@ctitud digit@l

Enric Bruguera Payà

P08/74506/01694

Universitat Oberta de Catalunya
www.uoc.edu

Índice

1. Utilizamos dispositivos electrónicos

Los ordenadores y los dispositivos informáticos nos permiten trabajar con informaciones digitales, comunicarnos con otros usuarios e interactuar con ellos. En su interior almacenan datos y documentos que para nosotros son importantes. De su mantenimiento y cuidado va a depender siempre el nivel de eficiencia con el que podremos utilizarlos individualmente y el grado de convivencia razonable con el que podremos desenvolvernos en los distintos ámbitos sociales electrónicos.

1.1. El ordenador

El ordenador es la principal herramienta que os permite trabajar con la información digital, comunicaros con fuentes de datos e interactuar con los otros usuarios. Es, por tanto, un instrumento fundamental de cuya utilización razonable va a depender la mayor, menor o nula eficacia de vuestras acciones de trabajo, ocio e interacción en el mundo electrónico. Y es, a la vez, vuestra herramienta básica de comunicación y convivencia con el resto de usuarios de las redes y dispositivos digitales.

Si utilizáis el ordenador personal, recordad que en él habéis ido depositando datos e informaciones que no deberían quedar a disposición de otros usuarios. Para ello es conveniente que seáis muy estrictos con las personas a las que dejáis acceder a vuestro terminal y que tratéis con el máximo respeto y prudencia los dispositivos electrónicos ajenos.

Si compartís el ordenador con otros usuarios, es aconsejable que eliminéis regularmente la información y los datos innecesarios y que trasladéis a otros dispositivos de almacenamiento –unidades portátiles de memoria como discos duros externos, lápices USB, CD...– los datos e informaciones que queréis preservar de miradas indiscretas. También podéis cifrar mediante contraseña la parte del disco duro a la que no queráis que nadie más pueda acceder. Cuando utilicéis ordenadores de otros usuarios o terminales instalados en espacios públicos (bibliotecas, cibercafés, etc.) podéis mejorar la seguridad y privacidad de los datos con unas sencillas medidas de precaución:

- Si habéis navegado por Internet, cerrad el navegador cuando terminéis la sesión y antes eliminad el historial de navegación (**Herramientas>Opciones>Privacidad**).

- No automaticéis el recuerdo de las contraseñas ni en el sistema operativo ni en el navegador.

- Evitad introducir datos personales, realizar operaciones comerciales o efectuar transacciones bancarias desde ordenadores y redes que no sean de total confianza.

- En todos los casos, preservad la privacidad de los datos personales (teléfono, dirección postal, etc.) con especial atención a los números del documento nacional de identidad y de las tarjetas de crédito.

1.2. La contraseña

Las contraseñas son un instrumento fundamental básico para controlar y restringir el acceso a los dispositivos electrónicos y a la información que contienen.

Un uso razonable y cuidadoso de las contraseñas nos evitará intrusiones indeseadas en los equipos, intromisiones en nuestra privacidad y la captura de datos personales por parte de terceras personas. Aunque existen individuos y programas informáticos capaces de reventar cualquier contraseña digital, en una aplastante mayoría de casos el robo o el descifrado de las claves personales son debidos a una gestión deficiente o descuidada del usuario. Para un uso eficiente y razonable de las contraseñas, os vendrá bien tener en cuenta lo siguiente:

- Idear contraseñas de ocho caracteres como mínimo, que combinen números y letras y varíen éstas en mayúscula y en minúscula.

- No utilizar como contraseña datos personales fáciles de averiguar, como la fecha de nacimiento, el nombre, los apellidos, el número de teléfono o la dirección de correo electrónico.

- Evitar escribir las contraseñas en papel o en documentos electrónicos almacenados en el mismo dispositivo.

- Como medida de precaución resulta muy efectivo cambiar con regularidad las contraseñas que tenemos establecidas para cada sistema y cada fichero.

- También es recomendable evitar el uso de palabras del diccionario en cualquier idioma, ya que algunos programas informáticos basan su método de ataque en la morfología de las palabras.

- No enviar nunca contraseñas en mensajes de correo electrónico ni incluirlas en conversaciones de mensajería instantánea.

- Es aconsejable no utilizar las mismas contraseñas en todos los sistemas o ficheros y disponer de claves de alta seguridad para acceder a aquellos enclaves de Internet que no nos ofrezcan garantía absoluta de seguridad.

Es imprescindible que mantengamos, respecto a las contraseñas ajenas, el mismo grado de discreción y respeto que exigimos para nuestras propias claves personales.

1.3. Programas

De los programas informáticos depende la gestión y la conservación de los datos, documentos y capacidad de interacción en la Red.

Podemos utilizar programas comerciales de pago (*software* propietario), programas abiertos de uso libre (*freeware*), programas de uso limitado (*sharewa-re*)... Cualquier opción puede ser legítima y adecuada, siempre que tengamos en cuenta lo siguiente:

- Nos aseguremos de utilizar programas informáticos legales (sean comerciales o de uso libre y abierto). La informática ilegal puede ser una fuente de virus, intrusiones ilícitas y problemas jurídicos.

- Nos presenten opciones de actualización regular.

- Hagamos un pequeño esfuerzo permanente de información sobre su funcionamiento, las actualizaciones y las opciones de seguridad.

El mejor programa para una funcionalidad determinada puede sernos absolutamente inútil si descuidamos nuestra responsabilidad en la información, básica pero constante, sobre su manejo seguro y actualización. Y, en la misma medida, un uso cívico de los programas informáticos nos ayudará a contribuir a una mejor convivencia entre los usuarios y a frenar fenómenos antisociales como la piratería y la copia indiscriminada de programas comerciales, la manipulación y alteración ilícita de programas abiertos o las iniciativas masivas de fraude, extensión de virus y programas maliciosos y captura indeseada de datos personales privados.

1.4. Seguridad

Los temidos virus informáticos constituyen una amenaza importante en la sociedad digital. Pero el primer peligro es no tomar medidas para garantizar la integridad de los dispositivos informáticos y de la información que almacena-

mos en ellos. Por eso, es imprescindible usar **siempre** un buen antivirus para detectar y neutralizar cualquier programa que pueda contaminar o dañar los ficheros, así como programas de seguridad que impidan que cualquier intruso pueda acceder al ordenador o a nuestros datos. Así, al usar programas de seguridad actualizados:

- Preservamos los ordenadores y la información.
- Garantizamos la privacidad de nuestros datos personales.
- Evitamos convertirnos en distribuidores de infecciones informáticas a otros usuarios y ser cómplices involuntarios de intrusiones dañinas en sus ordenadores.
- Contribuimos a una mayor fluidez de comunicación en los entornos digitales y ayudamos a optimizar el funcionamiento colectivo de las redes y de los ámbitos de convivencia que generan.

1.5. Antivirus

Los programas antivirus son herramientas informáticas específicamente diseñadas para detectar, neutralizar y eliminar cualquier otro programa informático que pueda introducirse en el ordenador o en los archivos con la finalidad de dañarlos, capturar nuestra información y datos personales o dar órdenes a nuestros dispositivos sin que nosotros podamos detectar o controlar esa actividad oculta.

El uso normalizado y cotidiano de información digital y redes telemáticas hace **imprescindible** la utilización de programas antivirus para:

- Evitar la entrada de programas dañinos a través de ficheros que podemos introducir en el ordenador mediante copias o transferencias de archivos procedentes de unidades de memoria como CD, DVD, lápices de memoria, discos duros externos, etc.
- Detectar y destruir programas maliciosos que pueden colarse en el equipo desde Internet, a través de mensajes de correo electrónico, ficheros adjuntados a correos o a la mensajería electrónica, códigos maliciosos ocultos en programas de las web que visitamos en nuestro recorrido por la Red o archivos y contenidos que nos descargamos de Internet mediante cualquiera de sus canales de suscripción, captura libre o intercambio.
- Garantizar que nuestros equipos, dispositivos y ficheros están limpios y que no se convertirán en focos difusores de infección por códigos mali-

ciosos de todos aquellos usuarios con los que interactuamos en la Red o a través del intercambio de ficheros entre dispositivos informáticos o de memoria.

Por los problemas y costes que puede evitarnos, la mejor inversión en seguridad nos la proporcionará un buen programa antivirus que

- Nos garantice actualización y protección permanente ante los centenares de nuevas amenazas víricas que diariamente surgen y se expanden a través de los dispositivos y redes electrónicas globales.

- Nos permita configurar y personalizar las opciones de detección, rastreo y eliminación de códigos maliciosos.

1.6. Hábitos clave

El uso cotidiano de las tecnologías y redes digitales puede aportar a nuestra vida diaria muchas más ventajas que inconvenientes. Para conseguirlo basta con que apliquemos a su utilización los criterios razonables y de sentido común que nos resultan efectivos en los demás ámbitos de la vida personal, social, laboral y profesional.

Como usuarios de dispositivos y redes electrónicas, tenemos en nuestras manos la opción de adoptar unos sencillos hábitos cotidianos que resultan clave a la hora de facilitarnos la actividad y acciones digitales con la máxima seguridad, privacidad y sentido cívico:

- Mantener el ordenador y los programas actualizados con los últimos elementos de seguridad y operatividad que sus fabricantes –si utilizamos informática comercial– o la Red –si somos usuarios de programas abiertos– lanzan regularmente al conjunto de usuarios.

- Utilizar habitualmente programas informáticos legales, tanto si son comerciales y de pago, como si son abiertos y gratuitos.

Programas informáticos

Lo importante es conocer su procedencia, que merezcan nuestra confianza –por contrato de compra o por los conocimientos y referencias que hemos adquirido de otros usuarios– y que presenten garantías de apoyo técnico comercial o de carácter abierto.

- Estar permanentemente informados sobre novedades relativas a los programas que utilizamos y los que nos pueden interesar. Y, sobre todo, asegurarnos de conocer permanentemente las alertas de seguridad que puedan producirse para poder identificar las que pueden afectarnos.

- Utilizar de forma cotidiana y normal herramientas de seguridad como **antivirus** y **cortafuegos**.

- Realizar de forma regular copias seguridad de todos aquellos elementos (programas, archivos, fotografías, datos, etc.) que queramos poner a salvo

de eventuales fallos o intrusiones en cualquiera de las máquinas que utilizamos.

- Recordar que, como usuarios de redes, las acciones individuales de cada uno de nosotros repercuten en el conjunto de la comunidad de usuarios: un uso personal seguro y sostenible de los dispositivos electrónicos tiene una dimensión social y cívica decisiva para que el colectivo de usuarios pueda utilizar la Red con más confianza, fluidez y seguridad.

Coste económico

El coste económico que pueden tener puede llegar a representar un ahorro incalculable de tiempo y dinero ante la entrada de intrusos y virus en nuestros equipos.

2. Gestionamos información digital

Los dispositivos y programas informáticos nos facilitan la creación, captura y almacenamiento de grandes cantidades de ficheros, datos y documentos.

Un abanico de opciones para el que es conveniente que tengamos claro:

- Dónde y cómo almacenamos la información.
- De qué manera nos aseguramos su recuperación en casos de emergencia.
- Cómo nos hacemos entender mediante códigos básicos de comunicación virtual.
- Cómo protegemos los documentos de texto.
- Qué normas debemos respetar cuando utilizamos información ajena.
- Por qué no deberíamos plasmar en papel una réplica de nuestro uso de información digital.

2.1. Las memorias

Memorias

Discos duros externos, unidades de memoria flash USB, discos DVD... los dispositivos para almacenar datos cada vez presentan más y mejores prestaciones con costes cada vez más razonables.

La proliferación de dispositivos digitales de memoria crece en proporción al aumento de su capacidad de almacenamiento de datos y la progresiva disminución de los precios.

Un uso razonado de estas unidades de memoria nos permitirá:

- Duplicar datos y archivos que queramos preservar de las incidencias de los ordenadores de uso diario (archivo de fotografías, vídeos, datos personales...).

- Efectuar copias de seguridad de todo aquello que no queremos mantener en el ordenador personal, expuesto eventualmente a la mirada de otros usuarios con los que compartimos terminal o abierto a posibles accesos indeseados desde la Red.

Los dispositivos de almacenamiento de memoria contienen datos y objetos digitales que son importantes para nosotros, así que deberemos tener con ellos cuidados similares a los que prestamos a:

- Las llaves de nuestro domicilio, ya que nuestros dispositivos también contienen claves y contraseñas para acceder a las posesiones más valiosas.

- Nuestro vehículo, ya que su contenido nos permite manejar nuestra información y datos digitales y movernos en la Red.

- Nuestra documentación personal, ya que con muchos de los datos que guarda cualquier otra persona podría suplantar nuestra identidad y efectuar todo tipo de operaciones económicas y sociales en nuestro nombre.

2.2. Gestión del texto

El tratamiento de la información textual sobre soportes digitales nos permite trabajar constantemente sobre ella, introducir cambios y mejoras y generar cuantas copias necesitemos sin más límite que la capacidad de memoria de los dispositivos de almacenamiento.

Todo ello nos reporta ventajas evidentes sobre las limitaciones de los textos manuscritos o fotocopiados, pero también nos obliga a adoptar criterios eficientes para que las grandes cantidades de documentos digitales que podemos crear no nos hagan del todo imposible el uso rápido de la información que contienen.

Cuando elaboremos, modifiquemos y reproduzcamos contenidos textuales, nos ayudará aplicar hábitos de higiene digital tan sencillos como:

- Nombrar los documentos de forma clara y concisa. Así podremos identificarlos fácilmente cuando necesitemos localizar la información que contienen.

- Ordenar los ficheros correctamente.
  - Por nombre, versión y fecha.
  - Usando las carpetas de forma eficiente. De forma similar a los ficheros, el árbol de carpetas nos permitirá una localización más rápida y eficiente de los documentos si las estructuramos con nombres claros y representativos y realizamos un esfuerzo continuado de ordenación de cada archivo en la carpeta correspondiente.

Localización de documentos

Un documento llamado "currículum_versión7_2008_08_27" nos permite localizar la versión del currículum que elaboramos el 27 de agosto de 2008 y nos permite hacerlo con más rapidez que si tenemos que buscar entre la lista de documentos "currículum", "curric", "curricul", "curri", etc.

- Eliminar documentos obsoletos que ya no presentan ninguna utilidad. Su acumulación en el disco duro y dispositivos de memoria no hará más que ocupar espacio e interferir en la localización de información relevante.

Localizar documentos

Un currículum bien presentado, un trabajo escolar excelentemente elaborado o la mejor memoria anual de la empresa... son textos absolutamente inútiles si están perdidos en las entrañas del ordenador sin que seamos capaces de localizarlos de forma rápida y eficiente cuando los necesitamos.

2.3. Copias de seguridad

Las copias de seguridad nos garantizan que las informaciones y datos van a seguir estando a nuestra disposición aunque las máquinas o programas sufran cualquier fallo que los bloquee o inutilice. Es fundamental, pues, realizar copias de seguridad de todos aquellos ficheros y documentos que queramos mantener a salvo de eventuales incidencias. Una copia de seguridad de los documentos importantes (ficheros de texto, hojas de cálculo, fotografías, archivos de vídeo, etc.) nos permitirá preservar la información:

- si perdemos o nos sustraen el ordenador o el dispositivo que contenía el fichero.
- si un fallo informático bloquea o inutiliza el dispositivo.
- si una intrusión en el sistema deja los ficheros al alcance de terceras personas.
- si, por error o distracción, dañamos o borramos la información del dispositivo.

Para que una copia de seguridad sea realmente útil conviene hacerla

- con un nombre de fichero distinto al del documento original y en otra ubicación y
- trasladándola a un disco duro distinto al del documento inicial, a un dispositivo de memoria (DVD, memoria flash, etc.) o a una red.

La opción más básica y sencilla para efectuar una copia de seguridad es duplicar el fichero en otro dispositivo mediante una simple opción de **copia**. Para que esta copia resulte efectiva como opción de seguridad, deberemos tener muy en cuenta:

Copias de seguridad

Las copias de seguridad en el mismo ordenador nos serán de nula utilidad en aquellos casos en los que esta máquina quede inutilizada o bloqueada. Es más recomendable realizar copias de seguridad en dispositivos, unidades o redes externas (CD, DVD, lápices de memoria, discos duros externos, unidades compartidas, etc.) y mantenerlos en óptimas condiciones de seguridad.

- Trasladar la copia a otro dispositivo distinto.

- Renombrar los archivos copiados de forma que podamos identificarlos fácilmente sin que la duplicidad de nombres de archivos dificulte eventuales recuperaciones de la información.

- Asegurarnos de que realizamos copias de seguridad actualizadas de los ficheros que queremos preservar y destruir versiones anteriores una vez guardadas las versiones actualizadas. Esto nos permitirá localizar más fácilmente la información y no confundirnos con la actualización de los datos propios.

También nos conviene analizar las opciones de copia de seguridad que nos proporciona el sistema operativo de nuestros dispositivos electrónicos:

Fácil identificación

Una copia de seguridad del fichero curriculum.doc es aconsejable que la renombremos curriculum_2008_10_25.doc, si la hemos realizado en esa fecha (25 de octubre de 2008).

- La copia completa a todos los directorios y ficheros previamente seleccionados en el dispositivo.
- La copia incremental a los ficheros nuevos o a aquellos cuya fecha de modificación haya variado.
- La diferencial sólo duplica los archivos en cuyo contenido detecta modificaciones.

Conviene analizar las opciones de copias automatizadas y programables que nos ofrece el sistema operativo que utilizamos en cada equipo.

Web recomendada

El Instituto Nacional de Tecnología de Telecomunicaciones ofrece, además, acceso y valoración de algunas herramientas para la copia de seguridad disponibles en la Red. Para más información podéis acceder a través de:

http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=13&pagina=0

2.4. Texto eficiente

El tratamiento digital de la información que redactamos nos permite numerosas y variadas posibilidades de creación, organización y gestión de los contenidos textuales, así como innumerables opciones de combinación con sonido, imagen estática, vídeo y animación multimedia.

Todas ellas pueden potenciar y amplificar la capacidad de comunicación e interacción de los textos, siempre que tengamos presente que las funcionalidades tecnológicas no anulan ni sustituyen las normas y convenciones del texto escrito, dentro y fuera de los ámbitos digitales.

El lenguaje

El uso de un lenguaje burdo, descuidado o incorrecto despoja de toda efectividad comunicativa al mensaje mejor tratado y más vistoso desde el punto de vista digital.

Si queremos asegurarnos un tratamiento digital efectivo y eficiente de la información textual, nos conviene redactar contenidos que:

- respeten las normas básicas de la ortografía y de la sintaxis,
- estructuren nítidamente lo que queremos comunicar y
- evidencien la corrección y competencia del autor.

Corrección del texto digital

El tratamiento digital del texto permite una corrección fácil e inmediata. Y precisamente por ello, un texto digital incorrecto delata a un autor descuidado que no se ha tomado la molestia de realizar una segunda lectura y corregir fallos evidentes. También delata a un autor incompetente, que no sabe utilizar los recursos digitales mínimos de tratamiento del texto.

La efectividad comunicativa

El desorden de ideas y conceptos, las repeticiones, los razonamientos recurrentes... restan efectividad comunicativa a cualquier texto, aunque sea realizado y presentado sobre soporte digital. Además, muestran una lamentable actitud cívica de falta de respeto hacia los interlocutores.

Por sus opciones y versatilidad, el texto digital nos define. De cada usuario depende plasmar en él su nivel de conocimientos y competencia, no sólo en el dominio necesario de los mecanismos informáticos del tratamiento de texto, sino también de sus capacidades en el dominio básico de la ortografía, la sintaxis y la ordenación elemental de ideas y conceptos para expresar de forma efectiva lo que quiere transmitir. Una competencia tanto más importante en la medida en la que también expresa el sentido cívico de su autor y la capacidad de interrelación y convivencia con el conjunto de usuarios del texto digital.

2.5. Texto seguro

No es aconsejable intentar un uso normalizado de dispositivos y programas digitales desde una preocupación obsesiva por la seguridad. Resulta más práctico y efectivo adoptar como habituales hábitos sencillos de información y prevención de eventuales riesgos elementales. Cuando trabajamos con programas de tratamiento de texto, es conveniente consultar sus opciones de seguridad y protección de documentos, de forma que podamos

- restringir el acceso al fichero, seleccionando mediante contraseña qué usuarios podrán abrirlo y

- determinar con qué nivel de intervención podrá operar cada usuario que acceda al fichero: sólo lectura, edición, modificación de contenidos...

El control de los ficheros

Un control que adquiere la máxima importancia en directorios y redes compartidas, en el ámbito profesional del trabajo y la empresa, si compartimos el ordenador personal en el ámbito doméstico y familiar o si utilizamos ordenadores y redes públicas para trabajar con nuestros documentos.

La mayoría de programas de tratamiento de textos permiten personalizar las opciones de seguridad a través de menús que suelen seguir el itinerario de **Herramientas > Opciones > Seguridad**. Es importante analizar las opciones de protección de documentos que nos brinda cada programa determinado de tratamiento de información textual, ya que esta breve y sencilla exploración inicial nos dará el control total sobre el contenido de los ficheros.

La seguridad es un factor determinante para una convivencia cívica fluida en entornos digitales de comunicación e interactividad

2.6. Contenidos y derechos

Los programas de tratamiento digital de la información nos ofrecen grandes facilidades para capturar, usar, insertar y manipular todo tipo de contenidos, tanto textuales como de imagen o de naturaleza multimedia. Pero debemos ser conscientes de que no todos los contenidos están a nuestra disposición para que los utilicemos sin limitaciones.

Cuando manejamos información digital, debemos distinguir entre:

- Contenidos sujetos a derechos de propiedad intelectual y derechos de autor. Son contenidos cuyo uso está regulado por la Organización Mundial de la Propiedad Intelectual (OMPI) en función de disposiciones legales que permiten a sus propietarios o titulares disponer de ellos sin que ninguna otra persona física o jurídica pueda utilizarlos legalmente sin su consentimiento.

- Contenidos de dominio público. Son aquellos cuyos derechos de propiedad intelectual ya han expirado y que pueden ser, por lo tanto, utilizados por cualquier usuario. Podemos trabajar con estos contenidos sin ninguna limitación.

- Contenidos *fair use*. Se trata de contenidos cuyos titulares de derechos de autoría y propiedad intelectual permiten explícitamente que sean utilizados de forma libre en determinados casos: si se utiliza sólo parte de la obra y se cita debidamente su origen y autoría, si se usa con finalidades educativas o de formación, si se emplea en iniciativas no comerciales y sin ánimo de lucro.

  El concepto *fair use*

  Tiene su origen en la jurisprudencia legislativa norteamericana e introduce la opción de un "uso razonable y legítimo" por parte de cualquier usuario de contenidos protegidos por derechos de autor. Podemos usar este tipo de contenidos en un trabajo escolar o universitario y siempre citando su origen, pero no podemos utilizarlos para publicar un libro cuyos titulares de propiedad y derechos seamos nosotros mismos.

- Contenidos *copyleft*. Son contenidos cuyos titulares de derechos de propiedad autorizan explícitamente a cualquier usuario a usarlos, modificarlos y distribuirlos. Es un tipo de licencia de uso de contenidos en expansión en Internet y suele presentar como única limitación la condición de que sus

usuarios mantengan la misma licencia *copyleft* para los nuevos contenidos que generen a partir de la utilización libre de los contenidos previos.

El concepto *copyleft*

Podemos usar contenidos con licencia *copyleft*, pero deberemos mantener ese uso libre en los nuevos contenidos que nosotros generemos. No podemos usar contenidos *copyleft* para escribir y publicar un libro que vayamos a someter a nuestra propiedad intelectual y por el que queramos obtener derechos de autor.

Atender al tipo de información que manejamos cuando usamos los distintos mecanismos de tratamiento de la información digital no sólo puede ahorrarnos más de un problema legal. También evidencia el grado de conocimiento, capacidad y civismo en el uso correcto de los contenidos, más allá de las habilidades técnicas de edición y presentación de textos. Por otro lado, incide decisivamente en un uso convivencial de la Red por parte del conjunto de los usuarios.

2.7. Plagio

En términos generales, se entiende como plagio el uso literal y deliberado de contenidos ajenos, sin citar su procedencia e intentando transmitir que su autoría nos corresponde y nos pertenece.

El uso de las tecnologías digitales y su gran facilidad para replicar contenidos de todo tipo y en todos los formatos (texto, dibujo, fotografía, vídeo...) favorece y facilita la copia con una doble repercusión:

- la vulneración de los derechos de autoría y propiedad intelectual del auténtico autor y
- el engaño del interlocutor al presentarle como creación propia una copia de otro original.

Pero conviene tener en cuenta que la misma tecnología que facilita el plagio, acelera su detección. Es fácil buscar, localizar, copiar, pegar o insertar contenidos ajenos para hacerlos pasar por creaciones propias. Pero es aún más rápido pegar un fragmento de texto en un motor de búsqueda, localizar una fotografía o activar un programa específico sobre plagio y verificar el origen real de un contenido, lo que pone al descubierto el intento de apropiación indebida.

Plagiar contenidos es

- Antisocial e incívico:
  - porque vulneramos los derechos de propiedad y autoría de los auténticos creadores de los contenidos que copiamos, y
  - porque intentamos engañar al interlocutor sobre la verdadera autoría de los contenidos.

- Inútil:
  - cualquier usuario detectará el engaño utilizando un simple motor de búsqueda,
  - un interlocutor cualificado localizará rápidamente la impostura gracias a los programas específicos de localización de copias, y
  - los usuarios de las redes sociales (blogs, comunidades virtuales, grupos de trabajo en entornos virtuales...) denunciarán de forma inmediata la copia.

El uso no acreditado de contenidos ajenos puede parecer una idea práctica a primera vista, pero en realidad puede traernos complicaciones muy graves, como

- la descalificación del trabajo académico y la suspensión de su valoración,
- problemas (advertencia, sanción...) en el puesto profesional,
- descrédito público ante la comunidad y las redes sociales donde expongamos nuestras supuestas creaciones y
- reclamaciones legales de los auténticos autores/propietarios de los contenidos.

2.8. Citación

La facilidad de localización y tratamiento de la información de texto que nos ofrecen los medios y herramientas digitales hace imprescindible adoptar unos hábitos claros y permanentes de citación de las fuentes de las que hemos obtenido la información que usamos y editamos. Un uso correcto de información procedente de otras fuentes pasa por:

- distinguir claramente mediante las opciones del procesador de texto las frases y párrafos que importamos directamente de otra fuente, al entrecomillarlos y utilizar un estilo diferenciado (cursiva, negrita, etc.) y

- utilizar las opciones de notas a pie de página para referenciar de forma completa las citas bibliográficas o webgráficas de donde hemos extraído determinados contenidos textuales e

Web recomendada

La Norma ISO-690 de Referencias Electrónicas nos proporciona indicaciones normalizadas sobre cómo citar de forma correcta las fuentes electrónicas de información. Para más información podéis consultar:

http://www.ugr.es/~pwlac/G00_Referencias_electronicas.html

- incluir enlaces a las fuentes electrónicas de la información que presentamos, como opción de aval y credibilidad de los datos que manejamos.

Usar informaciones ajenas sin citar su procedencia situará nuestros textos bajo la sospecha inmediata y sistemática del plagio o la copia ilícita. Además, contribuirá a la saturación de las redes con más datos y contenidos insuficientemente acreditados y, por lo tanto, sin ninguna garantía de credibilidad.

2.9. Hábitos sostenibles

2.9.1. Código libre

En términos generales, se entienden como programas de código libre (*free software* o programas libres) el conjunto de aplicaciones informáticas que pueden ser usadas, copiadas, modificadas y distribuidas libremente y sin restricciones entre usuarios.

Frente a los programas comerciales sometidos a licencias de pago, el uso de programas de código libre incide en una mayor sostenibilidad de la sociedad y las redes digitales, en tanto que

- otorgan a cualquier usuario el derecho de usar libremente este tipo de programas,
- permiten el estudio de sus códigos y la realización de adaptaciones para nuevas funcionalidades,
- autorizan la distribución abierta de todo tipo de copias de los programas y
- estimulan a introducir mejoras en las aplicaciones y difundirlas de forma libre y universal.

El uso de programas de código libre tiene una importante dimensión cívica y social de creación y difusión de las utilidades informáticas, ya que

- hace llegar aplicaciones digitales de forma gratuita a personas y sectores sociales que no tienen acceso a programas comerciales de pago,
- extiende al conjunto de usuarios la opción de mejorar los programas y acceder más fácilmente a esas mejoras,
- su desarrollo repercute en el beneficio de toda la comunidad en la medida que mejora las prestaciones y la seguridad para cada uno de sus usuarios y
- el carácter abierto estimula el sentido de pertenencia a una comunidad de usuarios y el intercambio de conocimientos individuales en la Red colectiva.

2.9.2. Impresión

Los programas informáticos de tratamiento de texto presentan grandes posibilidades para la impresión de contenidos digitales en soporte papel, de forma inmediata y en grandes cantidades. Un uso razonable de las opciones de impresión debería pasar por

- no imprimir de forma sistemática y compulsiva todos los contenidos que capturamos, tratamos y almacenamos en el ordenador,
- no considerar la copia impresa como una copia de seguridad: las únicas copias de seguridad útiles será las realizadas sobre soportes digitales,
- realizar pruebas y borradores en pantalla y no imprimir hasta estar seguros de que necesitamos una prueba sobre papel y
- distinguir qué uso real queremos dar a la información, ya que una impresión en papel puede ser útil para revisar información en lugares y momentos en los que no dispongamos de ordenador, dispositivos o redes pero es prescindible si vamos a leer ese texto junto a la pantalla del ordenador.

Copia en papel

Una copia en papel nos obligará a repetir manualmente la elaboración de un documento.

Un uso sostenible de la impresión de documentos nos ahorrará

- costes económicos personales, derivados del gasto en papel para la impresora y consumibles de tinta y
- costes sociales derivados del consumo de papel, los componentes químicos de las tintas y el reciclaje industrial de componentes con diversos grados de toxicidad (tóners, cartuchos de tinta, etc.).

3. Navegación segura

La conexión que utilizamos para acceder a Internet nos convierte en un nudo más de la Red planetaria de redes. La telaraña global pone en nuestro terminal grandes cantidades de información y opciones muy eficientes de comunicación, pero también nos expone a algunos riesgos que nos conviene prevenir.

Internet genera espacios sociales de intercambio e interacción entre personas, en los que las medidas de seguridad no son sólo elementos fundamentales para preservar la integridad y privacidad de nuestros dispositivos y datos, sino que constituyen también un factor básico de convivencia y civismo, en tanto que

- facilitan la fluidez de circulación de informaciones y datos,
- evitan la proliferación y la extensión de virus y códigos maliciosos,
- frenan la efectividad de iniciativas fraudulentas masivas relacionadas con los envíos de mensajes no solicitados (*spam*), captura ilícita de datos personales o intentos de estafa económica y
- ayudan a prevenir usos ilícitos de información privada (datos, fotografías, vídeos...) de cualquier usuario de la Red.

Nos conviene efectuar un uso seguro de Internet, por nuestro propio interés y porque éste coincide en sus principales objetivos con el interés social del conjunto de los usuarios. Cada uno de nosotros obtiene beneficios personales de un mejor funcionamiento global y colectivo de la Red, en la misma medida que cada uno de nosotros puede contribuir cotidianamente a que Internet sea mejor, más eficiente y más seguro.

3.1. Seguridad en la Red

La seguridad en la navegación y el uso de Internet tiene su factor básico y fundamental en los programas antivirus. Un ordenador conectado a Internet (sobre todo si la conexión es de banda ancha) mantiene siempre puertas abiertas al tráfico de datos y programas, ante los cuales debemos poner una barrera potente de análisis, detección y eliminación de todo aquello de lo que no podamos garantizar el origen y la fiabilidad.

Cuando estamos conectados a Internet debemos utilizar un antivirus solvente y fiable

- para preservar el equipo y los datos de eventuales intrusiones no deseadas, dañinas o fraudulentas y

- por el imperativo cívico de intentar evitar convertirnos en cómplices involuntarios de la distribución masiva de un código malicioso y de actividades ilícitas de quien quiera utilizar nuestro ordenador y la conexión de forma remota para perjudicar a otros usuarios.

Además de lo ya expuesto en el capítulo **Dispositivos electrónicos > Antivirus**, cuando nos conectamos a Internet debemos asegurarnos de que el antivirus nos garantice

- protección permanente ante cualquier intrusión en las redes y equipos,

- actualización constante de los virus y códigos maliciosos ante los que puede desplegar de forma automática acciones de rastreo, aviso, limpieza y desinfección,

- información y alertas actualizadas sobre nuevos riesgos y amenazas y

- opciones flexibles de configuración para que podamos determinar niveles de seguridad adecuados al uso cotidiano que realizamos de las redes y ficheros digitales.

Además del antivirus personal, también podemos utilizar complementariamente programas antivirus de uso libre para reforzar la acción preventiva:

- Desde el escritorio. Programas antivirus gratuitos que podemos instalar en cada uno de nuestros equipos para verificar la limpieza de archivos y ficheros que descargamos desde Internet o desde el correo electrónico. Su capacidad de uso sin conexión a la Red obliga a que los actualicemos regularmente para asegurarnos de que el nivel de protección no ha quedado obsoleto.

- Antivirus en línea. Opciones limitadas de rastreo y detección de virus y programas maliciosos, que funcionan desde la Red y que nos sirven, fundamentalmente, para verificar la limpieza de nuestra máquina y los ficheros cuando el antivirus nos ofrece resultados dudosos.

Web recomendada

El Instituto Nacional de Tecnología de Telecomunicaciones ofrece soluciones gratuitas actualizadas sobre antivirus de uso puntual y herramientas de desinfección. Para más información podéis consultar:

- antivirus de uso puntual:
  http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=1&pagina=0
- herramientas de desinfección:
  http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=8&pagina=0

3.1.1. Cortafuegos

Junto a los imprescindibles antivirus, los llamados cortafuegos o *firewalls* son programas de la máxima utilidad cuando usamos un ordenador conectado a Internet, ya que nos permiten controlar y restringir todo el tráfico de datos entre nuestra máquina y la Red. Este control puede resultar vital para impedir la entrada de virus y códigos maliciosos en el equipo y para cortar cualquier intento de captura y fuga de datos de nuestro ordenador desde la Red.

En síntesis, un programa cortafuegos actúa sobre las conexiones TCP/IP que regulan los protocolos de Internet mediante los que el ordenador intercambia información con la Red a la que está conectado.

Una correcta configuración nos permite:

- monitorizar al momento cualquier intento de entrada en el equipo y denegarlo si procede,
- controlar las conexiones salientes y evitar la fuga de información que programas espía o códigos maliciosos instalados inadvertidamente en el ordenador puedan intentar enviar a la Red,
- impedir que la actividad interna del ordenador sea visible en Internet y
- navegar de forma segura, al dar entrada y salida sólo a programas previamente autorizados por nosotros y preguntar en cada caso si autorizamos el acceso o la salida de programas que no hemos definido de forma explícita.

La mayoría de sistemas operativos presentan programas cortafuegos, pero en los ordenadores personales también podemos optar por herramientas gratuitas como las que ofrece el Instituto Nacional de Tecnología de Telecomunicaciones en su sede oficial.

Web recomendada

Podéis obtener herramientas gratuitas:
http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=2&pagina=0

Igual que en el uso de los antivirus, la utilización razonada y razonable de cortafuegos nos ayuda a mejorar el manejo de la Red en dos niveles fundamentales y profundamente relacionados, como son

- la seguridad personal y la integridad de equipos y datos y
- un uso social de la Red más sostenible, fluido y seguro por parte del conjunto de usuarios del que formamos parte.

3.1.2. Las redes Wi-Fi

Las llamadas redes Wi-Fi (Wireless Fidelity) permiten que los dispositivos electrónicos (ordenador, agenda electrónica, teléfono móvil, etc.) accedan sin cables a Internet o a otras redes de dispositivos si están lo suficientemente cerca de antenas repetidoras o *routers* de su señal correspondiente.

Las ventajas que nos proporciona una conexión Wi-Fi para poder utilizar la Red sin cables en cualquier lugar y en cualquier momento pueden aumentar o disminuir según el uso más o menos razonable que hagamos de ellas. En la Red doméstica, es conveniente que configuremos todos los parámetros de seguridad del *router* inalámbrico para evitar la eventual entrada de intrusos externos. Una red Wi-Fi doméstica correctamente configurada y protegida:

- Evita intrusiones externas que puedan conectarse a Internet y ocupar el ancho de banda que tenemos contratado (y por el que pagamos a la empresa proveedora del servicio).

- Evita que cualquier usuario en el radio de acción de la Red inalámbrica pueda introducirse en el ordenador y capturar datos e información personal.

- Evita que la Red facilite la introducción en nuestro equipo de virus y programas maliciosos.

De forma recíproca a las medidas de autoprotección, es recomendable el máximo cuidado y corrección cívica en el uso de redes inalámbricas de conexión ajena. Así, si utilizamos redes públicas o privadas de acceso autorizado, conviene ceñirse a las normas de uso establecidas y respetar la privacidad de los demás usuarios, sin utilizar las eventuales deficiencias de seguridad que podamos detectar para capturar informaciones o datos personales de otros usuarios.

En el caso de localizar redes Wi-Fi ajenas con bajo nivel de protección, es recomendable respetar su privacidad y evitar su uso, ya que éste no sólo sería fraudulento, sino que nos expondría a las intrusiones de virus y programas maliciosos que pudieran tener los ordenadores y las redes inalámbricas a las que accedemos de forma ilícita. El Centro de Seguridad del Instituto Nacional de Tecnologías de la Comunicación recomienda lo siguiente:

- Establecer y definir el número máximo de equipos que se puedan conectar al punto de acceso.

- Apagar el punto de acceso y el *router* cuando no se vaya a utilizar.

- Desactivar la opción de difusión del nombre de la Red inalámbrica para evitar que otros usuarios externos puedan identificar de forma automática los datos de la Red.

- Cambiar la contraseña por defecto que ya lleva incorporada el *router*, ya que muchos fabricantes utilizan la misma clave para todos los equipos.

- Utilizar sistemas de encriptación para impedir que el tráfico de la Red sea fácilmente legible. Se recomienda utilizar el sistema WPA, ya que el sistema WEP es inseguro.

- Desactivar la asignación dinámica de IP a nuevos dispositivos que soliciten la conexión a la Red. Es más seguro hacer depender cualquier conexión a una asignación manual de IP.

3.1.3. Antiespías

En un uso regular y normalizado de la Red es muy conveniente que reforcemos la seguridad del ordenador ante los llamados programas espía (o *spyware*).

Spyware

Son aplicaciones informáticas que suelen entrar e instalarse en el equipo de forma oculta cuando descargamos de la Red e instalamos en nuestra máquina determinados programas, gratuitos o no.

La acción de estos programas suele centrarse en recopilar información de nuestro sistema para enviarla a través de la Red a bases de datos, generalmente de carácter comercial, para utilizarlos posteriormente en iniciativas comerciales y publicitarias. Pero algunos de estos códigos maliciosos también pueden recopilar y robar con fines delictivos datos tan personales como las claves bancarias que tecleamos cuando operamos en nuestras cuentas. Para prevenir el espionaje informático indeseado es aconsejable:

- restringir la descarga de programas gratuitos a páginas que nos ofrezcan las máximas garantías de fiabilidad,

- leer cuidadosamente las condiciones de uso de programas gratuitos que podemos descargar de Internet e instalar en el ordenador e

- instalar programas antiespía, que
  - son complementarios de antivirus y cortafuegos, que ya detectan buena parte de los códigos maliciosos que intentan instalarse en el ordenador y
  - actúan específicamente contra códigos camuflados como programas normales para evitar las alertas de antivirus y cortafuegos.

Web recomendada

Podemos acceder a una amplia oferta de antiespías gratuitos, siempre que antes verifiquemos su solvencia y honestidad en centros de seguridad acreditados como el Instituto Nacional de Tecnología de Telecomunicaciones:

http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=10

3.1.4. E-comercio y banca electrónica

Si la seguridad general en el uso de Internet es importante, la precaución resulta trascendental cuando utilizamos la Red para efectuar transacciones comerciales u operaciones bancarias. En estos casos, lo que circula por la Red son las claves de acceso a nuestras cuentas y las contraseñas de nuestras tarjetas de crédito. La posibilidad de acceso, en definitiva, a nuestros recursos económicos.

Riesgo en la Red

Cuando lo que corre por la Red es el acceso a nuestro dinero, debemos ser conscientes de que no estamos expuestos a mayores riesgos que en el mundo presencial, como extraviar una tarjeta de crédito dentro de un bolso en un taxi, sufrir un atraco en un cajero automático, ser víctimas de un asalto en el portal del domicilio o sufrir un tirón en la calle.

Pero, igual que en la vida cotidiana presencial, nos conviene ser precavidos. Y en la Red debemos adaptar nuestra seguridad a las características del mundo digital:

- Ante todo, nos conviene efectuar operaciones económicas sólo en webs y páginas que nos merezcan una confianza total.

- Es necesario que verifiquemos la acreditación comercial y bancaria (dirección web, dirección de correo electrónico, dirección física, teléfono de contacto...) de la página en la que vamos a introducir las claves.

- Es imprescindible observar que la dirección de la página donde vamos a introducir claves y contraseñas comienza por http, que indica que se trata de una conexión segura y que aparece un *candado* () en la parte inferior derecha del navegador.

- Nos conviene asegurarnos de la validez de los certificados (pulsando en el *candado*), que coinciden con la entidad solicitada y que son válidos.

- Es aconsejable evitar el uso de equipos públicos (cibercafés, estaciones o aeropuertos, redes inalámbricas insuficientemente acreditadas...) para realizar operaciones comerciales o bancarias.

- También conviene desactivar la opción autocompletar si se accede desde un equipo distinto al habitual o se comparte equipo con otras personas.

- Siempre debemos cerrar la sesión de la web y el navegador cuando finalizamos la operación para evitar que alguien pueda acceder a los últimos movimientos o recuperar las claves que hemos utilizado.

La red presenta tantos riesgos como la vida cotidiana presencial y, como en ella, es necesario mantener actitudes razonables y de sentido común para prevenir eventuales ataques o descalabros económicos. El mayor porcentaje de robos y estafas en Internet no tienen su origen en sofisticados artilugios tecnológicos, sino en una gestión deficiente o descuidada de claves y contraseñas por parte de sus propietarios.

3.1.5. Precauciones adicionales

Filtros de contenido

Los llamados filtros de contenido son programas informáticos que permiten bloquear el acceso a determinadas páginas de Internet en función de palabras y expresiones clave que el usuario ha definido previamente.

Los filtros de contenido resultan útiles para controlar y restringir la llegada al ordenador de informaciones e imágenes que consideramos inconvenientes o inadecuadas y se utilizan sobre todo para prevenir que usuarios infantiles del ordenador doméstico encuentren fortuitamente contenidos a los que, por edad o nivel de formación, no deberían tener acceso.

Web recomendada

El Instituto Nacional de Tecnología de Telecomunicaciones proporciona una guía comentada de recursos gratuitos para el control parental en su página oficial: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=16&pagina=0

Junto a la prevención y bloqueo informático de determinadas páginas web por palabras clave de su contenido, la mayoría de expertos aconsejan completar el control parental del acceso de los menores a la Red con el fomento de hábitos educativos como:

- Educar a los menores sobre los eventuales riesgos que pueden encontrar cuando navegan por Internet.

- Acompañarlos en su uso de la Red, siempre que sea posible e intentando que el menor no sienta invadida su intimidad personal.

- Advertir muy seriamente a los menores de los peligros de facilitar informaciones personales (nombres, direcciones, teléfonos, contraseñas, fotografías, claves bancarias...) a personas desconocidas a través de cualquier medio, presencial o electrónico.

- Concienciar a los menores de que deben informar inmediatamente de cualquier conducta o contacto de la Red que les resulte incómodo o sospechoso.

- Acostumbrarles a crear cuentas de usuario específicas y limitadas para las actividades que quieran realizar en la Red.

P2P

Si somos usuarios de redes de intercambio de ficheros con otros usuarios, nos conviene tener en cuenta que los programas P2P que utilizamos se llaman así precisamente porque van de par a par (*peer to peer*), es decir, se dan entre iguales. Esto quiere decir que cuando nos conectamos a una de esas redes nos convertimos en cliente y servidor, al recibir y enviar archivos al mismo tiempo. Por nuestra propia seguridad y responsabilidad en la convivencia cívica en la Red, es importante que:

- Analicemos con cuidado todos los archivos que descargamos.

- Evitemos intercambiar programas o contenidos que no presenten garantías de respeto a los derechos de propiedad y autoría, ya que la distribución ilícita de información o ficheros protegidos podría plantearnos problemas legales e, incluso, implicarnos en delitos.

- Ejecutemos el programa cliente P2P (eMule, BitTorrent, Pando, Ares o Nosolodescargas, entre muchos otros) en una sesión de usuario con permisos limitados para aislarlo de otros componentes críticos del sistema.

- Prestemos la máxima atención a la extensión de los ficheros que descargamos para evitar introducir por error o despiste ficheros ejecutables (extensión.exe) cuando en realidad pensábamos descargar otro tipo de archivos.

- Modifiquemos el nombre de las carpetas de descarga.

- No pongamos a disposición del intercambio ficheros o contenidos que puedan ofender, herir la sensibilidad o atentar a la convivencia cívica con el resto de usuarios de este tipo de redes.

Precauciones

Modificar el nombre de las carpetas de descarga es importante, ya que muchos códigos maliciosos buscan rutas fijas para replicarse. También conviene prestar mucha atención a las casillas de las carpetas que realmente estaremos compartiendo en la Red. Una mala elección, o dejar activadas las carpetas que algunos programas P2P marcan por defecto, puede exponer a las redes de intercambio archivos y contenidos del disco duro que en ningún caso querríamos ver circulando por la Red.

3.2. Localización de información

3.2.1. Búsqueda en la Red

Internet pone a nuestro alcance una incalculable cantidad de información. Pero el dato que buscamos no siempre es visible y localizable de forma inmediata a causa de la proliferación de fuentes, de las diversas maneras de organizar la información y de su acumulación indiscriminada. Para buscar y localizar información de forma eficiente en la Red, nos ayudará:

- definir exactamente qué es lo que estamos buscando en cada caso,

- informarnos con regularidad sobre las nuevas herramientas de búsqueda disponibles en la Red, analizar su funcionamiento y probar sus actualizaciones,

- utilizar las herramientas de búsqueda generalista para localizar fuentes especializadas de información que puedan llevarnos a los datos específicos deseados y

- guardar y ordenar los resultados relevantes de las localizaciones de información como posibles fuentes, ya localizadas, que nos facilitarán posteriores búsquedas de información.

La red contiene prácticamente todas las respuestas que podemos necesitar. Tan sólo debemos formularle las preguntas correctas y de la forma adecuada. A veces el proceso lleva su tiempo, pero suele ser una inversión altamente rentable en resultados informativos y rapidez de localización.

3.2.2. La localización

Antes de empezar a utilizar cualquier motor de búsqueda de información nos puede ser muy beneficioso realizar algunas acciones previas que, aunque pueden representar una pequeña inversión inicial de atención, acabarán ahorrando tiempo y mejorando resultados:

- Plasmar los objetivos de búsqueda en una lista de términos concretos, representativos y definitorios que pensamos que presentan las máximas posibilidades de identificación por parte de la herramienta de búsqueda.

- En la lista de términos conviene incluir sinónimos y palabras relacionadas que puedan ayudar a delimitar el ámbito de localización del buscador, así como nombres de empresas o instituciones que pensamos que pueden contener datos o informaciones relacionadas con nuestros objetivos de localización.

- En determinados tipos de búsqueda o fases de localización puede ser aconsejable también definir frases literales muy concretas que creemos que pueden estar relacionadas con la información que buscamos.

- Analizar el funcionamiento y los criterios sintácticos de consulta que utiliza cada herramienta de búsqueda. Para hacerlo es aconsejable revisar las secciones de ayuda y preguntas más frecuentes (PMF o, en inglés, FAQ) que suelen presentar la mayoría de buscadores.

Además de conocer el funcionamiento específico de cada herramienta de búsqueda, cuando deseemos formular una consulta también nos ayudará tener en cuenta:

- el ámbito idiomático preferente donde buscamos la información y el idioma de uso del buscador que utilizamos,
- en búsquedas muy dirigidas y concretas puede ser útil el uso de frases textuales, normalmente entre comillas,
- combinar varios términos relacionados puede ser efectivo siempre que todos ellos sean muy definidos y hagan referencia a un objetivo muy concreto y
- el uso de letras mayúsculas y minúsculas puede hacer variar los resultados de la localización.

Buscando información

Si buscáis datos o información que podéis prever que estarán en la Red en inglés, formular las consultas mediante términos en catalán, por ejemplo, puede provocar resultados muy distorsionados.

El uso de las comillas

Para localizar, por ejemplo, el texto de *El Quijote* puede ser eficiente formular "en un lugar de la Mancha".

Consultas en función de la tipografía

Normalmente las consultas en minúscula devuelven resultados sin filtrar por criterio tipográfico, mientras que a menudo la consulta de términos con la letra inicial en mayúscula restringe los resultados a nombres propios.

3.2.3. Búsqueda avanzada

Los motores de búsqueda más potentes suelen presentar opciones de búsqueda avanzada que pueden sernos muy útiles para obtener un primer filtrado automático de los resultados localizados, siempre que hayamos definido y delimitado previamente los criterios en los que enmarcamos la búsqueda. Las opciones de búsqueda avanzada presentan como parámetros más frecuentes:

- La inclusión o exclusión de términos: nos permite definir si los resultados de la consulta deben incluir todos los términos introducidos en el formulario, si deben recoger todos los resultados que incluyen cualquiera de los términos planteados o si sólo deben presentar resultados sin determinados términos concretos.
- La posibilidad de restringir la búsqueda sólo a una frase o formulación concreta.
- Delimitar el retorno de resultados que estén redactados en un idioma determinado.
- Limitar la búsqueda a las fechas más recientes de actualización de las páginas contenidas en la base de datos del buscador.
- Definir si los términos de consulta deben aparecer en el título, en el texto completo, en la dirección electrónica de la página web o en los enlaces que contiene.

- Seleccionar el formato de la información de la que nos interesa recibir resultados.

- Buscar páginas con enlaces a una determinada web o dominio.

3.2.4. Credibilidad

La mayoría de criterios que nos serán útiles para verificar la credibilidad de los resultados de búsqueda están relacionados con la fuente de información donde localizamos contenidos. La mayor o menor presencia de estos criterios en una web, blog o motor de búsqueda avalará más o menos su fiabilidad. Los principales criterios de credibilidad que deberíamos tener en cuenta son:

- Autoría. Un autor identificado, sea individual o colectivo, proporciona más fiabilidad que una fuente informativa anónima, sobre todo si, además de identificarse, el responsable de los contenidos en cuestión presenta acreditaciones de carácter profesional y elementos de contacto, como una dirección de correo electrónico. Se trata de un criterio especialmente relevante en el caso de blogs e iniciativas de publicación personal de información en la Red.

- Filiación y autoridad. Más allá de la autoría personal, la credibilidad de cualquier página web pasa por la mención explícita y clara del organismo, institución o empresa de la que depende. La referencia a la entidad que suministra los contenidos o el apoyo económico de la publicación nos permitirá no sólo evaluar la fiabilidad, sino también el grado de autoridad de la fuente de información en su ámbito de actuación o conocimiento.

- Actualización. Un nivel fundamental de valoración de la información localizada está vinculado a las fechas de creación de aquel contenido, de su presentación en una determinada web y, sobre todo, de su última actualización.

- Créditos y procedencia. La citación explícita del origen de la información es una garantía clara de credibilidad, en tanto que sitúa los contenidos y nos permite acudir a la fuente original de la información para contrastar y ampliar datos. Es aconsejable someter a la revisión crítica y la verificación sistemática todos aquellos contenidos que localizamos si no aclaran cuál es su fuente originaria de información.

- Objetividad. En los casos de webs y páginas con publicidad, un criterio complementario de verificación de su credibilidad es la distinción clara y definida entre los contenidos informativos y los de carácter publicitario o propagandístico.

3.2.5. Certificaciones

Aunque no hay una única autoridad que acredite de forma universal la calidad y credibilidad de los contenidos que circulan por Internet, varias agencias y entidades han creado estándares de análisis y valoración de páginas web, la mayoría de los cuales están centrados en criterios de accesibilidad, legalidad, autocontrol y defensa de los consumidores y usuarios. Estas entidades tienen ámbitos bastantes heterogéneos y fragmentados de estudio y actuación y suelen asignar a las páginas que se someten voluntariamente a sus controles determinados sellos de calidad en reconocimiento de los requisitos que cumplen.

Pese a que ningún sello de calidad garantiza, hoy por hoy, la credibilidad de los contenidos de una determinada página web, el hecho de que una web determinada presente una acreditación u otra añade un cierto grado de fiabilidad, asociado al menos a la voluntad de los responsables de la página de someterse a determinados controles externos. Los principales sellos de calidad y control que podemos encontrar en páginas web son:

- ICANN (Internet Corporation for Assigned Names and Numbers). Se trata de una entidad que regula la asignación de dominios a Internet.

- IQUA (Agencia de Calidad de Internet). Su sello verifica parámetros sobre accesibilidad, usabilidad, seguridad, legalidad y protección de menores. Está avalada por instituciones públicas como el Consejo del Audiovisual de Cataluña o los consejos de Navarra y Andorra y el organismo Red.es, dependiente del Gobierno español.

- W3C. Este consorcio, formado por más de 400 asociaciones, emite una certificación de calidad internacional en función, sobre todo, de criterios de accesibilidad.

- AUI (Asociación Española de Usuarios de Internet). Más que sello de calidad, promueve la adhesión de webs con respecto a criterios de defensa de los intereses y los derechos de los usuarios de la Red.

- AI (Asociación de Internautas). Se trata de un organismo de defensa de los usuarios de Internet, sobre todo con respecto a operadoras telefónicas, empresas y servicios relacionados con la Red.

4. Comunicación sostenible

4.1. Correo electrónico efectivo

El correo electrónico es el instrumento que hasta este momento se ha revelado como más efectivo y utilizado en la comunicación personal virtual. Millones de personas de todo el mundo usamos constantemente el correo electrónico para comunicarnos de forma instantánea. Su efectividad tecnológica está fuera de toda duda. Su eficiencia como canal de comunicación depende del uso que hagamos cada uno de nosotros como usuario.

¿Cómo usar el correo electrónico con la máxima efectividad comunicativa?

Se puede llevar a cabo con hábitos muy sencillos y sin ninguna complicación tecnológica:

- Escribir bien
  - La mayoría de mensajes que intercambiamos se basan en el texto. Nuestros interlocutores entenderán mejor y más rápido mensajes redactados de forma correcta, estructurados de forma razonable, que no sean excesivamente largos y que no presenten repeticiones o reiteraciones innecesarias de ideas y conceptos.
  - La inmediatez de redacción y envío de mensajes que facilita el correo electrónico nos permite precisamente tomarnos unos minutos para ser correctos en la ortografía y la sintaxis del mensaje, releer y retocar el contenido varias veces hasta definir de forma precisa lo que queremos transmitir y enviar finalmente sólo el contenido necesario.
  - Hay que analizar las reglas específicas para redactar correctamente mensajes de correo electrónico: no son necesarias las abreviaturas propias de los mensajes de texto entre teléfonos móviles (p. ej. xq=porque no está justificado en un mensaje de correo electrónico; el uso constante de MAYÚSCULAS ES EQUIVALENTE A GRITAR Y ¿A QUIÉN LE GUSTA UNA COMUNICACIÓN A GRITOS?).

- Definir el mensaje
  - El tema o asunto del mensaje es muy importante porque permite al receptor organizar su atención y tiempo en función del título de nuestra llamada.
  - Debemos rellenar siempre el campo del tema o asunto del mensaje y debemos hacerlo condensando el elemento informativo principal del correo electrónico.

  - Cuanto más preciso y adecuado sea el tema/asunto de los mensajes que enviamos, más rápida y concreta será la respuesta de nuestro interlocutor.

- Identificar el mensaje
  - Las normas básicas de cortesía son fundamentales en el encabezamiento de los mensajes. No es lo mismo llamar por el nombre de pila a un amigo que dirigirse protocolariamente a una empresa o que omitir cualquier encabezamiento, de forma que el destinatario pueda pensar que recibe un correo automático no solicitado.
  - La firma es imprescindible para que el interlocutor pueda identificar al autor del mensaje. Debemos valorar con cuidado en cada caso qué datos incluimos en la firma del mensaje según el grado de confianza en nuestro interlocutor: nombre y apellidos completos, teléfono, dirección, otras direcciones profesionales de correo electrónico, etc.

La mayor efectividad de comunicación individual en el uso del correo electrónico coincide siempre con su mayor eficiencia cívica y social: pensar en el receptor suele ser la clave fundamental para hacer el mejor uso del correo electrónico.

4.2. Correo electrónico sostenible

El correo electrónico nos permite la transferencia instantánea de grandes cantidades de información mediante la opción de adjuntar ficheros a los mensajes. Ante esta posibilidad, debemos preguntarnos **siempre**: ¿es realmente necesario? Unos consejos básicos para una comunicación razonable y sostenible mediante el correo electrónico serían:

1) No adjuntéis ficheros con poca información.
Si necesitáis transmitir información condensable en diez o quince líneas de texto, es mejor copiar y pegarlas en el texto del mensaje. Evitaréis al interlocutor el tiempo necesario para bajar el fichero adjunto y le permitiréis dedicar ese tiempo de bajada y gestión a descubrir qué queréis decirle.

2) Mejor no adjuntar ficheros de gran tamaño.
  a) Aseguraos de que, al adjuntar un fichero de grandes dimensiones, va a ser de tanto interés para el interlocutor como para compensar el tiempo de conexión de bajada y para compensar el tiempo y espacio de gestión del fichero en su ordenador.
  b) Si creéis que debéis enviar un fichero adjuntado que supera las 500 kb, enviad antes un mensaje pidiendo permiso y justificando razonadamente el envío.

3) Utilizad un compresor para enviar ficheros muy pesados o conjuntos de archivos.

a) Programas de compresión de información como WinZip, WinRar o 7Zip reducen sensiblemente el tamaño de los ficheros que enviamos y agilizan su transmisión. También empaquetan en una sola carpeta diversos archivos, con lo que facilitamos al interlocutor la descarga del material enviado y su organización en el disco duro.

b) Antes de enviar ficheros comprimidos es conveniente que:

- Nos aseguremos de que nuestro interlocutor dispone del programa adecuado para descomprimirlos y acceder a ellos o que le facilitemos información para obtener el programa necesario.
- Hayamos acordado el envío con nuestro interlocutor y tengamos su autorización y la seguridad de que espera esos contenidos a los que va a dedicar tiempo de descarga y organización.

4) Evitad formar parte de las cadenas de mensajes.

a) Analizad qué mensajes reenviáis, a quién y por qué. El reenvío compulsivo de mensajes, con ficheros adjuntos, a toda la lista de contactos puede ocasionar una pérdida de tiempo y coste de conexión a todos aquellos que no estén muy interesados en formar parte de las cadenas de mensajes.

b) Aseguraos de que los mensajes que reenviáis a vuestros contactos no forman parte de cadenas de correo electrónico diseñadas para estafar a los usuarios, obtener de forma ilícita sus direcciones de correo electrónico o introducir en los equipos programas espía o virus informáticos.

4.3. Correo electrónico seguro

Junto a sus indudables ventajas, el uso intensivo del correo electrónico comporta también algunos riesgos que podemos prevenir de forma responsable con sencillos hábitos de seguridad, por nuestro propio interés y por la seguridad de los usuarios con los que nos comunicamos electrónicamente. La seguridad en el uso del correo electrónico depende fundamentalmente de rutinas tan sencillas como:

- No abrir ficheros adjuntos a mensajes de procedencia desconocida o cuya apariencia resulte directamente sospechosa. Antes de inspeccionar un mensaje de forma compulsiva conviene pararse a pensar unos segundos qué elementos y procedentes de quién vamos a introducir en nuestro equipo.

- Analizar con el antivirus de confianza cualquier documento recibido por correo electrónico antes de ejecutarlo en el ordenador.

- Configurar correctamente el antivirus para que analice los ficheros que abrimos desde el correo electrónico y nos avise y paralice inmediatamente la descarga si detecta elementos sospechosos.

- Utilizar filtros contra el correo electrónico no deseado y activar todas las opciones de bloqueo de este tipo de mensajes que nos ofrezca el programa de gestión de correo electrónico que utilizamos.

- No introducir la dirección de correo electrónico en formularios o listas de correo que no nos merezcan una confianza razonable.

- No difundir de forma colectiva las direcciones de correo electrónico que guardamos en la agenda o lista de contactos.

No facilitar la dirección de correo electrónico

Esta actitud preventiva debería incluir no responder nunca a mensajes dudosos ni a cadenas de correos para evitar que el mensaje de respuesta sea utilizado como confirmación de que nuestra cuenta de correo existe y es operativa.

Las claves básicas de una comunicación electrónica segura son, sobre todo, unos hábitos personales de manejo razonable, responsable y cívico de mensajes, ficheros y programas de correo electrónico.

4.4. *Spam*

La recepción masiva de mensajes de correo electrónico no solicitados constituye una de las plagas digitales de más difícil solución global por sus dimensiones y consecuencias inmediatas. El bombardeo intensivo del llamado *spam* provoca:

Envío a múltiples destinatarios

Si queremos enviar un mensaje a un grupo de contactos, conviene poner nuestra dirección en el campo del destinatario (Para) y utilizar el campo de copia oculta (CCO) para poner las direcciones de todos los destinatarios. Así, la dirección de cada uno de ellos no quedará expuesta a la vista del resto de destinatarios. De manera similar, debemos borrar el historial de destinatarios antes de reenviar un mensaje a diversas personas.

- ocupación estéril de gran parte del ancho de banda de todas las redes, troncales y sectoriales, de Internet,

- amplia pérdida de tiempo por parte de los usuarios para gestionar y discernir debidamente el correo basura de los mensajes importantes y proceder a la eliminación de las misivas electrónicas no pertinentes,

- riesgo de entrada en el equipo propio de virus y códigos maliciosos y la consiguiente pérdida de tiempo para detectar y eliminar eventuales infecciones y

- peligro de extensión de infecciones y estafas por un reenvío intenso de mensajes maliciosos a nuestros contactos, sea por la capacidad de códigos ocultos para reenviarse automáticamente, sea por una gestión descuidada de este tipo de mensajes por nuestra parte.

Y ante este uso indebido de las redes telemáticas, nos conviene, por lo tanto, responder de forma contundente:

- Utilizando varias direcciones de correo electrónico, que nos permitan aislar en buzones separados el correo basura y el intercambio de mensajes con nuestros contactos importantes.

- Evitando difundir nuestra dirección de correo electrónico en webs de baja fiabilidad, donde pueden ser fácilmente capturadas por los programas e individuos dedicados al tráfico de direcciones.

- Intentando no participar en cadenas de mensajes que confirmarán la validez de nuestra propia dirección de correo electrónico y pondrán al descubierto las de nuestros contactos.

- Protegiendo a los contactos de nuestra agenda, reenviándoles los mensajes poco fiables utilizando el campo CCO (con copia oculta).

- No respondiendo nunca a un mensaje indeseado o poco fiable ni a las instrucciones que algunos de ellos presentan para no recibir más mensajes similares: suelen ser falsas y confirman al emisario la validez de la cuenta de correo electrónico.

- Denunciando a las autoridades competentes el envío de *spam* y participando en la creación de listas negras.

- Utilizando filtros *antispam*:
  - Nos conviene configurar adecuadamente los filtros que pone a nuestra disposición el proveedor de la cuenta de correo electrónico.

- Pueden sernos muy útiles los refuerzos *antispam* que presentan numerosas herramientas gratuitas de protección, siempre que previamente acreditemos su credibilidad con el aval de organismos solventes.

Una forma de controlar el *spam*

Una dirección secundaria de correo electrónico para utilizar en formularios web o listas de correo nos será muy útil, ya que podremos desecharla fácilmente si se convierte en canal de distribución de mensajes no deseados.

Web recomendada

Un organismo solvente es el Instituto Nacional de Tecnología de Telecomunicaciones: http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=11&pagina=0

4.5. La netiqueta

En 1995, en plena prehistoria de Internet, la directiva de Intel Sally Hambridge ya intentó plasmar en un documento técnico el primer protocolo de buenas prácticas en el uso de la Red. Su iniciativa ha ido evolucionando en un sinfín de recomendaciones que, sin llegar a cristalizar en códigos de conducta, constituyen un auténtico manual del buen uso de los canales digitales de comunicación.

Web recomendada

Para más información acerca del primer protocolo de buenas prácticas en el uso de la Red podéis consultar: http://www.rfc.net/rfc1855.html

Se conocen popularmente con el nombre de *netiquette* (o netiqueta en su versión castellanizada), que ha surgido a partir de conjuntar el término francés *etiquette* (buena educación) con el vocablo inglés *net* (red). Sin que necesariamente debamos considerarla y asumirla como una normativa cerrada de comportamiento, la evolución de la netiqueta nos proporciona recomendaciones a tener muy en cuenta para aprovechar al máximo las potencialidades comu-

nicativas de los canales digitales a partir del sentido común y las convenciones sociales que los humanos ya habíamos ido desarrollando antes del surgimiento y el desarrollo de Internet. En síntesis, la netiqueta nos aconseja lo siguiente:

- Los mensajes de correo electrónico deben ser concisos y breves: conviene recordar que es más difícil leer en una pantalla que en papel.

- La presentación es importante: escribir en mayúsculas, por ejemplo, da impresión de gritar.

- Igual que en el mundo presencial, es recomendable no ser grosero.

- El tema del mensaje es imprescindible: hace a nuestro interlocutor más fácil el catalogar, priorizar y leer el correo.

- Cuando se envía un mismo correo a muchas personas, es mejor ocultarlos escribiendo sus direcciones en el campo BCC-CCO y poniendo la dirección propia en TO-Para.

- Conviene organizar las ideas y pensar bien qué se va a escribir. Tal vez os sirva hacer un borrador antes. También es bueno corregir la ortografía.

- Privacidad: el correo que se envía es público y permanente. No digáis nada por correo de lo que no queréis que quede constancia por escrito ni de lo que otros se enteren.

- Mejor no participar en cadenas de mensajes.

- Cuidado con los archivos adjuntos: si adjuntáis demasiados ficheros o son muy grandes tardan bastante en ser transmitidos por la Red y hacen más difícil su recepción por parte del destinatario. Por lo general se recomienda que, si el archivo adjunto supera los 500 kb, pidáis permiso para enviarlo.

- La firma de todos los mensajes es más que recomendable: acredita nuestra personalidad, avala el contenido y marca la finalización del contenido de la misiva electrónica. Es tanto más imprescindible cuando intercambiamos mensajes relacionados con el trabajo o los estudios.

Cadenas de mensajes

Hacer cartas-cadena tiene varias implicaciones. Gasta ancho de banda que podría ser mejor utilizado (y que le cuesta dinero a otras personas) y muy probablemente algún *spammer* va a capturar las direcciones y mandar muchos correos no deseados. Los chistes, archivos adjuntos de presentaciones PowerPoint y otras ocurrencias textuales o gráficas también caen sobre esta categoría, por lo que la regla puede resumirse en: mejor no enviar correos que las demás personas no están esperando ni desean especialmente.

Con recomendaciones más o menos vigentes a través de la evolución de Internet, la netiqueta nos recuerda la clave fundamental de la comunicación en red: formamos parte de un conjunto de personas interrelacionadas electrónicamente. Por lo tanto, cuanto más cívicas sean nuestras acciones individuales en la Red, mejor contribuiremos a la convivencia en sus distintos ámbitos sociales y más nos beneficiaremos individualmente de ello como uno más de sus miembros.

4.6. Interactuamos en redes sociales

Más allá de la localización de información y de la comunicación bidireccional, el uso de Internet nos permite interactuar en comunidades de distinto signo y formato como la mensajería instantánea, blogs, redes sociales... Se trata de distintos ámbitos de actuación electrónica donde nuestra actitud digital será decisiva para hacer más rápida, fluida, eficiente y directa la interacción inmediata y permanente con otros usuarios... o para dificultarla hasta el punto de hacerla imposible o peligrosa.

4.6.1. Mensajería instantánea

Los programas clientes de mensajería instantánea nos proporcionan las indudables ventajas de la comunicación permanente con otros usuarios en tiempo real. No obstante, también requieren algunos hábitos de uso razonable para que su eficacia comunicativa sea óptima.

Programas de mensajería instantánea

El popular Messenger de Windows, pero también Yahoo! Messenger, Google Talk, AIM, ICQ...

Desde el punto de vista de la gestión:

- Nos conviene ser selectivos cuando agregamos contactos: una lista extensa de amigos nos puede obligar a dedicar un tiempo excesivo a la atención de las peticiones de conversación.

- Configurar correctamente el estado en las redes de las que formamos parte nos ayudará a seleccionar las conversaciones que podemos y queremos atender en cada momento.

- La corrección sintáctica de los mensajes, y su tono, dependerán en cada caso del grado de familiaridad y confianza con el interlocutor o la Red de conversación. En conversaciones colectivas muy amplias, conviene mantener una redacción y un tono correctos y lo más neutros posible.

Y en la perspectiva de la seguridad:

- Es aconsejable evitar invitaciones a la conversación que resulten sospechosas o que tengan un origen desconocido, sobre todo si nos requieren que visitemos otras páginas web: pueden ocultar una fuente de transmisión de virus o programas espía.

- Cuando agreguemos contactos al cliente de mensajería, nos conviene tener un conocimiento razonable de quién es realmente el interlocutor. Es aconsejable la máxima precaución ante posibles contactos que nos resulten desconocidos.

- Ante los ficheros adjuntos, en la mensajería instantánea nos conviene mantener las mismas prevenciones que aplicamos en el uso del correo electrónico.

- En los mensajes instantáneos conviene no incluir nunca datos personales confidenciales como contraseñas, claves bancarias o números de cuenta, numeración de tarjetas de crédito...

4.6.2. Los blogs

El estilo, el tono y la corrección de las anotaciones son definitorios de la identidad y credibilidad del autor de un blog. Junto a la aceptación generalizada de estilos personales de redacción y expresión, el tipo de lenguaje y la forma de plasmarlo pueden acreditar o desautorizar un blog de forma global y potenciar o limitar sus expectativas de comunicación y relación. Tanto como autores como lectores de blogs, puede sernos de mucha utilidad tener en cuenta que:

- Desde el punto de vista de la comunicación con lectores y usuarios, la Redacción de anotaciones debería ir orientada a la conversación y a la apertura y mantenimiento de diálogos y debates.

Narraciones personales

La simple proyección de pensamientos subjetivos y narraciones personales no favorece el establecimiento de relaciones ni la creación de vínculos de comunidad con otros usuarios. Por lo tanto, tampoco ayuda a generar nuevas entradas ni circulación de comunicación.

- Desde la perspectiva de la visibilidad del blog, conviene redactar las anotaciones con brevedad y con tendencia a insistir en aquellos términos y conceptos que consideramos claves. Además de facilitar el comentario de los lectores, conviene recordar que los buscadores y sindicadores de contenidos incluyen el titular y las primeras frases de las anotaciones: lo que aparezca en los titulares y primeras palabras será el reclamo para atraer la atención de posibles lectores y sus eventuales intervenciones.

- La actualización frecuente de contenidos es fundamental parar mantener el movimiento comunicativo en el blog y generar dinámicas de relación, a la vez que también incide en el grado de credibilidad, tanto de los contenidos, como de la misma intencionalidad comunicativa del autor.

- El uso intensivo del enlace de hipertexto es uno de los elementos definitorios del blog como medio de edición y publicación y lo que lo diferencia de otros canales (como los basados en el papel) y de otros formatos (como los formatos electrónicos cerrados o fuera de red). Una utilización restrictiva de enlaces en un blog es claramente contradictoria con su naturaleza como medio de comunicación y relación en red.

Los blogs, igual que la mensajería instantánea y las redes sociales, nos convierten en miembros de comunidades en las que nos conviene actuar con actitudes digitales básicas de respeto y conducta cívica. De este modo, mejoraremos el funcionamiento y la fluidez e interacción entre los miembros de esas comunidades y nos beneficiaremos de mejoras como miembros de esas redes.

4.6.3. Redes sociales

El uso de la mayoría de canales de Internet, por su propia naturaleza, ya nos integra en redes sociales de características diversas: red de contactos del correo electrónico, grupos de contactos en programas de mensajería instantánea, telarañas de blogs y comunidades que comparten vídeos, archivos de audio...

Comunidades virtuales

Comunidades virtuales como Facebook o MySpace han consolidado el grupo de amigos por Internet como una de las redes sociales por excelencia, al dotar de canales tecnológicos de interacción permanente a sus usuarios y a sus amigos y conocidos, y a los amigos y conocidos de éstos, etc. en una telaraña prácticamente interminable de contactos, intereses y aficiones compartidas.

Formar parte de estas redes sociales presenta innumerables ventajas, siempre que adoptemos hábitos de uso y gestión tan sostenibles y razonables como los que exigimos a los otros miembros de la comunidad:

Los contactos

Los contactos por los contactos sirven de poco, ocupan mucho tiempo de gestión y generan un incalculable volumen de tráfico innecesario y estéril.

- Las redes sociales y los grupos de amigos facilitan el envío de mensajes y recomendaciones masivas a todos nuestros contactos: restringirlas a los casos necesarios hará que ahorremos recursos y evitará que nuestros contactos opten por dejar de serlo cuando se cansen de una insistencia repetitiva en asuntos que no les interesan.

- Nos conviene añadir y dejarnos ser añadidos a grupos de miembros con los que tenemos realmente intereses afines.

- Es recomendable no instalar aplicaciones de forma generalizada: una buena manera para seleccionar qué aplicaciones instalar es comprobar cuáles utilizan más asiduamente los amigos de la Red social.

- También conviene evitar enviar sistemáticamente invitaciones a todos los contactos: es mejor seleccionar a un grupo de amigos afín, previamente interesados en la recepción de dicha invitación.

- No añadir como amigos a gente desconocida: coleccionar amigos no hace más populares a los usuarios. Tampoco es recomendable aceptar como amigas a todas las personas desconocidas que lo soliciten, ya que son propensas a reenviar todo tipo de *spam* social.

- Participar sólo en grupos de intereses afines. La cantidad de contactos en una red social tiene una relevancia infinitamente menor que el conocimiento concreto expresado en participaciones y casos determinados.

4.6.4. Privacidad

La proliferación de redes sociales y de intercambio de archivos entre usuarios otorga especial sensibilidad a las cuestiones relacionadas con la privacidad de las personas, más allá, incluso, de los derechos legales explícitos de propiedad o autoría sobre los contenidos. Ante la multiplicidad de archivos de sonido, fotografías y vídeos que podemos obtener en la Red y gestionar fácilmente con los programas de tratamiento digital, nos conviene adoptar como límite razonable el respeto a la intimidad y la privacidad.

Respetamos la privacidad de los demás usuarios:

- No utilizando sin un permiso explícito sus fotografías y vídeos en nuestros propios ficheros digitales y menos si pensamos utilizarlos públicamente de forma presencial (presentaciones, trabajos, estudios...) o en la Red (blogs, vídeoblogs, redes sociales...).

- No distribuyendo esos contenidos en nuestra lista de contactos de correo electrónico, comunidades virtuales, redes profesionales o de formación...

Respetamos nuestra propia privacidad:

- Valorando cuidadosamente a quién y cómo enviamos o damos acceso a ficheros privados de sonido, imagen o vídeo.

- Analizando qué derechos de propiedad y gestión podremos mantener sobre nuestros ficheros de sonido, imagen o vídeo si los alojamos en determinados servidores gratuitos de Internet.

- Teniendo en cuenta que nuestros ficheros de imagen y sonido pueden seguir circulando en la Red más allá de las previsiones iniciales y que esa proyección puede persistir en el tiempo mucho más de lo que habíamos previsto o de lo que nos pueda interesar cuando pasen las semanas, los meses, los años...