

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



CAJA MADRID
OBRA SOCIAL



Comisión
de Libertades
e Informática

**Proyecto CLi - PROMETEO
2008/09**

Manual Práctico de 12 a 14 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

Capítulo	Contenido	Objetivos	Actividades	Pág.
Introducción.	Presentación del Manual.	Motivación.		2
1. El buen uso de Internet en el ordenador y en el teléfono móvil.	Actividades que pueden hacerse y el beneficio que nos aportan.	Valorar las posibilidades y ventajas que tienen ambas tecnologías.	Presente y futuro de Internet: reflexión y debate.	4
2. Problemas derivados de un mal uso de Internet:	La protección de datos personales y su privacidad: aspectos técnicos.	Conocer los procedimientos técnicos para favorecer nuestra intimidad.		6
• Compartir archivos: texto, fotos, vídeos.	Virus, antivirus, bloqueadores, cortafuegos. Evitar correos no deseados ("spams").	Detectar las posibles invasiones a nuestra privacidad y los medios para evitarlas.	Modificación de archivos: alteración de imágenes reales.	6
• Encuentros con personas desconocidas: "on line" y reales ("citas a ciegas").	Encuentros con otras personas por medio de la Red: los chats.	Identificar los peligros de contactar con personas desconocidas.	Análisis de imágenes con doble personalidad: la realidad engaña.	11
• Acoso electrónico ("cyberbullying").	Medios de acoso: – correo electrónico, – participación en un chat y en juegos "on line".	Reconocer los casos de acoso y saber actuar contra ellos.	Cibercuento: el espejo de Blancanieves.	13
• Fraudes por Internet: – compras, – suplantación de la personalidad "phishing".	La Identidad Electrónica.	Tomar conciencia de las precauciones necesarias para protegerla.	Phishing: definición, descripción de fotos. Análisis de un caso real.	15
3. El Correo electrónico.	Configuración y precauciones.	Aprender a configurar una cuenta de correo electrónico con garantías.	Configuración de una cuenta de correo electrónico.	19
4. Nuestros derechos: – somos ciudadanos (protección de datos personales), – somos personas.	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.	Caso práctico de denuncia a la Agencia de Protección de Datos.	22
5. Consejos para padres, madres o tutores.				30
6. Consejos para estudiantes.				32

Introducción

Las nuevas formas de información y de comunicación son uno de los sectores que más evolucionan cada día, especialmente por medio de Internet. Nos acercan a nuevos modos de conocimiento y tipos de relación con los demás. Hoy podemos tener acceso a casi toda la información deseada y unirnos a millones de personas de todo el mundo sin límite de tiempo y distancia.

Pero existen también riesgos si no hacemos un uso adecuado de todos estos avances. Por ello, la Comisión de Libertades e Informática ha realizado un estudio en el que han participado más de ocho mil estudiantes de colegios e institutos de diferentes Comunidades Autónomas con el fin de conocer vuestras preferencias sobre el uso de tecnologías como los ordenadores y los teléfonos móviles y su acceso a Internet, los reproductores de sonido y video..., así como otros muchos aspectos de interés. Un primer dato: casi un 30% de los estudiantes de tu edad se conectan a internet todos los días, frente al 20% que lo hacen sólo los fines de semana. El resto de manera más esporádica.

Este Manual es el resultado de las conclusiones extraídas de dicho estudio. Una de las más importantes es el desconocimiento que a veces tenéis de los riesgos ocasionados por el mal uso de Internet. Por ello, te ofrecemos alternativas para defenderte de sus peligros, especialmente en lo relacionado a la protección de tus datos personales: tu nombre, dirección, fotografía, una grabación de tu voz... Todo aquello que te identifica ante los demás y que podría llegar a circular por Internet sin ningún control. Además, para que se respete tu intimidad, te indicamos

los derechos que te amparan y la manera de defenderlos, si fuera necesario. Has de saber, que para autorizar el tratamiento o uso de tus datos personales por parte de otras personas se te considera **mayor de edad**, según la Ley, a partir de los 14 años.

De una manera fácil y práctica, el contenido de este Manual se estructura en tres grandes bloques:

1. **El uso de Internet:** beneficios que aporta y problemas derivados de su mal uso (virus y otras intromisiones, fraudes...).
2. **Nuestros derechos como ciudadanos**, en especial los vinculados a la protección de tus datos personales.
3. **Consejos para padres, madres, educadores y estudiantes.**

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. Añadiremos unos cuantos consejos que no queremos que olvideis.

Una auténtica aventura de conocimiento que te ayudará a enfrentarte a los nuevos retos tecnológicos.

¡Síguenos! ¡Será divertido!

Capítulo 1

EL BUEN USO DE INTERNET EN EL ORDENADOR Y EN EL TELÉFONO MÓVIL

El uso de Internet supone un gran beneficio para todos. Navegando por la Red con el ordenador o el teléfono móvil podemos conocer muchas cosas y comunicarnos con diferentes personas. ¡Y en tiempo real!

TÚ PUEDES:

- Chatear con tus amigos, conectados simultáneamente a una misma conversación en un momento dado. Ver sus nombres en la lista de tu ordenador e ir intercambiando mensajes. Incluso en muchos casos, la comunicación puedes hacerla mediante la transmisión de tu propia voz o imagen.
- Buscar información de temas que te interesan y aprender por ti mismo. Internet integra actualmente la mayor base de datos del mundo en soporte informático, el **World Wide Web** (www), formada por millones de páginas web repletas de información de todo tipo, que están repartidas por miles de servidores (ordenadores conectados permanentemente a la Red). ¡Que independencia!
- Hacer o completar trabajos que te piden en tu colegio o instituto. Imagina que quieres hacer visitas virtuales a las ciudades y lugares más importantes del mundo y, en algunos casos, recorrerlos en tres dimensiones. Todo delante de una pantalla y dirigido por ti mismo. ¡Sorprenderás a tus profesores y compañeros!
- Comunicarte con amigos y amigas o familiares que viven lejos, superando las barreras del tiempo y de la distancia. Dos mil o más kilómetros a tiro de un “click” de tu ratón o pantalla.
- Tener tu propia página web o tu blog. Un diario personal que puedes ir actualizando con todo aquello que te ocurre. Los blogs o foros permiten expresar tus opiniones sobre temas que te gustan.
- Compartir gustos e intereses con otras personas. El uso de Internet como fuente de información, puede propiciar el trabajo en grupo y el cultivo de actitudes sociales, el intercambio de ideas, la cooperación y el desarrollo de tu personalidad.



- Pasarlo bien: jugar, escuchar música o ver vídeos. Muchos juegos mejoran tus habilidades (rapidez, agilidad mental...) y ponen a prueba tu ingenio.

En la encuesta que realizamos a niños y jóvenes de la que te hemos hablado, dimos a elegir entre diferentes tecnologías y en la edad de 12 a 14 años. El resultado de su uso fue el siguiente:

El 50% prefiere el ordenador con acceso a Internet, el 26% el teléfono móvil, el 12% los reproductores de audio (MP3, MP4,...) y de fotografía o video, y el 9% el ordenador aún sin tener acceso a Internet.

TU REFLEXIÓN

Piensa al menos en cinco inventos o avances propiciados por el hombre que hayan revolucionado el mundo en los últimos veinte o treinta años, escríbelos. ¿Dónde situarías a Internet? Intercambia tu opinión con la de tus padres o compañeros de clase y escribe las coincidencias o diferencias.

1.
2.
3.
4.
5.

Coinciden:

.....
.....

Difieren:

.....
.....

Prueba también a adivinar el futuro de Internet y otras tecnologías. ¿Qué más nos permitirán hacer?

.....
.....

Capítulo 2

PROBLEMAS DERIVADOS DE UN MAL USO DE INTERNET

Probablemente te habrás preguntado, ¿quién controla todo lo que podemos encontrar en Internet?

En muchas ocasiones, nadie, por la gran cantidad de información disponible, aunque existen organismos y autoridades que velan para proteger a los ciudadanos ante posibles delitos. Además, ten en cuenta que Internet puede, a menudo, ofrecernos una visión parcial de la realidad con informaciones falsas o anticuadas.

Ahí radica su verdadero problema.

Internet puede convertirse en una auténtica bomba de relojería... y ¡estallar! si no tomas las precauciones adecuadas. Para ello debes conocer las limitaciones de este medio que te indicamos en los siguientes apartados.



PROBLEMA 1. COMPARTIR ARCHIVOS: TEXTOS, FOTOS, VÍDEOS...

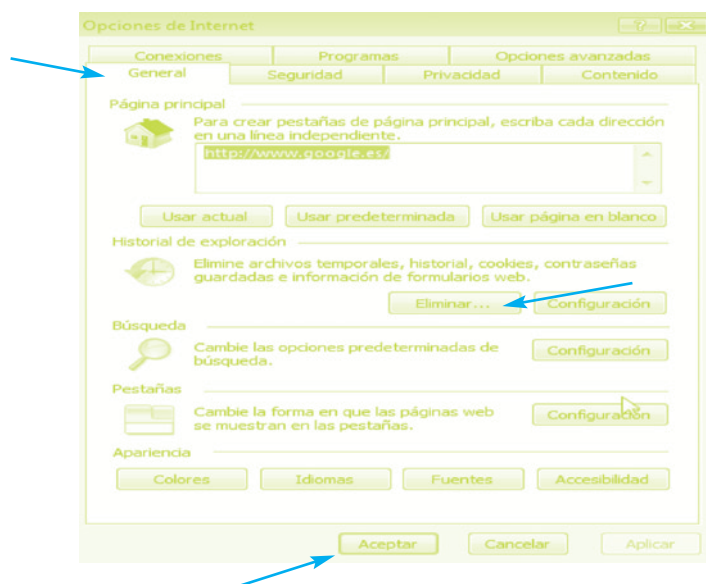
Tu ordenador lo apunta todo. Guarda las páginas web que has visitado, los archivos que te has descargado, tus contraseñas... Nunca olvida nada a no ser que tú se lo digas, y lo peor de todo, puede haber personas que utilicen sus conocimientos informáticos para acceder a esa información, espiar y hacerse con ella.

Como buen secretario tiene clasificado todo de esta manera:

- **Historial.** Aquí se almacenan 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.** Son archivos que contienen la dirección de la página que acabas de ver. Algunas son temporales, pero otras pueden permanecer en tu ordenador durante años. Los espías pueden hacer un seguimiento de aquellas que has visitado y acceder a tus archivos. De esta manera sabrán tus gustos y preferencias y con ello crear listas de posibles clientes que luego venden a empresas comerciales. Es importante que cada cierto tiempo se eliminen.

- **Archivos.** Almacenan las imágenes y contenidos de las páginas que has consultado en Internet para así acelerar su carga cuando vuelvas a entrar en ellas. Accediendo a estos archivos se pueden conocer los datos que ya has escrito. Si se borran, se tardará un poco más en cargar la página pero estarás protegido de los espías e intrusos informáticos.

Para evitar que alguien tenga acceso a tu ordenador te recomendamos que, junto a tus padres, borres estos archivos frecuentemente. Si el sistema operativo que usas es *Windows XP* y la versión anterior de *Internet Explorer* puedes hacerlo desde el "historial de exploración" (Herramientas > *Opciones de Internet*, haz clic en la pestaña General y elimina *el historial, las cookies o los archivos*, y aceptar).



Además, muchos archivos que te envían personas que no conoces bien pueden contener **VIRUS**.

¿Sabías que hay algunos muy difíciles de detectar por los antivirus del ordenador, pueden dañar tu equipo y todo lo que has guardado en él, como tu música, fotos, juegos y tareas? Estos son los virus más frecuentes:

- **Caballo de Troya o trojano:** se esconde detrás de algunos programas que nos descargamos creyendo que son inofensivos. Una vez descargado, el trojano se mete en tu ordenador y puede hacer todo lo que quiera con él.
- **Stealth:** es uno de los peores, que incluso intenta engañar al antivirus modificando sus datos para no ser detectado.
- **Parásito:** puede ir oculto en esos programas que incluye el mensaje de "ejecutar".
- **Gusano:** se propaga con muchísima facilidad ya que se transporta de un ordenador a otro a través del correo electrónico o la mensajería instantánea.
- **Cabir:** el virus del móvil. Viaja de móvil en móvil a través del *bluetooth*. Puede robarte tus mensajes de texto o contactos, seguir tus movimientos o escuchar tus conversaciones.

No te preocupes. Aquí te ofrecemos algunos consejos prácticos para protegerte del ataque de los virus:

1. Por supuesto, tener instalado en el ordenador:
 - **Un antivirus:** El ordenador es como una casa, debe estar cerrada para evitar que entre quien no deseas. A veces incluso, se instalan sistemas de vigilancia añadidos. ¿Hacemos lo mismo en nuestro ordenador? Para impedir que por las puertas de Internet se cuelen posibles intrusos necesitamos un programa de vigilancia que llamamos antivirus. Es nuestro sistema de seguridad, un guardaespaldas que se mantiene siempre alerta ante posibles programas dañinos que puedan colarse y hacer uso de los datos y archivos que tienes guardados. No olvides actualizarlo a menudo; si no es así su utilidad es casi nula.
 - **Un cortafuegos:** O *firewall* en inglés. Este tipo de programas son “el portero” de tu ordenador: nadie pasará sin su permiso. Te avisa de otros posibles programas que puedan dañarle y además, te protege ante los estafadores que quieran entrar.
2. No facilitar a nadie tu contraseña de acceso.
3. No abrir ni guardar archivos que te envíen personas desconocidas.
4. Instalar un programa anti “pop ups” para bloquear las ventanitas que, sin solicitarlas, aparecen en nuestro ordenador con esa publicidad tan molesta.

CORREO ELECTRÓNICO NO DESEADO

Habrás oído hablar de los CORREOS NO DESEADOS. Los denominados “SPAMS ” O CORREOS BASURA.

Se trata de mensajes o correos que suelen contener publicidad engañosa con fines comerciales.

Se aprovechan de nuestra curiosidad y parece que quieren solucionarnos la vida. En realidad, su intención suele ser, introducir un virus y controlar nuestro ordenador.

Son del tipo:

- *“Gana millones con el mínimo esfuerzo”.*
- *“El amor de tu vida te está esperando”.*
- *“Has sido seleccionado entre millones de personas para probar...(X)... Una nueva ilusión para tu vida. Envía tus datos al....(un número o dirección de correo electrónico) y recibirás gratuitamente...”.*



Te añadimos algunos consejos para evitar que entren en tu buzón:

1. **Elimina los mensajes de correo electrónico no deseados sin abrirlos.** En ocasiones, alertamos a los creadores de este tipo de correo con tan sólo abrir estos mensajes.
2. **No respondas a los mensajes de correo electrónico no deseados** a menos que estés totalmente seguro de su origen.
3. **Piensa dos veces antes de abrir archivos adjuntos o hacer clic en vínculos incluidos en mensajes instantáneos o correos electrónicos,** aunque conozcas al remitente. Si no estás seguro, elimina el mensaje. Si fuera imprescindible, guárdalo primero en tu disco duro , y usa tu antivirus antes de abrirlo.
4. **No reenvíes mensajes de correo electrónico en cadena.** Además de perder el control sobre quién pueda ver tu dirección de correo electrónico, podrías contribuir a la transmisión de un virus o un mensaje falso. Piensa que muchos de estos mensajes se utilizan a veces para recabar datos disfrazados de una buena causa: buscar una niña perdida, recabar firmas para un niño que necesita dinero para una operación urgente... ¡Siempre te piden que lo mandes "en cadena" a todas las personas que puedas!
5. **No proporciones datos personales en chats o por medio de correos electrónicos.** Podría tratarse de un engaño. Los sitios de confianza nunca piden así estos datos. Si recibes una solicitud de este tipo de una empresa en la que confías, comprueba la autenticidad del mensaje antes de responder. El teléfono es también un buen método para asegurarse.

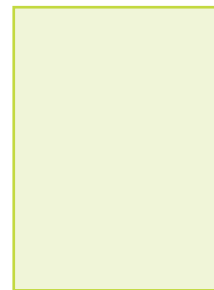


ACTIVIDAD. ALTERACIÓN DE IMÁGENES

Hay personas que ocultan su identidad y buscan averiguar información personal de otros utilizando nombres y otros datos falsos. Pueden pedirte datos como tu nombre y apellidos, tu DNI, tu correo electrónico, dirección, gustos o contraseñas, así como **tu foto**.

Si envías **fotos tuyas, de tus familiares o amigos** a sitios de Internet que no conoces pueden ser utilizadas para cosas muy diferentes a las que te imaginas.

Por eso, evita enviar y compartir fotos personales con estas personas. Una foto es para siempre. Piénsalo.



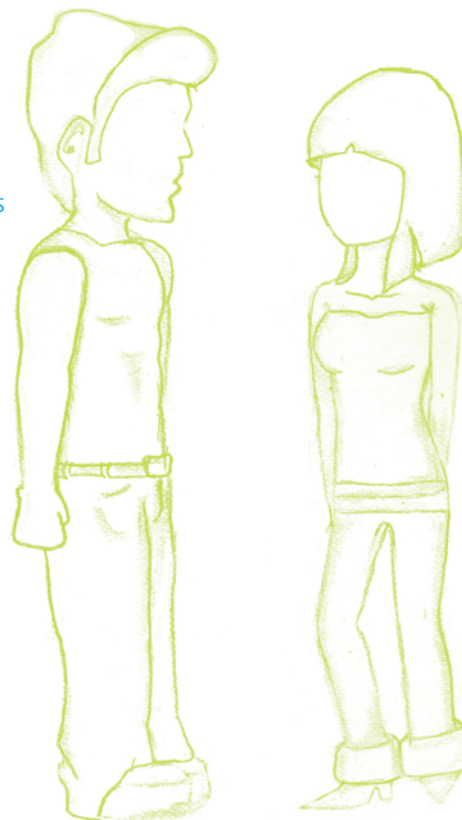
Mi foto

El *Bluetooth* de los teléfonos móviles es una forma muy sencilla y rápida de compartir fotos, programas y archivos. Ello incrementa el riesgo de que entren virus o te envíen *spams*. Ten precaución.

¿Sabías que a través de un programa de ordenador se cambian las fotos e imágenes, pudiendo ponerte junto a otras personas, en otros lugares, e incluso alterar la ropa, el pelo, etc?

Toma estos dibujos como una práctica y cambia tú mismo la imagen de estas personas, alterando el pelo, los rasgos de la cara, la altura, la forma de vestir...

Todo esto podría ser posible mediante cualquier programa de tratamiento de imágenes de tu ordenador.



RECUERDA

DAR TUS DATOS PERSONALES A DESCONOCIDOS MIENTRAS ESTÁS EN INTERNET ES PELIGROSO.

PROBLEMA 2. ENCUENTROS CON PERSONAS DESCONOCIDAS POR MEDIO DE LA RED (“ON LINE”) O REALES (“CITAS A CIEGAS”)

Piensa la cantidad de horas que pasamos frente a la presencia luminosa de una pantalla. Pantallas en casa, en el trabajo, en la calle, en los bares, en los bancos, en el metro, en el coche, pantallas de bolsillo en las agendas electrónicas, en las calculadoras, en los teléfonos móviles... Las pantallas nos seducen ocupando un espacio creciente en nuestras vidas.

Hoy, millones de hombres y mujeres de todas las edades utilizan las posibilidades que les ofrecen las Redes para comunicarse con personas a las que ni siquiera conocen físicamente. Muchos de ellos lo hacen para entretenerse, otros buscan amigos con los que compartir buenos momentos y hay quienes están a la búsqueda de “una relación sentimental”. Incluso hay personas que prefieren el contacto por medio de una pantalla y un teclado a encontrarse “cara a cara”. Sustituyen los gestos, las miradas, la presencia en general, por varios “clicks” del ratón. Internet aparece como un canal para facilitar las relaciones afectivas mediante herramientas como el correo electrónico, el chat o los sitios web.

En nuestro estudio nos habéis manifestado en un 70% que vuestra forma preferida de relación es el **chat**, y llega a ocupar hasta la mitad del tiempo en que estáis conectados. Como muchos de vosotros ya sabréis, el chat es como una gran sala de reuniones donde quien entra se encuentra de manera virtual con un montón de gente con la que puede compartir textos, voz, fotos, vídeos o programas desde su ordenador. En algunos casos se aprovecha para quedar en un lugar determinado. Son las “citas a ciegas”, que suelen ser muy peligrosas. Puedes pensar que muchas de estas personas son como tú en edad, gustos..., y tal vez no sea así. No conoces sus intenciones. Algunas pueden ser mayores de lo que dicen ser y con intenciones dudosas. Un 20% de las encuestas manifiestan que alguna vez habéis recibido alguna propuesta de este tipo. Los datos dicen que el 95% de los pederastas (mayores de edad que abusan sexualmente de menores), conocen a sus víctimas a través de los chat.



La realidad también puede engañarnos. Tiene muchas caras y, a veces, sólo vemos una. Te proponemos un pequeño juego. Observa la imagen de esta dama. Lleva un pañuelo en la cabeza y una pluma en el pelo. Calcula su edad y discútelo con tus compañeros.

Como has podido comprobar, a veces no nos ponemos de acuerdo en algo “aparentemente” fácil a la vista.

Quizás ya conoces el mito griego de Narciso. La versión del escritor clásico Ovidio nos cuenta que un día Narciso sintió sed y se acercó a beber a un arroyo, quedando fascinado por la belleza de su reflejo. Ni siquiera se atrevió a beber por miedo a dañarlo. Incapaz de dejar de mirarlo día y noche, finalmente murió contemplando su imagen. La flor que lleva su nombre creció en el lugar de su muerte (puedes ampliar esta información en Internet).

Observa el siguiente cuadro del pintor catalán Dalí en el que se representa este mito y describe el lugar en el que sitúa al personaje y los objetos que aparecen. Hablando de ordenadores, ¿qué crees que podría ser el fondo de agua cristalina en el que se mira Narciso?



“La metamorfosis de Narciso” (Salvador Dalí, 1937)

Escribe tus propias conclusiones de ambas actividades en relación a lo que estás aprendiendo:

Imagen de la dama:

.....

.....

Mito de Narciso:

.....

.....

RECUERDA

SI TE APETECE QUEDAR CON ALGUIEN QUE HAS CONOCIDO POR MEDIO DE LA RED DEBES CONTÁRSELO A ALGÚN ADULTO DE TU CONFIANZA.

PROBLEMA 3. ACOSO POR MEDIO DE INTERNET O DEL TELÉFONO MÓVIL (“CIBERBULLYING”)

En Internet, como el mundo real, existen personas en las que confiar y otras que intentan fastidiar en todo momento. Imagina que pudieran, de forma ANÓNIMA, usar internet a través del ordenador o el teléfono móvil para humillar, agredir, maltratar, insultar, amenazar o desprestigiar a los demás. Piensa que el anonimato puede ser el mejor disfraz que les sirve de refugio para enviar mensajes desagradables (violentos o de contenido sexual) o inventar historias que hagan sentirse mal a otros.

Muchas veces utilizan las fotos que sus “víctimas” tienen colgadas en Internet en su espacio personal (página web o blog), o incluso se cuelan en sus ordenadores mediante virus para robarles sus fotos, manipularlas y exponerlas en Internet avergonzando y humillando a la persona.

Normalmente suelen utilizar:

- El correo electrónico, la entrada en un chat o el envío de mensajes en el móvil.
- La participación en juegos de la Red, solicitándote información personal o determinadas tareas. Todo para permitirte “subir un nivel” del juego.

Si alguien te envía información desagradable en un chat, lo mejor es borrarle de tu listado de contactos. Esa persona no sabrá quién lo ha hecho. Nunca contestes a sus mensajes ni devuelvas sus llamadas. Lo mejor es no facilitar tu dirección de correo electrónico ni el número de tu teléfono móvil a desconocidos. Recuerda que si has facilitado estos datos, una vez ya grabados, son de dominio público y mucha gente tiene acceso a ellos.

En las encuestas realizadas, los insultos y la pornografía son los contenidos no deseados que más habéis recibido en vuestro ordenador o móvil (en dos de cada diez veces).



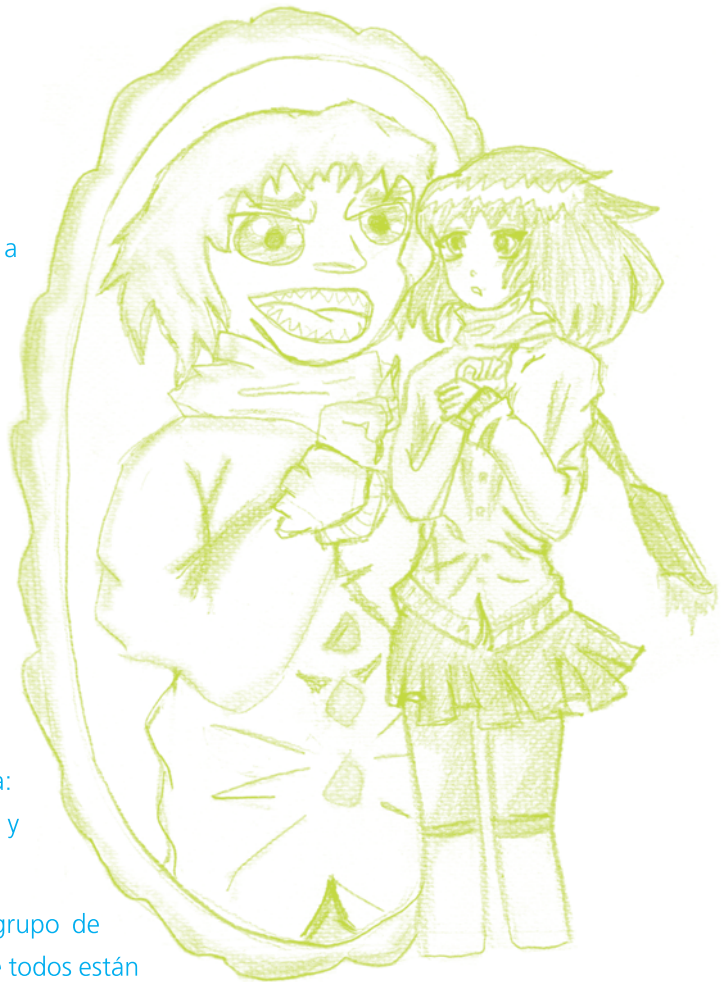
ACTIVIDAD. EL ESPEJO DE BLANCANIEVES

En este contexto, te proponemos que redactes un cibercuento basado en el clásico de “Blancanieves y los siete enanitos” utilizando los mismos personajes del cuento pero adaptados al tema que estamos tratando. Para ello te damos algunas pistas para que veas las semejanzas:

- reina malvada = el acosador
- espejo = pantalla del ordenador
- persecución a Blancanieves = acoso y persecución a alguien conocido
- siervo o vasallo de la reina = el enviado para acosar
- los enanitos = grupo de amigos
- casa de los enanitos = el refugio
- príncipe = persona que ayuda
- beso = solución ???

Escribe el final que quieras pero no te olvides de introducir en algún momento una frase parecida a: “Espejito, espejito mágico, ¿Quién es la mujer más bella y hermosa del Reino?”.

Y si te animas, puedes grabarlo en vídeo junto a tu grupo de amigos y presentarlo a tus compañeros (asegúrate de que todos están de acuerdo).



UN CASO REAL DE CIBERBULLYING

Para que completes tu información sobre esta forma de acoso te exponemos una noticia sobre un caso real. Lee atentamente la noticia y no olvides seguir nuestros consejos, ponerlo en conocimiento de tus padres o profesores e incluso denunciar el caso ante la Oficina del Defensor del Menor o la Policía 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 desvestiéndose 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.

PROBLEMA 4. FRAUDES POR MEDIO DE INTERNET

Te sorprendería saber que en España ha aumentado el número de compras por Internet en un 80% en el último año. Esto lo saben muy bien los ladrones informáticos, los “hackers”. Por ello, te recomendamos seguir estas señales de seguridad.

La URL o dirección del navegador debe comenzar con **https**: donde la “s” significa “Seguro”. Ejemplo:

[https:// www.tumejorbanco.com](https://www.tumejorbanco.com)

También es importante localizar el icono del candado en la barra de estado (parte inferior) del explorador.

Para saber si el sitio web en el que estás, 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 estás se trata de una web falsa.



Debes, en la medida de lo posible, conectarte desde un sitio seguro, como tu casa. Los sitios públicos como cibercafés, locutorios y bibliotecas son lugares más fáciles para que personas con malas intenciones puedan registrar todo lo que escribas en el teclado y apoderarse de tus datos confidenciales.

PHISHING, LA GRAN AMENAZA



Si sabes inglés seguramente al pronunciar la palabra “phishing” habrás imaginado su significado. Mirando los dibujos anteriores, intenta explicar en qué consiste.

.....

.....

.....

.....

.....

Vamos a profundizar un poco más en este tema.

Se habla de *Phishing* como el uso de técnicas para suplantar la personalidad y robar **la Identidad Electrónica** de alguien, logrando con ello tener acceso a áreas o servicios privados de manera ilegal.

¡Un auténtico delito de fraude!

¿QUÉ ES LA IDENTIDAD ELECTRÓNICA?

En Internet, para nuestra seguridad, todos disponemos de un **Nombre de Usuario** y una **Contraseña** que nos permite entrar en el ordenador a sitios privados, como el correo electrónico, o la Banca por Internet y a otros sitios públicos. Posiblemente habrás visto a tus padres acceder a su cuenta del banco, hacer o consultar la declaración de la Renta por Internet.

Unas veces inventas tu propia identidad electrónica y otras te la facilitan ya hecha (un banco o cualquier otro organismo), pero es conveniente cambiarla enseguida. A esto se le llama “personalizar”.

Vamos a hacer un ejercicio mental de letras. Esta es la identidad de alguien de tu edad. Haz de detective y descubre su verdadero nombre y contraseña. Escríbelos en la parte derecha:

Nombre de usuario: Mrt lpz frndz

Nombre de usuario:

Contraseña secreta: ## ## ####

Contraseña:

(La solución la puedes encontrar al final del Manual). Si has acertado, saca tus propias conclusiones.

Imagina ahora que un delincuente se apodera de la identidad electrónica de tus padres en su banco y quiere su dinero. ¿Cómo podría robarlo? Coméntalos con ellos en casa.

Los *Phishers* (delincuentes que llevan a cabo la actividad de *Phishing*) utilizan una combinación de ingeniería social y elementos técnicos para apropiarse de la Identidad Electrónica de alguien.

El procedimiento más utilizado es enviar correos electrónicos falsos diseñados para atraer a las víctimas hacia sitios igualmente falsos. El proceso típico es el siguiente:

1. Se difunde de forma masiva un mensaje (*spam*) en el que se informa de que los usuarios del “caja-bancoX” deben confirmar sus datos de acceso (identidad electrónica) a su cuenta bancaria.
2. El mensaje incluye un enlace a una página desde la que debe realizar la confirmación de sus datos personales.
3. El usuario accede al enlace que lleva a una página “similar” a la auténtica de “caja-bancoX” y con toda confianza introduce en ella tales datos. ¡Ya tiene la llave de entrada!
4. Como la página es falsa y está controlada por los estafadores, son ellos los que realmente reciben los datos del usuario, y con ellos tienen libre acceso a la cuenta real del usuario estafado y pueden sacar o gastarse todo su dinero.

Para que lo entiendas mejor, aquí tienes un ejemplo real de correo electrónico *phising* encontrado en Internet.

Una vez leído este ejemplo, completa los datos que te pedimos en este ejercicio para ayudarte a entender mejor el procedimiento que emplean los phishers (sigue los números):



1. Te envían este “spam” con el nombre de un supuesto banco llamado.....
2. Sin embargo, quién realmente envía el mensaje es....., con lo que no ves vinculación alguna con ese banco.
3. Identifica el asunto del mensaje así como el texto que escribe a continuación y explica qué quiere decir. ¿A qué datos se refiere tratándose de “Bancolombia”?
4. Si se colocara el ratón en el punto 3, tendrías un enlace hacia una página que simularía ser el banco, pero que en realidad es la página web de un estafador.

Si eres buen detective encontrarás en algún sitio la dirección real desde la que se envía el mensaje spam:..... ¡Ya les tenemos! No borres la prueba y acude a un adulto para que te aconseje.

RECUERDA

Ante este tipo de problemas, lo primero que debes hacer es contar a tus padres o a un adulto responsable lo que pasa, quién/es serán capaces de ayudarte. Si alguna vez llegas a estar en apuros, piensa que no eres el único que ha podido hacer algo equivocado.

Capítulo 3

EL CORREO ELECTRÓNICO

El correo electrónico, o en inglés “**e-mail**” (electronic mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente mediante sistemas de comunicación electrónicos. Su nombre proviene de su parecido con el correo postal y utiliza “buzones” intermedios, llamados servidores, en los que se guardan temporalmente los mensajes antes de dirigirse a su destino y de que el destinatario los reciba. Se requiere una dirección de correo electrónico que sea personal y única para cada usuario.

Cuando vayas a hacerte una cuenta de correo, ten en cuenta las siguientes sugerencias:

1. **Crea una dirección que no sea muy “típica”.** Evita usar datos fáciles y que revelen tu identidad (nombre, año de nacimiento...). Prueba a usar combinaciones de letras, números y otros caracteres, por ejemplo *pepo2lea4@.....com*.

Inventa ahora una que nunca vayas a utilizar.

.....@.....

2. **Disfraya tu dirección de correo electrónico** cuando la utilices en chat, foros de discusión o cualquier otro tipo de página Web. Copia de nuevo la anterior dirección que escribiste, pero sustituye ahora el símbolo (@) por la palabra *arroba* y el símbolo (.) por la palabra *punto*.

3. **Cuidado con las casillas marcadas de forma predeterminada.**

Algunas empresas incluyen casillas para indicar que cuentan con tu consentimiento para vender o proporcionar tu dirección de correo electrónico a otros. Si no estás de acuerdo, señálalo.

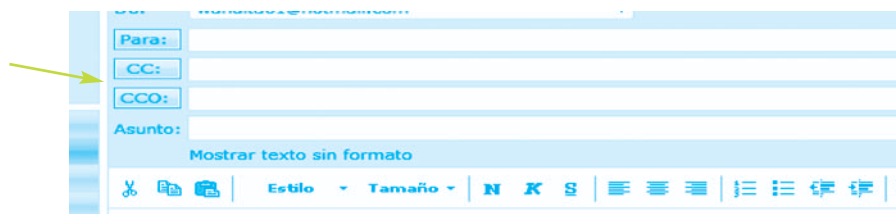
De lo contrario e inadvertidamente, podrías conceder tu permiso para que estas empresas compartan con otros tu información personal.

4. Cuando envíes mensajes a varias personas acuérdate de incluir sus direcciones 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 dónde pueden ir a parar! Un procedimiento para enviar mensajes con copia oculta puede ser el de buscar la opción de mostrar CC (copia) y CCO (copia oculta) e introducir las direcciones de tus destinatarios en la barra de CCO.



Pincha y te aparecerá esto:



Escribe las direcciones en la barra CCO.

Tu dirección de correo electrónico debes usarla, preferentemente, para las personas que conoces o que te dan seguridad.

Recuerda que también en tu teléfono móvil quedan grabados los nombres de las personas con las que has hablado o los mensajes enviados.

Observa en la siguiente página los datos que suelen pedirte para registrarte como usuario de una cuenta de correo:

¡BIENVENIDO!

Si quieres disponer de una cuenta de correo electrónico con nosotros sólo tendrás que contestar unas preguntas, escoger tu nombre de usuario y contraseña y ¡listo!

1. Tus datos personales

1.1 Nombre:

1.2 Sexo:

1.3 Fecha de nacimiento:

1.4 Lugar de nacimiento:

1.5 Código postal:

2. Selecciona tu ID (nombre de tu nueva dirección de correo) y contraseña

.....@.....com

Sólo se permiten letras, números, guiones bajos y un solo punto (.) 8 caracteres.

Ej: pepa4.lea @.....com

Si no está disponible la ID que quieres usar, cambia letras o un número para que sea única.

2.1 Contraseña

2.2 *Repite la contraseña (seguridad)

Por si olvidas tu contraseña, te damos una pregunta de seguridad:

Final del formulario

¿Estás de acuerdo?

Al marcar esta casilla, indicas que has leído y aceptas las condiciones de servicio y las del centro de privacidad, y también aceptas recibir las notificaciones oportunas en formato electrónico que te envíe esta empresa u otras.



Capítulo 4

NUESTROS DERECHOS

4.1 SOMOS CIUDADANOS: PROTECCIÓN DE DATOS PERSONALES

Piensa que, como ciudadanos residentes en España, y amparados por la Constitución Española (artículo 18), tenemos derecho al honor, a la intimidad personal y familiar y a la propia imagen así como a la protección de nuestros datos personales.

Son aquellos que nos permiten reconocernos como individuos únicos y diferenciados ante los demás: el nombre completo, la dirección de nuestra casa, las fotos propias o de la familia, la voz grabada en cualquier aparato, las huellas de los dedos de la mano...Nos pertenecen en propiedad desde el momento en que nacemos.

Cuando facilitas estos datos a una entidad (colegio, banco, club o ayuntamiento...) o alguien se hace con ellos, éstos son guardados en un fichero manual o informático, existiendo un RESPONSABLE del mismo, quien informa sobre su finalidad, contenido y uso; debe, además, guardar secreto absoluto sobre su contenido y tenerlos custodiados en un lugar seguro.

Ante él podemos ejercer nuestros derechos y de manera gratuita. Para los menores de 14 años lo harán sus padres o tutores. En tu colegio o instituto a la persona a la que te puedes dirigir como primer responsable suele ser el Director o el Secretario del centro.

También los Estatutos de Autonomía amparan y refuerzan estos derechos.

Estos son tus derechos:

1. Derecho de acceso a mis datos

Es la posibilidad de conocer los datos personales que otros tienen archivados o recogidos sobre ti, su origen y las comunicaciones o cesiones que se hayan hecho a otros o se vayan a hacer. Si queremos saberlo, nos dirigiremos al responsable del fichero, quien tendrá un plazo máximo de un mes para contestar.



2. Derecho de rectificación. Derecho de cancelación

Si creo que los datos que existen en ese fichero son erróneos, incompletos o inadecuados porque no son necesarios para el fin que se pretende, lo haré saber a su responsable para que:

- Rectifique los datos.
- Cancele los datos, los bloquee para que no puedan ser usados ni tratados e incluso los borre definitivamente.

Las solicitudes también las dirigiré al responsable del fichero, quién atenderá mi petición en un plazo de 10 días.

3. Derecho de oposición

También puedo solicitar que no se traten algunos de mis datos personales. Por ejemplo, que el número de teléfono de mi casa no aparezca en la guía telefónica de mi localidad.

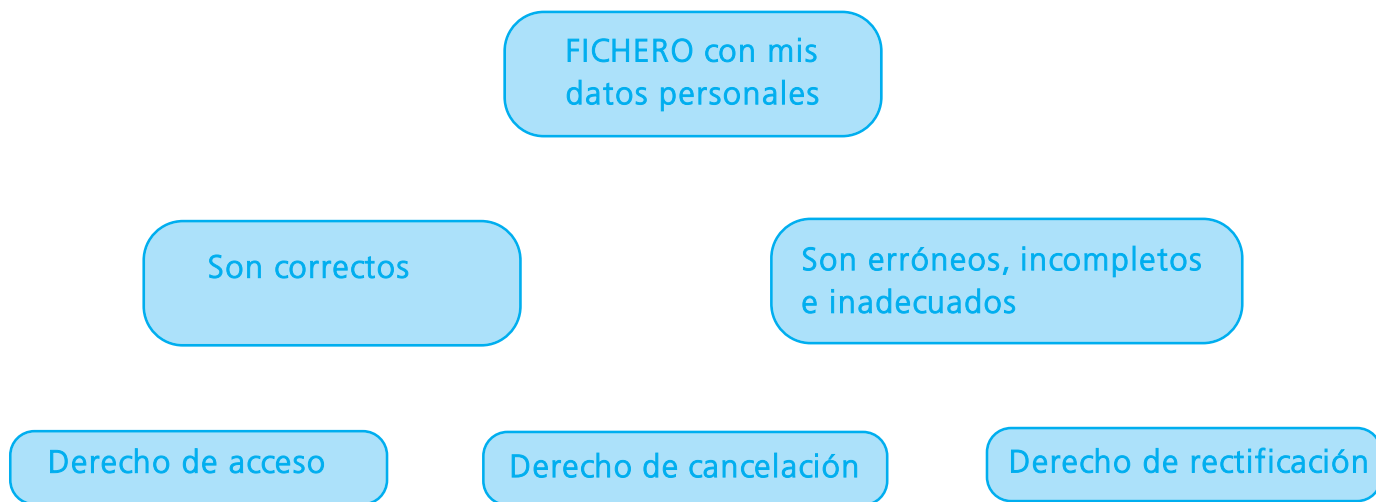
No olvides que:

- Eres el dueño absoluto de tus datos personales y no estás obligado a dárselos a nadie, excepto si una ley te obliga.
- Siempre tienes el derecho a controlarlos en todo momento y a saber qué hacen con ellos.
- Puedes dar tus datos y permitir su uso si eres mayor de 14 años. Si eres menor, sólo tus padres pueden hacerlo.
- Nadie, en ningún caso, puede obligarte a dar datos referidos a tu ideología, religión o creencias personales ni pueden ser usados sin tu consentimiento expreso y por escrito. Aquellos sobre tu salud, origen racial o vida sexual sólo podrán ser recogidos en el caso de que exista una Ley que lo disponga por razones de interés general.



- Desconfía de personas que solicitan tus datos personales con la excusa de querer completar los ya existentes. Piensa que los han podido obtener por Internet (concesión de becas para estudio, inscripción o participación en carreras o eventos deportivos, datos de tus padres, etc).
- Cuando te soliciten tus datos personales por cualquier medio, ya sea por teléfono, por escrito o por Internet, debes avisar a tus padres, por que tú y ellos debeis saber quién los necesita y para qué , dónde los van a tener guardados, de qué manera los van a tener seguros y quién es el encargado de utilizarlos.
- El responsable del fichero ha de pedir siempre MI CONSENTIMIENTO para ceder mis datos a otra entidad o empresa y debe informar siempre de la existencia de ese archivo, contenido, para qué va a usarlo, el origen de los datos, cómo los consiguió, tus derechos, quién son los destinatarios de la información, la identidad del responsable y la dirección.
- Siempre que se recojan tus datos deben figurar claramente los derechos de los que hemos hablado. Léelos tranquilamente con tus padres. 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)”.

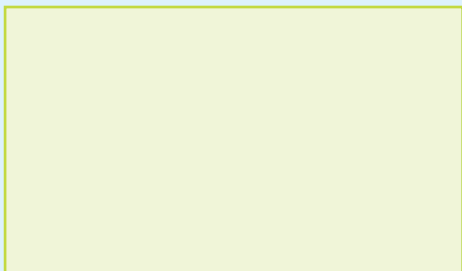


Te proponemos ahora un ejercicio práctico para aplicar estos derechos, mediante el estudio de un caso encontrado en Internet.

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

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.

4. Si facilitas tus datos, ¿Cuáles crees que deberían ser especialmente protegidos?

5. Ya sabes que tus datos personales pueden guardarse de manera manual o en un fichero informático. ¿Qué nivel de seguridad debe tener la empresa para guardarlos?

6. Existe una Ley de Protección de Datos Personales. Si se infringiera, ¿quién sería el responsable?

7. Imagina que, pasado un mes, alguien vinculado al programa aparece en la casa del concursante vendiéndole equipos de música y karaokes. ¿Qué debería haber solicitado el dueño de la empresa GLOBO TOUR RTV S.A. al concursante para poder usar esos datos de la manera que considerara más oportuna para otros fines?

8. Imagina que quieres denunciar a la productora por hacer un mal uso de los datos de que dispone.

Cumplimenta, junto a tus padres o profesor, el modelo de denuncia que te facilitamos a continuación:

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 D.N.I..... 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, País Vasco y Madrid, también se pueden interponer denuncias. Las puedes encontrar en los sitios web:

- Catalunya: “Agencia Catalana de Protecció de Dades” www.apd.cat
- País Vasco: “Agencia Vasca de Protección de Datos” www.avpd.euskadi.net
- Madrid: “Agencia de Protección de Datos de Madrid” www.apdcm.es

4.2 SOMOS PERSONAS

La Convención Internacional de los Derechos del Niño establece que TODOS los niños y niñas tienen derechos que deben ser respetados y promovidos por todas las personas.

Algunos de estos derechos son:

- Derecho a la protección contra toda forma de malos tratos (Art. 19).
- Derecho a un nivel de vida adecuado para su desarrollo físico, mental, espiritual, moral y social (Art. 27).
- Derecho al descanso y el esparcimiento, al juego y a las actividades recreativas propias de su edad (Art. 31).
- Derecho a ser protegido de toda forma de explotación que sea perjudicial para cualquier aspecto de su bienestar (Art. 36).



Capítulo 5

CONSEJOS PARA PADRES, MADRES O TUTORES

Internet puede ser un lugar excepcional para que los niños aprendan, se entretengan, charlen con amigos del colegio o, simplemente, se relajen y exploren. Pero al igual que el mundo real, la Web puede ser peligrosa para ellos. Antes de dejar que su hijo se conecte sin su supervisión, asegúrese de establecer un conjunto de reglas que todos puedan aceptar.

En nuestro estudio hemos detectado algunos datos preocupantes relativos a la facilidad de los jóvenes de esta edad a facilitar sus datos personales. Cerca de un 35% lo hacen sin problemas para ingresar en un club virtual o para hacer un casting, porcentaje que se supera al dar su e-mail o su número de teléfono móvil. Datos que además aumentan con la edad hasta los 17 años.

Si no sabe dónde empezar, a continuación le ofrecemos algunas ideas que puede comentar con ellos para enseñarles a utilizar Internet de forma segura.

DE CARÁCTER GENERAL

1. Intente estar al día en cuestiones de Internet y el teléfono móvil. Cuanta más información tenga acerca de estas tecnologías, mejor podrá ayudar a sus hijos a que hagan un buen uso de ellas.
2. Mantenga un diálogo fluido sobre lo que hacen en Internet, con quién hablan o qué paginas web visitan más. Establezca entre todos, unas reglas básicas de uso y consumo de las tecnologías. Disfrute de Internet con ellos.
3. Es recomendable que sitúe el ordenador en un lugar común de la casa. No es recomendable que tengan el ordenador en una habitación sin control.
4. Controle el tiempo que pasan sus hijos en Internet o usando el teléfono móvil. Establezca unos horarios de uso que se adapten al tiempo de estudio.
5. Dígalos que no deben acordar una cita “en persona” con amigos conocidos por Internet o por el teléfono móvil. Explíqueles que los amigos “en línea” pueden no ser quienes dicen ser.

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 usuario del ordenador puede y no puede hacer.
9. 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 compruebe 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.

10. Preste atención a los juegos que se descargan o intercambian con amigos. Asegúrese de que el contenido es adecuado para su edad y no incluye algún tipo de violencia.
11. 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 una web deben hacerlo sin infringir las leyes de derechos de autor.

SOBRE LA PROTECCIÓN DE DATOS PERSONALES

12. Hable con sus hijos de la importancia de proteger nuestros 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.
13. 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.

Capítulo 6

CONSEJOS PARA ESTUDIANTES

SOBRE EL USO DE LAS TIC

Para navegar por la Red sin tener problemas deberías:

1. Tener una contraseña secreta que no facilite información personal. No uses nunca tu nombre real. Si usas mensajerías o entras en chats privados, hazlo sólo con tus amigos. ¡Nunca hables con desconocidos!
2. Aprender a usar y mantener actualizado tu antivirus y otros bloqueadores. Así evitarás que entren espías que podrían tener acceso a la información que guardas en él.
3. No abrir ficheros ni mensajes de desconocidos así como descargar programas que no conoces.
4. Si abres un blog o tienes un espacio personal en la Red, invitar sólo a tus amigos a que puedan entrar. Si no es así, ¡tus datos podrían estar en manos de cualquiera!
5. No dar nunca tus datos personales a desconocidos: tu nombre o apellidos, dónde vives, tu usuario de Messenger, tu número de teléfono (móvil)...



Recuerda usar el ordenador y el teléfono móvil siguiendo los consejos de tus padres, tutores o profesores. Consúltales cualquier duda que tengas.

SOBRE LA PROTECCIÓN DE TUS DATOS PERSONALES

Imagina que en tu colegio una empresa está seleccionando a los mejores dibujantes de tu clase para ilustrar un libro de cuentos. Los más originales tendrán como premio un reproductor de música de última generación. Junto a los dibujos te solicitan que rellenes un formulario con tus datos personales. Recuerda que esa empresa debe:

6. Informarte para qué se van a utilizar, así como tus derechos en este tema: acceso a los datos que tiene sobre ti, rectificación (si son inexactos o excesivos), cancelación y oposición a esos datos.
7. Pedir tu consentimiento para su uso o tratamiento. Si eres menor de 14 años lo harán por ti tus padres o tutores.
8. Solicitarte sólo los datos necesarios para su finalidad (ej: para ingresar en un club deportivo no han de pedirte tus gustos musicales, ¿no crees?).
9. Hacer que estén seguros y se guarden con secreto.

Recuerda que existen organismos como la Agencia Española de Protección de Datos así como las Agencias Autonómicas (Madrid, Cataluña y País Vasco) que siempre te podrán ayudar gratuitamente ante cualquier tema que no conozcas.

Solución actividad problema 4

Nombre de usuario: marta lopez fernandez

Contraseña: aa oe eae

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 Zaroobe	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