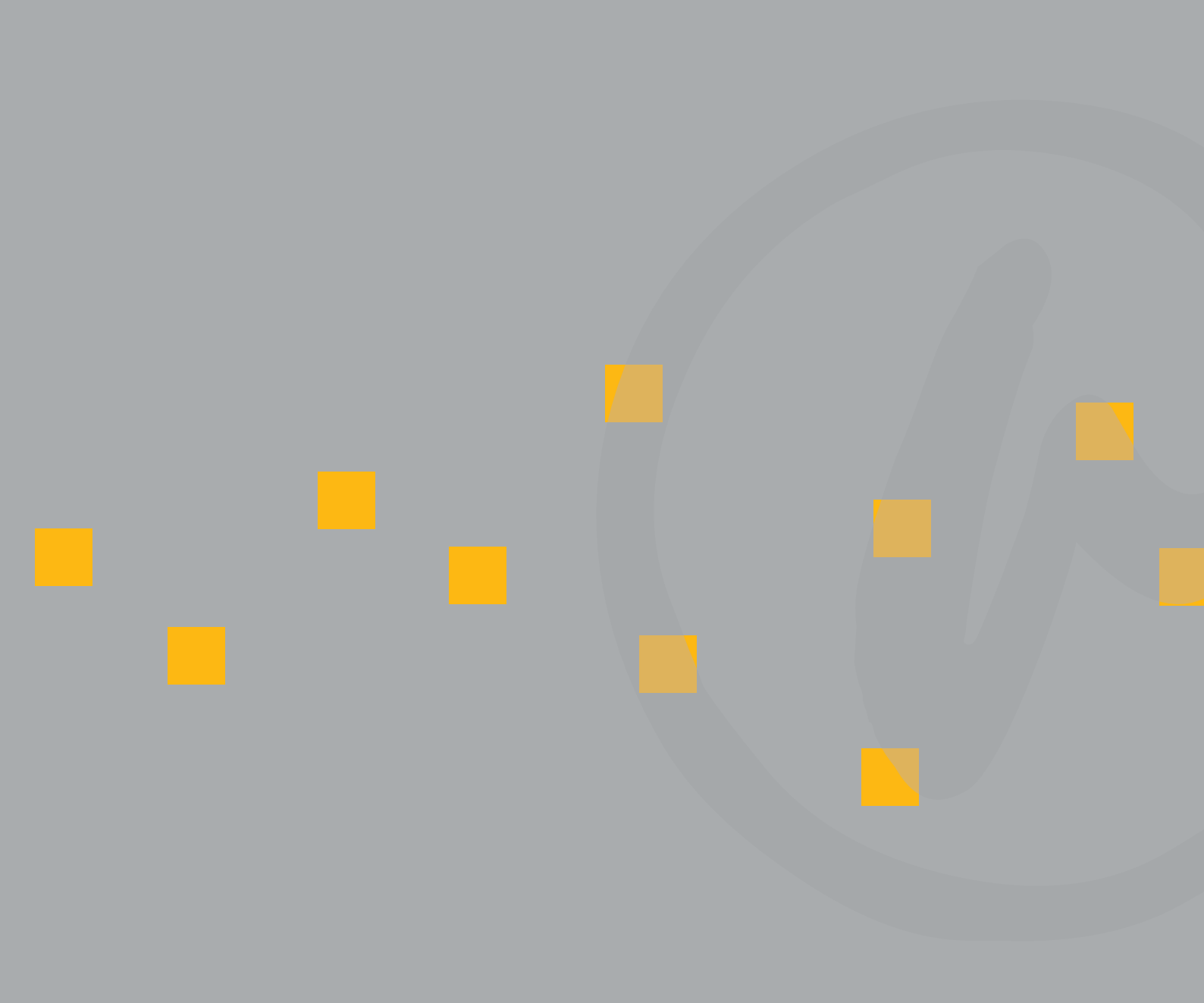
# RECOMENDACIONES A USUARIOS DE INTERNET

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



# RECOMEND@CIONES A USUARIOS DE INTERNET

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

# RECOMENDACIONES 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 es tal que aquél que no disponga de acceso a Internet se encuentra excluido de la vida económica y social. El acceso a las tecnologías de la información resulta esencial en todos los ámbitos de la vida personal, ya sea en el trabajo o el ocio, en el consumo, o en las relaciones con la Administración.

Todos sabemos que estas 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 en el ámbito personal o laboral. Es más, se apunta un crecimiento exponencial de los bienes y servicios que ofrecerá Internet en el plano de la interrelación personal y la generación de comunidades, -redes sociales y web.2.0-, en la organización de la vida personal y profesional. –agendas online, gestión de rutas y viajes, reconocimiento del entorno físico mediante fotografías-, en los servicios sociales, -tele-educación, tele-medicina-, en el control sobre bienes y personas, -geolocalización, etiquetas de identificación por radiofrecuencia RFID-, o en el marketing y la publicidad.

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, no está exento de riesgos. Internet es un medio en el que la delincuencia tecnológica pone buena parte de sus esfuerzos en tratar de sorprender a muchos usuarios, que confían en la red y en la información que encuentran o reciben a través de ella. 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.

En gran parte de los riesgos a los que nos exponemos en Internet existe un elemento común: requieren de un tratamiento previo de información personal, de datos personales. No es posible intentar estafar o remitir publicidad no deseada si previamente no se ha obtenido el dato del correo electrónico. El acoso a los menores a través de su propio chat privado exige acceder a datos de identificación para poder "invitarle". Los problemas vinculados al uso de un dato fundamental en nuestra sociedad, la imagen, requiere que alguien la haya puesto a disposición de la comunidad en Internet.

Por otra parte, muchos servicios de Internet se basan en el intercambio o consumo de información personal. Se ofrecen al usuario servicios aparentemente gratuitos pero cuya contraprestación no es otra que acceder a datos personales del usuario, -como su perfil de navegación, su lista de amigos, o el contenido de los mensajes que escribe o recibe-, obtener información directamente requerida al usuario con finalidades como la elaboración de perfiles de consumo o personalidad, o remitirle determinada información o publicidad. En estos casos la información legal y las políticas de privacidad suelen mostrar que no se trata de un "servicio gratuito", ya que el usuario "abonará" el servicio con su información personal.

Desde este punto de vista, la problemática de la protección de datos personales en Internet constituye una pieza fundamental. Es absolutamente necesario generar en el ciudadano una "cultura para la protección de sus datos en la Sociedad de la Información", ya que de ella dependerá que cada persona pueda hacer un uso seguro de Internet para lograr no sólo un mejor nivel de vida, sino también un verdadero control sobre su información.

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 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 en los que no confiemos.

- 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.

- La mayor parte de los navegadores incorporan sistemas de bloqueo de ventanas emergentes y de descarga de programas y archivos. Es recomendable mantener actualizado siempre su navegador.

- 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, y en particular las actualizaciones periódicas de antivirus y sistema operativo, 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.

Normalmente junto a las cuentas de correo corporativas o de empresa se suelen contratar servicios de correo electrónico gratuitos. Para poder disfrutar de los mismos será necesario facilitar información personal en el alta o registro de usuario, aceptar la recepción o emisión de publicidad personalizada o contextual, suscribirse a determinados programas de fidelización, entre otros.

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.

Esta práctica se ha generalizado todavía más en las redes sociales ya sea mediante la recopilación masiva de "amigos" o la promoción de falsas citas. La mayor parte de técnicas de recopilación y uso de direcciones de correo electrónico se han trasladado a las redes sociales en las que la condición de teórico "amigo" de quien las realiza ofrece confianza e incrementa el riesgo.

## 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

Es frecuente 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. La contraseña debería contar con un mínimo de ocho caracteres y cambiarse al menos en una ocasión al año.

  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. Es habitual 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. La existencia de políticas de privacidad comprensibles, la identificación del responsable del servicio con todos los datos necesarios para localizarle y el uso de certificados electrónicos de identificación proporcionados por un tercero de confianza, la presencia de información sobre el modo de contratar o la utilización de conexiones seguras para facilitar los datos o gestionar los pagos, son datos que deben ser tenidos en cuenta antes de utilizar este tipo de servicios.

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 dato personal 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 en las políticas de seguridad y solicitan datos personales y claves de acceso.

No deberá dejar desatendido el ordenador mientras se esté realizando una conexión segura en la que se estén proporcionando datos.

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 INSTANTÁNEA Y CHATS

La mensajería instantánea IRC, o chat privado, 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 acepte abrir ni descargue nunca imágenes, 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 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.

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.

- Lea las condiciones de uso del programa antes de aceptar el contrato, podría estar permitiendo el uso de su ordenador o el acceso a sus datos al proveedor del programa.

- En la instalación mediante procedimientos automáticos debemos hacer una copia previa del estado del sistema, y comprobar 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.

- Los programas de descarga 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.

- 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.

- Deberá valorarse la idoneidad de restringir el uso de estos sistemas en los centros de trabajo dado el riesgo de que se pueda llegar a compartir información contenida en los ficheros de la empresa.

- 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.

- Deberían valorarse los riesgos de instalar un servidor, ya que deberá publicar su dirección IP, por lo que mucha gente podrá conocer 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.

- 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.

Nunca comparta todo su disco duro. Use un disco duro dedicado en exclusiva o establezca una carpeta o directorio específico

## VIII 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, así como software específicamente diseñado para la telefonía IP, la videoconferencia y la multiconferencia.

Las ventajas sobre la telefonía tradicional son muchas; es un servicio mas barato, permite el nomadismo, es decir, el uso del mismo identificador de teléfono independientemente de la ubicación física del usuario, pero también tiene ciertos riesgos que el usuario debe tener en cuenta.

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.

- 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.

- 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. 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 mediante escuchas no autorizadas, uso excesivo del ancho de banda, etc…

- Lea con detenimiento las condiciones de uso del servicio y las políticas de privacidad.

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.

## IX LAS VIDEOCÁMARAS EN INTERNET

En Internet se utilizan las llamadas cámaras IP. A diferencia de las tradicionales la cámara IP se conecta a Internet directamente como cualquier ordenador conectado a la red. Por ello la visión de las imágenes captadas por la cámara puede realizarse desde cualquier ordenador conectado a Internet, a través del navegador habitual, sin más que introducir la dirección IP de la cámara.

Este tipo de cámaras se utilizan cada vez con mayor asiduidad para fines de videovigilancia y control laboral remota, promoción turística o comercial, información sobre el tiempo o el tráfico, o acceso a las imágenes de niños en guarderías o entornos escolares. Se trata de herramientas cuya instalación y uso es muy sencillo.

Habitualmente estas cámaras suelen disponer de mecanismos de control de acceso basados en usuario y contraseña de forma que, si este control se encuentra activado, cualquier ordenador que invoque su dirección IP deberá pasar dicho control antes de poder acceder a las imágenes.

Por otra parte, también se ha generalizado el uso de webcams domésticas como herramienta de comunicación entre los usuarios de sistemas de mensajería privada, o telefonía IP.

Pueden distinguirse así dos tipos de sujetos en relación con el uso de videocámaras. En primer lugar, se encuentran los usuarios activos, esto es, aquellos que instalan y usan las videocámaras, los cuales deberían tener en cuenta las siguientes recomendaciones:

- La captación de imágenes está sujeta a las normas vigentes y, cuando se trata de personas identificadas o identificables, debe cumplirse la LOPD.

- Deben respetarse los derechos de las personas cuya imagen se obtiene.

- Deberá garantizarse rigurosamente la seguridad y el secreto, cuando el acceso a las imágenes se produzca online. No debe permitirse el acceso en abierto a través de Internet a imágenes de personas identificadas o identificables sin su consentimiento.

- En aquellos casos en los que se facilite acceso a un colectivo -como el de todos los padres de un aula- deberán definirse los perfiles de acceso e informarse sobre las responsabilidades y obligaciones que les incumben por el acceso a los datos.

- La difusión de imágenes con finalidad promocional, turística o equivalente a través de Internet deberá realizarse de manera que no resulte posible identificar a las personas. Por ejemplo limitando la resolución, definiendo el ángulo de visión de modo adecuado, o buscando tomas en las que las personas no resulten identificables.

- Además, los usuarios poseen un perfil pasivo, esto es sus imágenes son captadas por videocámaras que pueden estar conectadas a Internet. Asimismo, estas imágenes pueden visionarse o usarse en el ámbito de relaciones privadas como la celebración de una videoconferencia. De ahí que sea recomendable:

- Cerciorarse por medio de la consulta de los carteles informativos de la existencia de videocámaras.

- Solicitar información a los responsables de las videocámaras.

- Ejercer, en su caso, el derecho de acceso a las imágenes.

- Respetar los derechos de aquellos con quienes celebramos videoconferencias no grabando o reproduciendo imágenes sin su conocimiento y autorización.

- No reproducir ni difundir las imágenes obtenidas con motivo del acceso a servicios de Internet como los de acceso de los padres a las aulas de guarderías.

## RECUERDE

La imagen es un dato de carácter personal cuya difusión o acceso no autorizado puede ser particularmente molesto o dañino.

Antes de instalar un videocámara que reproduzca imágenes en Internet asegúrese de que la captación sea lo menos intrusiva posible.

Debe garantizarse la seguridad impidiendo el acceso no autorizado a las imágenes captadas por cámaras IP.

En sus relaciones privadas cuando utilice webcams respete los derechos de los demás usuarios.

## X LOS BUSCADORES

El avance tecnológico ha planteado nuevas posibilidades de crear y acceder a la información en Internet, situación que obliga a considerar las repercusiones de la tecnología, que, en principio, es neutral, sobre los derechos de las personas.

En efecto, los buscadores de Internet tratan datos personales, bien facilitados por el propio usuario o derivados del uso del servicio, así como los que se obtienen del tratamiento y publicación de información personal indexada desde otras páginas web en su función de buscador.

El éxito de los buscadores gratuitos depende de la capacidad del prestador del servicio para facilitar a los usuarios los resultados de búsqueda más relevantes. De ahí que tenga una gran importancia la ordenación de las webs que aparecen asociadas a la búsqueda y la vinculación a ellas de mensajes publicitarios patrocinados, que suele ser el modelo de negocio de estas empresas.

Son servicios de la sociedad de la información sujetos no sólo a las garantías de la Ley Orgánica 15/1999 de Protección de Datos (LOPD), sino también de la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), que engloba en este concepto "la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet".

Dentro de estos servicios es posible distinguir entre el tratamiento de datos de los usuarios y el tratamiento de datos de terceras personas accesibles a través de buscadores. En el primer caso, el buscador puede establecer perfiles de navegación, indexar la IP, o utilizar las cookies con la finalidad de ofrecer información sobre las búsquedas o publicidad personalizada según el perfil del usuario. Una modalidad específica consiste en los servicios de búsqueda personalizada que guardan el historial de búsqueda y navegación del usuario.

Por otra parte, el usuario puede ser objeto de una búsqueda que recogerá cualquier información vinculada a los datos de la misma, nombre, apellidos, fotografías, vídeos, opiniones manifestadas en foros abiertos o cualquier otra información disponible en Internet en espacios públicos sin ningún tipo de barrera frente al buscador.

Por todo ello es necesario tener en cuenta las siguientes recomendaciones:

- Lea con detenimiento las condiciones de uso del servicio y las políticas de privacidad.
- Infórmese sobre el uso de cookies, barras de búsquedas u otros servicios vinculados al perfil de usuario o al historial de navegación.
- Borre con regularidad las cookies, los archivos temporales de Internet y el historial de navegación.
- No publique información innecesaria o inadecuada sobre terceros.
- Asegúrese de no facilitar o publicar datos innecesarios en espacios abiertos de Internet.
- Si cree que un determinado proveedor está ofreciendo indebidamente información sobre usted, ejerza sus derechos de acceso, rectificación, cancelación u oposición al tratamiento y solicite en su caso su retirada previo bloqueo de la misma.

## RECUERDE

El uso de un buscador genera tratamientos de información, por ejemplo, para ofrecer anuncios personalizados. Conozca las políticas de uso de su buscador preferido.

Recuerde borrar con regularidad las cookies, los archivos temporales de internet, así como el historial de navegación.

Los buscadores permiten a cualquier tercero obtener perfiles completos sobre nuestra información pública en Internet.

## XI LA WEB 2.0.

En los últimos años Internet ha evolucionado desde un modelo en el que el internauta ocupaba un papel pasivo, prácticamente de mero lector, a un papel activo y protagonista. El universo web se ha convertido en un espacio social dinámico donde los individuos se relacionan, interactúan y se vertebran en comunidades.

Las aplicaciones y servicios han evolucionado permitiendo que no resulte necesario tener un conocimiento experto. Basta con registrarse para acceder a un conjunto de programas y servicios que permiten editar nuestro blog y convertirnos en periodistas digitales, colgar nuestros vídeos e imágenes, o mantener una interacción en tiempo real con miles de personas en todo el mundo. Los mundos virtuales emulan el mundo físico generando entornos amigables que se perciben como el usuario del mismo modo que si existieran en el mundo físico. De hecho, algunos entornos imitan el mundo real con sus calles, tiendas y viviendas en el que el usuario actúa a través de un avatar, un alter ego virtual, que desarolla una vida paralela en el mundo de las redes.

Esta realidad que se ha denominado Web 2.0 no es únicamente un conjunto de recursos tecnológicos y servicios sino que ha creado un universo social propio poblado por comunidades locales, profesionales y globales, entre otras, cuya simple descripción requiere de un esquema claro de contenidos.

## LAS REDES SOCIALES

En éste ámbito, destacan las redes sociales, por su complejidad e incidencia en el derecho fundamental a la protección de datos las redes sociales. Se trata de un fenómeno que ha supuesto una verdadera revolución en Internet. A través de las redes sociales es posible compartir información personal y contactar con otros usuarios de la Red. En la práctica el funcionamiento de estos servicios comporta que cada usuario ponga a disposición de otros muchos, con los que no tiene porqué tener una relación de confianza, multitud de información personal. Generalmente en las redes sociales se denomina "amigo" a alguien que simplemente nos ha hecho llegar una tarjeta de presentación o que conforme a las reglas del portal "es amigo de un amigo". El empleo de expresiones del tipo "amigo", "tu muro", o "tu albúm de fotografías" ofrecen una falsa imagen de privacidad para lo que, si no se conoce el funcionamiento de la red social acaba siendo público y disponible para cualquier persona. De hecho, si se utilizan las configuraciones por defecto, lo habitual es que la información sea completamente disponible para cualquier tercero, incluidos los buscadores.

El gran volumen de datos personales que se vuelca en la red social hace necesario plantear las siguientes recomendaciones a los usuarios:

- Aprender las posibilidades de configuración y uso que la red ofrezca.

- Disponer de un perfil registrado en el que no se publique información excesiva de su vida personal y familiar, así como recurrir al uso de seudónimos o nicks personales permitiéndoles disponer así de una "identidad digital".

- Tener especial cuidado al publicar contenidos audiovisuales y gráficos en sus perfiles, especialmente si se van a alojar imágenes relativas a terceras personas.

- No etiquete contenidos audiovisuales con la identidad real de sus protagonistas ni ofrezca datos de terceros en su espacio sin su consentimiento.

- Revisar y leer las condiciones generales de uso y la política de privacidad de la red social en el momento de registrarse.

- Ejercer sus derechos de acceso a los datos que utilice el portal y el derecho de cancelación, o el de cancelar la suscripción cuando se verifiquen cambios en las condiciones legales y políticas de privacidad con los que no se esté de acuerdo.

- Configurar adecuadamente el grado de privacidad del perfil de usuario en la red social, optando por el que resulte más conveniente.

- Aceptar únicamente a aquellas personas conocidas o con las que se mantiene alguna relación previa y no publicar en el perfil información de contacto que permita ubicarnos físicamente.

- Emplear diferentes nombres de usuario y contraseñas para entrar en las distintas redes sociales.

- Utilizar contraseñas de ocho caracteres o más utilizando tanto letras como números, mayúsculas y minúsculas, así como tener un buen sistema antivirus debidamente actualizado.

## RECUERDE

Las redes sociales son una importante fuente para la obtención de información sobre las personas debe conocer bien su funcionamiento para proteger su identidad digital.

Debe garantizar la seguridad de su información mediante una configuración adecuada de su espacio y utilizando contraseñas adecuadas.

Cuando publica una foto o escribe en un blog puede estar incluyendo información sobre otras personas. Respete sus derechos.

En caso de problemas o desacuerdo con las políticas del portal, ejerza sus derechos.

## XII LA RESPONSABILIDAD DE LOS INTERNAUTAS

Los medios que la informática e Internet ponen a nuestra disposición nos permiten realizar muchas actividades en Internet. Gracias a ellos podemos editar audio y vídeo y compartirlos con el mundo entero, publicar nuestras fotografías y compartirlas, organizar actividades virtuales, convocar citas y encuentros masivos, o ejercer el periodismo ciudadano.

En todas estas actividades podemos estar tratando información y datos personales de terceros sin ser conscientes de nuestra responsabilidad personal y jurídica. Así por ejemplo, cuando se publica información sobre terceros y se ejerce como periodista se tienen los mismos deberes y responsabilidades que los profesionales de los medios de información. En la medida en la que en Internet cada ciudadano puede ser protagonista, editar su página personal, crear su web o mantener su blog, asumen con ello la responsabilidad.

Por ello es importante, tanto para usuarios como para responsables de los portales de Internet que permiten estas actividades:

- No publicar informaciones que no respondan a los requisitos de veracidad, interés público y respeto a la dignidad de las personas, y en particular a la juventud y la infancia.
- No difundir rumores o informaciones no contrastadas.
- Rectificar o retirar la información cuando de modo justificado lo solicite un afectado.

- Nunca publicar información que ponga en riesgo a la familia y en particular a los niños, ni nuestras amistades, vecinos, etc.

- Tener especial cuidado respecto a la publicación de información relativa a los lugares en que el usuario o un tercero se encuentra en todo momento. Podría poner en peligro a los usuarios, dado que permite a los posibles infractores conocer en todo momento donde se encuentra, qué está haciendo y hacia dónde se dirige el usuario, lo que puede suponer un grave riesgo para su integridad.

- No grabar ni publicar imágenes, videos o cualquier otro tipo de registro sin el consentimiento de los afectados.

- No tratar datos personales de terceros, especialmente cuando se divulguen a terceros, sin conocimiento y consentimiento de los afectados.

- Cumplir cuando proceda con las obligaciones de la Ley Orgánica de Protección de Datos.

- Informar sobre los deberes de los usuarios en los procedimientos de alta y registro.

- Elaborar y publicar códigos éticos que garanticen unas mínimas reglas de actuación de los usuarios o de las comunidades en las redes sociales.

## RECUERDE

En el mundo Internet  todos podemos ejercer el derecho a la información, la libertad de expresión o publicar contenidos audiovisuales.

El ejercicio de estos derechos está sujeto a reglas y debemos conocerlas.

Debemos siempre respetar los derechos de los demás y cumplir las leyes.

## XIII EL USO DE INTERNET POR MENORES

Las alternativas que ofrece hoy en día la red a nuestros menores son muy variadas y éstos cada vez hacen uso de Internet a edad más temprana. La protección de los datos personales de los menores en Internet adquiere una especial relevancia por la confluencia de distintos factores. En primer lugar, los menores no perciben necesariamente la necesidad de proteger su información personal y, sin embargo, ésta posee un alto valor económico para muchos sectores. El menor en Internet es un consumidor de ocio y publicidad, y un usuario muy activo en las redes sociales. Además, se ofrecen servicios a sus padres como la geolocalización, la videovigilancia o el control de asistencia a los que en muchas ocasiones se accede por medio de entornos web.

Por ello, se hace preciso señalar las siguientes recomendaciones en el caso de uso de Internet por menores dirigidas a padres y educadores:

- Los padres y educadores deben conocer cómo funciona Internet para saber los beneficios y también los peligros derivados de una mala utilización, y educar así a los menores en el uso de las nuevas tecnologías.

- Concienciar y educar a los menores sobre aspectos relativos a la seguridad, explicarles los conceptos básicos para una navegación segura.

- Los menores deben ser informados y formados acerca de los peligros en el uso de Internet, advirtiéndoles de que no compartan o faciliten información, ni intercambien fotografías con personas desconocidas y sin saber para qué van a ser utilizados; que no abran los ficheros adjuntos en los mensajes de correo electrónico y que eviten la descarga de archivos o programas.

- Instalar el ordenador en una zona común de la casa.

- Establecer unas normas sobre el uso de Internet en casa: el número de horas que se puede utilizar al día, qué páginas visitas, etc.

- Se debe navegar con los menores, ayudarles a distinguir los riesgos, asegurarse de que los niños no accedan a Internet a través de entornos no confiables o de que no intercambien datos personales ni fotografías con desconocidos.

- Los centros escolares y los ordenadores personales deben estar provistos de entornos controlados, cuentas de usuario restringidas que impidan instalar programas, filtros de contenidos y/o programas de ayuda y control de la navegación, asi como antivirus y el software de seguridad que corresponda.

- En el mundo de Internet existen entornos y servicios que pueden no ser seguros para un niño. Debemos ser particularmente cuidadosos en espacios como foros, chat o redes sociales. Son espacios que requieren que el niño conozca los riesgos y dependerá de su madurez la capacidad para utilizarlos. Ayúdale a comprender los riesgos y a escoger adecuadamente.

- Si el niño es menor de 14 años se necesita del consentimiento de madres, padres o tutores legales para que se puedan tratar sus datos. Si el niño es mayor de 14 años podrá consentir por sí mismo. Debemos conocer las condiciones de uso y políticas de privacidad de los sitios de Internet a los que se suscriban.

- Cuando alguien recoge datos de menores no puede solicitar datos de su entorno familiar salvo para entrar en contacto y pedir nuestra autorización. Si lo hacen no es un sitio en el que confiar.

- La información sobre el uso de los datos debe ser sencilla de modo que los niños sean capaces de entenderlo. Debemos asegurarnos de que se les informe sobre la identidad de quien trata los datos, de la finalidad y usos para los que se solicitan dichos datos, de si va a comunicarlos o cederlos a terceros y de si resulta obligatorio o no facilitarlos. Además deben facilitar una dirección para ejercer los derechos de acceso, rectificación, cancelación y oposición.

- El centro escolar, el AMPA (Asociación de Madres y Padres de Alumnos), el servicio de autobús, cualquier entidad que trate datos de menores en Internet deben cumplir con la Ley Orgánica de Protección de Datos. En Internet es donde se deben extremar las precauciones y no es aconsejable publicar fotos o datos que identifiquen a un niño, por ejemplo, situándole en el contexto de un colegio, una clase y/o actividad determinados.

- No obstante, el niño también tiene un derecho a la vida privada en el contexto familiar. La monitorización de su ordenador, el uso de videovigilancia o la geolocalización mediante el móvil son soluciones extremas. Deben usarse sólo cuando resulte imprescindible y teniendo en cuenta la proporcionalidad de la medida en función de su finalidad y de la edad del menor.

Los menores de edad también son usuarios de las redes sociales, por lo que tanto ellos como sus padres o tutores deberán atender a las siguientes recomendaciones:

- Verificar el modo de funcionamiento de la red social, el tipo de usuarios, la actividad y temática de la misma y las garantías de seguridad que ofrecen. Escoja aquellas redes sociales que realmente se adecuen al perfil de edad del niño y garanticen su seguridad.

- No revelar datos personales excesivos ni suministrar datos a desconocidos. En caso de duda, preguntar siempre a los padres o tutores.

- Si el usuario es menor de 14 años, es necesario que los responsables de la red social recaben el consentimiento paterno para permitir o no la suscripción del menor a estos servicios.

- No comunicar nunca el nombre de usuario ni por supuesto la contraseña de acceso, ni siquiera a los amigos o compañeros de clase.

- Si se detecta alguna conducta desagradable para el usuario, es recomendable comunicarlo siempre a los padres y denunciar a ese usuario dentro de la propia red social para que se tomen las medidas oportunas. Si se trata de una conducta delictiva se debe comunicar a las Fuerzas y Cuerpos de Seguridad del Estado.

- Explicar a los menores que no deben aceptar invitaciones de desconocidos y nunca deben quedar con personas que hayan conocido a través de Internet, y que en caso de que se haga, hacerlo siempre en compañía de los padres.

- Asegurarse de que los menores comprenden los riesgos de publicar material gráfico en Internet y sus posibles consecuencias.

- Controlar la información del perfil de usuario de los menores y asegurarse de que no utilizan su nombre completo para evitar que terceros puedan identificarles.

## RECUERDE

Los niños son nativos digitales, usan Internet como parte normal de su vida. Debemos educarles en un uso seguro de las redes.

Aprenda a usar las herramientas de Internet y a navegar con sus hijos con la finalidad de educarles.

Adopte medidas de seguridad físicas -ubicación del ordenador, horas para su uso- e informáticas.

Verifique la información legal, las políticas de privacidad de las redes sociales y los sitios de Internet que utiliza el niño.

## XIV COMPETENCIAS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Con respecto a 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.


GLOSSÁRIO

**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, 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.*

**Cadena de mensajes**

Conocido también como 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 interceptada (garantía de confidencialidad) o manipulada (garantía de integridad).

**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 P2P (Redes de intercambio de archivos)**

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* -malicious software-, 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**

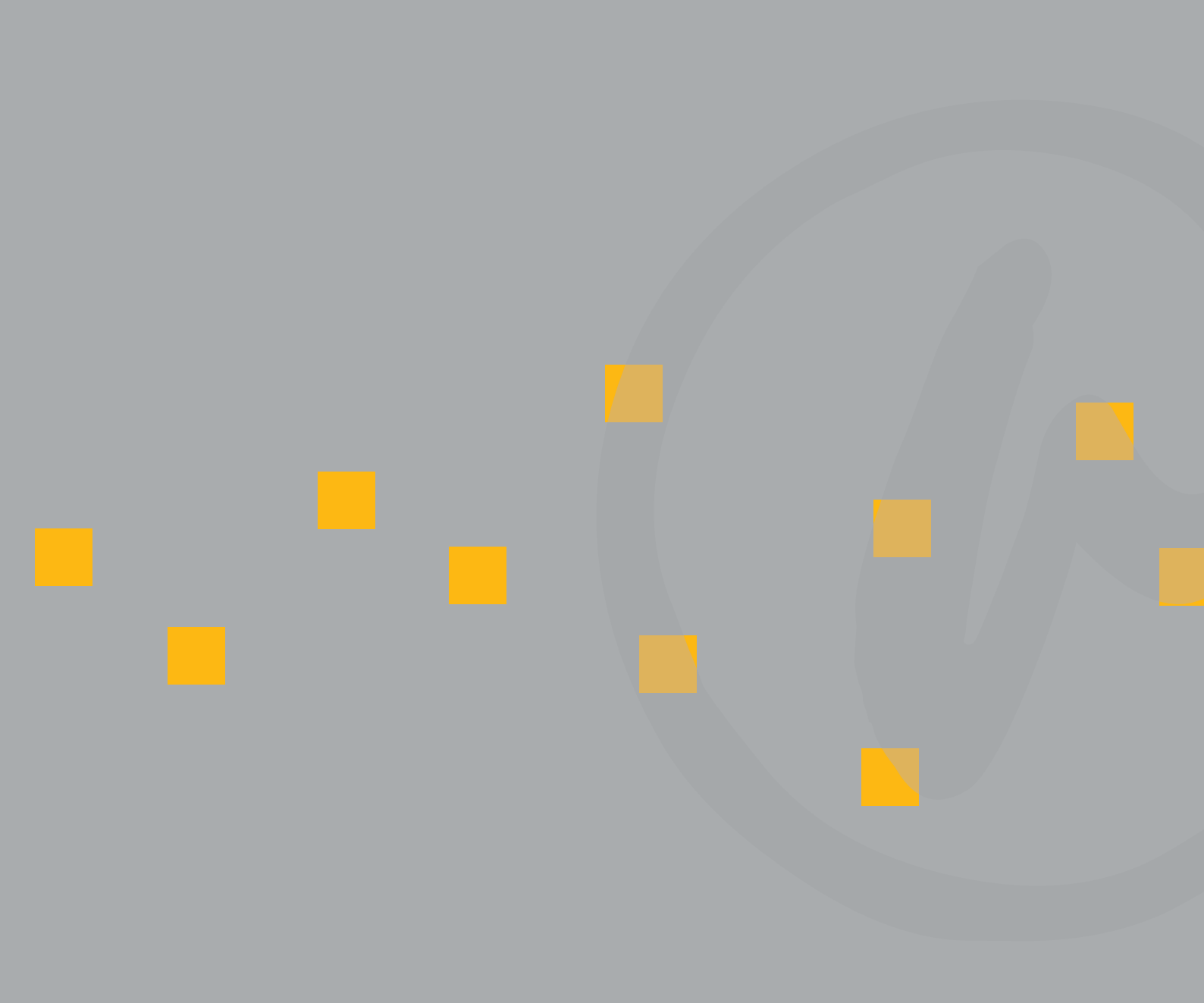
Se define así al conjunto de estándares y tecnologías que permiten el transporte de conversaciones de voz a través de una red como Internet. En inglés se utiliza el acrónimo VoIP.

**Web mail**

Ver *Correo Web.*

**WiFi (Wireless fidelity)**

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



www.agpd.es

www.agpd.es

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS