

Subvencionado por



Patrocinado por



En colaboración con



Agencia de Protección de Datos
de la Comunidad de Madrid



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos



**Proyecto CLI - PROMETEO
2008/09**

Manual Práctico de 15 a 17 años

Apoyado por el Ministerio de Educación y las Consejerías correspondientes de Andalucía, Catalunya, Euskadi, Extremadura y Madrid.

Equipo Directivo de la CLI:

Junta Directiva de la Asociación.

Equipo de Dirección del Proyecto CLI-PROMETEO:

Antoni Farriols, José Manuel Ferrer, José Carlos Vaquero.

Asesoría Jurídica:

Carlos Valero, Jordi Bacaria, Lola Albo, Ernesto Quílez.

Equipo Informático:

José Manuel Ferrer, Carlos Ramón Ferrer.

Colaboración especial en el diseño de viñetas:

M^º del Carmen Labarquilla.

Otras colaboraciones técnicas:

Javier García Álvarez

Manuales de Protección de Datos del Proyecto CLI-PROMETEO:

Manual de 9-11. Coordinación: Salustiano Asencio.

Manual de 12-14. Coordinación: Alberto Leal.

Manual de 15-17. Coordinación: Débora Caballero.

Maquetación:

Web y Media Diseñadores s.l.

Dirección del Manual:

Comisión de Libertades e Informática.

Impresión:

Centro Especial de Empleo Ponce de León.

Depósito Legal M-53404-2008

EDICIÓN PRIVADA

Copyright © 2008

Queda prohibido, la reproducción total o parcial de la obra sin permiso escrito por parte de la Comisión de Libertades e Informática.

La Comisión de Libertades e Informática (CLI) es una Asociación que trabaja activamente para la defensa del Derecho Fundamental a la Protección de Datos de Carácter Personal con el firme objetivo de concienciar a las Personas, Empresas y Administraciones de su importancia.

Forman parte de la CLI, además de personas interesadas, las siguientes organizaciones:

AI: Asociación de Internautas.

ALI: Asociación de Ingenieros e Ingenieros Técnicos en Informática.

APDHE: Asociación Pro Derechos Humanos de España.

FADSP: Federación de Asociaciones de Defensa de la Sanidad Pública.

UGT: Unión General de Trabajadores.

Proyecto CLI PROMETEO 2008/09

La CLI desarrolla el proyecto CLI-PROMETEO que se dirige a los niños y adolescentes para fomentar desde la escuela el uso de las tecnologías de la información y, al mismo tiempo, concienciar sobre la protección de datos de carácter personal.

Índice

Título	Contenido	Objetivos	Actividades	Pág.
Introducción.	Presentación del Manual.	Motivación.		2
Capítulo 1. El buen uso de Internet y del teléfono móvil.	Actividades que pueden hacerse y el beneficio que nos aportan.	Valorar las posibilidades y ventajas que tienen ambas tecnologías.	Propuesta de actuaciones. Test de adicción.	3
Capítulo 2. El mal uso de Internet: problemas que puedo tener.	La Protección de datos personales y su privacidad: aspectos técnicos.	Conocer de los procedimientos técnicos para favorecer nuestra intimidad.	Eliminación de historiales, "cookies", archivos, contraseñas automáticas.	6
Capítulo 3. 3.1. Compartir archivos: "El ataque de los virus".	Antivirus, bloqueadores "pop ups", cortafuegos. Evitar correos no deseados ("spam").	Conocer las posibles invasiones de nuestra privacidad y los medios para evitarlas.	Modificación de archivos: alteración de imágenes reales.	8
3.2. Encuentros con personas desconocidas: a través de la Red ("en línea") y reales ("citas a ciegas").	Encuentros con otras personas a través de la Red: los <i>chats</i> .	Identificar los peligros de contactar con personas desconocidas.	Análisis de imágenes con doble personalidad: la realidad engaña.	13
3.3. Acoso en la red: Cyberbulling.	- ¿Qué es? - ¿Dónde se da? - ¿Cómo puedo reconocerlo? Un caso real de "ciberbullyng".	Reconocer los casos de acoso y saber actuar contra ellos. Algunos consejos.	Debate: modelos de personalidad.	15
3.4. Fraudes por Internet: Técnica "phishing", compras por internet.	La Identidad Electrónica.	Tomar conciencia de las precauciones necesarias para protegerla.	"Phishing": estudio caso real.	18
Capítulo 4. El Correo Electrónico.	Configuración y precauciones.	Aprender a configurarse una cuenta de correo electrónico con la garantía necesaria.	Configuración de una cuenta de correo electrónico.	22
Capítulo 5. Nuestros derechos: (protección de datos personales).	Conocer los derechos que nos amparan. Derecho de acceso, rectificación, cancelación y oposición de datos personales. Modelos de denuncia.	Conocer los derechos sobre protección de datos personales de una manera activa.	Ejercicio práctico sobre un caso de denuncia a la Agencia de Protección de Datos.	24
Capítulo 6. Resumen y Conclusiones.	Consejos para padres, madres, educadores, educadoras y tutores legales.			31

Introducción

¿DE QUE VA ESTE MANUAL?

Internet, el teléfono móvil, el MP3, el MP4 o lo que formalmente se llaman las Tecnologías de la Información, (TI), son habituales en la vida de jóvenes como tu. Después de un estudio que hemos realizado con más de 8000 estudiantes de edades comprendidas entre los 9 y los 17 años, hemos comprobado que dedicáis gran parte de vuestro tiempo a ellas. Un 37% de vosotros habéis afirmado utilizar Internet todos los días. Pero, ¿sabes todo a cerca de las Tecnologías de la Información? ¿Haces un buen uso de ellas? ¿Sabes todos los peligros a los que estas expuesto cuando te conectas a Internet? Este Manual pretende darte las respuestas a estas preguntas. Queremos ampliar tu información y conocimiento sobre estas tecnologías, alertarte de los posibles peligros y darte las armas para defenderte. Además con este Manual deseamos concienciaros sobre la importancia de la protección de los Datos de Carácter Personal (tu nombre, apellidos, teléfono, dirección, DNI, tus fotos...). Son nuestra intimidad y debemos protegerla. Te informaremos sobre tus derechos y deberes en esta materia para que sepas hacer una buena utilización de tus datos.

¿CÓMO OS LO VAMOS A CONTAR?

El Manual esta dividido en varios capítulos con la siguiente estructura:

- Contenido: Aquí os damos toda la información que necesitáis sobre el tema. Os sorprenderá la cantidad de cosas que no sabemos sobre las Tecnologías de la Información.
- Consejos: En este apartado encontraras recomendaciones y consejos prácticos y técnicos para hacer un buen uso de las tecnologías.
- Actividad: Al final de cada capítulo te ofrecemos un pequeño juego para poner en práctica lo aprendido.

Este manual esta pensado para que te animes a leerlo y realizar las actividades con tus padres, tutores y profesores. Aprenderéis juntos muchas cosas y te podrán explicar todo aquello que no entiendas bien.

Al final del Manual también se incluye un apartado de consejos para padres, madres, educadores, educadoras y tutores legales.

Capítulo 1

EL BUEN USO DEL ORDENADOR (INTERNET) Y DEL TELÉFONO MÓVIL

En este capítulo queremos darte una lista de actividades que puedes hacer con Internet y el teléfono móvil y los beneficios que te pueden aportar. También te daremos una serie de consejos para hacer un buen uso de estas tecnologías y por último te podremos a prueba: ¿eres un adicto a las Tecnologías de la Información? Compruébalo haciendo el test que te proponemos al final de capítulo.

¿QUE ACTIVIDADES PODEMOS HACER CON INTERNET Y EL TELÉFONO MÓVIL?

- **Informarnos y aprender.** Internet es una enciclopedia gigante. Basta introducir en cualquier buscador de Internet los conceptos que queremos saber y obtendremos miles de resultados en nuestra búsqueda. Acontecimientos históricos, curiosidades, recetas, trucos, la biografía de nuestro artista favorito... la Red nos proporciona una cantidad de información infinita que nos ayuda a seguir aprendiendo.
- **Comunicarnos.** Telegrama, carta, *christmas* navideños... ¿Suenan antiguos? Pues hasta hace poco no había otra manera de comunicarse. Ahora gracias a Internet y el teléfono móvil podemos hablar con nuestros amigos y familiares en cualquier momento, da igual en que parte del mundo nos encontremos. Éste es sin duda uno de los mayores beneficios de las Tecnologías de la Información. Además, el anonimato que da Internet nos ayuda a perder la timidez y relacionarnos con mayor facilidad. Podemos conocer gente de todas las partes del planeta y con ello conocer nuevas culturas y costumbres que también nos ayudarán a ser más tolerantes. Los “*blogs*” o foros permiten expresar nuestras opiniones sobre temas que nos gustan. En definitiva nos ayuda a relacionarnos y socializarnos.
- **Divertirnos.** En la Red y en el teléfono móvil encontramos muchísimos juegos para entretenernos con nuestros amigos o solos. Nos ayudan a mejorar nuestras habilidades, poner a prueba nuestro ingenio y sobre todo a ¡divertirnos!
- **Viajar.** Además de poder tramitar nuestras vacaciones cómodamente desde casa, hay programas geniales que nos permiten ir a cualquier parte del mundo desde nuestro ordenador. Las pirámides de Egipto, la Estatua de la Libertad o la Torre Eiffel ¡sin movernos de la silla!

CONSEJOS PARA HACER UN BUEN USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Un 25,6% de vosotros habéis contestado que utilizáis Internet todos los días. ¿Pero se utiliza de manera adecuada? Te proponemos una serie de consejos y de actividades para que hagas un buen uso de las Tecnologías de la Información.

- 1. Tiempo.** Es importante que controles el tiempo que pasas frente al ordenador o al teléfono móvil. Son herramientas muy útiles pero como todo, hay que utilizarlas con moderación. Entre las clases, los deberes y demás actividades extraescolares te queda muy poco tiempo de ocio. No olvides pasar tiempo con tu familia y amigos, leer libros o escuchar tu música preferida. Así que echa las cuentas y organízate bien. ¡Hay tiempo para todo!
- 2. Información.** ¡Cuidado! en Internet hay mucha información fiable y cierta pero también hay mucha falsa. Antes de creerte todo lo que la Red te dice, pregunta a un adulto o contrasta la información con un libro que tengas a mano.
- 3. Diversión.** ¡Huye de aquellos juegos que tengan cualquier tipo de violencia o puedan traerte problemas!
- 4. Blogs, foros, chats...** Se siempre respetuoso y tolerante con las opiniones de los demás. No insultes ni amenaces o hagas algo que pueda causar daño a otros. Diviértete y ¡pasa de los malos rollos!
- 5. Compras.** Si has visto algo que te gusta en Internet consúltalo con tus padres o un adulto responsable. No te fíes de las ofertas ni de las promesas milagrosas ¡no existen!

ACTIVIDAD. ¿ERES UN ADICTO A LAS TECNOLOGÍAS DE LA INFORMACIÓN?

El 75,4% de vosotros habéis afirmado que siempre que os conectáis a Internet pasáis mas tiempo del que teníais planeado, pero ¿sabes si estas enganchado a ellas? Averígualo con el *test* que te proponemos. ¿Cuál de las respuestas sería la más parecida a la tuya?

- ¿Cuántas horas al día dedicas a Internet?:
 - A.** Menos de 1 hora. Hago muchas actividades y no tengo apenas tiempo para Internet.
 - B.** Entre 2-3 horas. Me gusta dedicar bastante tiempo de ocio, a conectarme para hablar con amigos y también para buscar información para clase.
 - C.** Más de 4 horas diarias. Casi siempre estoy delante del ordenador, jugando, hablando, buscando información que me interesa....
- ¿Cuántos "sms" sueles enviar con el teléfono móvil a amigos y familiares a lo largo de la semana?:
 - A.** Uno o dos como mucho. Solo envío sms para cosas importantes o momentos especiales.
 - B.** Entre 3 y 6 sms. Suelo enviar algún mensajito y contestar a los que me envían.
 - C.** Más de 7 mensajes a la semana. Pierdo la cuenta de los sms que envío. Aunque vea a mis amigos todos los días, nos enviamos mensajes continuamente. ¡Me encanta!

3. ¿Cómo te sentirías si durante una semana desapareciera Internet y el teléfono móvil?:
- A. Puedo aguantar una semana y más tiempo sin Internet y el teléfono móvil.
 - B. Me sentiría extraño/a, pero ¡una semana pasa enseguida!
 - C. ¡Me daría algo! ¡Que aburrimiento! ¿Cómo me comunico con mis amigos? Sería muy duro...
4. Cuando NO estas conectado o conectada a Internet o el teléfono móvil, casi siempre...
- A. Estoy haciendo deporte, hablando con mi familia, estudiando, leyendo...
 - B. Estoy viendo la tele o estudiando.
 - C. Estoy pensando en el momento de conectarme, mirar si me han escrito un correo o me han firmado en mi *blog*, ¡estoy deseando navegar!
5. Cuando estas conectado a Internet o usando el teléfono móvil, casi siempre...
- A. Estoy el tiempo justo para hacer lo que necesito y si mis padres me llaman o tengo otras cosas que hacer lo dejo enseguida.
 - B. Me divierto y me gusta navegar un rato, negocio con mis padres el tiempo que puedo usarlo y lo compagino con otras actividades.
 - C. Es el mejor momento del día, disfruto mientras estoy en Internet o utilizando el teléfono móvil. Si alguien me interrumpe o me dice que deje de usarlo... ¡me enfado muchísimo!

SOLUCIONES

- **Mayoría de respuestas A: “Ni fú ni fa”.** Eres una persona práctica y crees que las Tecnologías de la Información son sobre todo herramientas que nos hacen más fácil la vida, pero podrías perfectamente vivir sin ellas. Conoces mil formas alternativas para hacer lo que harías con Internet o el teléfono móvil.
- **Mayoría de respuestas B: “El justo medio”.** *“En el justo medio está la virtud”* esta frase te define. Utilizas las Tecnologías de la Información de forma moderada y no dejas de hacer otras cosas como estudiar o estar con tu familia. ¡Muy bien! Las Tecnologías de la Información son muy útiles y prácticas pero no debemos dejar que se conviertan en una obsesión. ¡Sigue así!
- **Mayoría de respuestas C: “¡Totalmente enganchado!”.** Debes tener cuidado. No debes de dar prioridad en tu vida a Internet o el teléfono móvil. Mientras estas conectado estas dejando de lado la relación con tu familia o los estudios, y esto puede traerte consecuencias graves. Debes Reducir el uso que haces de estas tecnologías y utilizar ese tiempo para hacer deporte, hablar con tus padres, leer o estudiar.

Capítulo 2

EL MAL USO DE INTERNET: PROBLEMAS QUE PUEDO TENER

LA PROTECCIÓN DE NUESTRA INTIMIDAD: ALGUNOS CONSEJOS TÉCNICOS

Como ya hemos visto, Internet tiene muchísimas ventajas pero también está lleno de peligros y riesgos. Cuando salimos a la calle estamos atentos de que no nos quiten o se nos pierdan nuestras carteras o monederos donde llevamos toda nuestra documentación, todos esos datos que nos identifican, como el DNI, nuestras fotos, esa entrada de tu concierto favorito, en definitiva protegemos nuestra intimidad. ¿Por qué no hacemos lo mismo en Internet? Los datos del estudio que hemos realizado revelan que el 45,8% de vosotros sabéis si vuestro ordenador esta protegido por antivirus o antiespías. En la tranquilidad de nuestras habitaciones nos creemos a salvo del mundo, pero en el momento en el que nuestro ordenador se conecta a la telaraña mundial, que es Internet, estamos totalmente desprotegidos, expuestos a millones de riesgos que nos traerán consecuencias graves si no tomamos las medidas oportunas.

TU ORDENADOR: “UN ROBOT CLASIFICADOR”

Tu ordenador lo apunta todo, guarda todas las páginas *web* que has visitado, las películas, o la música que has descargado, las búsquedas que has hecho en Google o Yahoo, tu correo electrónico, los datos que has rellenado en algún formulario de inscripción, tus contraseñas, tus conversaciones de Programa de mensajería instantánea..., todo. Nunca olvida nada a no ser que tú se lo digas y lo peor de todo: cualquiera que tenga unos conocimientos mínimos de informática podrá saberlo todo sobre ti y utilizar tus datos de forma inadecuada. Pero vamos por partes; tu ordenador lo tiene todo clasificado y guardado en distintos lugares, antes de darte algunos consejos informáticos para estar protegido de los ladrones de datos veamos que se guarda en cada sitio:

- **Historial:** Aquí se almacenan la gran mayoría de las páginas *web* que has visitado. Son algunas de las “huellas” que vas dejando por la Red, así que conviene borrarlas para que nadie las siga.
- **Cookies (huellas):** Son archivos que contienen la dirección de la página que acabas de visitar. Algunas son temporales, pero otras pueden permanecer en tu ordenador durante años. Los espías pueden hacer un seguimiento de las páginas *web* que has visitado y acceder a tus archivos, de esta manera sabrán tus gustos y preferencias; con ello crean listas de posibles clientes que luego venden a empresas comerciales. Es importante que cada cierto tiempo las elimines.
- **Archivos:** Las imágenes y contenidos de las páginas *web* que has visitado se almacenan en nuestro ordenador para así acelerar la carga de la página cuando vuelvas a visitarla. Pero a partir de estos archivos se puede acceder a los datos que

has escrito en las páginas *web* que has visitado. Al borrar estos archivos tardará un poco mas en cargarse la página pero estarás protegido de los espías y ladrones informáticos.

Ahora que ya sabes que guarda tu ordenador y donde lo guarda, te aconsejamos que cada cierto tiempo, al menos cada semana dediques cinco minutos a borrar todos estos datos que se quedan en tu ordenador y evitar que los ladrones de datos invadan tu intimidad. ¿Cómo? Sigue leyendo y podrás estar protegido en cuatro pasos sencillísimos. Si posees la última versión de Internet Explorer v.7 es muy fácil, solo tienes que abrir una página de Internet y seleccionar Herramientas > eliminar el historial de exploración y te aparecerá un cuadro como este:

En esta ventana puedes eliminar el historial, las *cookies*, los archivos y las contraseñas simplemente dando a eliminar en cada opción y después confirmando tu decisión.

Si tienes Windows Xp y la versión anterior de Internet Explorer, los pasos también son muy sencillos. Igualmente abre una página de Internet después selecciona Herramientas > Opciones de Internet, haz clic en la pestaña General y elimina el historial, las *cookies* o los archivos, después pulsa aceptar.

Para borrar tu historial con Firefox 7.x haz lo siguiente: Editar > Preferencias, haz clic en Navigator, selecciona Historial y haz clic en Borrar historial. Con las *cookies* es un paso parecido, para eliminarlas selecciona Herramientas > gestor de *cookies* > gestionar *cookies* almacenados y en el cuadro que te aparece podrás seleccionar las copias que quieres borrar o hacer clic en él botón Eliminar todos los *cookies* y Aceptar. Para eliminar los archivos con Firefox 7.x selecciona Editar> Preferencias y haz doble clic en Avanzadas. Selecciona caché y haz clic en el botón Vaciar Caché de disco.



Capítulo 3

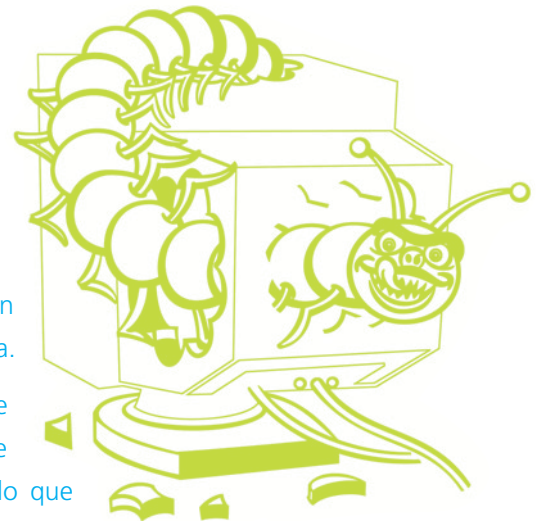
3.1. COMPARTIR ARCHIVOS: “EL ATAQUE DE LOS VIRUS”

Ahora ya sabes más sobre tu ordenador, pero todavía no estas a salvo y tienes una nueva misión: no dejar que se convierta en un zombi manejado por extraños y protegerle de todos los peligros que existen en Internet. ¿Todavía no sabes los nombres de estos atacantes? A continuación te damos toda la información que necesitas sobre estos malhechores y los escudos para estar protegidos:

VIRUS

Hay una plaga de ellos en Internet y aunque te sorprenda saberlo, también en el teléfono móvil. Son programas informáticos que se propagan con muchísima facilidad y son muy dañinos. A veces se manifiestan y sabemos que están ahí pero otras muchas se esconden en archivos o programas que nos descargamos pudiendo con ello destruir los datos de tu ordenador, sustraer tus datos personales, tus fotos... En definitiva manejando tu ordenador por ti, convirtiéndolo en un zombi. Hay una gran variedad de estos virus, te damos algunos nombres para que estés alerta:

- **Stealth:** es uno de los peores ya que está en tu ordenador sin que te des cuenta, infectando todo lo que encuentra. Incluso vacila al antivirus modificando los datos para no ser detectado.
- **Parásito:** puede ir oculto en esos programitas en lo que nos dice “ejecutar”, te suena ¿verdad?
- **Gusano:** Se propaga con muchísima facilidad ya que se transporta de un ordenador a otro por medio del correo electrónico o la mensajería instantánea.
- **Caballo de Troya o troyano:** Se esconden detrás de algunos programas que nos descargamos creyendo que son inofensivos. Una vez descargado ese programa, el troyano se introduce en tu ordenador y puede hacer todo lo que quiera con él.
- **Cabir:** El virus del teléfono móvil. Viaja a través del *bluetooth*. Si entra en tu teléfono móvil podría sustraerte tus mensajes de texto o contactos, seguir tus movimientos o escuchar tus conversaciones. Ten cuidado al utilizar el bluetooth y no aceptes archivos de gente que no conozcas.



ESCUDOS PARA DEFENDERTE DE LOS VIRUS

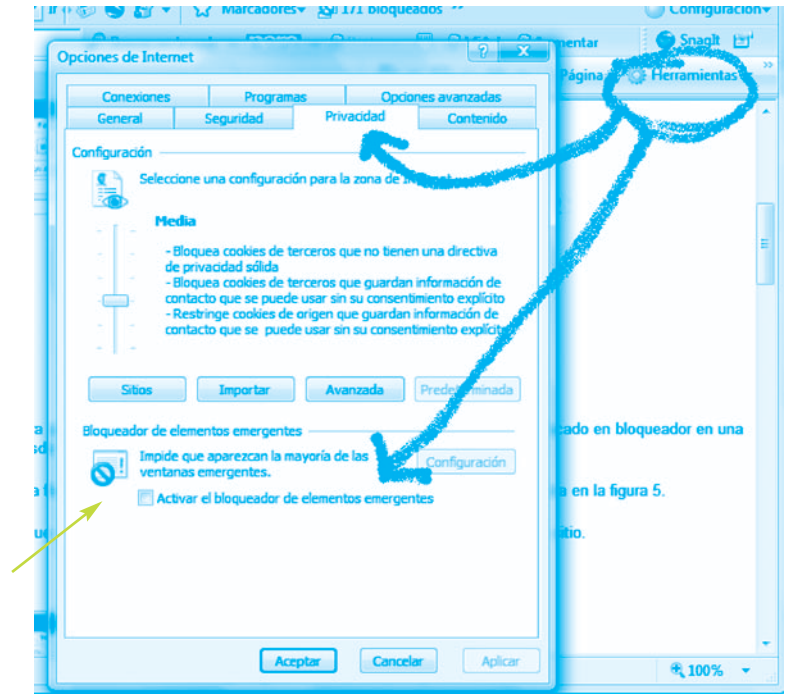
- **Antivirus:** Es importantísimo que tengas instalado en tu ordenador un antivirus. Estos paquetes son algo parecido a nuestros guardaespaldas; se mantienen siempre alerta de posibles programas dañinos que puedan colarse en tu ordenador y hacer uso de los datos y archivos que tienes guardados. Por ello te recomendamos que para estar más seguro siempre tengas instalado un antivirus. Además preocúpate de actualizarlo cada cierto tiempo, estos paquetes tienen una caducidad y en el momento que se pase la fecha volverás a estar en riesgo.
- **Cortafuegos:** O *firewall* en inglés. Este tipo de programas son el portero de tu ordenador; nadie pasará sin que él les dé permiso de hacerlo. Te avisa de posibles programas que quieren hacer algo malo en tu ordenador y te hacen invisible ante los posibles ladrones en busca de víctimas. En algunas páginas *web* encontraras descargas gratuitas de cortafuegos y es recomendable que te hagas con uno de estos “porteros”.

RECUERDA

Consulta siempre con tus padres o tutores a la hora de borrar cualquier documento, cookie o historial del ordenador para evitar males mayores, haz lo mismo cuando instales un antivirus o cortafuegos.

POP-UPS O VENTANAS EMERGENTES

Otro de los riesgos de Internet son las dichas ventanitas de publicidad que aparecen delante de alguna página *Web* que intentamos leer. No nos dejan navegar tranquilamente, ralentizan nuestra conexión y nos llevan a otras páginas que no queremos visitar mientras intentamos cerrarlas desesperadamente. Estas son las llamadas *pop-ups*. Si quieres acabar de una vez con estas molestas ventanitas sigue los siguientes pasos: abre una página *web*, ve a herramientas > opciones de Internet > ve a la pestaña de privacidad y activa la casilla de bloqueador de elementos emergentes. Algunas versiones de Internet Explorer incluyen esta opción directamente en Herramientas.



- También puedes hacerte con un programa bloqueador de *pop-ups*. Revisan periódicamente los programas que se han instalado en tu ordenador sin tu conocimiento y que te agobian con las ventanas emergentes o *pop-ups*. ¡Así estarás totalmente seguro de que no volverán a molestarte!

CORREO BASURA O SPAM

Como su propio nombre indica son basura y por tanto no debes abrirlos nunca.

Normalmente son correos con fines comerciales pero muchas otras veces esconden virus, troyanos o gusanos que pueden dañar nuestro ordenador, sustraernos datos o meternos en serios problemas.

- ¿Cómo identificarlos? Algunos servidores de correo electrónico nos avisan de que el mensaje puede ser un posible spam, pero en la mayoría de las ocasiones no. Normalmente son de personas que no conoces y con asuntos del tipo:
 - *"Gana millones con el mínimo esfuerzo"*
 - *"El amor de tu vida te está esperando"*
 - *"¿Problemas? Desde hoy en adelante ya no"*

¡Pero no te fíes! Existe la posibilidad de que recibas un spam desde el correo de un amigo o conocido, de tu banco, de alguna institución que conozcas, incluso desde tu propia dirección electrónica, informándote de que tu mensaje no ha llegado al destinatario. En estos casos los mensajes vienen con un archivo adjunto; ¡no lo abras! Sigue la segunda regla de oro de la informática: "ante la duda, borra".

Los *spammers* (gente que envía correo basura) se aprovechan de nuestra curiosidad o del deseo de solucionar nuestros problemas con la intención de meternos un virus y con ello poder controlar nuestro ordenador convirtiéndolo en un *zombie*. Te recomendamos que estés siempre alerta y no te fíes de ningún correo antes de contrastar que vienen de un lugar fiable.

- ¿Cómo llegan hasta mi correo? Hay diversas formas de que los *spammers* se hagan con tu dirección de correo.
 - Si incluiste tu dirección al participar en un foro o al registrarte en una página *web*.



- Puede que, al apuntarte a una página, hayas aceptado recibir correo basura sin ni siquiera estar de acuerdo.
- Es posible que algún amigo haya incluido tu dirección en una de esas páginas *web* que te piden que lo reenvíes a otros amigos.
- Te han podido sustraer la dirección de bases de datos de empresas o instituciones privadas.
- Quizás hayas sido víctima de un ataque de los *spammers* que se dedican a crear direcciones de correo al azar.
- ¿Cómo puedo deshacerme del correo basura? Desgraciadamente no hay forma de deshacernos de estos molestos correos, pero si podemos darte una serie de consejos prácticos para evitarlos.
 - Crea una nueva cuenta de correo electrónico si los *spam* te invaden continuamente.
 - Hazte con otra cuenta secundaria que utilices para registrarte en páginas *web* o en foros.
 - Ponle un nombre complicado a tu cuenta, que incluya números, guiones... así te harás mas resistente a los programas de búsqueda automática de direcciones, por ejemplo: *nuevas467tecnologías9_@protegete.com*
 - No te registres ni des tus datos en aquellas páginas que puedan poner en riesgo tu seguridad.

LOS 10 MANDAMIENTOS DEL GUERRERO INFORMÁTICO

1. Instalaré y actualizaré mi antivirus y cortafuegos.
2. No descargaré ni ejecutaré archivos adjuntos sin antes verificar que el remitente es de confianza.
3. No me registraré ni daré mis datos en páginas inseguras.
4. No me descargaré programas de procedencia desconocida. Podrían estar infectados y traer un virus a mi ordenador.
5. Ante la duda... ¡borraré! Cualquier correo que me haga desconfiar, lo borraré inmediatamente.
6. No mandaré ni colgaré mis fotos. Estas podrían ser usadas por otras personas violando con ello mi intimidad.
7. No me dejaré engañar ni seducir por correos que me prometan milagros.
8. Seré cuidadoso a la hora de compartir mi *pen drive (memoria USB)* y pasaré el antivirus siempre. Incluso nuestros amigos podrían contagiarnos con un virus que tengan en su ordenador al compartir estas herramientas.
9. No abriré ni mandaré mensajes cadena. Sólo se trata de técnicas utilizadas por los piratas informáticos para recolectar más y más direcciones y hacer de las suyas.
10. No haré nada que pudiera causar alguno de estos problemas a otras personas.

MODIFICACIÓN DE ARCHIVOS: ALTERACIÓN DE IMÁGENES REALES

¿POR QUE NO DEBES COLGAR TUS FOTOS EN INTERNET?

Si cuelgas tus fotos en Internet cualquiera puede acceder a ellas y manipularlas a su antojo, ridiculizándote o metiéndote en problemas. Mira lo que le pasó a este pobre chico.

* Esta es la foto original que colgó en Internet



* Esto es lo que hicieron con ella...

Fuente: www.youtube.com

ACTIVIDAD. ADIVINA EL FINAL DE LA HISTORIA

Te proponemos un juego: adivina el final de esta historia basada en un hecho real. Lee atentamente y elige uno de los tres posibles finales. No hagas trampas y ¡no leas la solución hasta el final!

Karl Schofield, inglés, de 39 años e ingeniero de telecomunicaciones, es detenido y arrestado por un delito de pornografía infantil. La policía ha encontrado en su ordenador 14 fotos pornográficas de menores. Se enfrenta a una pena de 10 años de cárcel por cada foto encontrada, es decir, 140 años detrás de las rejas.

¿Cuál crees que es el final de la historia?

Opción A: Karl es condenado a prisión, si han encontrado esas fotos en su ordenador es porque él se las ha descargado, no hay otra manera de que el las tuviera, así que ¡a la cárcel!

Opción B: Este hombre es condenado e ingresa en prisión, pero al cabo de algunos años uno de sus mejores amigos confiesa que fue él mismo el que metió las fotos en el ordenador de Karl, como venganza por un antiguo conflicto que tuvieron.

Opción C: Karl es inocente y no ingresa en prisión. Sus abogados pueden demostrar que esas fotos pornográficas fueron colocadas en su ordenador por un Caballo de Troya.

SOLUCIÓN

¿Has elegido la última opción? ¡Pues has acertado! Karl Schofield era totalmente inocente. Jamás se había descargado esas fotos y fue víctima de los piratas informáticos. Sus abogados consiguieron demostrar que se había instalado en su ordenador

un caballo de Troya desde donde se habían descargado esas fotos sin el conocimiento del dueño, por medio de su correo electrónico o al aceptar descargar otro archivo. Karl consiguió salir de esta, pero perdió su trabajo y pasó dos años horribles hasta que se supo la verdad. Así que tómatelo en serio y ¡protégete cuando estés conectado a la Red!

(Caso real extraído de la noticia: "Trojan horse defence results in child porn acquittal". Fuente: <http://www.out-law.com>. 25/04/2003).

3.2. ENCUENTROS CON PERSONAS DESCONOCIDAS: A TRAVÉS DE LA RED ("EN LÍNEA") Y REALES ("CITAS A CIEGAS")

En el estudio que hemos realizado, observamos que uno de los mayores usos que hacéis de Internet y el teléfono móvil es el contacto con otras personas a través de los *chats*, mensajes de teléfono móvil o mensajería instantánea, el 65,7% de vosotros afirmáis que utilizáis los *chats* para conocer gente nueva sumado al 69,5% que lo hace mandando mensajes cortos de teléfono móvil. Por eso queremos que sepáis los beneficios y los riesgos que conlleva entablar relaciones con personas desconocidas.

ENCUENTROS CON OTRAS PERSONAS A TRAVÉS DE LA RED: LOS CHATS

El mundo ha cambiado y las formas de relacionarse también. Antes nuestros amigos eran los que hacíamos en el colegio, en el instituto, en la discoteca o en nuestro lugar de vacaciones pero ahora podemos tener amigos en Argentina sin haber salido de nuestra habitación. Los *Chats* y comunidades virtuales definidos como conversaciones *on line* en tiempo real que se establecen entre dos o mas personas, son utilizados por gente de todas las edades y condiciones sociales y es que son muchos los beneficios que aportan:

- Estar acompañado siempre que quieras. Basta con ponerte un apodo o nick e ingresar en un *Chat* para estar conectado con millones de personas de todo el mundo.
- Enriquecer tu conocimiento de otras culturas y costumbres lo que te hará ser mas tolerante con las personas que sean diferentes.
- Gracias al anonimato que proporcionan los *Chats* vencemos nuestra timidez y complejos así nos será mucho más fácil entablar relaciones con otras personas.



IDENTIFICAR LOS PELIGROS DE CONTACTAR CON PERSONAS DESCONOCIDAS Y SABER ACTUAR

No todas las personas tienen buenas intenciones en Internet así que ten mucho cuidado y ¡no te fíes!

- Las personas con las que charlas por Internet pueden mentirte en su edad, su aspecto físico o su profesión. Incluso la foto que te manden puede no ser real. ¡No confíes!
- Algunas de estas personas pueden ser mucho mayores que tú y con malas intenciones. El 95% de los pederastas, (mayores de edad que abusan sexualmente de menores), conocen a sus víctimas a través de los *Chat*.
- En Internet es muy fácil mentir y disimular ser otro tipo de persona. Normalmente te tratarán con excesiva amabilidad, te echarán piropos incluso cuando no te han visto, te prometerán llevarte a sitios que tus padres no te dejan como un concierto o una discoteca... No te creas todo lo que te dicen.
- La mayoría te pedirá verte por la cámara *web*, incluso te rechazarán si no lo haces. Intentarán convencerte de que hagas lo que quieren ver. No te dejes convencer y no aceptes ninguna videoconferencia con extraños.
- Es muy normal que te pidan fotos o datos personales como tu dirección o zona donde vives. Nunca envíes tus fotos ni des tus datos personales a nadie.
- No aceptes archivos de personas que conoces del *Chat* podrían incluir alguno de los virus de los que te hemos hablado y sustraerte tus fotos y datos personales. Incluso las canciones o las fotos que te envían pueden ser peligrosas.
- No quedes con extraños que conozcas en la Red. La gran mayoría de las veces, es de tipo de citas acaban en fracaso. En los casos más leves la persona no es físicamente como decía ser, pero existe la posibilidad de que sea un depravado e intente abusar de ti.
- Habla con tus padres o tutores de las relaciones que estableces por Internet. Ellos siempre mirarán por tu bien y te podrán orientar mejor sobre la clase de persona que hemos conocido.
- Si te saltas todos estos consejos y decides quedarte con una de estas personas que conociste en Internet, ¡nunca vayas sólo/a! Convince a tu grupo de amigos e id todos juntos.

ACTIVIDAD. ANÁLISIS DE IMÁGENES CON DOBLE PERSONALIDAD: LA REALIDAD ENGAÑA

A veces la realidad no es la que crees ver. Por ello te proponemos este sencillo juego que demuestra que a veces la realidad engaña. ¿Qué ves en cada imagen? ¿Encuentras las dos personalidades? Hallaras las soluciones en la página siguiente.



SOLUCIONES:

Imagen A: Podréis ver a una vieja y a una joven de perfil. (La nariz de la vieja es la mandíbula de la joven).

Imagen B: Un trompetista y el rostro de una mujer.

Imagen C: Depende como mires esta imagen verás un conejo o un pato, (las orejas del conejo son también el pico del pato).

Imagen D: En esta imagen de negro: un jarrón, de blanco: dos caras mirándose.

Moraleja: ¿Has conseguido ver las dos personalidades en cada imagen? Esto es sólo un ejemplo de como la realidad puede engañarte. Con las personas que conocemos en los *chats* puede pasarnos lo mismo; que se disfrace de joven pero en realidad sea una vieja o que veas a un saxofonista (imagen B) pero detrás se encuentre el rostro de una mujer. Se siempre muy cuidadoso y no confíes en todo lo que te digan, ya has podido comprobar que la realidad a veces, engaña.

3.3. ACOSO EN LA RED: CIBERBULLYNG

En el estudio hemos detectado que un 21,9% de los alumnos encuestados reconoce haber recibido alguna vez insultos o comentarios violentos o racistas a través de la Red. Ese puede ser el principio de un acoso, que cuando es a través de las Tecnologías de la Información se llama *ciberbullyng*. Nos preocupa mucho este tema y con este capítulo intentaremos acercarte un poco más a una triste realidad como es el *ciberbullyng*. Te informaremos de su significado, algunas claves para reconocerlo y consejos para saber actuar en estos casos.

¿QUÉ ES?

Es el uso de Internet, el teléfono móvil o los videojuegos para humillar, agredir, maltratar, difamar, insultar, amenazar o desprestigiar a compañeros o personas conocidas con una edad semejante.

¿DÓNDE SE DA?

Podemos encontrarnos con el *ciberbullyng* en *chats*, foros, sms, *blog*, fotologs, juegos en línea, videojuegos virtuales, nuestro espacio o conversaciones de mensajería instantánea, o incluso ser víctimas sin darnos cuenta mientras alguien se vale de sus conocimientos informáticos para introducirse en nuestro ordenador y manipular la cámara *web*, sustraernos los datos y contraseñas o fotos.

¿CÓMO PUEDO RECONOCERLO?

A continuación te damos algunos ejemplos concretos de *ciberbullyng* para que puedas reconocerlo:

- **Fotos.** Utilizan las fotos que sus “víctimas” tienen colgadas en Internet, ya sea en su espacio, fotolog, incluso a veces se cuelan en sus ordenadores mediante troyanos o virus para sustraerles sus fotos, manipularlas y exponerlas en Internet avergonzando y humillando a la persona. En ocasiones las exponen en *webs* para votar al más feo o al más tonto cargando su perfil de puntos y que aparezca en los primeros puestos de este ranking. Otras veces las utilizan como arma para chantajear a su víctima advirtiéndole de que enseñará la foto en cuestión si no hace lo que él le diga.
- **Suplantación de la personalidad.** Con los datos de otra persona editan perfiles o páginas *web* haciendo comentarios ficticios sobre sus experiencias sexuales, manías o cualquier otro comportamiento que sirva de burla. Se hacen pasar por ellos en foros o páginas escribiendo opiniones que ofenden a otras personas, comentarios violentos que provoquen su expulsión inmediata de la página sin poder volver a acceder a ella.
- **Amenazas.** Los acosadores se valen de sms, correos electrónicos o videos para amenazar e insultar a su víctima.
- **Ataque a la intimidad.** Se introducen dentro del correo electrónico manipulándolo, leyendo los mensajes, registrándoles en páginas para que sean víctimas de correos basura o de virus informáticos.

SABER ACTUAR

Si has reconocido algunos de estos síntomas en tu entorno, te damos algunos consejos para que sepas actuar y frenar este acoso.

- Coméntalo con tus padres o profesores, ellos son adultos y te ayudarán a buscar una solución mas rápidamente.
- Se siempre muy cuidadoso con tus datos personales y tus fotos, no sabes que uso pueden hacer de ellos. ¡Cuánto menos sepan de ti mejor!
- Puedes poner tu nombre y apellidos o apodos en cualquier buscador de Internet para comprobar si alguien ha suplantado tu personalidad o ha utilizado tus datos personales para hacerte daño.
- Guarda todas las pruebas del acoso, los mensajes de texto, los correos electrónicos, los videos o las conversaciones de mensajería instantánea.
- Acude a especialistas en informática para identificar al “ciberagresor”.

UN CASO REAL DE CIBERBULLYNG

Para que completes tu información sobre esta forma de acoso te exponemos una noticia real de un caso de *ciberbullyng*. Lee atentamente la noticia y no olvides seguir nuestros consejos y denunciar el caso si tú o alguien de tu entorno lo padece.

Llega el e-bullying: Chantaje a compañeros de clase por la Red

“La Guardia Civil ha detenido a dos escolares de 17 años, en Crevillente (Alicante) que habían inventado una forma muy curiosa de chantajear a sus compañeros. Los dos menores crearon un troyano (virus informático) que conseguía activar las cámaras webs de los ordenadores en las casas de sus compañeros, a los que grababan sin que los supieran en situaciones comprometidas (como desvistiendo en la habitación).

Después les amenazaban con difundir las imágenes en el colegio si no les pagaban “pedían entre 100 y 200 euros” explican en la Benemérita.

Falsificación de tarjetas

Los dos menores tenían grandes conocimientos en informática y ayudaron a otros dos jóvenes, mayores de edad y detenidos en Madrid, a falsificar tarjetas de crédito y efectuar con ellas compras ilegales de Internet.

Llegaron a estafar 60.000 euros”.

Fuente: www.20minutos.es 03/08/08.

ACTIVIDAD

- Debate: *Ciberbullyng* versus Modelos de personalidad.

Anima a tus profesores y compañeros o a tu familia en casa, a tener un debate sobre el *ciberbullyng* y los modelos de personalidad. Elegid un moderador y seguir el guión que te proponemos a continuación.

- ¿Cualquier persona puede ser víctima de *ciberbullyng* o sólo las personas mas débiles, e inseguras?
- ¿Cuál creéis que es el perfil del ciberagresor? Os proponemos dos opciones:
 - Un compañero con el que te llevas bien, que es popular, hace deporte, saca buenas notas en clase.
 - Un compañero que saca malas notas, siempre se mete en peleas, no se lleva bien con casi nadie y apenas acude a clase.
- ¿Una persona que acosa a un compañero, es un enfermo o una mala persona que sólo busca divertirse mientras hace daño a los demás?
- ¿Creéis que si se es víctima del *ciberbullyng* se debe denunciar, se debe contar a los padres o se debe callar y dejarlo pasar?
- ¿Qué tipo de condena pondríais a un ciberagresor? ¿Una mas leve porque quizás es un enfermo y necesita ayuda? ¿o una pena mas dura?

3.4. FRAUDES POR INTERNET: TÉCNICA DEL "PHISHING". COMPRAS POR INTERNET

Otra forma que tienen los piratas informáticos de apropiarse de tu identidad es por medio de los fraudes y las estafas, a esto en la jerga cibernética se le llama phishing. En la encuesta un 38,7% de vosotros reconocéis que frecuentemente recibís publicidad no deseada, es decir aquella que vosotros no habéis solicitado y que se cuelan en vuestro correo intentando vender sus productos. Esto puede ser el comienzo de una estafa o phishing, así que sigue leyendo y aprende como puedes reconocerlo y las precauciones que debes tomar para no ser víctima de estos ladrones.

3.4.1. IDENTIDAD ELECTRÓNICA. TÉCNICA DEL "PHISING"

Identidad electrónica:

- ¿Qué es? Son tus datos personales, todo aquello que dice algo de ti, que te diferencia del resto de personas en edición digital: tu nombre y apellidos, tu dirección, tu DNI, el número de la tarjeta de crédito, teléfono, fecha de nacimiento, tus fotos, tu agenda, tus contraseñas...
- ¿Cómo llega tu identidad a Internet? Seguro que más de una vez, para poder utilizar servicios de Internet te han pedido que te registres, lo que supone rellenar interminables formularios que no sólo te piden tus datos personales si no que te preguntan sobre tus aficiones, gustos, ideología, religión, raza o vida sexual. Así es como llegan tus datos a Internet, sin que tu de des cuenta, eres tú mismo el que los proporcionas. Ten mucho cuidado.
- ¿Para que? Toda la información que das libremente en estos cuestionarios o formularios pueden no ser utilizados para un buen fin. En algunos casos, quieren tus datos para fines comerciales. Es fácil: Saben mucho sobre ti y por tanto saben qué venderte y cómo vendértelo. Pero ¡cuidado! en ocasiones también pueden pedirte tus datos para ¡robártelos! Ándate con ojo y no seas víctima del phishing, ¿Qué es eso? Sigue leyendo y te enteraras de todo.

La Firma Electrónica

Es una clave personal para usarla por Internet. Necesitas obtener un certificado digital. La firma electrónica es un poco compleja ya que se basa en dos números: una clave pública y otra privada con una relación matemática entre ellos. Cuando se firma electrónicamente se genera lo que se llama huella digital que es totalmente diferente en cada documento. Con una segunda función la huella se cifra con una clave privada y ya tenemos la firma electrónica. El que recibe la firma deberá aplicar la clave pública para asegurar la originalidad de la misma y que ha sido enviada por su titular.

¿Qué es eso del phishing?

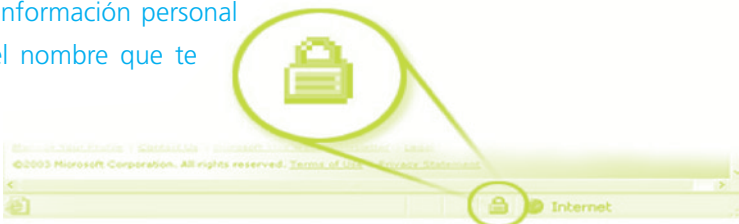
Es una estafa, un timo para apropiarse de tu identidad y utilizarla en Internet. Estos ladrones se valen de engaños por medio de correos electrónicos o ventanas emergentes para conseguir sus objetivos.

¿Cómo se apropian de nuestros datos?

Primero nos mandan un correo electrónico haciéndose pasar por sitios *Web* de nuestra confianza, como el banco, una empresa conocida, páginas *web* de Redes sociales como Facebook, Hi5, Myspace o páginas de envío de postales electrónicas. Después nos dicen que vayamos al enlace que aparece en el mensaje y que nos transportará a una *web* pirata semejante a la original. Una vez allí nos pedirán nuestros datos con cualquier excusa. Como creemos que el sitio *web* es de confianza los daremos sin ningún problema y el estafador ya tiene lo que quería. Ahora utilizará tus datos para hacer compras, abrir cuentas de correo, o cualquier cosa que se le ocurra.

PRECAUCIONES PARA PROTEGER NUESTRA IDENTIDAD

- Si te piden tus datos a cambio de algún servicio ¡desconfía! Ya sabes a donde pueden ir a parar...
- No te registres en páginas inseguras.
- No respondas a correos electrónicos que te solicitan información personal. Las empresas de prestigio nunca solicitan contraseñas o información personal por correo electrónico. Cuando te llegue algún correo de este estilo llama a la entidad y comprueba que es verdad.
- Cuando te llegue algún mensaje con un enlace ¡no lo sigas! Pueden llevarte a una *web* falsa y engañarte para que des tus datos.
- Aunque en la barra de direcciones aparezca la dirección correcta: ¡sigue desconfiando! Los piratas informáticos saben falsearlas y que parezca que son las reales. Teclea la dirección en la barra de direcciones para asegurarte que entras en la página *web* original.
- Para saber si el sitio *web* en el que estas, es seguro, comprueba que tienes un icono con un candado amarillo cerrado. Esto significa que el sitio *web* protege toda la información personal que des. Haz doble clic sobre el candado; si el nombre que te aparece no coincide con el sitio en el que estas se trata de una *web* falsa.
- ¡Atrévete a romper los mensajes cadena!
"Tendrás mala suerte en el amor si no reenvías



esto a 20 personas en menos de 2 minutos”. ¿Te suena verdad? Pues no te creas nada, lo único que se pretende con estos correos es almacenar más y más direcciones para mandarles publicidad y basura.

- Pon contraseñas para acceder a tu *blog* o fotolog, así te asegurarás de que sólo entra quien tu quieres.
- Si no lo has podido evitar y has sido víctima del *phishing*: ¡denuncia! Existe un Centro de denuncias de Fraude en Internet, ellos colaboran con las autoridades legales que se encargaran de coger a estos ladrones de identidad.

3.4.2. COMPRAS POR INTERNET

Recuerda que eres menor y no puedes hacer compras por Internet, los resultados de nuestro estudio revelan que tenéis esto bastante presente ya que sólo el 9.4% de vosotros admitís hacer compras por Internet, pero sí que un alto porcentaje consultáis catálogos de compra o venta (41,4%). Es importante que sepas que en la Red nos bombardean con millones de ofertas y de productos maravillosos a precios increíbles que en realidad son un engaño. Las páginas de subastas o de compras están llenas de timos y estafas que sólo pretenden sustraerte el dinero y tu identidad. Así que ten mucho cuidado y si te ha gustado algo y quieres comprarlo consúltalo con tus padres o tutores y sigue estas recomendaciones que te damos a continuación.

- Hacer las compras sólo en empresas serias y reconocidas y siempre bajo una conexión de Internet segura.
- Cómo en cualquier otro sitio te pedirán que te registres, elige bien la contraseña, que no sea fácil de adivinar.
- Asegúrate de que estás en la página oficial de la empresa y que no ha sido falseada por los piratas informáticos. Comprobar que la dirección comienza por “**https**” que nos dice que la página es segura, y si hay un candado en el rincón inferior de la pantalla.
- No os fíes de las ofertas increíbles que venden productos a un precio muy inferior que en el mercado. Aunque para un anunciante sea más barato anunciar sus productos por Internet, es imposible comercializar productos a precios muy por debajo de lo que se dan en el mercado.
- Comprueba los comentarios de otras personas sobre su experiencia de comprar en esa página *web*, siempre nos darán pistas sobre el sitio *web* en cuestión.
- No des tus datos personales ni datos bancarios por correo electrónico.
- Utiliza formas de pago seguro, un sistema que permita pagar cuando ya hayas recibido el producto. Desconfía si no puedes realizar el pago de esta manera.
- Nunca utilices datos personales como tu fecha de nacimiento o tu número de DNI a la hora de poner una contraseña, son datos muy fáciles de conocer y que pueden poner en riesgo tu privacidad.

ACTIVIDAD. PHISHING. ESTUDIO DE UN CASO REAL

Te mostramos un caso real de estafa por Internet.

Un ciudadano de Toledo recibe en su correo electrónico este mensaje:

Hola estimado usuario de Banco XXXX!

Por favor, lea atentamente este aviso de seguridad. Teniendo en consideración los frecuentes casos del fraude, hemos decidido implementar la confirmación de su cuenta cada mes. Le pedimos que llene todas las ventanillas para verificar su identidad. Si Ud no pone sus datos no podremos verificar su identidad y su cuenta será bloqueada.

Le saluda atentamente El servicio de la seguridad de Banco XXXX.

Teclee el Número de Usuario :

Clave de Acceso:

Introduzca su Clave de Operaciones:

Clave Secreta de su Tarjeta (PIN que utiliza en los cajeros):

Aparece el logotipo del banco y el mensaje parece de confianza así que nuestro pobre amigo contesta a todas las preguntas que le hacen y da sin ningún tipo de problemas sus datos y contraseñas por que no quiere que su cuenta sea bloqueada.

¿Qué pasó después?

Se trataba de un fraude. Dos ciudadanos de nacionalidad rusa consiguieron mediante este correo electrónico todas las claves de las tarjetas de crédito de su víctima y retiraron 21.500 euros de su cuenta. Por suerte estos ladrones fueron detenidos por la policía cuando intentaban cobrar la transferencia en un banco de un pueblo cercano.

¿Qué debería haber hecho este hombre?

Primero: ¡desconfiar! Cualquier mensaje que nos pida nuestros datos debe ponernos en alerta.

Segundo: Debería haber llamado a su banco y comprobar que efectivamente lo indicado en el correo electrónico es verdad.

Tercero: Lo mas importante de todo: no dar sus datos ni contraseñas a través de correo electrónico.

Fuente: www.elpais.com. "Dos detenidos en Gavà por estafar 21.500 euros mediante 'phising' 12/11/2000.



Capítulo 4

EL CORREO ELECTRÓNICO

Es un servicio muy útil que nos permite comunicarnos con nuestra gente de forma inmediata. En este capítulo te contamos como configurar tu propia cuenta de correo electrónico y las precauciones que debes tener.

CONFIGURACIÓN

1. Necesitas conexión a Internet ya sea en tu ordenador o en el teléfono móvil.
2. Debes pedir permiso a tus padres o tutores para poder crear una cuenta. Los menores de edad no pueden legalmente hacerlo sin autorización.
3. Elige el servidor que mas te guste para crear tu cuenta de correo, hay infinidad de ellos en Internet. *Yahoo, Hotmail, Gmail...*
4. Una vez elegido tu servidor ve donde te indique registro o crear una cuenta de correo.
5. Te pedirán algunos datos personales. Antes de darlos ya sabes que debes comprobar que el sitio *web* es seguro.
6. Elige un nombre para tu dirección y una contraseña.
7. Por último te pedirán que marques una casilla aceptando las condiciones de servicio y de privacidad del portal de Internet en cuestión. ¿Qué es esto? Es una especie de contrato entre tú y el portal. Es recomendable que leas estas condiciones, así sabrás cuales son los servicios que te ofrecen, los derechos que se reservan como por ejemplo poder hacer modificaciones en los servicios siempre que quieran, las normas que debes seguir para hacer un buen uso. En la mayoría de los casos en este "contrato" también estas aceptando que te manden publicidad a tu correo. Algunos servidores te permiten evitar esto, simplemente indicando que no quieres recibir información de ofertas ni promociones, pero en otros no.

PRECAUCIONES

- Elige una dirección de correo que no contenga tus datos personales, nombre y apellidos o fecha de nacimiento. Alterna mayúsculas y minúsculas, números, ponle guiones... así será mas difícil que los piratas y estafadores informáticos la encuentren.

SI: *ejemplo758Mi_cUenta@servidor.com*

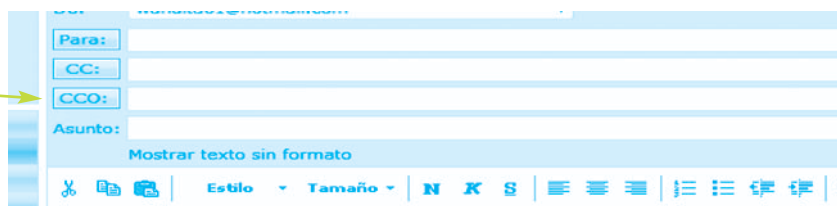
NO: *minombreyapellidos@servidor.com*

- Haz lo mismo con tu contraseña. Evita que sean datos evidentes como la fecha de tu cumple, o palabras fáciles de adivinar.
- No des tu dirección de correo electrónico a cualquiera. Ahora ya sabes que pueden hacer con ella.
- Cuando envíes mensajes a varias personas acuérdate de incluirlos en Copia Oculta . Así evitaras que el resto de personas conozcan las demás direcciones y circulen por la Red con el peligro que eso supone. ¡No sabemos donde pueden ir a parar! Para enviar mensajes con copia oculta en Hotmail, busca la opción de mostrar CC (copia) y CCO (copia oculta). Introduce las direcciones de tus destinatarios en la barra de CCO.



Pincha y te aparecerá esto:

Escribe las direcciones en la barra CCO.



- No abras mensajes con archivos adjuntos de origen desconocido o sospechoso y mucho menos te los descargues. Pueden contener virus.
- Si reenvías algún mensaje a varios destinatarios, borra los datos del envío anterior (remitente y de los destinatarios).
- No reenvíes los mensajes cadena; no se lo pongas fácil a los estafadores informáticos.
- Nunca te fíes de los mensajes cadenas. En ocasiones vienen disfrazados de una buena causa como una niña perdida, un niño que necesita apoyo para una operación, etc. Ya sabes que lo único que pretenden con estos correos es almacenar direcciones.
- Asegúrate siempre que entres en otros ordenadores que no sean el tuyo, de desactivar las casillas que dice: Recordar mi cuenta o Recordar mi contraseña en este equipo. Ten cuidado de no dejarte tu correo abierto.
- Recuerda que tu dirección de correo electrónico está protegida por la ley, igual que cualquier dato personal tuyo. Si alguien te lo sustrae o hace un mal uso de él, ¡denuncia!

sesión

s Live ID:
(ejemplo555@hotmail.com)

ntaseña:
¿Ha olvidado la contraseña?

- Recordar mis datos en este equipo (?)
 Recordar mi contraseña (?)

Capítulo 5

NUESTROS DERECHOS: PROTECCIÓN DE DATOS PERSONALES

El estudio realizado revela que muchos de vosotros no conocéis las garantías de la protección de datos, (el 39.8% de los alumnos encuestados no la conoce) así como, vuestra tendencia a facilitarlos en foros, casting, *chats*, concursos o comunidades virtuales. En este capítulo te contamos cuales son tus derechos en esta materia y cuales son las obligaciones de aquellos que te solicitan los datos. Es importante que estés bien informado y sepas cuando están atentando contra tu intimidad.

- ¿Sabes que hay una ley de Protección de Datos personales? La ley en cuestión se llama **LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.**
- ¿Qué dice esta ley? ¿Qué derechos tengo?

Tengo derecho a...

- Que me informen de la recogida de mis datos.
- Saber para que quieren mis datos.
- Conocer la identidad y dirección de quien los solicita, normalmente del responsable del tratamiento de mis datos o su representante.
- A negarme a proporcionarlos, a no ser que una ley me obligue a ello.
- Acceder a ellos siempre que quiera, a rectificarlos o cancelarlos y oponerme a su tratamiento en determinadas circunstancias.

Los que me piden los datos están obligados a...

- Garantizar la seguridad de mis datos evitando que se pierdan, se manipulen o alguien acceda a ellos sin autorización.
- A pedir mi consentimiento para el tratamiento de mis datos.
- A contestarme a todas las preguntas que les plantee sobre la utilización de mis datos.
- A mantener el secreto profesional respecto de mis datos, incluso cuando las relaciones con ellos se hayan terminado.
- A cancelar o rectificar mis datos en un plazo de 10 días en el caso que yo lo solicite.
- A no utilizar mis datos con otra finalidad distinta a la que me ofrecieron en mi captación.
- A no proporcionar o vender mis datos a terceros sin mi consentimiento.
- A crear un fichero y notificarlo a la Agencia Española de Protección de datos o a la autoridad autonómica competente en protección de datos.

Datos especialmente protegidos o también llamados Datos sensibles

- No podrán nunca obligarte a dar datos relativos a tu ideología, tu religión, tus creencias, tu origen racial, tu salud o tu vida sexual.

No se aplicará lo dicho en los apartados anteriores...

- Cuando el tratamiento de los datos tenga fines históricos, estadísticos o científicos. (por ejemplo el censo o el padrón).

ALGUNAS DEFINICIONES QUE DEBES CONOCER

Datos personales

Son todos aquellos datos que nos identifican como individuos únicos y diferenciados de los demás o que permiten identificarnos; así tenemos nuestro nombre completo, Documento Nacional de Identidad, señas de casa, nuestra propia imagen recogida en una foto, video o película, nuestra voz, nuestras huellas digitales, los datos referentes a nuestra salud o a nuestra estructura corporal y mental, aquellos datos que revelen de alguna forma nuestra ideología, religión o creencias, nuestra orientación sexual y algunos otros de uso menos frecuente o de menor relevancia.

Somos personas

Todas las personas con independencia de nuestra nacionalidad, que nos encontramos en España, tenemos derecho a que nuestros datos personales no sean revelados a nadie, son de nuestra exclusiva propiedad, de conformidad con nuestra Constitución y las leyes que la desarrollan, entre otras, la **LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**, las cuales nos garantizan el derecho a la protección de datos personales, al honor, a la intimidad personal y familiar y a la propia imagen.

Pero es que nuestra Constitución y las leyes también protegen nuestros datos personales una vez revelados a los demás por nosotros mismos y/o publicados por cualquier medio, con o sin nuestro consentimiento; permitiéndonos controlar en todo momento el buen uso y la circulación de nuestros datos.

Regla General

La regla general es que cada uno de nosotros es dueño de sus datos personales y no está obligado a facilitarlos; quien quiera utilizarlos, debe pedirnos permiso, es decir, ha de hacerlo con nuestro consentimiento, o sea, debe contar con nuestra conformidad.

Excepción

Estamos obligados a facilitar nuestros datos personales cuando una Ley nos obligue a ello de manera clara y con una finalidad concreta. Por ejemplo: la Ley de Registro Civil obliga a nuestros padres a facilitar los datos personales de sus hijos recién nacidos para incorporarlos a un archivo, con el fin de identificarlos y atribuirles una nacionalidad.

DERECHOS PARA PROTEGER TUS DATOS

Derecho de Información

Cuando te soliciten tus datos personales por cualquier medio oral o escrito, tienes derecho a que te informen sobre la necesidad de la recogida, finalidad o propósito de esa recogida, consecuencias de tu negativa a darlos, de la localización del archivo que contendrá tus datos y de la identidad de la persona responsable del funcionamiento de ese archivo y específicamente deben informarte de los derechos siguientes:

Silencio absoluto: nadie y en ningún caso puede obligarte a declarar datos referidos a tu ideología, religión o creencias personales. Ninguna Ley te obliga a ello.

Consentimiento expreso: si eres mayor de 14 años, solamente mediante tu consentimiento o autorización expresa y por escrito, pueden solicitarte y usar tus datos de carácter personal que revelen tu ideología, religión, creencias, afiliación sindical, origen racial, vida sexual o datos referentes a tu salud; solo pueden tratarlo cuando una Ley lo autorice expresa y claramente, por razones de interés general y con una finalidad concreta o con tu consentimiento.

Acceso: posibilidad de conocer los datos personales que otros tienen archivados o recogidos sobre ti, el origen de esos datos y las comunicaciones o traspasos que se hayan hecho a terceros (otros aparte de ti y el responsable del archivo al que accedes), salvo las limitaciones que la Ley impone para algunos archivos oficiales.

Rectificación: una vez que hayas accedido a conocer tus datos en poder de otros, tienes derecho a que los rectifiquen en el sentido que estimes conveniente.

Cancelación: en este mismo sentido, tienes derecho a que tus datos personales sean bloqueados, cancelados o definitivamente borrados. Cuando resulten excesivos para la finalidad para la cual fueron recogidos, inadecuados o impertinentes (que no vienen a cuento).

Oposición: tienes derecho a oponerte al uso y circulación de tus datos personales obrantes en poder de otros y a oponerte a las valoraciones sobre determinados aspectos de tu personalidad, basadas únicamente en el tratamiento de tus datos personales.

Cuando alguien tenga tus datos sin que tú lo sepas y además pretenda utilizarlos, previamente debe informarte de la existencia de ese archivo y de su dirección, de su contenido, de la identidad del responsable, del origen de los datos o de cómo los consiguió y de la posibilidad que tienes de acceder a ellos, oponerte a su uso, rectificarlos o cancelarlos. Esta obligación de informarte no existe cuando una Ley lo permita, cuando tus datos sean tratados con fines históricos, estadísticos o científicos o cuando por cualquier causa justificada resulte imposible informarte.

Seguridad: la persona responsable del registro y del tratamiento de tus datos y quienes trabajen para él, deben guardar secreto absoluto sobre su contenido y tenerlos guardados en un archivo seguro, sin que cualquiera pueda fácilmente acceder a ellos.

IMPORTANTE: cuando la recogida de tus datos se haga por escrito, mediante cuestionarios u otros impresos, deberán figurar claramente en el papel todos los derechos que acabamos de exponer, de tal forma que antes de escribir puedas leerlos con tranquilidad y después de entenderlos, ejercitarlos en el acto si lo estimas conveniente, en función de la situación en que te encuentres. En el caso de Internet, debes leer con detenimiento las condiciones de servicio y la política de privacidad. Al final de cada formulario deberías encontrar frases tipo como:

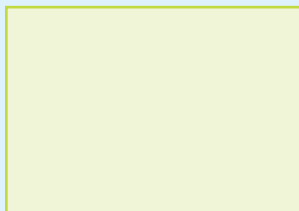
“Los datos personales serán recogidos y tratados en el fichero (...), cuya finalidad es (...), inscrito en el Registro de Fichero de Datos Personales de la Agencia de Protección de Datos de..... y podrán ser cedidos a (.....), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (nombre y dirección)”.

Te proponemos ahora un ejercicio práctico para aplicar estos derechos, mediante el estudio de un caso encontrado en Internet.

El próximo mes de enero va a comenzar la 5ª edición del programa de TV “ Te damos una oportunidad”. Para presentarte al casting has de rellenar esta ficha de inscripción y enviárnosla por Internet.

FICHA DE INSCRIPCIÓN

Foto actual, indicando el peso, altura y medidas (si eres mujer).



Nombre y apellidos:

Fecha de nacimiento: DNI o pasaporte:.....

Estado civil:Teléfono móvil:

E-mail:

Profesión actual (indica si estudias, trabajas o estás parado):

Nombre de los padres y DNI:Raza:

Enfermedades que padeces o alergias:Religión:

Condición sexual (heterosexual u homosexual).....

¿Estarías dispuesto a?:

• pintarte el color del cabello	SI	NO	DEPENDEN
• cortarte el cabello	SI	NO	DEPENDEN
• desfilas en ropa de bañó	SI	NO	DEPENDEN
• realizar desnudos parciales (topless)	SI	NO	DEPENDEN
• ser grabado durante el día sin saber cuándo	SI	NO	DEPENDEN
• ¿Consentiría la emisión de esas imágenes grabadas seleccionadas por la productora Globo Tour RTV?	SI	NO	DEPENDEN

Aficiones:

.....

.....

Indica si te has presentado antes algún otro concurso de TV y en qué cadena.

.....

.....

Una vez finalizadas las pruebas de selección, se publicará en nuestra página web el nombre, DNI y la dirección de correo electrónico de cada uno de los seleccionados por la EMPRESA GLOBO TOUR RTV S.A. Barcelona.

Una vez leída la ficha de inscripción del casting, contesta a estas preguntas:

1. ¿Estarías dispuesto a presentarte a este casting? Razona tu respuesta.

.....

.....

2. ¿Cuál es el fin principal que pretende esta empresa cuando solicita estos datos?

.....

.....

3. ¿Qué datos crees que son innecesarios para ese fin previsto? Enuméralos y justifica tu respuesta.

.....

.....

DENUNCIA ANTE UNA AGENCIA DE PROTECCIÓN DE DATOS

Si alguna vez crees que no se han cumplido tus derechos en materia de protección de datos, explicados con anterioridad en este manual, debes interponer una denuncia para que se cumpla la ley y no hagan un mal uso de tus datos. Para ello deberás presentar un escrito de denuncia en los términos que se prevén en el artículo 70 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Dicho escrito deberá contener:

- Nombre y apellidos del interesado y, en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones.
- Hechos, razones y petición en que se concrete, con toda claridad, la solicitud.
- Lugar y fecha.
- Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.
- Órgano, centro o unidad administrativa a la que se dirige. (En su caso sería la Subdirección General de Inspección de Datos de esta Agencia).
- Igualmente deberá acompañar los documentos.



Dicha denuncia puedes interponerla a través de la página web de la Agencia Española de Protección de Datos, como el modelo que te presentamos a continuación. www.agpd.es

DENUNCIA ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

DATOS DEL AFECTADO⁽¹⁾. (si eres menor de edad, el representante legal: tus padres).

D. / D^a. , mayor de edad, con domicilio en la C/ Plaza n^o.....
Localidad.....Provincia C.P.
Comunidad Autónoma..... con DNI..... correo electrónico.....

DATOS DEL PRESUNTO RESPONSABLE. (serían de la empresa GLOBO TOUR, si los conocieras).

Nombre / Razón social:.....
Dirección de la Oficina / Servicio:
C/ Plaza n^o C. Postal Localidad.....
..... Provincia Comunidad Autónoma
C.I.F. / D.N.I.

De acuerdo con lo previsto en el artículo 37, d) y g) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, viene a poner en conocimiento del Director de la Agencia Española de Protección de Datos los siguientes hechos que justifica con documentación anexa (la dirección de la página de Internet, en este caso)al presente escrito:

HECHOS

.....
.....

En virtud de cuanto antecede,

SOLICITA, que previas las comprobaciones que estime oportuno realizar, se dicte acuerdo de iniciación del procedimiento sancionador, con el fin de atajar la actuación señalada contraria a lo dispuesto en la Ley Orgánica 15/1999, y que se me notifique la resolución que recaiga en el mismo al amparo de lo previsto en los artículos 126 y 128 del Real Decreto 1720/2007, de 21 de diciembre que la desarrolla.

Ena.....de.....de 20.....

Firmado:

ILMO. SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. C/ Jorge Juan, 6.- 28001 MADRID

⁽¹⁾ La denuncia puede presentarse por el propio afectado, en cuyo caso acompañará copia del DNI o cualquier otro documento que acredite la identidad y sea considerado válido en derecho. También puede concederse la representación legal a un tercero, en cuyo caso, además, se deberá aportar DNI y documento acreditativo de la representación de éste.

En las Agencias de Protección de Datos ya creadas en las Comunidades Autónomas de Cataluña, Euskadi y Madrid, también se pueden interponer denuncias. Las puedes encontrar en las páginas WEB:

- Cataluña: "Agencia Catalana de Protecció de Dades" www.apd.cat
- Euskadi: "Agencia Vasca de Protección de Datos" www.avpd.euskadi.net
- Madrid: "Agencia de Protección de datos de Madrid" www.apdcm.es

También sería interesante que consultarais la página web www.datospersonales.org en la que podréis encontrar toda la actualidad en materia de protección de datos personales.

Capítulo 6

RESUMEN Y CONCLUSIONES

Este Manual es el resultado del estudio que vosotros nos habéis ayudado a realizar con vuestra participación. vuestras respuestas nos han orientado a la hora de elegir los temas a tratar. Nos han desvelado el uso que hacéis de Internet y del teléfono móvil. La finalidad de este texto es acercaros un poco más a las Tecnologías de la Información, que conocierais, no solo los beneficios, sino todos los riesgos a los que estáis expuestos y daros las claves para protegeros y saber actuar.

A continuación os ofrecemos también consejos para padres, madres, educadores, educadoras y tutores legales. Esperamos que os sean de utilidad.

Consejos para padres, madres, educadores, educadoras y tutores legales

DE CARÁCTER GENERAL

1. Intente estar al día en cuestiones de Internet y el teléfono móvil. Cuanta más información tenga a cerca de estas tecnologías, mejor podrá ayudar a sus hijos a que hagan un buen uso de ellas.
2. Hable con los chicos sobre lo que hacen en Internet, con quien hablan o que páginas visitan más. Establecer entre todos, unas reglas básicas de uso y consumo de las tecnologías.
3. Es recomendable que sitúe el ordenador en un lugar común de la casa. NO deje que tengan el ordenador en su habitación.
4. Controle el tiempo que pasan sus hijos en Internet o usando el teléfono móvil. Estableced unos horarios de uso que se adapten al tiempo de estudio.
5. Fomente las actividades en familia y anímele a que haga deporte, teatro o cualquier otra alternativa al ordenador y el teléfono móvil.

SOBRE EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

6. Instale un antivirus, cortafuegos y programas de filtrado de correo basura en su ordenador y asegúrese de actualizarlos cada cierto tiempo.
7. Prepare diferentes inicios de sesión personalizados para cada hijo o hija.
8. Configure su cuenta como la de administrador del equipo para poder controlar lo que cada uno de sus hijos puede y no puede hacer.
9. Configure la cuenta de sus hijos para protegerle de todos los peligros de Internet. En los exploradores de Internet de

todos los sistemas operativos existe la posibilidad de un control paterno. Lo encontrará en la opción de **Herramientas > Opciones de Internet > Contenido**.

Pincha en la opción de control parental y podrá desactivar algunos juegos que no quiere que sus hijos utilicen y recibir en su cuenta información sobre las actividades de la cuenta de sus hijos, semanalmente o diariamente.

Encontrará también la opción de Asesor de Contenido. En la pestaña de **Clasificación** podrá indicar, moviendo el cursor, el nivel de sexo, miedo, desnudez o lenguaje soez, a lo que quieres exponer a tus hijos cuando acceden a Internet, (el nivel mas estricto es el 0, a la izquierda del todo).



10. Cree una lista de los sitios *Web* que sus hijos puedan visitar siempre o que no puedan visitar nunca. Para ello siga en la opción de **Asesor de Contenido** en la pestaña de **Sitios aprobados**.

Escriba la dirección de la página *Web* en cuestión y seleccione "Siempre" o "Nunca".

11. Cree una contraseña para que sus hijos no puedan cambiar la configuración que les ha echo en su cuenta y entren a los sitios *Web* que has valorado como peligrosos. Para ello vaya a la pestaña de **General** en la opción de **Asesor de Contenido**.

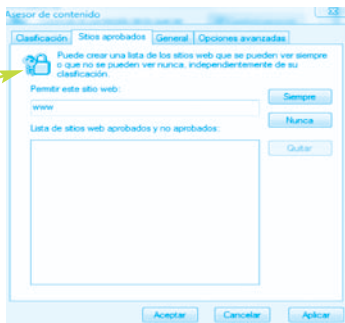
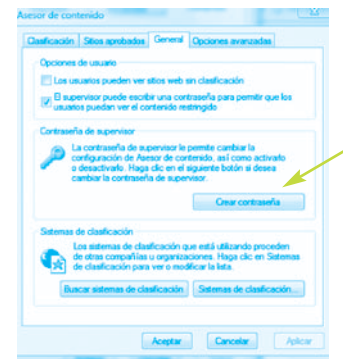
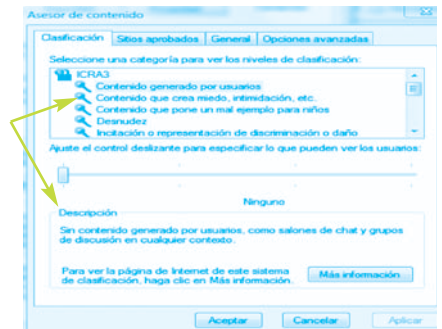
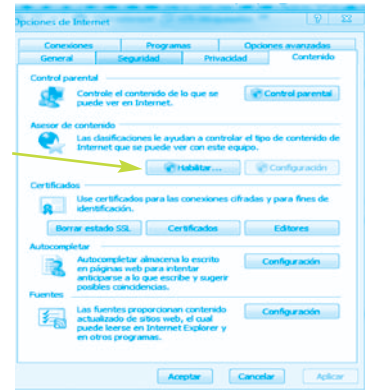
Si quiere proteger más a sus hijos cuando estén en Internet, existen programas con mas opciones de seguridad y configuraciones diferentes en el mercado.

12. Alerte a sus hijos sobre los beneficios pero también de los peligros del *Chat* y de quedar con personas desconocidas. Si sus hijos mandan mensajes o visitan salas de *chat*, usan videojuegos en línea u otras actividades en Internet que requieran un nombre de inicio de sesión para identificarse, ayúdeles a elegirlo y asegúrese de que usan contraseñas seguras, que no las comparten con nadie y que no revelan ninguna otra información personal.

En el mercado existe una amplia variedad de programas con más opciones de seguridad y de filtrado de contenidos.

13. Preste atención a los juegos que se descarguen que intercambien con amigos. Asegúrese de que el contenido es adecuado para su edad y no incluye violencia.

14. Acompañe a sus hijos si van a descargar programas, música o archivos aunque sean legales. Enséñeles que si comparten archivos o toman textos, imágenes o dibujos de la *Web* deben hacerlo sin infringir las leyes de derechos de autor y propiedad intelectual y puede ser ilegal.



SOBRE LA PROTECCIÓN DE DATOS PERSONALES

15. Hable con sus hijos de la importancia de proteger los datos personales. En este Manual incluimos los derechos que nos amparan como ciudadanos incluidos en la legislación de Protección de Datos de Carácter Personal, tanto Estatal como Autonómica.
16. Enseñe a sus hijos adolescentes a que nunca faciliten información personal sin su permiso cuando utilicen el correo electrónico, salas de *chat*, mensajería instantánea, rellenen formularios de registro y perfiles personales o participen en concursos en línea.

Resumen de consejos

- Controla el tiempo que pasas frente al ordenador o al teléfono móvil. No olvides estudiar y pasar tiempo con tu familia.
- Se siempre respetuoso y tolerante con las opiniones de los demás, en *blogs*, foros o *chats*.
- Ten precaución con las ofertas y las promesas milagrosas que te hacen por Internet. Si has encontrado algo que te gustaría comprar por Internet, consulta siempre a tus padres o un adulto responsable.
- Para proteger tu intimidad acuérdate de borrar periódicamente el historial, las cookies y los archivos de tu ordenador.
- Instala un antivirus y cortafuegos en tu ordenador para estar protegido de los virus y troyanos. Acuérdate también de actualizar las versiones con frecuencia.
- Para que no te molesten las dichas ventanitas emergentes de publicidad (pop-ups), bloquéalas siguiendo los pasos que te hemos mostrado en el manual o hazte con un programa bloqueador de pop-ups.
- Analiza bien los correos electrónicos que llegan a tu dirección, si llevan un archivo adjunto, provienen de un remitente desconocido para ti o su titular te hace promesas milagrosas, conviene que los borres antes de abrirlos, pueden tratarse de los conocidos correo basura o spams.
- Para hacerte mas resistente a los programas de búsqueda automática de direcciones, ponle un nombre complicado a tu cuenta, que no delate alguno de tus datos personales como puede ser tu nombre o apellidos o fecha de nacimiento y que incluya números, guiones... por ejemplo: nuevas467tecnologías9_@protegete.com. Haz lo mismo con tu contraseña.
- No cuelgues tus fotos en Internet, ya sabes que los piratas malintencionados podrían hacer un mal uso de ellas.
- Ten mucha precaución cuando te conectes a un *Chat*. Nunca reveles tus datos ni los de tus padres, ni envíes tus fotos a personas desconocidas. Evita las citas con personas que has conocido a través del *Chat* y si finalmente decides hacerlo nunca vayas solo/a.
- Para proteger tus datos de carácter personal y evitar ser víctima de los fraudes en la Red, no te registres en páginas inseguras ni respondas a correos electrónicos que te solicitan información personal y aseguraté siempre que la página que estás visitando es la original.
- Si crees que tus datos han sido utilizados de una manera inadecuada, recuerda que tienes derechos y que hay una ley de Protección de Datos de Carácter personal que te ampara, así que no dudes en denunciarlo a las autoridades competentes.

RELACIÓN DE CENTROS EDUCATIVOS
QUE HAN PARTICIPADO EN EL PROYECTO
CLI PROMETEO 2008-09

ANDALUCÍA

IES Aurantia	Almería
IES Cárbula	Córdoba
IES Delgado Hernández	Huelva
IES Iulia Salaria	Jaén
IES La Janda	Cádiz
IES Martín Rivero	Málaga
IES Néstor Almendros	Sevilla
IES Villanueva del Mar	Granada

CATALUNYA

Ceip Jacint Verdaguer	Barcelona
Ceip Pere Vila	Barcelona
Col·legi Lestonnac	Barcelona
Escola Thau	Barcelona
IES Salvador Espriu	Barcelona

EUSKADI

Cep Aitor Ikastola	Guipuzcoa
Cep Angel Ganivet-Izarra-Sta. Lucia	Álava
Cep Atxondo	Vizcaya
Cep Barrutia	Vizcaya
Cep Derio	Vizcaya
Cep Harri Berri Oleta	Guipuzcoa
Cep Lateorro	Álava
Cep Maestro Zubeldia	Vizcaya
Cep San Gabriel	Vizcaya
Cep Urretxindorra	Vizcaya
Cep Velázquez-M.Cervantes	Vizcaya
Cep Zaldupe	Vizcaya
IES Ategorri	Vizcaya
IES Balmaseda	Vizcaya
IES Barrutialde	Vizcaya
IES Bengoetxe	Vizcaya
IES Derio	Vizcaya
IES Egape Ikastola	Guipuzcoa
IES Lezo	Guipuzcoa
IES Zaraobe	Álava

EXTREMADURA

Ceip Ntra. Sra. de La Caridad	Badajoz
Colegio Claret	Badajoz
IES Sáez de Buruaga	Badajoz
IES Tamujal	Badajoz
IESO Vía Dalmacia	Cáceres

MADRID

Colegio Sagrado Corazón	Madrid
IES Cervantes	Madrid
IES Isabel La Católica	Madrid
IES José de Churriguera	Madrid
IES Prado de Santo Domingo	Madrid



**Comisión
de Libertades
e Informática**

C/ José Ortega y Gasset 77, 2ªA - 28006 Madrid
Tels. 914 023 204 · 915 237 566 · Fax 915 238 621
secretaria@asociacioncli.es · www.asociacioncli.es