



## Privacidad en la Red

# A salvo de miradas

Los correos electrónicos pueden cifrarse para que el emisor tenga la certeza de que sólo el receptor por él previsto accede a su contenido



Imagínese la situación. Si quisiera presentar a su jefe una brillante idea que pudiera interesar a la competencia, ¿la redactaría en una tarjeta postal que tuviera en el anverso un paisaje de Benidorm? Pues esa es la forma habitual de proceder con el correo electrónico. Rara vez se "cierra el sobre" en las comunicaciones digitales, por lo que cualquiera que se encuentre en el recorrido del email y tenga unas nociones mínimas de informática puede leerlo sin mayor impedimento.

La inseguridad no es una característica inherente a Internet. La Red ofrece formas de lacrar digitalmente los envíos y hacerlos inviolables. Es lo que se conoce como **cifrado o encriptación**. La potencia de los ordenadores actuales y la calidad de los algoritmos desarrollados convierten en un juguete a las máquinas nazi Enigma que tuvieron en jaque a los aliados durante la Segunda Guerra Mundial. La única posibilidad para desentrañar un mensaje cifrado con los métodos actuales consiste en la fuerza bruta: decenas de los supercomputadores más potentes trabajando en común durante años sólo podrían desenmascarar un único mensaje.

**Firma digital.** No obstante, la encriptación también tiene sus problemas. No todo el mundo está dispuesto a pasar por el engorro de cifrar y

descifrar cada mensaje que le llega. Por eso, los programas de encriptación permiten quedarse a medio camino entre la seguridad total (que al menos implica que emisor y receptor se pongan de acuerdo sobre cuál de los sistemas utilizar) y la alegre despreocupación con la que se remiten en la actualidad la mayoría de emails. A ese medio camino llega la firma digital. Al final de cada correo electrónico se añade una serie de números y letras creadas *ad hoc* para ese mensaje en particular. Con la aplicación apropiada, el receptor puede comprobar

### Abracadabra

>En el mundo digital las llaves no tienen por qué ser físicas. Las claves (palabras o números que el interesado cobija en su memoria) son indispensables para encender el teléfono móvil, sacar dinero de un cajero automático, conectarse a Internet o leer el correo electrónico. En definitiva, para identificarnos como el usuario legítimo de esos objetos.

>Pero, ¿cómo escoger una clave segura? Una sucesión aleatoria de números y le-

### NAVEGAR A LA CARTA

#### ➔ Kriptópolis ([www.kriptopolis.com](http://www.kriptopolis.com))

Una de las webs españolas más completas sobre privacidad en la Red. Se encuentra en plena transformación tecnológica, por lo que muchos de sus servicios no funcionan como debieran.

#### ➔ PGP ([www.pgp.com](http://www.pgp.com))

Privacidad Bastante Buena (Pretty Good Privacy). Curioso nombre para uno de los sistemas de cifrado de documentos más laureados de todos los tiempos. La decisión de ocultar el código fuente (las tripas) del programa PGP ha provocado recelos en un numeroso grupo de usuarios, que ha creado alternativas libres y transparentes como GnuPG.

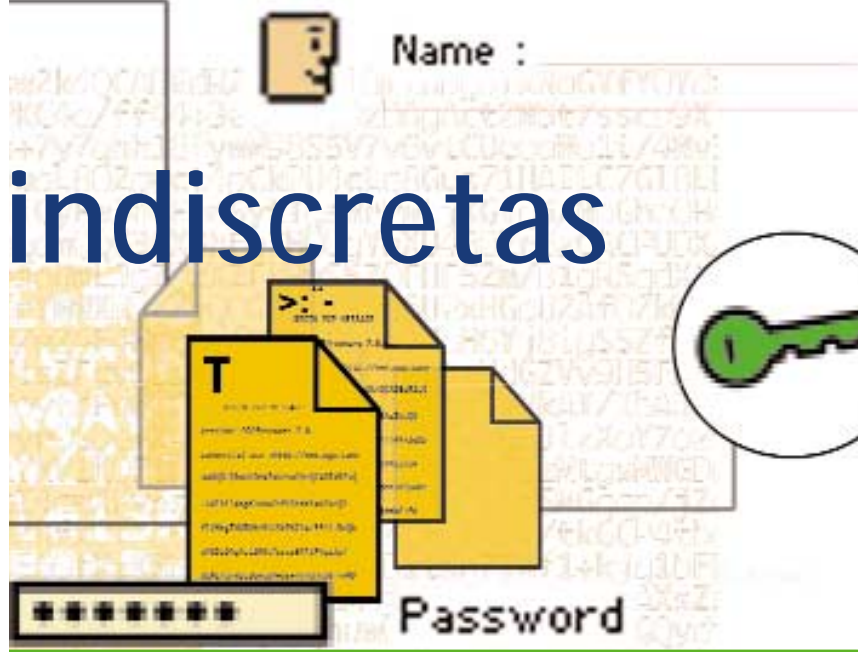
#### ➔ Recursos sobre criptografía ([cys.derecho.org/recursos/cripto.html](http://cys.derecho.org/recursos/cripto.html))

Amplio listado con enlaces variopintos desde los que descargar los programas que convertirán al ordenador casero en un fortín. Un buen punto de partida para profundizar en el uso (y en los debates que suscita) la privacidad en la Red.

#### ➔ Electronic Frontier Foundation ([www.eff.org](http://www.eff.org))

Organización que defiende las libertades civiles de los cibernautas. Desde sus orígenes se ha destacado por promover una Red que, en vez de un gigantesco mercado, sea un foro común donde prime la libertad de expresión y el respeto a la privacidad de los usuarios.

GP MESSAGE-----  
Firmware 7.0.3 for non-commercial use <http



# indiscretas

tras (como sX8c76d) es prácticamente infranqueable, pero del todo inútil. Si la clave es demasiado complicada resultará difícil de recordar. Por el contrario, claves obvias como el equipo de fútbol o el nombre del perro pueden ser descubiertas con un poco de astucia por parte del asaltante digital. De hecho, cualquier nombre o palabra común es potencialmente peligroso: hay programas concebidos para rastrear enormes diccionarios y probar miles de términos hasta encontrar con el que abre el cerrojo electrónico.

La solución radica en el equilibrio entre comodidad y fiabilidad, aunque hay pequeños trucos para conseguir passwords eficaces.

>El sistema más habitual es utilizar palabras comunes a las que se añade faltas ortográficas de forma intencionada: ecclipse, varko o hislote. Resultan fáciles de recordar (la evidencia del error ayuda a que se fijen en la memoria) y no hay diccionario que pueda recoger el conjunto de alteraciones posible.

>Otra técnica más refinada, y que crea claves que

podrían parecer aleatorias, es el uso de refranes o muletillas: clbdvvppltar, lo que es lo mismo, las siglas de "Cuando las barbas del vecino veas pelar, pon las tuyas a remojar". Cuanto más imaginativa y personal sea la frase, menos posibilidades habrá de que alguien la averigüe.

>Y, por supuesto, no se debe jamás apuntar la clave y, menos aún, entregársela a nadie. No hay razón alguna para que una empresa que le ha permitido tener una clave se la pregunte después.

**Esteganografía: la opción más avanzada.** Para los más precavidos está la esteganografía. En la criptografía clásica, el remitente está seguro de que sólo las personas autorizadas entenderán el mensaje. Sin embargo, el emisor no podrá ocultar que la comunicación ha tenido lugar. Un ejemplo: si encontramos una carta cifrada de Pedro a Juan no la podremos leer, pero sí sabremos a ciencia cierta que Pedro le ha dicho algo a Juan. Además, se ha tomado la molestia de usar un método criptográfico para que nadie conozca el contenido de la comunicación. Y eso, hoy por hoy, resulta sospechoso.

Ahí entra en juego la esteganografía, una técnica que oculta la mera existencia de la comunicación. Hay programas de ordenador capaces de empujar cualquier información en las fotos digitalizadas de la última visita al parque de atracciones, también los hay que construyen textos simples que no levantarían sospechas (parecen estar escritos por niños), tras los que se esconden los mensajes auténticos. Y es que, ¿quién se va a molestar en intentar la descryptación de una información que no parece estar encriptada?

**Dudas razonables.** Sin embargo, todos estos sistemas suscitan dudas razonables. Un juez puede decretar la intervención de un correo o de una línea telefónica, pero no hay forma física de descifrar un mensaje sin la colaboración de su propietario. Organizaciones de defensa de la libertad civiles en Internet, como Electronic Frontier Foundation, defienden el uso de la criptografía argumentando que prohibir las técnicas de cifrado sólo ayudará a los criminales, ya que las técnicas están tan extendidas que los delincuentes no tendrán problemas en seguir usándolas, mientras que el común de los mortales se verá privado de un derecho básico como la privacidad. En definitiva, se trata de la enésima reedición del viejo debate sobre el equilibrio entre seguridad y libertad.

si el remitente es quien dice ser, y, lo que es aún más importante, si el mensaje ha sido manipulado durante su trayecto por el ciberespacio.

Cifrar o firmar digitalmente los mensajes no es exclusivo de usuarios muy avanzados. Cualquiera que disponga de los tutoriales apropiados (*Kriptopolis.com* dispone de documentación práctica) puede instalar un programa de esta índole. Después, el acto de encriptar o firmar un envío se limita a hacer clic en un botón de la aplicación habitual de correo electrónico.

Con la firma digital  
el receptor puede  
comprobar si el  
remitente es quien  
dice ser y si el mensaje  
ha sido manipulado