AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Recomendaciones dirigidas a usuarios de internet

SUM@RIO

I. INTRODUCCIÓN

La llamada "Sociedad de la Información", entendida como la definición de la extraordinaria expansión de las tecnologías de la información y las comunicaciones y, en especial, de Internet como vehículo de la nueva Sociedad del Conocimiento, se ha constituido en una herramienta imprescindible para el desarrollo individual y colectivo de los pueblos.

Su incorporación a la vida ordinaria de los individuos ha hecho ya y lo hará, aún más, en el futuro, que prácticamente aquél que no disponga de acceso a Internet se encuentre excluido de la vida económica y social.

Todos sabemos que las nuevas tecnologías de las telecomunicaciones ofrecen innumerables ventajas, como la comodidad para realizar muchos trámites que ya no nos exigen desplazarnos personalmente a realizar una determinada gestión, o la posibilidad de mejorar la eficiencia en el empleo de los recursos.

Ahora bien, el entorno de Internet que, por sus innegables ventajas, se constituyó en un instrumento que debía de ser propiciado por los diferentes Gobiernos, sin embargo, también se convirtió en un medio para que la nueva delincuencia tecnológica pusiera buena parte de sus esfuerzos en tratar de sorprender a muchos usuarios, que creían que la red no podía nada más que favorecerles a todos los niveles. Por ello, resulta prioritario emplear todos los medios a nuestro alcance para crear en los actores intervinientes en Internet un entorno de confianza para el empleo de este nuevo medio.

Desde dicho punto de vista, la problemática de la protección de datos personales en Internet se constituye en pieza fundamental para que se haya de generar en el ciudadano una "cultura para la protección de sus datos en el nuevo entorno digital de la Sociedad de la Información", ya que de ella dependerá que cada persona pueda hacer un uso seguro de Internet para lograr un mejor nivel de vida.

Con el fin de contribuir a ir generando dicha cultura de la protección de datos en el ámbito de la Sociedad de la Información a través de Internet, la Agencia Española de Protección de Datos ha elaborado, con motivo del Día Mundial de Internet que se celebra el día 17 de mayo, las siguientes recomendaciones, en las que se analizan los principales riesgos que, hoy en día, aparecen en la Red y se enumeran algunas instrucciones para tratar de prevenir sus efectos.

II. SERVICIOS DE NAVEGACIÓN

Los riesgos existentes al navegar a través de la red pueden ser numerosos. Por ejemplo, las ventanas emergentes o "pop-up" que son ventanas adicionales que se abren cuando se visitan algunas páginas web pueden contener anuncios o presentar ofertas especiales tras las cuales se puede ocultar la instalación de un software malicioso.

Las operaciones de descarga de archivos también pueden entrañar riesgos, ya que esta operación puede utilizarse para que se instale en el equipo un software malicioso con diferentes finalidades: borrado de datos, ralentización del sistema, robo de datos de contraseñas y de datos personales, seguimiento de los sitios web visitados, etc.

A la hora de facilitar datos de carácter personal en la red hay que asegurarse de la identidad de quién procede a la recogida de los mismos, facilitando, en todo caso, exclusivamente los necesarios para la finalidad con la que se recaban.

A la vista de los posibles riesgos que puede suponer navegar por Internet, conviene tener presentes las siguientes recomendaciones:

- El equipo deberá protegerse adecuadamente utilizando para ello un software de antivirus y de seguridad específico.

- Debería configurarse de manera adecuada el software del navegador con las opciones de seguridad más restrictivas y eficaces.

- El software instalado en el equipo se deberá actualizar periódicamente con objeto de disponer en el mismo de la última versión, prestando especial atención al sistema operativo, al software antivirus, al propio navegador y a las opciones disponibles de seguridad.

- El intercambio y la entrega de datos de carácter personal debería efectuarse, exclusivamente, en aquellos sitios que cuenten con protocolos seguros. En todo caso, antes de facilitar datos de carácter personal hay que asegurarse de que el sitio web dispone de política de privacidad y que en la misma se facilita, entre otra información, la identidad y dirección del responsable y la finalidad con la que se recaban los datos, los cuales deberán ser los estrictamente necesarios para la finalidad de que se trate.

- El intercambio y la entrega de datos de carácter personal deberá efectuarse, exclusivamente, en aquellos sitios que cuenten con protocolos seguros y en los que se respeten los principios previstos en la legislación en materia de protección de datos. En todo caso, antes de facilitar datos de carácter personal hay que asegurarse de que el sitio web dispone de política de privacidad y que en la misma consta, entre otra información en materia de protección

de datos, la identidad y dirección del responsable y la finalidad con la que se recaban los datos, los cuales deberán ser los estrictamente necesarios para la finalidad de que se trate.

- El equipo deberá protegerse a través de una contraseña que restrinja el inicio de sesión y que impida que un tercero pueda acceder a él. Las contraseñas deberán mantenerse, por supuesto, en secreto, no revelándose a ningún tercero y no serán anotadas en lugares fácilmente accesibles.

- Deberá evitarse acceder a los sitios web a través de enlaces incluidos en mensajes de correo electrónico o en sitios web de terceros.

- Con objeto de evitar que se pueda realizar un seguimiento de las visitas efectuadas a otros sitios web, se borrarán del equipo periódicamente los archivos temporales y las "cookies", teniendo en cuenta que, en este último caso, el usuario puede configurar el navegador para evitar la grabación de las "*cookies*" en el equipo.

- Con objeto de evitar la instalación de software malicioso, deberá disponerse de utilidades que permitan el bloqueo de las ventanas emergentes.

- Deberán adoptarse las precauciones oportunas antes de proceder a la descarga de archivos asegurándose, antes de hacerlo, de la confianza o acreditación del sitio web desde el que se realizará.

- En aquellos equipos que no sean de uso personal, deberá desactivarse la opción que poseen los navegadores que permite el almacenamiento de las contraseñas o el guardar información relativa al inicio de las sesiones (usuario y contraseña). También se prestará especial atención para deshabilitar la opción de los navegadores que permite mantener un historial de direcciones web, nombres de usuarios y contraseñas con el fin de permitir su uso en la cumplimentación automática de formularios. Resulta especialmente conveniente que, al finalizar la sesión de navegación en esos equipos, se eliminen todos los archivos temporales, las "cookies" y el historial de Internet que se encuentra en el navegador.

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

RECUERDE

Es conveniente la utilización de software antivirus y de seguridad específicos, así como configurar el software del navegador con las opciones de seguridad más restrictivas.

Es imprescindible actualizar periódicamente el software del equipo con objeto de disponer de las últimas versiones.

El intercambio y la entrega de datos de carácter personal deberá efectuarse en los sitios web que dispongan de protocolos seguros y de política de privacidad.

El equipo deberá protegerse mediante contraseña, impidiendo con ello los inicios de sesión y accesos no autorizados.

Deberá asegurarse la confianza o acreditación de los sitios web antes de proceder a la descarga de archivos.

III. CORREO ELECTRÓNICO

El correo electrónico (e-mail) es el servicio de comunicación que ha alcanzado un mayor nivel de desarrollo en Internet, tanto a nivel de comunicación privada como en el ámbito de las relaciones profesionales y comerciales. En ese sentido, el mismo hecho de su éxito y nivel de utilización lo convierte en uno de los medios más utilizados de difusión de software malicioso y de contenidos no solicitados que pretenden tener una difusión masiva con un coste reducido para sus autores.

El usuario que quiera utilizar el servicio de correo electrónico necesitará un programa cliente instalado en el equipo del que disponga - un ordenador personal, un teléfono móvil, u otro dispositivo que permita el acceso a Internet - configurado para la utilización de una o más direcciones de correo electrónico de las que sea titular. Por otro lado, esa dirección de correo electrónico lleva aparejada la existencia de un fichero que hace las funciones de buzón de correos, cuya gestión lleva a cabo un programa servidor instalado en los equipos del Proveedor de Servicios de Internet con el que se haya contratado el servicio. El acceso al buzón de correos ha de requerir la introducción de un identificador de usuario y una clave de acceso.

En otros casos, el acceso al correo electrónico se podrá obtener realizando una conexión al proveedor de servicio utilizando un navegador, lo que permite su uso con independencia de que se disponga en ese momento de un dispositivo de acceso propio. Este modo de acceso, al que se ha venido en denominar correo-web, tiene hoy en día un gran nivel de difusión derivado de su facilidad de acceso, bajo coste y la puesta a disposición por parte de la generalidad de los Proveedores de Servicio de un conjunto de servicios de valor añadido - antivirus, filtros de mensajes no deseados, agendas de direcciones, etc. - que facilitan una mejor y más sencilla experiencia de usuario. No obstante, la utilización del servicio de correo web lleva implícita la asunción de los riesgos descritos en el apartado dedicado a los servicios de navegación web.

Dentro del correo electrónico se pueden distinguir tres tipos de riesgos referentes a la protección de datos personales:

LA RECOPILACIÓN DE DIRECCIONES DE CORREO ELECTRÓNICO

Hay que tener en cuenta que la dirección de correo es la forma más común de registrar la "identidad" de una persona en Internet y puede servir de base para la acumulación de información en torno a la misma. Esta dirección se utiliza en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, utilizando, por ejemplo, instrucciones incluidas en los programas para transmitir la dirección de correo electrónico del cliente sin que éste sea consciente de ello, o configuraciones de seguridad en los navegadores que permiten a un sitio web conocer las direcciones de correo electrónico de sus visitantes.

En este sentido, la inclusión de datos en directorios de personas accesibles al público en Internet, sin las adecuadas medidas de seguridad, supone exponer a los usuarios a que sus datos puedan ser recopilados sin su conocimiento y utilizados para otros fines. Existen programas específicamente diseñados para dicho fin, práctica que se conoce como "cosecha" ("harvesting") de direcciones de correo electrónico, que son posteriormente utilizadas para el envío masivo de comunicaciones no solicitadas. Idéntica consecuencia puede suponer la participación por parte de los usuarios en cadenas de mensajes, sin adoptar precauciones como eliminar las direcciones de destinatarios que han ido siendo incluidas en las sucesivas retransmisiones del mensaje, que suelen ser recopiladas por programas específicos o por el usuario que ha originado la cadena. Esta práctica, conocida también como "hoax", permite la difusión de mensajes de correo electrónico de contenido normalmente engañoso, con la finalidad no declarada de obtener direcciones de correo electrónico para su uso posterior o de servir a intereses específicos del autor. Además de las consecuencias aquí descritas, suelen tener un alto grado de incidencia en el nivel de servicio de los sistemas gestores de correo electrónico.

LA SUPLANTACIÓN DE IDENTIDAD

Hay que considerar que todos los servicios aquí tratados no facilitan, de forma generalizada, el establecimiento fiable de la identidad de emisor y receptor. Tampoco se utilizan habitualmente mecanismos que garanticen la confidencialidad en el intercambio de la información. Por estos motivos, deben considerarse los riesgos de suplantación de la personalidad o violación del secreto de las comunicaciones a la hora de remitir por correo electrónico información de relevancia.

LA INSTALACIÓN DE SOFTWARE MALICIOSO

No es infrecuente que aparezcan, a menudo, avisos relativos a la aparición de un "nuevo virus o gusano" cuyo principal canal de distribución es el servicio de correo electrónico.

Uno de los formatos de inclusión de este tipo de piezas de software en los mensajes de correo son ficheros anexos modificados, cuya estructura esconde instrucciones para instalar nuevos programas o versiones modificadas de alguno preexistente, por lo que hay que procurar ser cuidadosos en su manejo, verificando siempre que su origen corresponde a una fuente de confianza y que disponemos de los adecuados medios de protección.

Por último, hay que hacer mención como riesgo asociado al correo electrónico el derivado de la difusión de mensajes de contenido engañoso o fraudulento, que son utilizados como vehículo de obtención de información sensible de los usuarios relacionados con otros servicios de Internet, como puedan ser la banca en línea. Aunque a este tipo de fenómenos se les dedica atención específica en este documento, también le son de aplicación las recomendaciones que seguidamente se detallan.

En todo caso, las recomendaciones relativas al uso del servicio de correo electrónico son las siguientes:

- Para acceder a su cuenta de correo electrónico, además de su código de usuario utilice una contraseña. Elija una contraseña que no sea una palabra de los idiomas más utilizados (una combinación aleatoria de letras mayúsculas y minúsculas, números y símbolos es una buena elección) y cámbiela de forma periódica.

  No utilice la opción de "*Guardar contraseña*" que, en ocasiones, se le ofrece para evitar reintroducirla en cada conexión.

- Si no quiere hacer pública su dirección de correo electrónico, configure su navegador para que no se la facilite a los servidores Web a los que accede.

- Conviene tener en cuenta, antes de proporcionarlos, que tanto nuestra dirección de correo electrónico como el resto de datos que proporcionamos para su inclusión en un directorio o lista de distribución, son susceptibles de ser utilizados sin nuestro conocimiento para fines diferentes de aquellos para los que fueron suministrados.

- Sea consciente de que cuando envía mensajes de correo a una variedad de destinatarios, está revelando las direcciones de correo electrónico de los mismos que figuran en los campos "*Destinatario*" o "*Con Copia (CC)*" a todos los receptores del mensaje. Para evitarlo, puede incluir los destinatarios del mensaje en el campo "*Con Copia Oculta* (CCO)" de tal forma que ninguno de los receptores podrá acceder a la dirección de correo electrónico del resto de los destinatarios.

- Configure su programa de correo en el nivel de seguridad máximo. Si es Vd. usuario de correo web, decántese de ser posible por un proveedor de servicios que ofrezca análisis del contenido de los mensajes; Además, configure su navegador en el máximo nivel de seguridad posible.

- Mantenga actualizado su programa cliente de correo electrónico, su navegador y su sistema operativo.

- No abra los mensajes que le ofrezcan dudas en cuanto a su origen o posible contenido sin asegurarse, al menos, que han sido analizados por su software antivirus.

- Active los filtros de correo no deseado de su programa de correo electrónico.

- Procure no utilizar para usos personales la dirección de correo electrónico que le haya sido proporcionada en el marco de su relación laboral. Tenga en cuenta que, en algunos casos, los mensajes de correos de esas cuentas pueden ser monitorizados por la entidad responsable de las mismas. En todo caso, solicite ser informado de las limitaciones de uso establecidas así como de la posibilidad de que sea monitorizado el contenido del buzón de correo asociado.

- Evite reenviar cadenas de mensajes.
- Si ha de remitir mensajes a un conjunto de usuarios conocido, utilice, si su programa cliente de correo lo permite, las direcciones de grupo.
- Lea cuidadosamente las condiciones del servicio que su proveedor de correo electrónico ha de poner a su disposición, haciendo especial hincapié en todo lo referido a la obtención y uso de sus datos de carácter personal, así como los medios de los que dispone para garantizar la privacidad de sus mensajes.
- Si va a enviar por Internet documentos privados, es conveniente utilizar sistemas que permitan el cifrado de su contenido.

RECUERDE

Use de forma cuidadosa su dirección de correo electrónico.

Mantenga actualizados su sistema operativo, programa de correo y antivirus.

No proporcione su dirección de correo electrónico si no está seguro de las intenciones de aquél que se la requiere.

Evite difundir cuando no sea necesario las direcciones de correo electrónico de otras personas de las que disponga por motivos personales o profesionales.

No reenvíe mensajes sin haber comprobado de forma previa que no representan un riesgo potencial para sus destinatarios. No siga los mensajes en cadena.

Infórmese de las condiciones de prestación del servicio de correo electrónico del que disfrute. Solicite información y siga las limitaciones de uso de las cuentas de correo que utilice en el marco de sus relaciones laborales o profesionales.

IV. VIRUS, GUSANOS Y ATAQUES DE INGENIERÍA SOCIAL

Podemos encontrar en Internet un conjunto de programas, denominados en su conjunto "malware" o software malicioso, que son creados con la intención principal de provocar daños, utilizar los recursos de los usuarios o recabar información de utilidad para los creadores o usuarios de los mismos. Por otro lado, Internet es también zona de práctica para aquellos que aplican técnicas de ingeniería social con el objetivo de recabar información relevante de los usuarios que pueda ser utilizada para obtener algún tipo de beneficio, generalmente económico. Entre estas prácticas están de plena actualidad las conocidas como "phising" y "pharming", cuyos ataques están alcanzando gran nivel de virulencia provocando importantes daños en sectores como la banca en línea en Internet.

Los "virus" son programas que, incorporados en ficheros ejecutables o con formatos de uso común por los sistemas operativos habituales, logran acceso al sistema con la finalidad de ejecutarse y, en la mayoría de los casos, reproducirse mediante copia que se aloje en otros ficheros o en otros sistemas. El nivel de peligrosidad de los virus se establece en función de los daños que es capaz de producir en el sistema - desde la aparición de mensajes hasta la total destrucción de la información de los equipos infectados - y de su velocidad y facilidad de propagación.

Su desarrollo y creación tienen mucho que ver con las vulnerabilidades existentes en el software de uso común, por lo que una primera barrera de prevención la encontraremos en mantener actualizado y al día nuestro sistema, además de utilizar herramientas de detección y desinfección. Además, hoy en día existen numerosos servicios públicos donde podremos encontrar cumplida información sobre cualquier virus, además de información sobre como prevenir sus ataques.

El término "gusano", o "gusano de Internet", denomina a aquellos programas diseñados para ser capaces de trasladarse a través de redes de computadores con el fin de realizar una actividad concreta incorporada en su código. Aunque su finalidad no tiene en principio que entrañar peligro, estos programas pueden instalar un virus, instalar un programa que actúe en segundo plano sin conocimiento del usuario, o dedicarse a consumir ancho de banda del sistema utilizándolo para realizar acciones como el envío masivo de correo electrónico.

En cuanto a los "troyanos" o "caballos de Troya" son, como su propio nombre indica, programas que simulan realizar una función distinta a aquella para la que han sido diseñados, y que entran en el sistema bajo el disfraz de software útil para el usuario. Una variante de éste tipo de software malicioso son las "bombas lógicas" programas que permanecen inactivos en el sistema hasta que son activados por la ocurrencia de un evento o por el mero paso del tiempo, y que permanecen ocultos en el código del programa.

Podemos definir al "phising" como una forma de ingeniería social en la que se

intenta obtener de forma fraudulenta información sensible de una víctima suplantando la identidad de un tercero de confianza. El principal objetivo ha sido hasta el momento la información de acceso de usuarios de banca en Internet o sitios web dedicados a las subastas, en los que es factible tener acceso a cuentas bancarias y tarjetas de crédito.

El cauce más habitual de difusión de estos ataques es el correo electrónico. No es inhabitual recibir mensajes remitidos supuestamente desde los servicios de atención al cliente de un banco que nos requieren, por ejemplo, la introducción de un código de usuario y su clave de acceso para "validarlos" en un formulario que simula ser parte del sitio web de una entidad financiera. Otra modalidad, de reciente aparición, es la que utiliza el canal telefónico, realizando una llamada al domicilio del usuario simulando hacerlo desde el Centro de Atención al Cliente de un Proveedor de Servicios de Internet y solicitando al usuario que introduzca datos de carácter personal en un formulario colocado en un sitio Web controlado por los atacantes.

En cuanto al "pharming", de mayor complejidad técnica en su desarrollo, podemos decir que trata de conducir al usuario a un sitio web simulado, alterando bien los servidores del sistema de nombres de dominio de Internet (DNS) o bien manipulando ficheros en los equipos de los usuarios con la finalidad de que redirijan las peticiones de acceso a determinados sitios web a otros sistemas controlados por el atacante.

Aunque la mayoría de los ataques son detectados y rechazados por los servicios de prevención de los que disponen los proveedores de servicio y las entidades implicadas, siempre hay un margen de tiempo hasta que se ponen en marcha las medidas de protección reactiva, en el que somos vulnerables a este tipo de ataques, por lo que hay que tener en cuenta las siguientes recomendaciones:

- No instale software que no proceda de una fuente fiable. Utilice los servicios de descarga del fabricante o los sitios autorizados por él para la obtención de nuevas versiones o actualizaciones.

- Utilice programas antivirus, y, si dispone de ellos, instale cortafuegos y programas especializados en el control de "*spyware*" y sus variedades. Consulte de forma periódica los sitios web con información sobre la aparición de nuevas variantes y formas de prevención.

- Realice periódicamente copias de seguridad del contenido de su equipo.

- Tenga en cuenta que su entidad financiera o prestador de servicios no le va a solicitar nunca información sobre su identificador de usuario y palabras de paso. Rechace los mensajes de correo que así se lo soliciten, los que no estén redactados en su idioma habitual de comunicación con su entidad, o los que no sean remitidos por su entidad.

- Si su entidad puede proporcionárselos, adopte sistemas adicionales de control de acceso a sitios web con información sensible, como puedan ser tarjetas de coordenadas o dispositivos de generación de claves de acceso. Cuantos más niveles de seguridad disponga para su acceso, más difícil será para un atacante poner en compromiso sus bienes.

- Actúe con prevención frente a ofertas económicas que ofrezcan grandes beneficios en poco tiempo y con poco esfuerzo. Pueden llevarle, de aceptarlas, a su participación involuntaria en actividades delictivas.

- Ante cualquier duda, consulte al servicio de atención al cliente de su entidad o proveedor de servicios. Si ha sido objeto de un ataque, y ha proporcionado información, comuníquelo igualmente a los servicios pertinentes de las Fuerzas y Cuerpos de Seguridad.

RECUERDE

Sea cuidadoso con los programas que instala.

Mantenga actualizados su sistema operativo y antivirus. Añada programas "cortafuegos" y de detección y eliminación de software espía.

No proporcione información sobre sus identificadores de usuario y mucho menos sobre sus claves de acceso.

Acuda en caso de duda a los servicios de atención al cliente de su entidad o proveedor de servicios.

Adopte sistemas adicionales de seguridad en el acceso a sus cuentas de servicio.

Manténgase todo lo informado posible.

V. COMERCIO Y BANCA ELECTRÓNICA

Los portales de comercio electrónico permiten la adquisición y venta de productos y servicios utilizando Internet como canal de comunicación.

El usuario debe dedicar un pequeño esfuerzo en conocer los servicios y el tipo de información a que puede tener acceso.

Para acceder a los servicios deberá acreditar su identidad. En la actualidad, el medio más extendido es la utilización de códigos de usuario y palabras de paso, aunque desde hace tiempo es posible utilizar certificados digitales expedidos por la Fábrica Nacional de Moneda y Timbre u otros proveedores de servicios de certificación. El DNI electrónico, que ya ha empezado a distribuirse, y que en breve estará disponible para todos los ciudadanos españoles, podrá ser utilizado para acreditar de forma fehaciente la identidad de un ciudadano en Internet.

En este ámbito conviene tener presente las siguientes recomendaciones:

- Navegue por portales conocidos.
- Siempre que sea posible utilice certificados digitales como medio para acreditar su identidad.
- Asegúrese que realiza los trámites desde un equipo libre de software malicioso.
- Compruebe que la dirección que figura en el navegador corresponde con el portal de la entidad a la que queremos acceder
- Nunca aporte datos personales, identificadores de usuario ni contraseñas si no se ha establecido una conexión segura entre el navegador y el servidor al que se accede.
- Verifique que el certificado del sitio web con el que se ha establecido la conexión segura ha sido emitido para la entidad a la que nos conectamos y por una Autoridad de Certificación que nos ofrezca confianza.
- Desconfíe de cualquier correo electrónico que solicite identificación de usuario, contraseña o firma electrónica. Ponga este hecho en conocimiento de los responsables del portal.
- En los sistemas de autenticación de usuario basado en contraseñas no utilice las mismas contraseñas en los sistemas de alta seguridad que en los de baja seguridad.

- En caso que utilice certificados digitales tenga en cuenta que el titular de éstos es el responsable de su custodia y conservación. En ningún caso deberá comunicar a un tercero la contraseña que permite activar la clave privada de firma. Solicite inmediatamente a la Autoridad de Certificación la revocación de un certificado en caso de tener conocimiento o sospecha de compromiso de la clave privada. Es muy recomendable estar bien informado del documento de la "*Declaración de Prácticas de Certificación*" emitido por la Autoridad de Certificación.

- Nunca deje desatendido el ordenador mientras está conectado y se ha establecido una conexión segura, utilice protectores de pantalla con contraseña o active las funciones de bloqueo del terminal.

- En caso de utilizar certificados digitales almacenados en una tarjeta criptográfica no dejar ésta conectada al lector del ordenador. Cuando no sea necesario utilizar los certificados extraiga la tarjeta aunque continúe utilizando los servicios del portal.

- Introducir datos financieros sólo en sitios web seguros. Además, el acceso a dichas páginas debe hacerse tecleando directamente la dirección de la banca electrónica en la barra de dirección del navegador.

- Utilice para sus compras una tarjeta de crédito específica para estos fines, con límite de gasto reducido.

RECUERDE

Antes de aportar ningún tipo de datos personales deberá asegurarse que se ha establecido una conexión segura con el portal.

El mejor procedimiento para identificar nuestra identidad ante un portal de administración, comercio y banca electrónica es utilizar certificados digitales. El DNI electrónico, que ya ha empezado a distribuirse, y que en breve estará disponible para todos los ciudadanos españoles, cumple con todos los requisitos de seguridad para autenticar nuestra identidad en Internet.
Desconfiar de los correos electrónicos que informan de cambios políticas de seguridad y solicitan datos personales y claves de acceso.

Deberá prestar especial atención y desconfiar de los correos electrónicos que informan de cambios políticas de seguridad y solicitan datos personales y claves de acceso.

No deberá dejar desatendido el ordenador mientras está conectado y establecido una conexión segura.

Habrá de mantener el anonimato en los formularios de petición de datos de sitios web, excepto cuando sea imprescindible el aportar datos personales para obtener un servicio.

VI. SERVICIOS DE MENSAJERÍA ELECTRÓNICA Y CHATS

La mensajería instantánea es un método de comunicación en línea similar al correo electrónico, aunque suele resultar más rápido.

La comunicación mediante un programa de mensajería instantánea presenta algunos riesgos similares a los del correo electrónico, aunque hay otros peligros específicos de este procedimiento de intercambio de mensajes.

Por otro lado, las salas de chat en las que se sostienen conversaciones son lugares virtuales de Internet, en los que unos participantes escriben mensajes que aparecen en los equipos del resto de manera casi inmediata.

Las conversaciones de mensajería instantánea y chat no son exactamente lo mismo, ya que la primera normalmente se refiere a una conversación entre dos personas, mientras que chat es una conversación en grupo.

Conviene tener en cuenta las siguientes recomendaciones para el uso seguro de la mensajería instantánea:

- Tenga cuidado a la hora de crear un "*nick*". Cualquier programa de mensajería instantánea le pedirá que cree un "*nick*", que equivale a una dirección de correo electrónico. Este "nick" no debe proporcionar información personal, directa ni indirectamente.

- Cree una barrera contra la mensajería instantánea no deseada. Evite que su "*nick*" o su dirección de correo electrónico aparezcan en áreas públicas (tales como grandes directorios de Internet o perfiles de la comunidad en línea) y no los facilite a desconocidos. Algunos servicios de mensajería instantánea vinculan el "*nick*" a la dirección de correo electrónico en el momento en el que el usuario se registra. Cuanto mayor sea el número de personas que puedan conocer su dirección de correo electrónico, más serán las posibilidades de recibir ataques de correo electrónico no deseado e ingeniería social.

- En una conversación de mensajería instantánea, nunca debe facilitarse información personal confidencial.

- Comuníquese únicamente con las personas que figuran en la lista de contactos o conocidos.

- No abrir nunca imágenes, ni descargar archivos, ni vínculos de mensajes de remitentes desconocidos.

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

- Cuando no esté disponible para recibir mensajes, se debe cuidar la forma en que se da a conocer esa circunstancia.

Respecto de los *chats* conviene tener presente las siguientes recomendaciones:

- No facilite nunca datos personales en una sala de chat. No envíe nunca fotografías suyas a otras personas que conozca en una sala de *chat*.
- Si le piden que introduzca un apodo o que se registre para participar en un *chat*, elija un apodo que no revele su identidad personal.
- Consulte las condiciones, el código de conducta y las declaraciones de privacidad del sitio de chat antes de iniciar la conversación en línea.

RECUERDE

El *nick* no debe proporcionar información personal.

No deberá facilitar datos que puedan afectar a nuestra intimidad, tales como nombres de pantalla o direcciones de correo electrónico, a interlocutores no conocidos.

No deberá abrir ficheros ni ejecutar programas adjuntos a un mensaje no solicitado o procedentes de remitentes desconocidos.

Cuando facilite datos personales en una sala de chat, deberá tener en cuenta que todos los usuarios que se encuentren conectados en ese momento tendrán acceso a dichos datos.

VII. EL USO DE INTERNET POR MENORES

Las alternativas que ofrece hoy en día la red a nuestros menores son muy variadas y cada vez estos hacen uso de Internet a edad más temprana. Por ello, se hace preciso señalar las siguientes recomendaciones en el caso de uso de Internet por menores:

DE CARÁCTER GENERAL:

- Los menores más jóvenes deberían estar acompañados de un adulto siempre que estén conectados. Para ello es conveniente que el equipo se encuentre en un lugar común de la casa.

- Es conveniente crear un entorno de acceso a Internet personalizado.

- Los menores deberán ser enseñados a no compartir o facilitar información personal a través de Internet.

- Los menores deberán acceder a través de Internet con cuentas usuario limitadas o restringidas, que no faciliten un acceso en modo "*administrador*"

- Los padres deberán vigilar que los menores no intercambian información con desconocidos.

RESPECTO DE LA NAVEGACIÓN Y LA RECOGIDA DE DATOS PERSONALES A TRAVÉS DE INTERNET.

- En los navegadores deberán utilizarse software especial con capacidad de filtrar aquellas páginas de contenido no adecuado y de elaborar informes de actividad de los sitios visitados o de las personas con las que se haya conversado.

- Deberán habilitarse utilidades para evitar la aparición de ventanas emergentes, ya que a través de ellos se puede recabar información de carácter personal de los menores o mostrar contenidos no adecuados.

- Los padres deberán asegurarse de que los menores sólo acceden a sitios adecuados y en los que se respeten los principios previstos en la legislación en materia de protección de datos. En todo caso, antes de facilitar datos de carácter personal, hay que asegurarse de que el sitio web dispone de política de privacidad y que en la misma se facilita, entre otra información en materia de protección de datos, la identidad y dirección del responsable y la finalidad de los datos recabados, los cuales deberán ser los estrictamente necesarios para la finalidad de que se trate.

RESPECTO DE LA UTILIZACIÓN DEL CORREO ELECTRÓNICO:

- Los menores más jóvenes deberían compartir una dirección de correo electrónico familiar en vez de tener una cuenta propia.

- Se deberá hacer uso de utilidades de filtrado de correo electrónico para evitar la recepción de correos no solicitados o de contenidos no adecuados.

RESPECTO DE LA UTILIZACIÓN DE OTROS SERVICIOS:

- En la utilización de los servicios de mensajería instantánea los menores deberán evitar el dialogar con desconocidos.

- Los menores más jóvenes no deberán participar en las salas de chat o, en todo caso, utilizar aquellas que dispongan de supervisión o moderación, utilizando siempre para las conversaciones las áreas públicas.

- En los juegos a través de la red hay sistemas que permiten la conversación de viva voz con el contrincante. En estos casos, deberá utilizarse un software de distorsión que impida el reconocimiento de la voz real del menor.

RESPECTO DE LA PROTECCIÓN CONTRA SOFTWARE MALICIOSO:

- El equipo deberá configurarse adecuadamente para evitar los accesos no autorizados de terceros, activando por ejemplo la protección mediante contraseña, y el software de sistema y de antivirus deberá encontrarse permanentemente actualizado con las últimas versiones.

- Con objeto de evitar la instalación de software malicioso en el equipo, deberá informarse a los menores de que no deben abrir los ficheros adjuntos en los mensajes de correo electrónico y evitar la descarga de programas. Asimismo, deberán configurarse los programas de mensajería instantánea para no permitir la recepción de ficheros de otros usuarios.

RECUERDE

El software del antivirus y del equipo debe encontrarse permanentemente actualizado y el acceso al mismo restringido mediante contraseña. Los menores deben acceder al equipo a través de cuentas de usuario limitadas o restringidas.

Los menores deben ser informados acerca de los peligros en el uso de Internet, advirtiéndoles de que no compartan o faciliten información desconocidos, que no abran los ficheros adjuntos en los mensajes de correo electrónico y que eviten la descarga de archivos o programas.

Los menores deben acceder a Internet a través de entornos personalizados, pudiendo utilizarse para la navegación software de filtrado de páginas de contenido no adecuado y que permita la elaboración de informes de actividad de sitios visitados.

Deberá utilizarse software que permita el bloqueo de las ventanas emergentes.

Los menores deberán utilizar las salas de chat que dispongan de moderador o supervisor.

VIII. LOS SERVICIOS "*PEER TO PEER*"

Las redes entre iguales, también conocidas como "Peer to Peer" o "P2P" son un medio de intercambio de ficheros en el que se establece una comunicación en los dos sentidos, de tal forma que a la vez que se descargan se ponen a disposición del resto de la red la parte descargada, sin tener que esperar a completar el fichero. Esto permite que la información viaje a gran velocidad y que se pueda compartir una enorme cantidad de ficheros sin tener que disponer de un único ordenador que almacene toda la información, pues la carga tanto de ancho de banda como de espacio en disco se reparte entre todos los participantes.

Estas redes se basan en un pequeño programa que se instala en el ordenador que quiera participar en dicha red. Establece unos directorios en los que almacena los ficheros descargados, que son puestos a su vez a disposición del resto de los componentes de la red. También necesitan servidores que indexen los contenidos y permitan encontrar la información que se encuentra distribuida entre todos los participantes de dicha red.

Por todo ello se hace preciso seguir las siguientes recomendaciones para los usuarios de estos servicios:

- Para acceder a las redes "*P2P*" es imprescindible instalar un programa, por lo que debe descargarse siempre de sitios reconocidos, a ser posible desde la página del creador del programa.

- En la instalación mediante procedimientos automáticos debemos hacer una copia previa del estado del sistema, y comprobar una vez instalado que tan solo se ha instalado el programa que queremos. Muchos de los clientes más conocidos instalan a la vez software malicioso que puede hacer nuestro sistema inestable o incluso rastrear nuestras conexiones o las teclas que se pulsan.

- Algunos clientes pueden controlarse vía web o mediante la conexión a un puerto determinado a través de Telnet. Limite éste acceso a las direcciones IP de su red interna. Establezca un puerto no estándar, siempre por encima del 1024, para la comunicación administrativa con el programa.

- Los programas clientes se mantienen ejecutándose en todo momento, y con los accesos de tarifa plana, el ordenador está expuesto 24 horas al día. Por ello, es conveniente la instalación de un cortafuegos que limite el acceso a los puertos del equipo.

- Como toda pieza de software, el cliente está expuesto a fallos en la programación; mantenga actualizado el software.

- Deberían valorarse los riesgos de instalar un servidor, ya que deberá publicar su dirección IP, por lo que mucha gente conocerá dónde esta su equipo y qué software tiene. Tampoco conseguirá que los ficheros se descarguen más rápido y el consumo de ancho de banda aumentará espectacularmente.

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

- En algunas redes es posible definir un nombre de usuario. Procure que no sirva para su identificación personal; es preferible utilizar un seudónimo.

- No todos los ficheros son lo que dicen ser. El nombre del fichero no implica que contenga aquello que dice contener. Es preferible no descargar ficheros ejecutables o que puedan contener software malicioso, por ejemplo, las macros de los documentos de texto.

- El contenido de los ficheros es muy variado. Vigile los ficheros que descargan sus hijos, y en caso necesario, siempre le será posible evitar la instalación del software o incluso limitar las conexiones a los puertos conocidos.

RECUERDE

Deberá mantener en todo momento actualizado el software y el Sistema Operativo.

Es conveniente la instalación de un cortafuegos que proteja el acceso no deseado al propio ordenador.

Deberá extremar las cautelas para no descargar programas ejecutables o ficheros sobre los que no se tenga la completa seguridad de que no contienen software malicioso.

Deberá valorar los riesgos de instalar el software servidor.

IX. LA TELEFONÍA IP.

Los servicios de llamadas a través de Internet utilizando el protocolo IP, también conocida como "telefonía IP" o "VoIP" no son algo nuevo, aunque sí su popularización. Básicamente este sistema transmite llamadas de voz de manera similar al envío de correos electrónicos, es decir, convierte la voz en paquetes de datos para poder transmitirlos a través de Internet, como cualquier otro paquete de información.

Las empresas de telefonía usan esta tecnología en sus grandes redes troncales, las encargadas de transmitir un gran volumen de llamadas. A nivel de particulares se han venido utilizando en redes "P2P", a través de ordenadores conectados entre sí. Pero últimamente se está extendiendo el uso de aparatos similares a los teléfonos y con un número asignado, gracias a la implantación de la Banda Ancha.

Las ventajas sobre la telefonía tradicional son muchas; es un servicio mas barato, permite el nomadismo, es decir, el uso del mismo número de teléfono independientemente de la ubicación física del usuario, pero también tiene ciertas dificultades, la principal de ellas deriva de la definición de este servicio como telefonía.

La Comisión del Mercado de las Telecomunicaciones lo ha diferenciado de la telefonía tradicional, por lo que no está afectado por las regulaciones sobre el servicio telefónico.

En esta nueva realidad conviene tener presente las siguientes recomendaciones para los usuarios de estos servicios:

- Por ahora no es un servicio de telefonía, por lo que no puede sustituir ni en calidad ni en prestaciones al teléfono tradicional. Puede que no tenga acceso a los números de emergencia (112, 091...) Y como no garantiza unos mínimos de calidad, puede que no funcione cuando se necesite. Por ahora no es un sustituto del teléfono tradicional.

- Cuando contrate uno de estos servicios, asegúrese de que la comunicación se establece utilizando una encriptación suficientemente fuerte. Si utiliza encriptación débil o inexistente no se está garantizando la privacidad en las comunicaciones que recoge el artículo 18 de nuestra Constitución.

- Las llamadas no dependen de la ubicación física del llamante. Tanto el número que aparece en la pantalla de su teléfono como el que viene reflejado en su factura puede que no coincida con quien realmente ha realizado la llamada.

- Como toda pieza de software, el programa de telefonía IP está expuesto a fallos en la programación; mantenga actualizado el software.

- Si accede al sistema "*VoIP*" desde un ordenador de uso público, recuerde eliminar todas las pruebas de su uso, especialmente la información de acceso al sistema, así como los ficheros temporales que puedan haber quedado grabados.

- Recuerde que algunos programas de "*VoIP*" permiten transmitir ficheros, con lo que debería tener precaución con los datos así obtenidos. En todo caso, vigile que no contienen virus u otras modalidades de software malicioso.

- Recuerde que algunos programas de "*VoIP*" permiten transmitir imágenes, por lo que si conecta una cámara a su sistema VoIP asegúrese de que solo transmite las imágenes que desea transmitir. Tenga cuidado con los fondos o los movimientos bruscos de cámara y recuerde que la imagen también es un dato de carácter personal.

- El acceso a "*VoIP*" a través de conexiones inalámbricas mantiene todos los riesgos antes mencionados así como los propios de estas redes: posibilidad de intercepción de los paquetes mediante escuchas no autorizadas, uso excesivo del ancho de banda, etc…

RECUERDE

Actualmente la "*VoIP*" no sustituye al teléfono tradicional, ya que no están asegurados ni el secreto de las comunicaciones ni los servicios básicos.

Deberá mantener en todo momento actualizado el software y el Sistema Operativo.

Tendrá que vigilar los ficheros e imágenes transmitidos durante las conversaciones.

La "*VoIP*" a través de redes inalámbricas no sustituye a la telefonía móvil tradicional y añade los peligros inherentes a este tipo de redes.

X. COMPETENCIAS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

A tenor de lo señalado, conviene que el usuario de Internet conozca que la Agencia Española de Protección de Datos tiene competencias sobre las siguientes materias:

- Cumplimiento de la normativa de protección de datos a tenor de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Respeto de la prohibición de emisión de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente, en los términos de los artículos 21 y 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

- La tutela de los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, en los términos previstos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

RECUERDE

Dispone de más información sobre las competencias de la Agencia Española de Protección de Datos en su página www.agpd.es.

XI. GLOSARIO DE TÉRMINOS

Ancho de Banda (Bandwidth)

Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps). Una buena analogía es una autopista. Mientras más carriles tenga la calle, mayor cantidad de tráfico podrá transitar a mayores velocidades. El ancho de banda es un concepto muy parecido. Es la cantidad de información que puede transmitirse en una conexión durante una unidad de tiempo elegida.

Attachment

Ver ***ficheros anexos.***

Cadenas de mensajes

Conocido también cadena de correo electrónico, es un sistema de propagación rápida de mensajes - en muchos casos engañosos - utilizando el correo electrónico y solicitando al usuario que lo recibe que lo remita al conjunto de usuarios que conozca.

Certificado electrónico

es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. (artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Cifrado

Tratamiento de un conjunto de datos, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos.

Conexión segura

Métodos de encriptación (habitualmente mediante *"protocolo SSL"*), que impide que la información intercambiada entre un ordenador personal y el servidor al que se conecta pueda ser accedida (garantía de confidencialidad) o manipulada (garantía de integridad) en caso de ser interceptada.

Cookie

Pieza de información que se almacena en el equipo del usuario que accede a una página web a través del navegador. Dicha información puede ser recuperada por el servidor en futuras visitas.

Correo electrónico no deseado

Mensajes de correo, habitualmente de contenido publicitario, que son remitidos a los usuarios sin que estos lo hayan solicitado previamente o hayan prestado su consentimiento. En muchos casos, se difunden de forma masiva y utilizando medios ilícitos para la obtención de direcciones de correo y para el proceso de envío.

Correo Web

Sistema de acceso al correo electrónico que se realiza utilizando el navegador de Internet y el *protocolo http*. Existen numerosos Proveedores de Servicio de Internet que ofrecen este servicio de forma gratuita o con coste reducido, aunque también puede ser utilizado por otras entidades en beneficio de sus usuarios.

Cortafuegos

Elemento de seguridad que sirve para filtrar los paquetes que entran y salen de un sistema conectado a una red.

Cosecha de Direcciones

Proceso por el cual se obtienen, utilizado software creado para ese propósito, direcciones de correo electrónico de usuarios que son recopiladas de sitios Web o de mensajes de correo.

Declaración de prácticas de certificación

Documento que especifica los procedimientos de la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, (artículo 19 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Dirección IP

Conjunto de números que identifican a un ordenador cuando se conecta a una red que utiliza el protocolo IP.

Directorios

Ficheros accesibles desde Internet que contienen información sobre usuarios a efectos de su localización por terceros. Pueden ser públicos - repertorios de abonados a servicios de telefonía - o privados - directorio de alumnos de una universidad - e incluir todo tipo de información.

DNS

Acrónimo de *Domain Name Service*.
Ver ***Servicios de nombre de Dominio***.

Documento Nacional de Identidad electrónico

Es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos. (artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Ficheros anexos

Ficheros - gráficos, de texto o ejecutables - que se adjuntan a mensajes de correo electrónicos. Se conocen también como ficheros adjuntos.

Firewall

Ver ***Cortafuegos.***

Firma electrónica

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. (artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica).

Gusano informático

Programa de ordenador - puede ser considerado una clase de virus informático - diseñado con la finalidad de replicarse a si mismo y reenviarse de un equipo a otro de forma automática, utilizando para ellos las funciones de sistema operativo que controlan la transmisión de información. Los gusanos pueden ser preparados para realizar otras acciones.

Harvesting

Ver ***Cosecha de Direcciones***.

Hoax

Ver ***Cadenas de mensajes.***

Ingeniería social

Conjunto de prácticas y técnicas aplicadas a la obtención ilegal de información sensible manipulando la voluntad de sus legítimos propietarios.

Nomadismo

Uso de un mismo número de teléfono independientemente de dónde se encuentre físicamente el usuario.

Nick

Nombre o pseudónimo que utiliza un usuario de mensajería instantánea.

P2P

Ver ***Redes entre iguales.***

Paquete de información

La unidad de datos que se envía a través de una red.

Partición

Cada una de las secciones lógicas en las que se divide un disco duro. Cada partición puede tener su propio sistema de ficheros, y en los sistemas Windows se comportan como discos duros independientes.

Peer to peer

Ver ***Redes entre iguales.***

Pharming

Técnica que trata de obtener información confidencial de los usuarios redirigiendo las peticiones realizadas a través del navegador a sitios Web controlados por terceros que simulan la apariencia de los que mantienen los Prestadores de Servicios de Internet. Habitualmente se realizan manipulando el ordenador del usuario o los servidores de nombres de dominio (DNS) en Internet.

Phising

Técnica de Ingeniería Social que trata de obtener información confidencial de usuarios simulando la identidad de entidades Prestadoras de Servicios de Internet.

Pop-up

Ver ***Ventana emergente***.

Portal de Internet

Conjunto de páginas web con servicios y contenidos como chats, foros, correo web, juegos, callejero, buscador, noticias, horóscopo, traductor, etc.

Proveedor de Servicios de Internet

Entidad pública o privada que ofrece servicios en Internet disponibles al público o a un colectivo concreto de usuarios.

Puerto

Conexión lógica que se establece entre dos dispositivos para el intercambio de datos.

Redes entre iguales

Se denominan así a las redes establecidas entre sistemas que pueden funcionar de forma simultánea como clientes y servidores. La denominación procede del término inglés "*peer to peer*", utilizándose también el acrónimo *P2P.*

Redes Troncales

Se denominan así a las redes de gran capacidad que conectan entre sí a Proveedores de Servicios de Internet separados geográficamente.

Servicio de nombres de Dominio

Servicio disponible en Internet que relaciona el nombre de un servicio prestado por un Proveedor de Servicios de Internet - por ejemplo un sitio Web - con su dirección IP, a efectos de su localización por el equipo del usuario.

Software malicioso

Virus, gusanos y otro tipo de ***malware*** -**mal**icious soft**ware**-, diseñado para insertar *troyanos* o *spyware* en sistemas de información, son causantes de daños muchas veces irreparables y de la recogida de información confidencial en sistemas informáticos.

Spam

Ver ***Correo electrónico no deseado.***

Spyware

Modalidad de software malicioso que, una vez alojado en un dispositivo permite el acceso al mismo a terceros con la finalidad de utilizar sus recursos y usarlos en su propio beneficio.

Telnet

Protocolo que permite la conexión remota a un ordenador.

Troyano o Caballos de Troya

Modalidad de software malicioso que una vez alojado en un dispositivo, permite el acceso al mismo a terceros con la finalidad de utilizar sus recursos y usarlos en su propio beneficio.

Ventana emergente

Ventana web que se abre sobre la ventana activa y que se utiliza en muchos casos para incluir información de carácter publicitario.

Virus informático

Programa de ordenador que tiene la capacidad de modificar o utilizar otros programas para replicarse y realizar algún tipo de acción que abarca desde la propagación de un mensaje, la destrucción total o parcial de la información almacenada en los equipos, su modificación o la utilización de los recursos disponibles.

VoIP

Ver ***Voz sobre IP.***

Voz sobre IP

Se define así al conjunto de estándares y tecnologías que permiten el transporte de conversaciones de voz a través de una red como Internet. En inglés se utiliza el acrónimo VoIP.

Web mail

Ver ***Correo Web.***

WiFi (Wireless fidelity)

Sistema de redes de área local a través de dispositivos inalámbricos.