puede ampliar esta información con la *"Guía para proteger y usar de forma segura su móvil"* que es accesible gratuitamente en la página web del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

↘ www.inteco.es

— No perder nunca de vista el teléfono en lugares públicos, pues resulta muy atractivo a los delincuentes para su manipulación o robo. No prestar el teléfono móvil a personas extrañas. En caso de intento de robo, preservar la integridad física y renunciar al móvil.

— Activar el **código PIN** (código personal que permite, o impide, acceder a la tarjeta SIM del teléfono) y mantener en lugar seguro el **código PUK** (código de seguridad que permite desbloquear el teléfono si se ha errado en la introducción del PIN en tres ocasiones).

— Activar la opción de **bloqueo** del terminal con solicitud de contraseña para desbloquearlo. Aunque el teléfono no permita hacer llamadas telefónicas, puede permitir el acceso a los datos que contiene (información personal).

— Utilizar siempre **contraseñas** robustas para proteger el acceso y sus conexiones (Ver al respecto la utilización de buenas contraseñas -página 25- en el apartado dedicado al ordenador).

— Vigilar el **consumo** en la tarifa telefónica e informarse, de inmediato, ante cualquier anomalía. En el caso de los menores es muy recomendable utilizar el sistema de tarjetas prepago.

— No abrir **correos electrónicos**, ni aceptar archivos, si no se conoce al remitente. No contestar nunca a **SMS** de desconocidos. Instalar siempre software original para estar en condiciones de pedir soporte al fabricante.

— No dejar nunca el **Bluetooth** encendido si no lo está usando. El Bluetooth es una excelente tecnología para la transmisión de datos y voz (manos libres del coche), pero su nivel de seguridad no lo es tanto (depende del uso adecuado que haga el usuario). En todo caso, solicite autorización para cada conexión y desactive la opción que permite que el teléfono móvil aparezca como visible para los demás.

— Acostumbrarse, y acostumbrar a los menores, a **pedir permiso** antes de fotografiar a amigos o conocidos. En lugares como colegios, gimnasios o piscinas fotografiar con el móvil está prohibido.

— No contestar nunca a **SMS** de contenido amenazante. Si se reciben amenazas a través del móvil es aconsejable anotar la hora de la llamada, guardar el mensaje y ponerlo en conocimiento de la dirección del centro escolar y/o de la policía (ver el capítulo Perspectiva legal).

— Comprobar periódicamente los **números de teléfono almacenados** en los teléfonos móviles de los hijos menores.

Debe usted saber, además, que las compañías Telefónica, Orange, Vodafone y Yoigo suscribieron el 12 de diciembre de 2007 un 'código de conducta de operadores móviles para el fomento de un uso responsable por parte de menores de edad a los servicios de contenidos de comunicaciones electrónicas móviles en España'. Puede verlo en:

↘ www.gsmeurope.org/documents/eu_codes/spain_codigo.pdf

Algunas preguntas y respuestas

Es de capital importancia guiar a los menores durante sus primeros pasos y servir de ejemplo en la práctica.

¿Cuál es la edad adecuada para empezar a interactuar en la Red?

Debe considerar que es más relevante el modo de conectarse a Internet que la edad que tenga el menor. Cada vez es más frecuente la presencia de menores en la Red, y esto sucede a edades más tempranas. El sistema educativo, de hecho, fomenta la conexión a la Red durante el horario escolar.

Es de capital importancia **guiar a los menores** durante sus primeros pasos y **servir de ejemplo** en la práctica. Estas primeras aproximaciones, ante la ausencia de criterios del menor para estar conectado, son de especial importancia. Al principio, **siéntese con ellos** siempre que estén conectados. Asegúrese de que van comprendiendo y practicando los principios fundamentales de una navegación segura. **Anticípese a la información** que, sin duda, recibirán fuera del hogar.

En el *"Centro de Protección de Microsoft: seguridad de los niños en línea"*, por ejemplo, puede encontrar un buen apoyo a sus dudas en la *"Guía para padres sobre la seguridad en línea"*.

www.microsoft.com/latam/athome/security/default.mspx

¿Los menores se pueden volver adictos a Internet?

Internet constituye una herramienta interesante para los jóvenes, especialmente para los que poseen conocimientos informáticos, porque puede ayudarles a aumentar su autoestima. No obstante, un uso excesivo puede aislar todavía más a los niños más tímidos de los demás o apartarles de otras actividades, como las tareas escolares, el ejercicio, el descanso o la oportunidad de pasar el tiempo con los amigos.

La adicción, de cualquier tipo, es una conducta que supone una pérdida de control por parte del adicto sobre su manera de comportarse. Además, genera una pérdida de interés por otras actividades gratificantes y constituye una interferencia notable en su vida.

El uso abusivo de estas tecnologías puede generar **síntomas** alarmantes que los padres deben aprender a reconocer:

— Sensación placentera, o incluso **euforia**, mientras se permanece conectado y estado emocional perturbado (**ansiedad**, **impaciencia**, **irritabilidad**…) cuando la actividad es interrumpida.

— Deseo intenso de repetir la conducta, con **incremento progresivo del tiempo de conexión**, asociado a la negación o minimización de la propia conducta.

— Deterioro de las relaciones sociales y familiares. **Aislamiento**. Deterioro en el rendimiento escolar.

— Problemas físicos derivados de la falta de sueño (**fatiga**, **debilidad**, **somnolencia**…) y de ejercicio físico.

Si se da alguna de estas circunstancias, o tiene dudas, consulte a un especialista.

➘ www.tecnoadicciones.com

¿Es adecuado que los menores tengan sus propias cuentas de correo electrónico?

Los niños pequeños deben compartir una dirección de correo electrónico familiar en vez de tener una cuenta propia. A medida que crezcan y deseen más independencia puede asignarles una dirección propia, pero durante ese tiempo **deben haber recibido formación sobre el tema**. El correo puede seguir estando en la bandeja de entrada de la familia. Pregunte a su proveedor de servicios de Internet (ISP) las opciones que ofrece para cuentas de correo electrónico de familia y utilice filtros de correo electrónico para evitar la recepción de correo no deseado, mensajes no solicitados y envíos fraudulentos.

¿Es posible saber qué páginas visitan los menores cuando se conectan?

Existen varias posibilidades a este respecto, pero la más sencilla es la revisión del Historial de conexión a Internet que ofrecen todos los navegadores en sus menús. El historial de navegación registra los sitios web que se visitan. Los navegadores ofrecen este servicio porque es útil para ofrecer sugerencias de búsqueda según los sitios web que se han visitado anteriormente. De todos modos, tenga en cuenta que el historial puede ser borrado en cualquier momento por el menor.

¿Qué debo hacer si acosan a mi hija o a mi hijo en línea?

Cualquier situación de acoso, o sospecha del mismo, es una emergencia. Los problemas de ciberacoso entre adolescentes cada vez son más frecuentes (ver el apartado Las amenazas personales: Grooming, Ciberacoso y Sexting en el capítulo Problemas de seguridad relacionados con menores).

Si se produce el acoso, puede **bloquear** a la persona que envía los mensajes con las opciones de bloqueo que incluyen la mayoría de los programas de correo electrónico y de mensajería instantánea. Guarde los mensajes de correo electrónico que incluyan acoso y reenvíelos a su proveedor de servicios de correo electrónico. La mayoría de los proveedores disponen de directivas de uso adecuado que prohíben el acoso.

En caso de que el problema no se solucione de inmediato, actúe de manera resolutiva y **denuncie** la conducta indeseable (ver sistemas de denuncia en el capítulo Perspectiva legal.

¿Funciona el software de filtrado?

Las herramientas de filtrado pueden resultar útiles con los jóvenes para complementar, no reemplazar, la

La mejor manera de proteger a los hijos es educarles para que hagan un uso responsable y seguro de todas las posibilidades que ofrece la Red.

supervisión de los padres. No obstante, los filtros y los bloqueadores no son infalibles y, a veces, no bloquean todo el material inadecuado. También es posible que bloqueen, por exceso de celo, mucho contenido útil que los niños pueden necesitar para sus tareas escolares. Son problemas asociados al empleo de automatismos, cuya función es la de apoyo a los padres, no la de sustitución de los mismos.

Ningún filtro puede proteger totalmente al menor de otros usuarios con malas intenciones. Siempre habrá personas que traten de encontrar la manera de saltarse las medidas de seguridad. Por eso, **la mejor manera de proteger a los hijos es educarles** para que hagan un uso responsable y seguro de todas las posibilidades que ofrece la Red.

Aunque los filtros pueden resultar útiles cuando los hijos son pequeños, a medida que crezcan tienen que desarrollar un **comportamiento en línea seguro y responsable**.

¿Qué es el control parental? ¿Cómo funciona?

El control parental es una herramienta muy útil para padres con menores bajo su responsabilidad. Con ella se pretende evitar, en la medida de lo posible, que los menores accedan a contenidos de Internet inapropiados.

Se basa en la aplicación de **filtros** sobre los contenidos a los que pueden acceder los menores, impidiéndoles o permitiéndoles el acceso. Cuando el menor se conecta a una página web, el navegador solicita un usuario y contraseña (la primera vez en cada sesión) predefinidos. Una vez introducidos, comprueba la catalogación de la página y en el caso de que no esté permitida para el menor, se le impide el acceso.

El sistema de filtrado es personalizable y puede contratarlo con su compañía telefónica.

Le puede interesar ver, al respecto, la guía *"Cómo activar y configurar el control parental de los sistemas*

operativos" del Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnologías de la Comunicación

↘ www.inteco.es

Mi hijo adolescente quiere comprar en línea. ¿Cómo puedo saber que el sitio es seguro?

Antes de dejar que su hijo adolescente utilice la tarjeta de crédito en línea, debe indicarle unas directrices claras acerca de las compras en línea y lo que debe tener en cuenta para que las transacciones sean seguras y estén protegidas.

Antes de comprar en un sitio Web, se debe buscar como mínimo:

— Un icono de candado cerrado en la esquina inferior de la página, lo que indica que sólo el usuario y el sitio web pueden ver las transacciones que se realizan.

— Un https (la "s" significa que es seguro) al comienzo de la dirección del sitio web que se muestra en el cuadro de direcciones del explorador.

Los elementos anteriores se pueden falsificar, por lo que es importante que diga a sus hijos que le pregunten antes de realizar compras en línea, con lo que usted se convertirá en el juez final para determinar si un sitio web es seguro o no lo es.

¿Cómo puedo evitar los elementos emergentes en mi equipo?

La forma más sencilla de evitar los elementos emergentes (pop-up) es utilizar un software que los bloquee. Los modernos navegadores Internet Explorer, Mozilla Firefox y Safari disponen de un sistema directo de bloqueo de elementos emergentes configurable a través del menú Herramientas>Opciones.

↘ http://support.mozilla.com/es/kb/Ventanas+emergentes

↘ http://windows.microsoft.com/es-es/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions

¿Debo activar o debo desactivar las actualizaciones automáticas del sistema operativo?

Es muy recomendable **mantener activada** la opción Actualizaciones automáticas que ofrecen los sistemas operativos, y también todo el software antivirus de calidad. Las actualizaciones son adiciones al software que sirven para prevenir problemas o corregir errores (vulnerabilidades) en el equipo a medida que se van descubriendo. Con ello se consigue más estabilidad del equipo y se asegura una mayor seguridad en el sistema.

↘ www.consumer.es/web/es/tecnologia/software/2009/08/24/187121.php

¿A qué edad deben disponer los menores de un teléfono móvil?

El uso de teléfono móvil se ha extendido entre los menores de una manera muy rápida, en parte, por el interés intrínseco de disponer de esta tecnología y en parte, por la presión de las compañías de telefonía, para las que este segmento de la población es una importante opción de futuro.

Debe usted reflexionar seriamente sobre el tema antes de dar el paso, comprender los riesgos que entraña en contraposición con los beneficios que aporta (pregúntese: ¿para qué necesita un móvil una niña/o de X años?) y, en cualquier caso, **marcar unas normas muy estrictas** sobre la utilización del aparato por el menor.

Recomendaciones para una conexión segura

Internet es una opción importante en la formación y el ocio de los menores, pero es necesario tener buenos hábitos de seguridad para que puedan disfrutarlo plenamente.

En general, es muy útil consensuar **reglas familiares** para las conexiones a la Red, plasmarlas en un papel cerca del ordenador y respetarlas estrictamente. Un ejemplo puede ser:

— No registrarse con nombres de usuario que incluyan datos personales reales, ni publicar información sobre la verdadera identidad.

— No revelar nunca las contraseñas, dirección o el número de teléfono.

— No publicar nunca fotografías inadecuadas o que puedan revelar la identidad, ni emplear nombres de usuario provocativos.

— No compartir nunca información con desconocidos con los que se ha contactado a través de la Red.

— No reunirse nunca con desconocidos contactados a través de Internet.

— No abrir nunca archivos adjuntos de procedencia desconocida.

Consejos para una navegación segura en la Web

— **Proteger el ordenador con contraseña** que restrinja el inicio de sesión y que impida que un tercero pueda acceder a él sin nuestro conocimiento. Las contraseñas deberán mantenerse, por supuesto, en secreto y no revelarse a ningún tercero o ser anotadas en lugares fácilmente accesibles.

— **No facilitar datos personales** si no existe una completa seguridad sobre quién los va a recibir. En ningún caso más de los estrictamente necesarios.

— **Nunca intercambiar información** sin que la conexión sea segura. Es muy fácil saber si se ha establecido una conexión segura porque en el ordenador el comienzo de la dirección de la página contactada es https en lugar de http. Además, en la parte inferior del navegador (barra de estado) aparece un candado cerrado.

— **Actualizar** los sistemas operativos y navegadores con los parches (actualizaciones automáticas recomendadas) que publican las empresas que los diseñan.

— No contratar servicios en proveedores de Internet que le proporcionen una dirección IP fija, ya que esto haría fácil localizar al menor cuando está navegando u obtener datos importantes sobre él. **Contrate** preferiblemente servicios de Internet con una dirección IP dinámica. Es lo más frecuente, pero cerciórese.

— Asegurarse de que el ordenador tiene instalado un software **antivirus** de calidad y que se actualiza automáticamente a diario.

— Utilizar las opciones de **control parental** que incorporan los sistemas operativos, los programas antivirus y los navegadores web. Es muy conveniente dedicar un tiempo, antes de su uso, a configurar de manera adecuada el sistema operativo y el software del navegador con las opciones de seguridad y restricción, todas ellas muy explícitas, que se ofrecen en el menú de Herramientas de los navegadores y en el menú Inicio de los sistemas operativos.

— Adoptar las precauciones oportunas antes de proceder a la descarga de archivos asegurándose, antes de hacerlo, de la confianza o **acreditación del sitio web** desde el que se realiza.

— Estar atentos para detectar si el equipo da señales de que ha sido instalado un **software malicioso**. Entre los signos que podrían indicar que este software se encuentra instalado en el equipo se encuentran los siguientes: la página principal u otros elementos de la configuración del navegador han cambiado, algunas páginas web no son accesibles, las ventanas emergentes aparecen de manera interminable, se han instalado nuevas barras de herramientas, el equipo funciona con gran lentitud...

— En un hogar con menores, la decisión sobre la **ubicación del ordenador** de la familia es importante. Es recomendable colocar el ordenador en una **zona familiar** con mucho movimiento y que limite el número de horas que los niños puedan utilizarlo.

Recomendaciones relativas a la utilización del correo electrónico

— **No abra** mensajes de correo de origen desconocido; elimínelos directamente. Ante la más mínima sospecha, no siga los enlaces que contienen.

— **No ejecute** ningún archivo adjunto que venga con el texto del correo, particularmente si desconoce su procedencia o se trata de mensajes muy sugerentes. En último extremo, no lo abra antes de analizar el archivo con su software antivirus.

— **No participe** en cadenas de mensajes o, en todo caso, adopte precauciones, como eliminar las direcciones de destinatarios que han ido siendo incluidas en las sucesivas retransmisiones del mensaje.

— **Use los filtros antispam**. Estos filtros, que vienen integrados por defecto en los programas de correo electrónico, evitan que aparezca mucho correo no deseado en la Bandeja de entrada.

— **No facilite** nunca datos de **usuario** o **contraseña**.

— **Evite** utilizar la opción Guardar contraseña que, en ocasiones, se le ofrece para evitar la molestia de reintroducirla en cada nueva conexión.

— **No facilite** la dirección electrónica con demasiada "ligereza".

— **Configure** el programa de correo en el **nivel de seguridad máximo**. Tenga permanentemente activado un buen antivirus con defensa proactiva y el firewall. Active los filtros de correo no deseado que le ofrezca el programa de correo electrónico que utilice.

— Sea consciente de que cuando envía mensajes de correo a varios destinatarios está **revelando las direcciones** de correo electrónico de los mismos, que figuran en los campos Destinatario o Con copia (Cc). Para evitarlo, puede incluir los destinatarios del mensaje en el campo Con copia oculta (Cco); de esa manera, ninguno de los receptores podrá acceder a la dirección de correo electrónico del resto de los destinatarios y el mensaje llegará igual.

Consejos para la utilización de los servicios de mensajería instantánea y chats

— **Establezca normas** fijas y consensuadas sobre lo que es correcto durante la navegación web, particularmente durante las charlas (chats) en línea.

— **No facilite nunca datos confidenciales** (contraseñas, nombres de usuario, dirección, colegio, etc.) a través de estos canales. **No envíe** nunca fotografías a personas que conozca en una sala de chat.

— **Evite invitaciones** a visitar salas que le resulten sospechosas o que procedan de desconocidos. Tenga precaución al conversar o agregar contactos desconocidos.

— Asegúrese de que sus hijos **eviten** los salones de charla ".alt", que se centran en temas alternativos que pueden ser inadecuados para los menores.

— **Rechace** los usuarios no deseados, es decir, de los que no quiera recibir mensajes. Comuníquese únicamente con las personas que figuran en su propia lista de contactos.

— **Tenga cuidado** a la hora de crear un apodo nick. Este "alias" no debe proporcionar información personal, directa ni indirectamente.

— **Cree una barrera** contra la mensajería instantánea no deseada. No facilite a desconocidos su apodo o su dirección de correo electrónico y evite que aparezcan en áreas públicas tales como grandes directorios de Internet o perfiles de la comunidad en línea.

— **No abra** nunca imágenes, ni descargue archivos ni vínculos de mensajes, de remitentes desconocidos.

— En caso de utilizar un equipo público, **no seleccione** la característica de Inicio de sesión automático. Quienes usen ese mismo equipo después de usted podrían ver su nick y utilizarlo para conectarse.

La mayor parte de los operadores colaboran activamente en la prevención de los riesgos que implican estas tecnologías mediante el empleo de herramientas automáticas de bloqueo de palabras clave o detección de usuarios que utilicen diferentes nombres. En algunos canales puede haber, incluso, moderadores. No dude en preguntar la política que sigue al respecto su compañía de telefonía.

Recomendaciones sobre los programas de intercambio P2P

— Para acceder a las redes P2P es imprescindible **instalar un programa** (gratuito), que debe descargarse siempre de sitios reconocidos; a ser posible, desde la página del creador del programa.

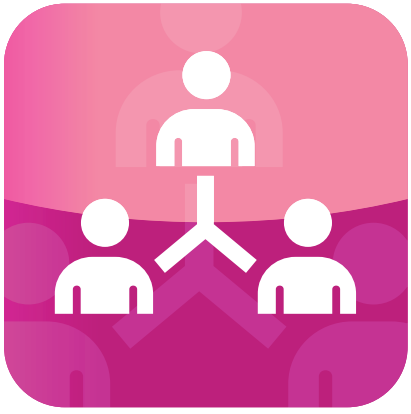
— Antes de instalar el programa es conveniente hacer una **copia de seguridad del sistema** y comprobar, una vez instalado, que solo se ha instalado el programa que queremos, pues algunos de estos programas instalan, al mismo tiempo, software malicioso, que puede hacer nuestro sistema inestable o incluso rastrear nuestras conexiones o las teclas que se pulsan.

— Establezca para la conexión un **puerto no estándar**, siempre por encima del 1024, para la comunicación administrativa con el programa.

— Los programas clientes son capaces de mantener una comunicación abierta durante las 24 horas del día. Con las actuales facilidades de acceso a Internet mediante una tarifa plana, cada vez es más frecuente. Por eso, es muy conveniente la instalación o **activación de un cortafuegos** que limite el acceso a los puertos del equipo.

— Debe **valorar los riesgos** de instalar un servidor en su ordenador, ya que deberá hacer pública su dirección IP, con lo que mucha gente conocerá dónde está su equipo y qué software tiene. No conseguirá que los ficheros se descarguen más rápido y el consumo de ancho de banda aumentará mucho.

— Al instalar un programa P2P está **compartiendo una parte de su disco duro**, de manera que toda la información que allí resida será también accesible a terceros. Elija con cuidado el directorio que va a compartir y procure que esté en una partición distinta de la del Sistema Operativo. Es preferible que lo instale en un disco distinto, aunque lo ideal es utilizar un ordenador exclusivamente para este propósito.



— Comprenda que **los ficheros pueden no ser lo que dicen ser**. El nombre del fichero no implica que contenga aquello que dice contener. Es preferible evitar descargar ficheros ejecutables (terminados en .exe) o, en caso de hacerlo, no ejecutarlos nunca antes de haber sido inspeccionados por un buen antivirus convenientemente actualizado.

— **No autorice la descarga libre** de ficheros por parte de sus hijos menores. Establezca pautas de seguridad claras y manténgalas.

Recomendaciones referidas a las conexiones inalámbricas

— **Apague el punto de acceso** cuando no vaya a utilizarlo. No se conecte a puntos de acceso desconocidos, particularmente si es fácil.

— **Desactive la difusión del nombre de su red Wi-Fi** (también llamado SSID) para evitar que equipos externos identifiquen automáticamente los datos de su red inalámbrica.

— **Cambie la contraseña que aparece por defecto**, ya que muchos fabricantes utilizan la misma clave para todos sus equipos.

— **Utilice encriptación WPA** (o mejor WPA2 si su sistema lo permite), para evitar la captura de los datos que envíe. El protocolo WEP es más simple y ofrece una encriptación más débil.

En la página web de la Oficina de Seguridad del Internauta aconsejan unos sencillos hábitos en el uso de las tecnologías:

↘ www.osi.es/econf/Protegete

Orientaciones referidas a los videojuegos

Visite la página web especializada www.guiavideojuegos.es/index.htm, donde se puede descargar la *"Guía para padres sobre videojuegos"*:

- www.guiavideojuegos.es/guia.pdf
  Desarrollada por PROTÉGELES y la Asociación Española de Madres y Padres Internautas (AEMPI).

Consejos referidos a los teléfonos móviles

— **No facilite los números de teléfono**, tanto fijo como móvil, a personas desconocidas que los soliciten, pues pueden estar intentando conocer las características de la línea.

— Ante una llamada telefónica equivocada **corte la comunicación** rápidamente para evitar el posible desvío de llamadas con cargo a la factura de su línea telefónica.

— En el caso de tener contratada la modalidad de "llamada a tres", **extreme las precauciones**, ya que con un programa informático se puede rastrear la línea y producirse una intrusión en ella para realizar llamadas internacionales con cargo al titular del teléfono.

— **No acepte** llamadas a cobro revertido si no está absolutamente seguro de conocer a quien lo pide.

— Tenga en cuenta que **nunca es necesario** llamar por teléfono a prefijos de tarifación adicional.

NOTA sobre los servicios de llamada telefónica a través de Internet (VoIP), como Skype:

No son estrictamente un servicio de telefonía, por lo que no pueden sustituir ni en calidad ni en prestaciones al teléfono tradicional. Puede, por ejemplo, que no tenga acceso a los números de emergencias (112, 091, etc.) y puede que no funcione cuando se necesite. No garantiza unos mínimos de calidad más allá de los que decida el propio fabricante.

A modo de recordatorio: Decálogo de recomendaciones

III

I. **Eduque** a sus hijos sobre los posibles peligros que pueden encontrar en la Red. Para ello, aprenda el funcionamiento básico de los ordenadores y de Internet, asegúrese de que comprende esa información y **predique con el ejemplo**. Informe a los menores de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad. Oriente a sus hijos sobre la importancia de discriminar lo que está bien y lo que está mal en la Red (igual que en la vida real). Intercambie conocimientos con sus hijos sobre novedades en lo referente a las TIC.

II. **Acompañe** al menor en la navegación. Los menores más jóvenes deberían estar siempre acompañados de un adulto durante la interacción con la Red. Disfrute de las posibilidades de Internet con sus hijos. Anímeles a compartir sus dudas. Intente que sus hijos le cuenten con naturalidad lo que descubren en Internet. **Dedique tiempo a fomentar hábitos correctos de comunicación** (igual que hace con las lecturas o la higiene personal). La mejor manera de asegurar que las actividades cibernéticas de sus hijos sean positivas es **hablando con ellos**.

↘ www.privacyrights.org/spanish/pi21.htm

III. Inculque en el menor **hábitos de seguridad** estrictos en la navegación por Internet en lo relativo a la información personal. Cuando las aplicaciones informáticas (programas de mensajería, videojuegos, chats, etc.) soliciten contraseñas, ayúdele a configurarlas correctamente. **Los padres deben vigilar** que sus hijos no intercambian información con desconocidos. Internet retiene todo rastro de tráfico, por lo que la información que transporta puede ser rastreada.

IV. **Los menores deben ser enseñados**, explícitamente, a no facilitar información personal a través de Internet. Advierta de la importancia de **no compartir información personal** a través de la Red (dirección, teléfono, escuela a la que van o dónde les gusta jugar). Nunca es necesario para disfrutar de la Red. Lea la política de privacidad de los sitios que visitan sus hijos. Los mejores sitios explican muy bien la información que recogen.

V. Inste a sus hijos a **respetar la propiedad** en la Red. Explíqueles que la descarga o realización de copias ilegales del trabajo de otras personas es incorrecto e ilegal. Acostumbre al menor a **buscar herramientas gratuitas** en la Red para cubrir sus necesidades como primera opción, pues es divertido, retador y proporciona grandes sorpresas. Hay múltiples opciones para la búsqueda de herramientas gratuitas, como:

↘ www.softonic.com

↘ http://es.wikipedia.org/wiki/Portal:Software_libre

VI. **Explíqueles** los problemas de participar en comunicaciones con contenidos indeseables (charlas provocadoras, racistas, humillantes, extremistas, etc.) o que les hagan sentirse incómodos. Haga énfasis en la necesidad de **respetar reglas de buen comportamiento**, del mismo modo que en la interacción personal. Internet es un sistema de comunicación entre personas, por lo que debe ser

utilizado con precaución y con respeto hacia quien está al otro lado.

VII. **Preste atención a las amistades en la Red**, de la misma manera que se preocupa por las amistades presenciales. Una vez que se ha contactado con alguien, lo mejor será descubrir tanto como pueda sobre esa persona. El menor debe comprender que, aunque la persona con la que está chateando pueda parecer digna de confianza, en Internet uno nunca puede realmente saber quién se encuentra al otro lado, por lo que **se debe ser lo más precavido posible**.

VIII. **Establezca reglas familiares**, fáciles de cumplir, que se conviertan en rutinas desde el primer momento. Asegúrese de que las cumplen todos los integrantes de la unidad familiar. Demuéstrelo permitiendo al menor acompañarle en sus propias búsquedas en la Red. **Enséñele su manera de actuar** e invítele a emularla.

IX. **Vigile el tiempo de conexión** del menor a Internet para evitar que desatienda otras actividades. Controle las facturas telefónicas. Establezca presupuestos para "gastos en línea" y supervise que se cumplen. Haga comprobaciones periódicas sobre el uso que sus hijos hacen del ordenador. Sitúe los ordenadores en espacios compartidos, pero no agobie al menor con permanentes inspecciones u obligaciones disuasorias, pues probablemente cambiará el lugar de conexión a espacios fuera del hogar. En caso de necesidad, utilice herramientas que le ayuden a controlar el tiempo de conexión. En la página web Internet segura de la Agencia de Calidad de Internet (IQUA) puede encontrar un *"Listado de herramientas de control"*

➘ www.internetsegura.net Pestaña Recomendaciones

X. **Cree una cuenta de usuario limitada** para el acceso del menor al sistema operativo. Es muy conveniente crear un acceso personalizado a los ordenadores, a través de la opción de Creación de cuentas de usuario que ofrecen todos los sistemas operativos. Los menores deberán acceder a través de Internet con cuentas de usuario limitadas o restringidas, que no faciliten un acceso al ordenador en modo 'administrador'.

➘ http://windows.microsoft.com/es-XL/windows-vista/What-is-a-user-account

En la página web del Instituto Nacional de Tecnologías de la Comunicación puede encontrar una *"Guía de menores en Internet para padres y madres"*.

➘ www.inteco.es/extfrontinteco/img/File/intecocert/Proteccion/menores/guiapadresymadres.pdf

- **Predique con el ejemplo**
- **Hable con sus hijos**
- **Enseñe a sus hijos a no facilitar información personal**
- **Establezca reglas familiares**

Perspectiva legal

El concepto de "delito informático" es complejo. Una aproximación europea al problema es el *"Convenio sobre la ciberdelincuencia"* que aprobó el Consejo de Europa en el mes de noviembre del año 2001 y que está pendiente de ratificación por España.

➘ www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

En el ámbito legal existe, no obstante, un cuerpo legal creciente, fuera del ámbito penal, que pretende regular diversos aspectos de la Sociedad de la Información:

— **Ley de Atención y Protección a la Infancia y la Adolescencia** [BOPV 30-03-2005]

— **Ley de Propiedad Intelectual** [BOE 22-04-1996]

— **Ley Orgánica de Protección de Datos** [BOE 14-12-1999]

— **Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal** [BOE 25-06-1999]

— **Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico** [BOE 12-07-2002]

— **Ley General de Telecomunicaciones** [BOE 04-11-2003]

— **Ley de Firma Electrónica** [BOE 20-12-2003]

— **Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos** [BOE 23-06-2007].

— **Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones** [BOE 19-10-2007]

— **Ley de Medidas de Impulso de la Sociedad de la Información** [BOE 29-12-2007]

Si una persona cree que ha encontrado imágenes ilegales en Internet, puede denunciarlo a través de la web de la Asociación Internacional de Líneas Directas de Internet (INHOPE), que forma parte del *"Programa de Seguridad en Internet de la Comisión Europea"*.

➘ http://inhope.org/en/index.html

En caso de haber sido víctima de un fraude o ante cualquier indicio de actividad ilegal, se puede recurrir:

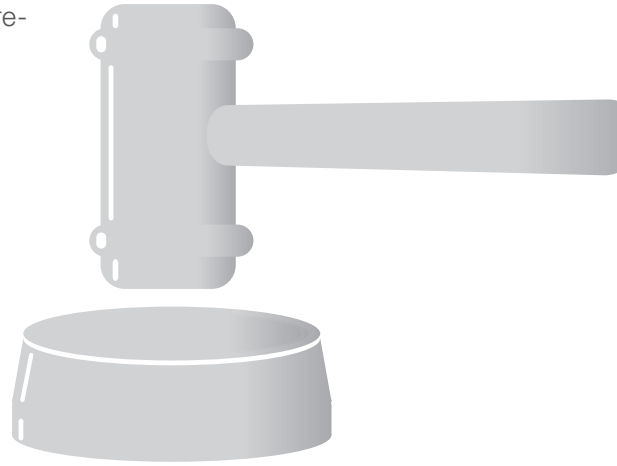
— a la **Ertzaintza**, que dispone de la Sección Central de Delitos en Tecnologías de la Información (SCDTI), con la que se puede contactar a través de su web www.ertzaintza.net (pestaña "servicios en la web"), en cualquiera de sus comisarías o mediante la dirección de correo electrónico delitosinformaticos@ertzaintza.net.

— al Grupo de Delitos Telemáticos (GDT) de la Unidad Central Operativa (UCO) de la **Guardia Civil** www.gdt.guardiacivil.es, que contiene mucha información interesante sobre el tema y permite descargar un formulario de denuncias www.gdt.guardiacivil.es/denuncias.php.

— a la Brigada de Investigación Tecnológica (BIT) del **Cuerpo Nacional de Policía** [CNP] en la página web www.policia.es o a través de las direcciones de correo electrónico

- **Fraudes en las telecomunicaciones**: delitos.telecomunicaciones@policia.es
- **Pornografía infantil**: denuncias.pornografia.infantil@policia.es
- **Fraudes en Internet**: fraudeInternet@policia.es
- **Virus, ataques, seguridad lógica**: seguridad.logica@policia.es
- **Antipiratería**: antipirateria@policia.es

Cabe destacar también el sistema de denuncias online del portal www.protegeles.com para temas específicos que atenten contra los derechos de los menores.



Glosario

"BLOG" o BITÁCORA: herramienta de comunicación muy novedosa que pone a disposición del internauta la posibilidad de introducir libremente contenidos en una página web y compartir conocimientos. Recopila cronológicamente los textos enviados por los autores, apareciendo primero el más reciente. Por lo general, los lectores pueden escribir sus comentarios, los autores responder a ellos y, de esa manera, generar un diálogo. Existen, incluso, espacios web de este tipo especialmente diseñados para los móviles y el acceso WAP, SMS y MMS para actualizar y consultar blogs.

CRIPTOGRAFÍA: tecnología que permite cifrar (escribir en clave) y descifrar información para permitir un intercambio de mensajes que sólo puedan ser leídos por las personas a las que van dirigidos y que posean los medios para descifrarlos.

DIRECCIÓN IP: número que identifica a cada ordenador conectado a Internet. Puede ser siempre el mismo número (IP fija) o modificarse, de manera automática, en el tiempo (IP dinámica). En un entorno doméstico, la utilización de una direccion IP dinámica es más segura.

FORO: aplicación web que permite recopilar, por escrito y de manera ordenada, las opiniones de todos los participantes sobre un tema en 'hilos de conversación'. A diferencia de las wikis, no se pueden modificar los aportes de otros miembros a menos que se tengan ciertos permisos especiales, como los asignados a moderadores o administradores.

HARDWARE: conjunto de componentes eléctricos, electrónicos, electromecánicos y mecánicos que integran la parte visible de un ordenador. Tiene gran capacidad de trabajo automatizado, pero necesita del software para poder interactuar con él.

IRC o "CHAT" (charla en tiempo real)**:** comunicación escrita, realizada de manera casi instantánea a través de Internet entre dos o más personas, ya sea de manera pública, a través de los llamados chats públicos (mediante los cuales cualquier usuario puede tener acceso a la conversación) o privados. Las tertulias se asocian a salas y canales donde coinciden varios usuarios interesados por los mismos temas. Los chats aportan un excelente servicio, pero pueden ser peligrosos si el menor contesta de manera inadecuada a comentarios durante el transcurso del intercambio. Fomentan el anonimato de los participantes a través de la creación de nicks (alias, sobrenombre, apodo) para identificarse.

"LA RED": por antonomasia se refiere a **Internet**, que en realidad es un conjunto de redes interconectadas, a través de las cuales se puede tener acceso a servicios especiales de gran interés en el mundo actual: navegación por páginas web, intercambio de mensajes de correo electrónico, conversaciones privadas o públicas en tiempo real, etc.

MENSAJERÍA INSTANTÁNEA: método de comunicación en línea similar al correo electrónico, aunque se realiza en tiempo real y ofrece funcionalidades añadidas (admite conversaciones de voz y visualización de imágenes, por ejemplo). Permite, sin problemas, las conversaciones en grupo y el intercambio de archivos. Es muy parecido al chat, pero para poder participar, obliga a incluir, además de un nick, el correo electrónico.

↘ Yahoo! messenger, Windows live messenger, Google talk

NAVEGADOR WEB: software que permite visualizar la información que contiene una página web. Es el medio de interacción con Internet más sencillo y más utilizado. El navegador interpreta el código en el que está escrita la página web y lo presenta en pantalla, permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la Red mediante enlaces o hipervínculos.

"PEER TO PEER" (P2P): Redes formadas por ordenadores interconectados entre sí, sin intermediarios, que permiten el intercambio directo de información y contenidos en cualquier formato. El principal interés de las redes 'entre iguales', es que permiten el intercambio de material en los dos sentidos, de tal forma que, a la vez que se descargan los ficheros, se ponen a disposición del resto de la red las partes del fichero que ya han sido descargadas.

"PODCASTING": distribución de contenidos de audio o vídeo mediante un sistema de redifusión de contenidos (programas de radio, charlas, conferencias, etc.) que permite descargar ficheros, previa suscripción, para escucharlos o verlos cuando se desee. En iTunes, el popular software de Apple Computer, por ejemplo, se ofrece el acceso a múltiples líneas de información en formato de audio para descargar al ordenador.

RED SOCIAL: aplicación web que permite conectar con amigos e incluso realizar nuevas amistades.

SISTEMA OPERATIVO: software diseñado para servir de enlace entre el ordenador (el hardware) y el usuario. Es el primer programa informático que se carga, automáticamente, al encender el ordenador.

SOFTWARE: conjunto de programas (aplicaciones informáticas) que hace posible el entendimiento con la máquina (sistema operativo) y la realización de tareas específicas: escribir un texto, ver una película, impedir la entrada de virus dañinos, etc.

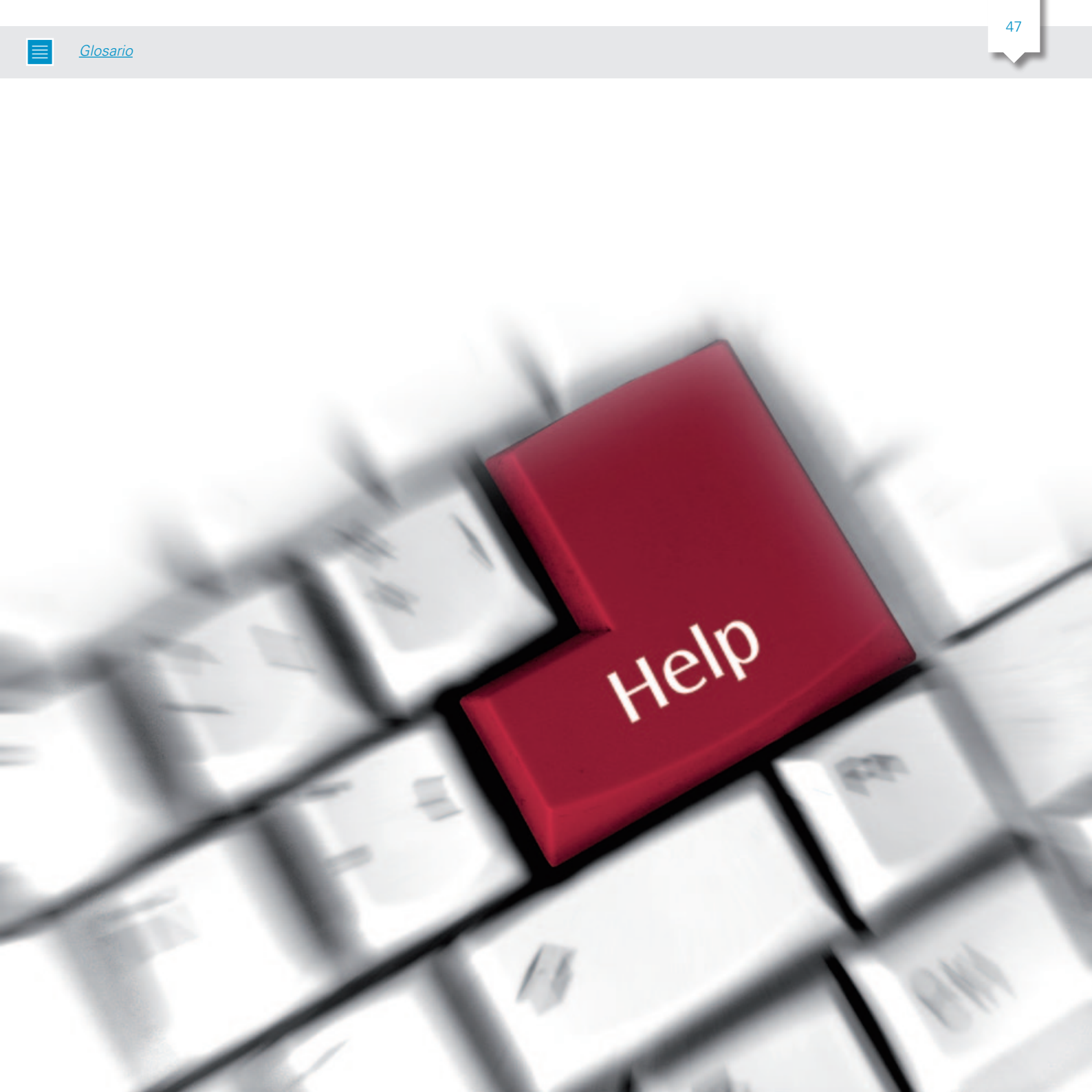
TELEFONÍA SOBRE IP: conjunto de nuevas funcionalidades de la telefonía, entre las que destaca la posibilidad de transmitir la "voz a través de Internet" (VoIP). Con este sistema se convierte la voz en paquetes de datos susceptibles de ser transmitidos a través de la Red, como los ficheros de vídeo, los documentos de texto o las fotografías. La razón de su éxito (Jingle o Skype) es que permite evitar los gastos de telefonía (principalmente de larga distancia) que genera la Red Pública Telefónica Conmutada tradicional. Las ventajas sobre la telefonía tradicional son enormes: es mucho más barato (gratuito si tenemos tarifa plana) y permite telefonear independientemente de la ubicación física del usuario. La Comisión del Mercado de las Telecomunicaciones lo ha diferenciado de la telefonía tradicional, por lo que no está afectado por las regulaciones sobre el servicio telefónico.

VIDEOCONFERENCIA: comunicación simultánea bidireccional de audio y vídeo, que permite mantener reuniones entre personas situadas en lugares alejados entre sí. También puede ofrecer servicios como el intercambio de informaciones gráficas o imágenes fijas y la transmisión de ficheros. Se basa en la posibilidad técnica de comprimir digitalmente los flujos de audio y vídeo en tiempo real.

WEB 2.O (web social)**:** evolución tecnológica de la comunicación en Internet consistente, básicamente, en la posibilidad de interactuar directamente con las páginas web, que pasan de ser un sistema unidireccional y estático a un sistema que permite el intercambio en las dos direcciones (leo el contenido, pero también lo genero). Las redes sociales, los blogs y las wikis pertenecen a esta nueva filosofía de comunicación.

↘ Flickr, Gmail, Delicious, Wikipedia, Plaxo, Googledocs, Wikispaces, Doodle

"WIKI": páginas web que pueden ser editadas por múltiples voluntarios a la vez, empleando exclusivamente el navegador web. Los participantes pueden crear, modificar o borrar un mismo texto que comparten.


Help

Fuentes de información: Páginas web de interés

Se consideran fuentes de información de gran interés, las siguientes:

- Instituto Nacional de Tecnologías de la Comunicación
  www.inteco.es
- Euskadi en la Sociedad de la Información
  www.euskadi.net/eeuskadi/new/es/index.html
- Ciberfamilias (Lugar de reunión para padres y educadores)
  www.ciberfamilias.com/index.htm
- Pantallas amigas
  www.pantallasamigas.net
- Chavales. Esta es nuestra web
  www.chaval.es
- Asociación de usuarios de Internet
  www.aui.es
- Instituto de la Juventud
  www.injuve.migualdad.es/injuve/portal.portal.action
- EDEX
  www.edex.es
- Oficina de seguridad del internauta
  www.osi.es/Seguridad_Internauta
- WIREDSAFETY (en inglés)
  www.wiredsafety.org
- Agencia Española de Protección de Datos
  www.agpd.es/portalweb/index-ides-idphp.php
- Ararteko. Defensoría del pueblo
  www.ararteko.net
- Defensor del menor de la Comunidad de Madrid
  www.defensordelmenor.org
- Defensor del menor de la Comunidad de Andalucía
  www.defensordelmenor-and.es
- Consejo superior de administración electrónica
  www.csae.map.es

- Asociación de internautas
  www.seguridadenlared.org/menores
- Oficina de atención al usuario de telecomunicaciones
  www.usuariosteleco.es
- Agencia de calidad de Internet (IQUA)
  www.Internetsegura.net.
- Asociación española de padres y madres internautas (AEMI)
  www.aempi.com
- Centro de alertas de seguridad de McAfee
  http://home.mcafee.com/advicecenter/default.aspx
- Información sobre seguridad de Panda Security
  www.pandasecurity.com/spain/homeusers/security-info
- Centro de protección de Bitdefender
  www.bitdefender.es/site/virusinfo
- PROTÉGELE
  www.protegeles.com
- Asociación Acción contra la pornografía infantil
  www.asociacion-acpi.org
- Proyecto CERES (CERrtificación ESpañola) de la Fábrica Nacional de Moneda y Timbre
  www.cert.fnmt.es
- Internet segura, de la Agencia de calidad de Internet (IQUA)
  www.iqua.net
- Código de autorregulación sobre contenidos televisivos e infancia
  www.tvinfancia.es/default.htm
- UNICEF
  www.unicef.org/spanish
- Juegos
  www.secukid.es
  www.navegacionsegura.es/home/triviral.html

Algunos lugares de aprendizaje

KZguneak

KZgunea es una red de centros de acceso y formación gratuita sobre Internet puesta en marcha por la colaboración del Gobierno Vasco con el Ayuntamiento de Vitoria-Gasteiz.

En estos KZgune va a encontrar:

— **Cursos básicos** de aprendizaje de Internet y de Administración electrónica.

— **Cursos temáticos** y **seminarios avanzados** para la utilización práctica de Internet: banca on line, viajes, compras, seguridad, familia, correo electrónico...

— **Cursos dirigidos a microempresas** para que adapten su gestión diaria al uso de las TICs.

— **Exámenes para la obtención del certificado** de competencias básicas en nuevas tecnologías (IT Txartela).

Los KZgune se hallan ubicados en los siguientes **Centros Cívicos**: Aldabe, Arriaga, El Pilar, Hegoalde, Ibaiondo , Iparralde y Lakua.

Para más información consultar la página web www.kzgunea.net

Saregune

Es un centro situado en el casco viejo de Vitoria-Gasteiz y financiado conjuntamente por el Gobierno Vasco y el Ayuntamiento de Vitoria-Gasteiz. En él puede utilizar los ordenadores de manera gratuita para **navegar** y **mirar el correo**, y también se imparten **cursos** para enseñar a la población a manejarse con todo tipo de aplicaciones informáticas. Están especializados en todo lo que tiene que ver con la Web 2.0. El equipo de personas que lo atiende habla varios idiomas y es totalmente intercultural. La finalidad del centro es hacer consciente a la población del barrio de la potencialidad de las nuevas tecnologías.

Está ubicado en Cantón de Sta. María 4, bajo, y su dirección electrónica es www.saregune.net

Internet Zuretzat

Con el objeto de impulsar la alfabetización digital de la ciudadanía, la iniciativa Internet Zuretzat, dependiente del Departamento de Educación, Universidades e Investigación del Gobierno Vasco, pone en marcha **acciones formativas dirigidas a los familiares del alumnado** de los centros escolares. Estos cursos se realizan en el propio centro escolar y son impartidos por especialistas. Para realizar cualquier consulta se puede acceder a la página web www.internetzuretzat.net o llamar al teléfono 945 01 61 49. Más información en formatec@kzgunea.net

Cursos de Formación

Son acciones formativas organizadas por el Departamento de Promoción Económica y Planificación Estratégica del Ayuntamiento de Vitoria-Gasteiz. Estas acciones están dirigidas a personas ocupadas y desempleadas interesadas en mejorar sus posibilidades de inserción en el mercado de trabajo, cambiar su perfil laboral o ampliar conocimientos en materias relacionadas con su actividad. Se ofertan dos tipos de cursos: presenciales y cursos e-learning (a distancia). Para más información, consulte la página web www.vitoria-gasteiz.org/formacion

Cursos de Introducción a la Informática. Montehermoso

El Centro Cultural Montehermoso Kulturunea ofrece **cursos de introducción a la informática** para grupos, asociaciones y colectivos. Utilizando la informática y las tecnologías de la comunicación como recursos, se elaborarán programas adecuados al alumnado, insistiendo en las áreas que más puedan interesarles: Internet, seguridad en la Red, iniciación al uso del ordenador, búsquedas de contenidos… Su objetivo es acercar las tecnologías de la información a la ciudadanía ajustando su conocimiento a sus necesidades reales. Los grupos son reducidos (máximo 12 personas) y la duración de los cursos se establece de acuerdo a los objetivos planteados por la persona responsable del grupo. Más información en el 945 16 18 59 o en www.montehermoso.net

Bibliografía

- AFTAB, P. *"Internet con los menores riesgos"*. ISBN: 84-9726-310-3. Edex. 2005
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *"Guía de seguridad de datos"*. NIPO: 052-08-003-6. 2008
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Recomendaciones a usuarios de internet"*. NIPO: 052-08-007-8. 2009.
- FARRAY, JI. *"Cultura y educación en la sociedad de la información"*. ISBN: 84-9745-027-2. Netbiblo. 2002
- ALMUZARA, C. *"Estudio práctico sobre la protección de datos de carácter personal"*. ISBN: 84-8406-582-0. Editorial Lex Nova. 1ª ed. 2005
- ASENSIO, G. *"Seguridad en internet"*. ISBN : 84-9763-293-1. Nowtilus ed. 2006
- GARCÍA SANZ, RM. *"El derecho de autor en internet"*. ISBN: 84-7879-939-7. Colex. ed constitución y leyes. 1ª ed. Madrid. 2005
- GRALLA, P. *"Cómo funciona internet"*. Anaya multimedia. Madrid. 1º ed. 2007
- OCDE - MAP. *"Directrices de la para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad*. NIPO: 326-04-035-2. 2004
- INTECO (INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN). *"Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres"*. Marzo 2009.
- JOYANES, L. *"Las redes sociales: de la mensajería instantánea a los weblogs"*. Sociedad y utopía: Revista de Ciencias Sociales, 24: 93-122 (2004)
- PROTÉGELES (CANOVAS, G). *"Cibercentros y seguridad infantil en internet"*. Noviembre 2002.
- PROTÉGELES (CANOVAS, G). *"Seguridad infantil y costumbres de los menores en el empleo de la telefonía móvil"*. Mayo 2005.
- PROTÉGELES (CANOVAS, G). *"Seguridad infantil y costumbres de los menores en internet"*. Noviembre 2002.
- PROTÉGELES (CANOVAS, G). *"Videojuegos, menores y responsabilidad de los padres"*. Diciembre 2005.
- WEBSENSE SECURITY LABS. *"State of internet security Q1-Q2"*. 2009